Advances in Social Science, Education and Humanities Research (ASSEHR), volume 300
2018 International Workshop on Education Reform and Social Sciences (ERSS 2018)

Analysis of the Status Quo of Artificial Intelligence and Its Countermeasures

Xinyun Xiong

North China Electric Power University, Baoding 071000, China.

3182365226@qq.com

Abstract. Nowadays, with the great attention of governments and the gradual formation of the industrial structure, artificial intelligence is in the stage of rapid development. The breakthrough in the development of artificial intelligence stems from three factors: the increase of large amounts of data, the emergence of various excellent algorithms, and the tremendous improvement in the performance of computer hardware. However, any new technology and new application have two sides. The artificial intelligence technology and its application not only bring convenience to people, but also bring security risks. To this end, this paper explores the status quo and trend of the development of artificial intelligence, analyzes the security risks it brings, and proposes countermeasures and suggestions.

Keywords: artificial intelligence; development; security; two-sidedness.

1. Introduction

Artificial intelligence is one of the most popular and controversial areas of technology in recent years. Any high technology has two sides, and artificial intelligence is no exception. Some people believe that the major breakthroughs in technological innovation and application in the field of artificial intelligence are expected to lead the new technological revolution and industrial revolution, and will have a tremendous impact on the social, economic, military and other fields. In addition, artificial intelligence can also benefit human beings in manufacturing, transportation, education, medical care, and services. Others believe that artificial intelligence is a major threat to humanity.

2. Overview of Artificial Intelligence

2.1 Concept.

Artificial intelligence refers to the ability of computers to think like human beings. It is a comprehensive discipline that integrates the frontiers of computer science, statistics, brain neurology and social sciences. It can replace human beings for identification, cognition, analysis and decision making.

2.2 History.

In 1956, at a conference hosted by Dartmouth College, a computer expert named John McCarthy first proposed the term "artificial intelligence." After this meeting, artificial intelligence ushered in its first rapid development. For the next ten years, computers have been widely used in mathematics and natural language to solve problems in algebra, geometry, and English. In the 1970s, artificial intelligence encountered technical bottlenecks, mainly in three aspects. First, the lack of computer performance led to many early programs that could not be applied in the field of artificial intelligence. Second, as the complexity of the problem rises, the program is overwhelmed. Third, there is a serious lack of data, and there is not enough database to support the program for deep learning, which can easily lead to the machine not being able to read enough data to be intelligent. As a result, artificial intelligence has encountered six years of research barriers. In 1980, Carnegie Mellon University designed a set of "expert systems" called XCON for digital equipment companies. This is a computer intelligence system with complete expertise and experience. However, by 1987, the performance of desktops produced by Apple and IBM exceeded the general-purpose computers produced by vendors such as Symbolics, and the expert system was no longer available. Beginning in the mid-1990s, with

Copyright © 2019, the Authors. Published by Atlantis Press.

This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

the gradual development of neural network technology and the fact that people began to have objective and rational knowledge of AI, artificial intelligence technology began to enter a period of steady development. On May 11, 1997, IBM's computer system "Deep Blue" defeated world chess champion Kasparov, and once again triggered discussions on AI topics in the public domain. In 2006, Hinton made a breakthrough in the field of deep learning in neural networks, and it was also an iconic technological advancement in the field of artificial intelligence.

3. Status and Trend.

3.1 Great Potential in Industry Applications.

"AI+" is the continuation and upgrade of "Internet+", which promotes the transformation of traditional industries into automation and intelligence. At present, artificial intelligence has great potential in the fields of industry, finance, transportation, medical care, insurance, security, etc. In the future, "AI+" will spawn more new formats and open up broader market space.

3.2 The Commercial Value of Artificial Intelligence is Being Re-examined.

Investment in artificial intelligence is becoming more rational, and investors are more concerned with the commercial and application value of artificial intelligence. With the transformation of academic research into industrial applications, the demand for commercial applications will be the main factor driving the development of artificial intelligence industry in the future.

3.3 The New Technology Revolution is Urgently Needed.

At present, artificial intelligence mainly relies on data-driven perception intelligence, and its development is limited by factors such as algorithm efficiency and hardware performance. On the one hand, deep learning algorithms rely heavily on massive data and superior computational efficiency, and are unexplained. On the other hand, exponential growth in hardware performance that supports the development of artificial intelligence will not be sustainable. Therefore, the artificial intelligence relying on deep learning may encounter bottlenecks in the future, and the research on cognitive intelligence represented by migration learning and brain-like learning is becoming more and more important.

4. The Threat Brought About by Artificial Intelligence.

4.1 The Security of Cyberspace.

When artificial intelligence technology is used in cyber-attacks, its self-learning and self-organizing capabilities can be used to intelligently find vulnerabilities and identify key targets, thereby improving attack efficiency. For example, malware that integrates artificial intelligence can automatically target more attractive targets, and crimes such as hijacking industrial equipment, ransom, and the like will become more common, and traditional cybersecurity systems are threatened.

4.2 Personal Privacy.

The application of artificial intelligence technology enhances the ability of personal information collection and personal data mining, and increases the risk of privacy leakage. For example, intelligent systems based on biometrics such as fingerprints, faces, and irises collect and master a large amount of user privacy. The artificial intelligence system can re-learn and re-infer according to the data collected by it, and get more information related to user privacy.

4.3 Personal Safety.

Artificial intelligence systems have certain ability to make decisions. In the event of cognitive bias or cyberattacks, the system may make misjudgments, take wrong actions, and even endanger personal safety.

4.4 Social Stability.

The application of artificial intelligence will promote the upgrading of the industry and cause unemployment. Prior to the establishment of a new social division of labor, the impact of artificial intelligence on employment may raise the risk of social security.

5. Recommendations.

5.1 Improve the Defense Ability of Cyberspace.

Artificial intelligence technology can both enhance the ability of network attacks and enhance the ability of network defense. The government should actively guide and promote the development of research institutions and network security companies, and strengthen the research on the application of artificial intelligence technology in the field of network security. At the same time, the government should build a platform based on artificial intelligence for network attack and defense drills, develop mature network security products, and improve the level of automation and intelligence of network security protection.

5.2 Strengthen Legislation and Technology Research.

In the era of massive data and artificial intelligence, privacy protection should start from two aspects: legislative supervision and technological capability improvement. On the one hand, in view of the decentralization of the legal provisions on the protection of personal information in China, it is necessary to speed up the unified legislation, especially to clarify the principles, procedures, confidentiality and protection obligations of enterprises to collect user information, as well as related responsibilities for improper use and data disclosure. On the other hand, the application of new technologies such as block chains in personal privacy protection should be strengthened.

5.3 Strengthen the Security of Artificial Intelligence Applications.

It is necessary to strengthen the research of artificial intelligence technology, enhance the maturity of core algorithms and learning models, strengthen the cognitive ability of artificial intelligence, improve the transparency and interpretability of decision-making, and ensure the robustness of decision-making in intelligent applications. The government should take the initiative to build a safety assessment evaluation system for artificial intelligence applications, develop evaluation criteria, build an artificial intelligence application security test verification platform, and verify the security vulnerabilities of artificial intelligence systems to improve the security and reliability of artificial intelligence applications.

5.4 Optimize Discipline Setting and on-the-Job Training.

For the social employment reform triggered by the development of artificial intelligence industry, the professional settings of colleges and universities should be dynamically adjusted, and the cross-disciplinary disciplines related to artificial intelligence should be added, and the number of enrollment quotas for artificial intelligence alternative occupations should be gradually reduced or even eliminated. Staff members should be guided to establish a lifelong learning philosophy. The government should improve the system of on-the-job training and re-employment training, increase jobs in the field of intelligent economy, and minimize the social risks caused by unemployment.

References

[1]. Wang Tian. Research on the development of artificial intelligence industry and its countermeasures [J/OL]. China Business Theory, 2018(26): 167-168[2018-10-08]. https: //doi. org/10. 19699 /j.cnki.issn2096-0298.2018.26.167.

[2]. Liu Tingting. The development trend of artificial intelligence and security challenges [N]. People's Post and Telecommunications, 2018-09-17 (003).

[3]. Wang Fei. Research on the status quo and trend of deep learning based on artificial intelligence [J]. Computer fans, 2018 (10): 140-141.

[4]. Miao Xiaomeng. On whether artificial intelligence will replace human thinking [J]. Communication World, 2018 (08): 285-287.

[5]. https://blog.csdn.net/u013162035/article/details/79535577.