Analysis of Military Information Construction under the Background of Artificial Intelligence

Jian Pan[1], Kang Yi[1], Hua Fang[1], Yuting Zhao[1], Keke Du[1], Wenjuan Liu[1]

[1]The Experimental Training Base of College of Information and Communication National University of Defense Technology, Xi'an 710106, China

Abstract. On the basis of sorting out the development history of artificial intelligence technology and its status quo in military application, the paper discussed the challenges in military application of artificial intelligence technology in information warfare, constructed a framework for the application of artificial intelligence in the field of military information, and put forward constructive thoughts and suggestions on how to accelerate the intelligent application in the field of military information.

1 Introduction

Artificial intelligence (AI) technology has entered a period of rapid growth since 2016 and is recognized as the revolutionary technology most likely to change the world in the future. The Party and the state attach great importance to the development of artificial intelligence technology, and regard the development of artificial intelligence as a major strategy to enhance national competitiveness and safeguard national security. During the ninth collective study of the Political Bureau of the CPC Central Committee on October 31, 2018, President Xi pointed out that it is necessary to deeply understand the significance of accelerating the development of a new generation of artificial intelligence, strengthen leadership, make good plans, clarify tasks, lay a solid foundation, and facilitate its deep integration with economic and social development, so as to promote the healthy development of the new generation of artificial intelligence in China. The development of artificial intelligence is driving revolution in military affairs and will profoundly change the shape of war. Therefore, it is of great significance to actively study the influence of artificial intelligence on the construction of military information, to seize the strategic commanding height of military information.

2 The development of artificial intelligence and its application in the military

Artificial intelligence originated in the 1950s and 60s, when Alan Turing, known as the "father of computers", proposed the idea of "Turing test", that was, if a machine could talk to humans without being identified, then the machine was intelligent [1]. By the 1970s, the development of artificial intelligence was underestimated for the first time, and the development of technology faced bottlenecks such as insufficient computer performance, serious data missing, and poor resolution of the complexity of problems [2]. After entering the 1990s, with the development of neural network technology, artificial intelligence began to enter a period of steady development. In 1997, IBM's computer system "Deep Blue" defeated Kasparov, the world chess champion, which was regarded as a landmark event in the development of artificial intelligence. After entering the 21st century, with the proposal and continuous improvement of deep learning algorithms, artificial intelligence had once again entered an explosive period. Internet giants such as Google, Microsoft, and Baidu, as well as numerous startup technology companies, had invested heavily in research and development of artificial intelligent products, raising another round of intelligent frenzy [3].

At present, the application of artificial intelligence in China is mainly concentrated in the fields of security, finance, medical care, education, retail, robots and intelligent driving [4]. In the field of robots, the current hotspots are focused on children's education/care robots, entertainment robots, family service robots, venue robots (catering/hotel/ bank guide, shopping guide or transportation robots). In the field of smart homes, smart speakers, smart cameras, smart set-top boxes, smart routers, smart air purifiers and other products have begun to enter people's lives. In addition, intelligent recommendation systems, intelligent investment consultants, intelligent education, and intelligent navigation have been integrated into all kinds of APPs used by people in daily life. Compared with other fields, the commercialization of smart medical treatment is more cautious. Most of them are introduced into specific departments of the hospital with a single product, and play a role in auxiliary screening and diagnosis [5].

With the mature development of artificial intelligence technology and the large-scale construction of unmanned

372835803@qq.com

autonomous combat platforms, unmanned combat will become a revolutionary new type of combat. Artificial intelligence technology will be applied to the entire process of warfare, for example, intelligent perception, intelligent decision-making, intelligent control, unmanned platform, innovative combat process, etc. The US military began to explore the application of artificial intelligence technology in the military field very early. The US Defense Advanced Research Projects Agency (DARPA) launched the "Deep Green" program in 2007, with the goal of embedding simulation into the command and control system to improve the speed and quality of commanders' in-flight decisions. From 2009 to 2014, DARPA had launched a large number of basic technology research projects, to explore and develop relevant technologies for autonomously acquiring, processing information, extracting key features, and mining association relationships from different types of multi-source data such as text, images, sound, video, sensors [6]. Meanwhile, our military has also long begun to explore the research of artificial intelligence technology in the field of military information, but these technologies are currently only applied to some unmanned products / platforms. Among them, image recognition technology based on deep learning is most widely used in unmanned reconnaissance, target recognition, unmanned driving, anti-terrorism operations, path planning and other scenarios.

3 Challenges in the application of artificial intelligence in the field of military information

In the next 15 years, the field of artificial intelligence will focus on the development of human consciousness systems, including 6 core technologies of computer vision, machine learning, text language processing, natural language processing, robotics and biometric identification technology [7]. Although the prospects are promising, the current artificial intelligence technology is far from mature, so if it is to be widely used in the field of military information, it still faces the following major challenges:

First, it cannot meet the application scenarios of low power consumption. Strong computing power is the foundation of artificial intelligence, without which there will be no artificial intelligence. Today's artificial intelligence systems use hundreds of GPUs to improve computing power. GPU provides the basic structure of multi-core parallel computing, with a large number of cores, and can support parallel computing of large amounts of data. At the same time, GPU has higher memory access speed and higher floating-point arithmetic capabilities, so that the ability to process learning or intelligence can be greatly enhanced. However, the use of GPU also means that the computing device must have a larger volume and high-power consumption, which makes artificial intelligence technology can only be used on some relatively large equipment and devices, and cannot be applied to some low-power occasions, greatly limiting the application scenarios of artificial intelligence technology.

Second, artificial intelligence algorithms are particularly flawed. The success of artificial intelligence, especially deep learning technology, stems from a large amount of data and repeated training. The huge amount of data accumulated in the Internet era and the large increase in computing capacity brought by cloud computing have greatly released the potential of deep learning algorithms. But deep learning algorithms also have their own shortcoming, the lack of common-sense reasoning ability. As early as 1984, the United States began a project to build a database of common sense, which has not yet been completed. Even on the basis of a common sense library, it is still difficult to achieve artificial intelligence with comprehension ability, and from the perspective of security, pure data-driven systems are also susceptible to interference because of poor robustness. Therefore, the system will still make big mistakes even after training with a large number of samples. In fact, in practical applications, some leading enterprises, such as SenseTime and Megvii, have also proved it. On the premise that the accuracy of the trained system model is as high as 99%, the system will still make lots of "retarded" mistakes [8].

Third, the technology has security and protection loopholes. It is mainly manifested in the following aspects: The first one is the possibility of incurring hacker attacks. The possibility that the system being attacked by hackers and the program being modified cause the artificial intelligent weapon to take wrong actions cannot be ruled out. The algorithms and software that mainly drive artificial intelligence are written by humans, so human defects and technical loopholes are inevitable. The researchers have found that it is possible to train an own alternative neural network by detecting the operation of another neural network. Using alternative neural networks can generate generic hacker images to deceive the original neural network, namely a black-box attack [9], which means that relying too much on the current artificial intelligence technology will cause disastrous consequences, once it is cracked or exploited by the enemy. Second, it may not be possible to take all the complex factors of the military environment into account when designing artificial intelligence systems. If a system faces an environment that had never been considered during design, the system will malfunction or fail. Third, the system's response to emergencies is unpredictable. For artificial intelligence systems that learn after deployment, the behavior of the system is largely determined by the unsupervised learning phase. In this case, it is difficult to predict the behavior of the system [10]. The fourth is the existence of loopholes in technology replication, which are once mastered by terrorist groups or hostile forces, it is easier to manufacture more powerful weapons, which may thus lead to new terrorist attacks or a military expansion competition.

4 Framework design of the application of artificial intelligence in the field of military information

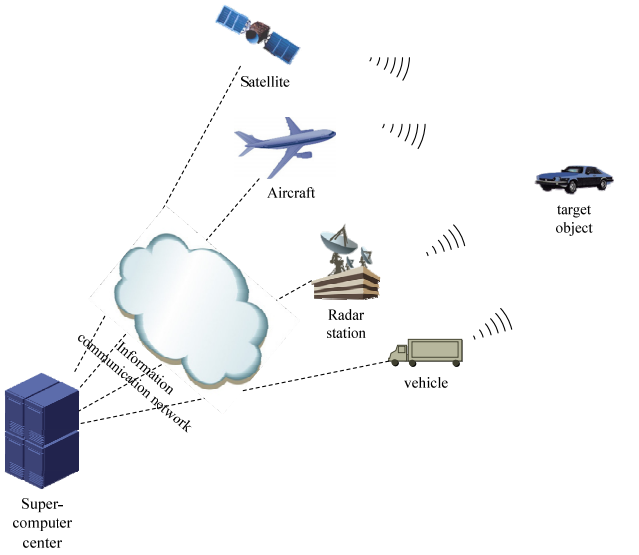
The success of artificial intelligence algorithms benefits from massive data and high-performance computing power. In general, the more types of data sources, the more accuracy of the algorithm can be improved

comprehensively through cross-analysis between data. There are many ways to obtain source data from the ground, air and sea and other various platforms, but not every type of platform is suitable for installing computing devices with large power consumption. Therefore, a good application framework must be designed to make full use of a large amount of source data to improve the accuracy of the algorithm, and meanwhile ensure the available high-performance computing power for data analysis. In summary, the application of artificial intelligence in the field of military information can be roughly divided into three frameworks-centralized, distributed and hybrid types.

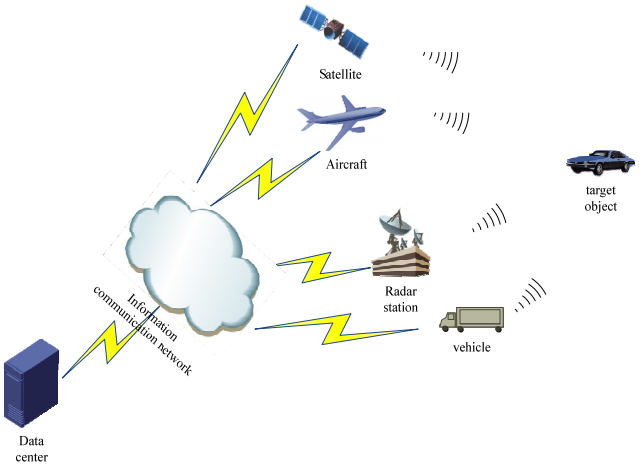
The main feature of the centralized framework is that all computing is concentrated on the back end, and the supercomputer center is used to complete the main computing work, whose advantage is that the heterogeneous data from various platforms can be used to analyze and compute the target, to improve the accuracy of algorithm recognition. However, the disadvantage of this framework is that a large amount of real-time data needs to be transmitted through the information communication network, which brings great pressure to the network. At the same time, the reliance on the supercomputer center also makes the anti-destructive ability poor in wartime.

The distributed framework does not establish a separate computing center, while each platform separately sets up computing platforms to complete the computing, share key data with each other through the information communication network, and store the necessary data in the data center. The advantage of this framework is that the network load is light and the damage resistance is strong, but its disadvantage is the limited computing power of each platform, which cannot guarantee a high recognition rate.

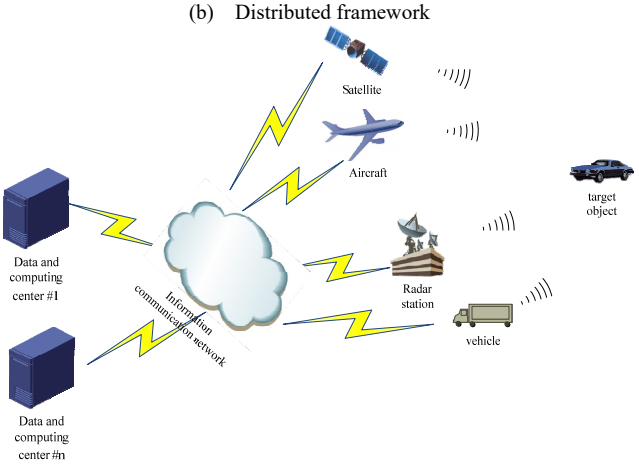
The hybrid framework is the integration of the above two frameworks, and each platform has preliminary analysis and computing capabilities. After appropriate filtering, the data is classified and submitted to the data and computing center for computing, and the key data will be shared after computing. The keys to the application of the hybrid framework are that, first, each platform must have a certain computing power and be capable to filter the data, to reduce the amount of real-time data; second, data of various platforms can be appropriately classified and centralized, for example, the data acquired by aerial platforms can be centralized. The target characteristics reflected by such data are relatively similar, suitable for classification and centralized operation; Third, the key data is shared through the information communication network to improve the comprehensive recognition rate.



(a) Centralized framework



(b) Distributed framework



(c) Distributed framework

Fig1. The frameworks for the application of artificial intelligence in the field of military information

From the above analysis, it can be seen that the hybrid framework has the main advantages of centralized and distributed frameworks and is the most feasible way. However, the technology system of the hybrid framework is relatively complicated and needs to deal with the balance between the data and computing center and each platform, and between the data and computing center, and design their own modes to divide work and perform data cooperation with each other. The overall design and

planning must be done in advance, but a step-by-step mode can be adopted when construction. According to the task classification and urgent needs, some of the platforms and data and computing centers should be built first, and after they become mature, the next batch should be built as urgently needed. Finally, the overall construction of the system will be completed step by step.

5 Some Suggestions on accelerating the intelligent construction of military information

Although the research and development of the global military autonomous system is increasing, the process is "gradual", and organizations still "work hard to achieve leapfrog progress from development to application." [11] The emergence of the artificial intelligence era will reshape the future global military to some extent. To seize the opportunities for the construction and development of artificial intelligence in the military field, it must arrange in advance, plan ahead, and do a good job in the following aspects.

5.1 Strengthen strategic leadership and strive for technological leadership

The first is to improve the development strategy of artificial intelligence choose the areas suitable for its application scenarios to focus on development according to the characteristics of artificial intelligence technology, and simultaneously handle the dialectical relationship between technological development and security protection. The second is to build a key laboratory of military artificial intelligence, build up a computing platform and data center for technological development, especially speed up data construction, and set up a variety of big data platforms for confidential military data management and sharing, to prepare data for various application. The third is to actively research and develop the key technologies of artificial intelligence, especially to focus on the research and development of active defense technologies to improve core competitiveness. The fourth is to set up a benchmark of artificial intelligence technology, establish standardized test methods and indicators for the testing of artificial intelligence systems, and meanwhile establish an artificial intelligence test platform to build a safe and accurate test platform environment for a large number of mission-sensitive data in the military field.

5.2 Strengthen military-civilian integration and promote innovation and development

The first is to actively boost the commercial application of artificial intelligence, encourage the application of scientific research results, promote the transformation of technological innovation and achievement, and form a good industrial ecology for the development of artificial intelligence. The second is to support cross-departmental and cross-border data sharing and business cooperation, promote mechanism innovation, and effectively transform the big data dividend into a direct driving force for the development and application of artificial intelligence [12]. The third is to explore the military transformation of suitable and mature commercial application projects and accelerate the paces of construction and application of military artificial intelligence systems.

5.3 Strengthen security governance and improve prevention capabilities

The first is to clarify the responsible department of the security governance of artificial intelligence, simultaneously continue to increase investment to focus on building technical standards, governance systems and governance capabilities for failure prevention, interference prevention, destruction prevention and control prevention. The second is to strengthen research on major international common issues such as robot alienation and safety risk management and control, support international cooperation, and actively participate in the formulation of international standards and rules.

References

1. Zhong Wang. Analysis of the four development stages of artificial intelligence [EB/OL]. http://net.zol.com.cn/687/6874705.html, 2018-05-07
2. hely. Comment on the development, industry and players of artificial intelligence technology: the same growth as “big data” [EB/OL].http://www.raincent.com/content-10-8198-1.html, 2016-12-21
3. Bai Jiahao of The Founder. The first commercial landing of artificial intelligence: the resurgence and industry explosion [EB/OL]. https://baijiahao.baidu.com/s?id=1593639206505292634&wfr=spider&for=pc, 2018-02-28
4. Hanlin Ji, Jiadong Huang. The Development and Application of Artificial Intelligence Industry in China. Software Guide, 2018(12): 1~5
5. Muffin Guan. 2018 China Artificial Intelligence Report：AI + vertical field is in full bloom, and intelligent life is getting closer [EB/OL]. http://www.sohu.com/a/226092108_313745, 2018-03-22
6. Zhenzhen Jia, Haiming Shi. Intelligent warfare in the eyes of the US military [EB/OL]. https://www.sohu.com/a/231359114_358040, 2018-05-12
7. Yang Yang. In the 85th year of the Army Day, how can artificial intelligence and military construction continue to write a new chapter of science and technology? [EB/OL]. https://www.iyiou.com/p/78171.html, 2018-08-01
8. IM2Maker.Artificial intelligence has reached the bottleneck! Academicians "jointly" opposed deep learning and point out the future development direction of AI.[EB/OL]. http://www.im2maker.com/news/20180703/a8b7a3af

22b5dc59.html, 2018-07-03

9. Akhtar NAMian A . Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey[J]. IEEE Access, 2018:1-1.
10. Li Wang. Reflection on the penetration and application of artificial intelligence in the military field [J]. Science & Technology Review, 2017(15):17-21.
11. Yang Liu. Application prospects and risks of artificial intelligence in the military field [EB/OL]. http://dwz.cn/4V1Gyyy.2018-4-30
12. Shizhong Wu. Don't be an "outsider" and think of the development and safety of the new-generation artificial intelligence [EB/OL]. https://www.sohu.com/a/233758853_283001, 2018-06-01