The Development and Application of Computers and Information Technology in the Military

*Yinxion*g Zhang*

College of Computer Science and Engineering, University of Electronic Science and Technology of China, 611731,Chengdu, China

Abstract. In the context of the new era of information technology, military operations and research have become increasingly reliant on computers and informatization. Military organizations are adopting cutting-edge technologies such as artificial intelligence, big data analytics, and cyber warfare strategies. This paper aims to explore the development and application of computers and information technology in the military field. Firstly, the paper introduces the evolution and innovations of computer and information technology over the past half-century. It then discusses related disciplines, including big data, the Internet of Things (IoT), cloud computing, and sensor technologies, along with relevant concepts and practical applications, providing theoretical support for the research. The paper also presents the current state of military informatization among major countries and regions worldwide. Furthermore, it elaborates on the future trends and directions of computer and information technology in the military. Finally, the paper highlights the importance of military informatization for national defense security and territorial sovereignty and outlines future developmental directions.

1 Introduction

Since entering the 21st century, the rapid development and widespread application of computer and information technology have profoundly changed the research and development direction across various fields. Its impact on the military sector is particularly prominent. In the wave of the information age, the forms of warfare and battlefield environments are becoming increasingly complex and dynamic. Traditional military means can no longer meet the demands of modern warfare. As an important support for national security and national interests, the development and application of military power must keep pace with technological advancements, continually introducing new technological means to enhance combat capabilities and improve the efficiency of warfare.

Researchers in big data focus on intelligence analysis by mining open-source and traditional military intelligence. This approach aims to obtain more comprehensive and accurate enemy intelligence. Additionally, they establish large-scale military operations data models to simulate and analyze various factors (such as troop strength, equipment, terrain, and weather) under different operational scenarios. This helps military commanders

* Corresponding author: 2023070340051@std.uestc.edu.cn

formulate and evaluate operational plans before combat. By analyzing historical and simulated data, they can predict the potential outcomes of different decisions, thereby selecting the optimal operational plans.

In the field of Internet of Things (IoT) research, scholars utilize battlefield situational awareness technologies by connecting various sensors, weapon systems, and combat platforms into a vast IoT. This integration enables seamless information exchange on the battlefield. For instance, researchers are exploring how to use IoT technology to connect soldiers' individual equipment (such as helmets and weapons) with command centers in real time. This enables soldiers to transmit battlefield conditions instantly and receive real-time instructions and intelligence updates.. Additionally, this technology is applied to optimize logistical support. By equipping transportation vehicles and storage facilities with IoT sensors, comprehensive monitoring of military logistics and supplies throughout the entire process can be achieved.

In the area of informatization and cloud computing, scholars have used cloud computing to provide elastic computing and storage resources for the construction of military information systems, so as to meet the needs of different operational tasks. For example, during large-scale military exercises or wars, cloud computing can quickly provide the required resources. In addition, scholars study the encryption technology and access control technology of military information in the cloud computing environment to ensure the security of military information. At the same time, they also study how to prevent attacks from the network, such as hacking, malware attacks, etc., to ensure the stable operation of military information systems.

In the research on sensors, researchers have concentrated on improving sensor performance. Research is conducted on detection distance, accuracy, anti-jamming ability and other aspects. For example, in the case of radar sensors, research on how to improve their detection ability of stealth targets; in the case of infrared sensors, research on how to reduce the impact of ambient temperature on their detection accuracy, etc.

Secondly, researchers fused multiple sensors. By fusing different types of sensors (such as radar, optoelectronic, acoustic and other sensors), more comprehensive and accurate target detection and identification can be realized. Scholars study algorithms and architectures for multi-sensor fusion to improve the overall effectiveness of military sensor systems.

The development and application of computer and information technology in the military has become an important field of modern military research, and many scholars have conducted research from different perspectives, laying a solid foundation for promoting the process of military modernization.

This paper will explore the development and application of computer as well as informatization in the military, focusing on the application of key technologies such as big data, Internet of Things, informatization, cloud computing and sensors in the military field.

2 The History of Computer Technology in the Military

The development of computers in the military can be traced back to the mid-20th century and has gone through several important stages of technological innovation and development since then. This section discusses the history of computer technology in the military, which is divided into the early stages, developmental innovations, modernization, and the wave of information technology. By reviewing the technological innovations and advances in each phase, it aims to show how computers and information technology have changed the way modern military operations are conducted and their efficiency.

2.1 Initial stage

The world's first electronic computer was born in 1946, when it was around the time of World War II, military science and technology on the urgent need for high-speed computing tools, which promoted the development of computer technology. During this period, computers were mainly used for computational research related to scientific research and national defense. For example, the United States during World War II began to use computers for ballistic calculations, code breaking and other work, providing important support for the victory of the war.

The computers at this stage are bulky and limited in performance, but they have been able to provide some basic computational support for the military field, helping the military to carry out complex calculations, data analysis and simulation predictions. For example, preliminary calculations and simulations of the ballistic trajectory of weapons, explosion effects, etc., through the computer to provide reference for the design and development of weapons.

2.2 Development innovation

With the development of integrated circuit technology, the size of the computer is reduced, the performance is improved, not only to improve the efficiency of the command center, but also applied to the automated control of weapons and equipment. This makes the computer more conveniently applied to the military field, not only in the military research institutions and command centers that have been widely used, but also began to gradually equipped to the troops at the grass-roots level. For example, the U.S. Army in this period began to use small computers for battlefield data collection and processing, improving the efficiency of combat command.

The development of computer technology provides the basis for the informatization of military command systems. The armies of various countries have begun to develop and apply a variety of military information systems, such as command automation systems (C3I systems), which have realized the integration of intelligence collection, command decision-making, communication and liaison functions. These systems are able to quickly process a large amount of battlefield information, provide commanders with real-time battlefield situational awareness, and greatly improve the efficiency and accuracy of command decision-making.

Computer technology is widely used in the automated control of weapons and equipment, such as missile guidance systems, aircraft autopilot systems, ship navigation systems and so on. These automated control systems can automatically control the operation and attack of weapons and equipment according to preset programs and target information, improving the precision and combat effectiveness of weapons and equipment.

2.3 The Wave of Informatization

With the rise of Internet technology, the field of military communications has undergone great changes. The armies of various countries have begun to build military-specific computer networks, realizing high-speed communication and information sharing among troops. For example, the U.S. Defense Information System Network (DISA), which connects the information systems of all military branches, has formed a huge military information network, providing strong communication support for operational command, intelligence transmission, and logistical support.

Computer simulation technology has been widely used in military training and combat simulation. Through the establishment of virtual battlefield environments and combat models,

soldiers can train in simulated environments to improve their combat skills and their ability to cope with complex battlefield situations. At the same time, combat simulation also provides military commanders with an effective means of evaluating combat scenarios and predicting the outcome of war, which helps to formulate more scientific and reasonable combat plans.

The development of artificial intelligence technology has laid the foundation for the emergence of intelligent weapons. The combination of computer technology with sensor technology and control technology has given rise to a series of intelligent weaponry, such as intelligent missiles, unmanned combat aircraft and unmanned submarines. These intelligent weapons and equipment can autonomously search, identify and attack targets, with high combat efficiency and survivability.

2.4 Modernization development

With the rapid development of information technology, the application of big data technology in the military field is becoming more and more important. The army needs to acquire valuable intelligence information by collecting, storing, analyzing and mining massive battlefield data to provide support for military decision-making. For example, big data technology is used to analyze the enemy's combat operations, weapons and equipment performance, personnel deployment and other information, to predict the enemy's operational intentions and combat strategies, and to formulate corresponding countermeasures.

Cloud computing technology provides new solutions for military logistics support. By building a military cloud computing platform, the army can realize the centralized management and sharing of logistics resources and improve the efficiency and flexibility of logistics support. For example, in the procurement, transportation and warehousing of materials, cloud computing technology can achieve real-time tracking and management of materials and optimize the logistics support process.

Quantum computing technology, as an emerging computing technology, has a powerful computing capability and parallel processing capability and has a broad application prospect in the military field. Although quantum computing technology is still in the development stage, the armies of various countries have begun to pay attention to and study its applications in the military field, such as password cracking, intelligence analysis, combat simulation and so on.

3 Computers and the use of information technology in the military

3.1 Application of big data in related fields

As mankind enters the era of big data, the explosive growth of information makes people face complex data processing needs. The development of big data technology provides strong support for data processing in the information age. In the future information war, the use of massive multi-dimensional data will become the key to victory. Through big data mining technology, massive information in the military field can be effectively utilized to improve operational efficiency, predict battlefield posture, and change the face of future war [1].

Combat simulation generates a large amount of simulation big data, and big data has important uses in this regard. First, combat damage simulation. For example, based on the tank detachment tactical integrated exercise simulation system, the use of data mining technology on the tank detachment combat process of the probability of destruction model research, the use of decision-making power to analyze the model, better to meet the needs of

the tank detachment combat destruction research for the detachment of the combat intelligence simulation research to provide a certain reference. Second, combat simulation data mining. Starting from the analysis of the composition of combat simulation data, a data mining oriented combat data warehouse construction method is proposed to incorporate system data, simulation data, simulation results and simulation management data, which has a positive reference value for collecting and acquiring data from the real world [2].

3.2 Application of the Internet of Things in related fields

The IoT refers to a huge information network formed by combining various information devices, such as infrared sensors, satellite positioning systems, laser scanners and other devices, with the Internet [3]. The purpose of the component IoT is to connect all objects to the network for more efficient identification, localization, monitoring, operation and management. IoT is widely used in all aspects of modern society, such as smart transportation, smart agriculture, smart healthcare and so on. Meanwhile, the development of IoT has also had a profound impact on the military field. This section will introduce some relevant applications of IoT in the military field as well as case studies.

One application of IoT in the military is equipment networking perception technology. Battlefield tactical perception system, usually using unmanned aircraft or artillery throwing mode, to the enemy key target area spread sound, light, electromagnetic, vibration, acceleration and other miniature integrated sensors, close-range reconnaissance and perception of the target area of the combat terrain, enemy deployment, equipment characteristics and troop activities and movements, etc.; and can be organically fused with satellites, aircraft, various types of sensors on the ship to form an omni-directional, full spectrum, full time domain, full-dimensional reconnaissance surveillance and early warning system, thus providing accurate target location. It can also be organically integrated with various sensors on satellites, aircraft and ships to form an omnidirectional, full-spectrum, full-time-domain, full-dimensional reconnaissance, surveillance and early-warning system, thus providing accurate target localization. For example, in the U.S.-Vietnam War, the U.S. Army used the unattended vibration sensor “Tropical Tree” to listen to the vehicles on the “Ho Chi Minh Trail”. When the personnel, vehicles and other targets in its vicinity, “Tropical Tree” will be able to detect the target generated by the vibration and sound information, and immediately send the data via radio to the command centre. Command and management center to process the information data, to get the location of the marching personnel, vehicles, size and direction of travel and other information, and then direct the air warplanes to implement the bombing, and achieved very impressive results [4].

Internet of Things technology plays an important role in the optimization and guarantee of logistics systems. Through the electronic information tag system, military supplies can be automatically identified, located and classified, thereby improving the efficiency of sending and receiving operations and achieving dynamic monitoring throughout the process. At the same time, combined with radio frequency identification (RFID) and satellite positioning technology, important materials can be efficiently managed and operated [5].

In the soldier's electronic life monitoring system, RFID and wireless communication technology are used to monitor vital signs in real time and improve emergency rescue preparation and guard dispatch capabilities. Internet of Things technology also optimizes the supply chain management of military logistics, tracking the flow of materials through sensors, identifying bottlenecks and delays, and thus reducing costs.

In addition, with the advancement of human-computer interaction technology and the Internet of Things, military smart wearable equipment makes operation more convenient and enhances the real-time connection and dynamic control of combat personnel, equipment and networks. For example, the US Army funded the research of the "Mind Control Robot"

project, which aims to remotely control robots to perform combat tasks through thoughts and improve the overall effectiveness of combat systems [6].

3.3 Impact of Informationization and Cloud Computing in Related Fields

Cloud computing is the use of Internet technology to integrate information technology processing power into a large-scale scalable way to multiple external customers as a service to provide a kind of computing, so that a variety of application systems can be based on the need to obtain computing power, storage space and a variety of software services. In today's information war, how to complete the intelligence fusion of large-scale target information in a short period of time, conduct situational threat analysis, and then provide auxiliary decision-making information [7]. Referring the idea of cloud computing to the military network can effectively solve the above problems.

In modern military and war, high-efficiency information sharing and intelligence transmission is the key to victory, and cloud computing has achieved certain results in this area. For example, in July 2008, the U.S. Department of Defense and Hewlett-Packard reached a cooperation, Hewlett-Packard will help the U.S. Department of Defense to establish a cloud computing infrastructure. Through the establishment of a cloud computing strategy, the construction of fast-access computing environment, in order to allocate server resources to the Defense Information Systems Agency customers when needed. The Rapid Access Computing Environment will be delivered through a web portal that can take the Defense Information Systems Agency to a new level of speed and flexibility, and greatly enhance the reliability of the cloud computing service model. With the Rapid Access Computing Environment, users will not have to invest in hardware and software licenses, and will be able to run applications in an on-demand environment faster and at a lower cost. This web-based cloud computing model allows U.S. military personnel to configure and use servers on the Defense Information Systems Agency network at any point in time [8].

Under the cloud computing environment, the “cloud” distributes user applications and calculations on different servers, and user terminals no longer process and obtain data solely on local servers. When some of the computing centers and server groups in the cloud fail or are interfered or even destroyed by the enemy, the cloud as a whole can still maintain normal operation and can be maintained and optimized by deploying new servers and updating application software. “Cloud” performance, thus improving the wartime survivability of information systems. War has always taken attacking or destroying the other side's command structure as the primary goal, and once the command structure is attacked, it is very likely to cause command paralysis. With cloud computing, even if the command center is attacked, the commander can still command the troops by relying on the cloud terminal, and the survivability is greatly improved [9].

When combatants are faced with complex information on the battlefield, cloud computing and interactive equipment can greatly help soldiers reduce interference from the outside world, so as to analyze and grasp the initiative of the battlefield situation. For example, the U.S. Army has developed a wearable “skin biosensor” that can monitor a number of physiological indicators responded to by the wearer's sweat in full time, and transmit the data information to the intelligent terminal for summarization and analysis . Intelligent name tags made using this technology can enable commanders or group trainers to grasp the physiological changes of combatants or trainees in real time, accurately determine the survival status of frontline combatants or trainees' real-time changes in their physical signs, and provide powerful data support for the application of force and training organization [10].

3.4 Sensor Networks Technologies in Related Fields

With the gradual increase of people's requirements for computing power, communication power and sensing power, high-performance sensors have attracted great attention. Sensors integrate the logical information world with the real physical world, profoundly changing the way of interaction between man and nature; they can be widely used in many fields. Among them, the military field is particularly prominent [11].

In the military domain, sensor networks will become an integral part of the command, control, communication, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) system. The C4ISRT system is a comprehensive battlefield command system that integrates command, control, communication, computing, intelligence, surveillance, reconnaissance and targeting. The system is designed to provide efficient decision support and battlefield situational awareness for modernized warfare and is widely valued by military developed countries. Because the sensor network is composed of dense, low-cost, randomly distributed nodes, the self-organization and fault-tolerance ability make it will not lead to the collapse of the whole system because of the damage of some nodes in malicious attacks, which makes the sensor network suitable for application in harsh battlefield environments, including the monitoring of troops, equipment and materials, surveillance of conflict zones, reconnaissance of enemy terrain and defense, locating the target of attack, assessing the damage, scouting and detecting nuclear, equipment, and materials, as well as monitoring of conflict areas. Reconnaissance and detection of nuclear, biological and chemical attacks. In the battlefield, commanders need to know the situation of troops, weapons, equipment and military supplies in a timely and accurate manner, and the sensors laid will collect the corresponding information and send the data to the command center through the convergence node, and then forwarded to the command headquarters, and finally fused with the data from the battlefields to form a complete map of the battlefield situation of the army. In war, the surveillance of conflict zones and military sites is also crucial, through the laying of sensor networks, a more covert way to observe the enemy's defense in close proximity; in addition, the sensor nodes can be deployed in the enemy's position, through the covert way to quickly collect combat-related intelligence, before the enemy has not yet responded to gain the battlefield advantage. Sensor networks can also provide accurate target localization information for fire control and guidance systems. In biological and chemical warfare, the use of sensor networks to detect blast centers in a timely and accurate manner will provide troops with valuable reaction time, thereby minimizing casualties. Sensor networks can also avoid direct exposure of nuclear reaction forces to nuclear radiation.

Multimedia sensor networks have the characteristics of rapid deployment and self-organization, so they are very suitable for application in the military field. It can realize the monitoring of enemy troops and equipment, real-time battlefield surveillance, target location, battlefield assessment and other functions. For example, in 2003, the U.S. Defense Advanced Research Projects Agency led the Network Embed and System Technology project successfully validated the wireless sensor technology for accurate positioning capabilities, the project uses audio sensor networks all the enemy forces to carry out accurate positioning of combat personnel, positioning accuracy of 1.5 m, positioning latency of 2 s. In 2003, the project was completed in August. In August 2003. The U.S. Army in Ohio carried out a “straight line in the sand (A Line in the Sand) system” project research, this system is mainly to study the wireless sensor networks in the target identification, target classification and target tracking aspects of the realization. Through the integrated imaging and unattended ground sensor system, the direction of travel of people and vehicles can be detected, classified and determined in a passive manner, and can provide high-resolution images of the detected scene.

With the development of computer and sensor miniaturization and intelligent weaving technology, intelligent devices have achieved the goal of "wearing on the body", greatly

expanding the physiological functions of the human body. For example, the US Army's "Land Warrior" system, as a representative of portable integrated combat systems, embeds microcomputers, sensors, reconnaissance imaging equipment and communication and navigation equipment into combat equipment, and builds five subsystems: smart helmets, protective equipment, weapons, computing/radio equipment and software, thereby improving the comprehensive combat capabilities of individual soldiers on the battlefield, such as command and communication, navigation and positioning, situational awareness, coordinated operations and self-protection.

In addition, related companies have developed intelligent protective equipment. For example, Lemur Design Studio in Colombia launched a smart shoe called "Save One Life". The sole is equipped with a metal detector. When a suspicious mine is detected, the connected smart watch will sound an alarm to indicate the location of the suspicious object. The British company Intelligent Textiles Ltd integrates electronic devices into wearable fabrics through weaving technology. The "Spirit" smart fabric launched not only provides thermal insulation, but also has mobile power, data connection and bulletproof protection functions.

4 The future development trend of informationization and network weapons

Since the 1990s, military forces in various countries have established cyber warfare units to control the network and information battlefield, disrupt enemy network systems, control wars, and weaken enemy combat capabilities.

4.1 Case Study

As a leading military power in the world, the United States attaches great importance to the construction of cyber warfare capabilities. As early as 2002, the United States established the "Joint Cyber Warfare Functional Command" and gradually established multiple specialized agencies such as the "Cyber Command" and the "Global Cyber Warfare Joint Operations Group", responsible for unified command of cyber warfare operations and ensuring network attack and defense capabilities in future wars.

After the dissolution of the Soviet Union, Russia realized the importance of information security for national strategic development. By the end of 2003, Russia had completed the transition from traditional password device security to the information security industry, forming an information security industry group dominated by large enterprises. The Russian military specializes in developing computer viruses to reduce the effectiveness of enemy electronic information systems, with the joint participation of military and civilian talents such as linguists, mathematicians, cryptographers, and hackers. In this field, especially "remote virus weapons" and "microwave weapons" pose a direct threat to enemy command and control systems.

The Indian military has established a joint computer emergency response team consisting of the army, navy, and air force, and has set up a specialized cyber warfare and cybersecurity department to ensure information sharing and effective response capabilities in networked warfare.

The Japanese Self Defense Forces have established the "Cyber Special Forces" to prepare for future information warfare, and plan to form a 5000 member "Cyber Team" to focus on developing "cyber weapons" that can damage other countries' cyber systems. At the same time, South Korea has established an information warfare center to monitor defense computer networks in real-time and respond quickly to cyber attacks.

4.2 Future Trends

Modern warfare is gradually evolving into intelligent warfare, which may become the "third revolution of war" after gunpowder and nuclear weapons. The emergence of artificial intelligence weapons will fundamentally change the way of warfare, shifting from "human to human" warfare to "machine autonomous killing". Countries are exploring armies composed of AI weapons in order to gain the upper hand in future wars.

The improvement of information technology level and the expansion of combat space have led to a qualitative leap in the combat capabilities of various military branches in modern warfare. With the development of information technology, the traditional military service combat mode is facing challenges and urgently needs a new concept of joint operations. For example, the experience of the United States in the Iraq War demonstrated the necessity of achieving unified command and coordination among various branches of the military and demonstrated the need for new joint combat capabilities.

5 Conclusion

This paper discusses the development and application of computer technology and informatization in the military field and analyzes its far-reaching impact on many aspects of modern warfare methods, command and control, intelligence collection, combat training, weapon systems and logistical support. Through the introduction of advanced computer technology, military commanders are able to rapidly acquire and process information in the complex and changing battlefield environment, so as to make more scientific and efficient decisions. In addition, the application of information technology significantly improves the accuracy and timeliness of intelligence analysis, providing strong support for military operations.

It can be seen that future wars will rely more on information technology, which requires military personnel to continuously improve information technology literacy and adapt to the operational requirements under the new situation. At the same time, network security and electronic warfare capabilities are becoming more and more important, and a sound network protection system must be established to deal with potential cyber threats.

The results of this study not only provide a theoretical basis for the formulation of military strategy but also provide a new perspective for subsequent research. In future research, the potential application of emerging technologies such as artificial intelligence and quantum computing in the military field can be further explored, as well as how to effectively integrate various informatization means in order to enhance the overall combat capability. These studies will provide sustained impetus for military modernization and national defence construction in individual countries.

Reference

1. S. P. Wang, Q. D. Li, C. Zhao, A review of research on military application of big data mining technology. Ship Electronic Engineering. **40**, 17-22 (2020)
2. G. P. Xiao. Internet of things technology and its military applications. Internet of Things Technology, **3**, 62-64+67 (2013)
3. L. J. Zeng, H. Zhang, Z. Li. Exploration of cloud computing and its application in military. Modern Electronic Technology, **32**, 23-26 (2009)
4. J. Su, Y. Zhang, W. Chen, et al. Research on the application of cloud computing in military combat command. Software Guide, **12**, 15-17 (2013)

5. W. Deng, D. Zhang. Military application and development trend of smart wearable devices. National Defense Science and Technology, **37**, 57-60 (2016)
6. G. Liu. The Sharp Weapon of Informatization War--Network Warfare. Science and Technology Innovation Herald, **09**, 24-25 (2011)
7. F. Y. Wang, J. Chen. Overview of Information Security Construction of Russian Federation and Army. International Information, **04**, 27-30 (2010)
8. F. Ren, H. Huang, G. Lin. Wireless sensor networks. Journal of Software, **7**, 1282-1291 (2003)
9. Y. He, T. Huang, S. Feng. Application of wireless sensor network technology in military. Internet of Things Technology, **1**, 64-66 (2011)
10. L. Wang. Thinking about the penetration and application of artificial intelligence in the military field. Science and Technology Herald, **35,** 15-19 (2017)
11. J. Lu. PLA Daily Cross-domain coalition, new trend of future joint operations. 2020.9.8 (2020). http://www.81.cn/jfjbmap/content/2020-09/08/content_270364.htm