**The era of intelligent warfare is accelerating**

Source: People's Forum Academic Frontier, May, 2021

Author: Wu Mingxi

Editor: Chen Luying

2021-08-18

<https://www.rmlt.com.cn/2021/0818/622319.shtml>

【Abstract】Since the new century, the rapid development of intelligent technology with artificial intelligence (AI) as the core has accelerated the process of a new round of military revolution, and the competition in the military field is accelerating towards the era of intellectual power. The combat elements and diversified combinations represented by "AI, cloud, network, group, and terminal" constitute a new battlefield ecosystem, and the winning mechanism of war has completely changed. The AI ​​system based on models and algorithms will be the core combat capability, running through all aspects and links, playing a multiplying, transcending and active role. The platform is controlled by AI, the cluster is guided by AI, and the system is decided by AI. The traditional human-based combat methods are replaced by AI models and algorithms, and intellectual power becomes the core power of future wars. The stronger the intelligent combat capability, the more hope there is to win without fighting.

【Key words】artificial intelligence, unmanned battlefield, ecological warfare, form

【Chinese Library Classification Number】TP18 【Document Identification Code】A

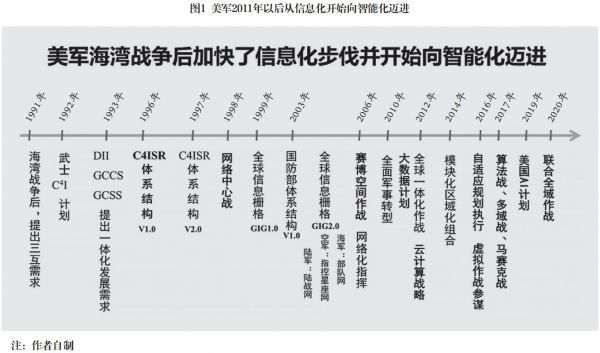
【DOI】10.16619/j.cnki.rmltxsqy.2021.10.005

[Author Profile] Wu Mingxi is the chief scientist and researcher of China Ordnance Industry Corporation, deputy secretary-general of the Science and Technology Committee of China Ordnance Industry Group, and deputy director of the Science and Technology Committee of China Ordnance Science Academy. His research interests include national defense science and technology and weapon equipment development strategy and planning, policy and theory, management and reform research. His major works include "Intelligent Warfare - AI Military Vision" and so on.

**Competition in the Intellectual Property Era**

The history of human civilization is the history of understanding and transforming nature, as well as the history of understanding and liberating oneself. Human beings have continuously enhanced their capabilities, reduced their burdens, freed themselves from constraints, and liberated themselves by developing science and technology and developing and using tools. The control of war has also been constantly changing, enriching, and evolving with the advancement of science and technology, the expansion of human activity space, and the development of the times. Since the 19th century, mankind has successively experienced the control and competition of land power, sea power, air power, space power, and information power. With the rapid development of intelligent technologies such as artificial intelligence (AI), big data, cloud computing, biological cross-talk, unmanned systems, and parallel simulation, and their deep integration with traditional technologies, the ability of human beings to understand and transform nature has been changed from the perspectives of epistemology, methodology, and operating mechanism. It is accelerating the promotion of major collective technological changes such as machine intelligence, bionic intelligence, group intelligence, human-machine fusion intelligence, intelligent perception, intelligent decision-making, intelligent action, intelligent support, as well as intelligent design, research and development, testing, and manufacturing, and accelerating the evolution of the war form to the control and competition of intellectual property rights.

Intelligent technology is developing rapidly and has been highly valued by major countries in the world, becoming a powerful driving force to support the leapfrog development of military capabilities. The United States and Russia have placed intelligent technology at the core of maintaining their strategic position as global military powers. Their development concepts, development models, organizational methods, innovative applications, etc. have undergone major changes, and they have carried out substantial applications and practices of military intelligence (see Figure 1).



In August 2017, the US Department of Defense stated that AI wars are inevitable in the future and the United States needs to "take immediate action" to accelerate the development of AI war technology. The "Third Offset Strategy" proposed by the US military believes that a storm of military transformation marked by intelligent armies, autonomous equipment and unmanned warfare is coming; to this end, they have listed intelligent technologies represented by autonomous systems, big data analysis, and automation as the main development direction. In June 2018, the US Department of Defense announced the establishment of the Joint Artificial Intelligence Center, which, under the guidance of the national artificial intelligence development strategy, coordinates the construction of the US military's intelligent military system. In February 2019, then-US President Trump signed the "American Artificial Intelligence Initiative" executive order, emphasizing that the United States' continued leadership in the field of artificial intelligence is crucial to maintaining the country's economic and national security, and requires the federal government to invest all resources to promote innovation in the field of artificial intelligence in the United States. In March 2021, the US National Security Commission on Artificial Intelligence released a research report, pointing out that "for the first time since World War II, the technological advantage that is the backbone of the US economic and military power is threatened. If the current trend does not change, China has the power, talent and ambition to surpass the United States and become the global leader in artificial intelligence in the next decade." The report believes that in order to maintain national security and enhance defense capabilities, the United States must use artificial intelligence quickly and responsibly to prepare for these threats. The report concludes that artificial intelligence will change the world and the United States must take the lead.

Russia also attaches great importance to the technological development of artificial intelligence and its military application. The Russian military generally believes that artificial intelligence will trigger the third revolution in the military field after gunpowder and nuclear weapons. In September 2017, Russian President Vladimir Putin publicly stated that artificial intelligence is the future of Russia, and whoever can become a leader in this field will dominate the world. In October 2019, Putin approved the "Russian National Artificial Intelligence Development Strategy before 2030", which aims to accelerate the development and application of artificial intelligence in Russia and seek a world-leading position in the field of artificial intelligence.

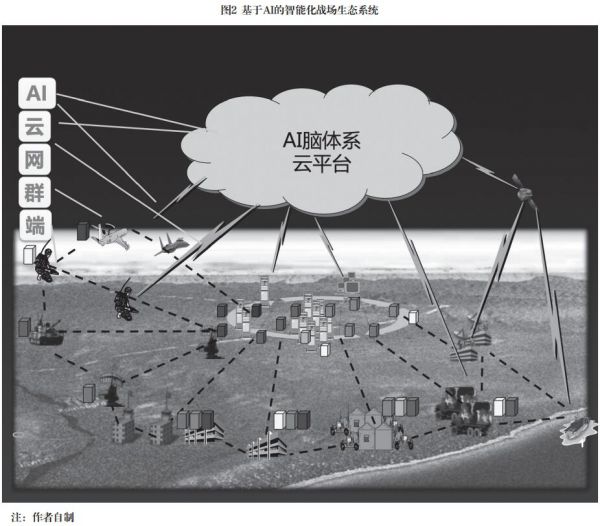
In July 2017, the State Council of China issued the "New Generation Artificial Intelligence Development Plan", which proposed the guiding ideology, strategic goals, key tasks and guarantee measures for the development of the new generation of artificial intelligence by 2030, and deployed to build the first-mover advantage in the development of artificial intelligence and accelerate the construction of an innovative country and a world science and technology power.

Other major countries and military powers in the world have also launched their own AI development plans, indicating that the global competition for "intellectual rights" has been fully launched. Land power, sea power, air power, space power, information power, intellectual power, etc. are all the results of scientific and technological progress and the products of the times. They all have their own advantages and disadvantages, and some theories are constantly expanding with the changes of the times. From the development trend of control over wars in modern times, it can be seen that information power and intellectual power involve the overall situation, and their weight is heavier and their influence is greater. In the future, with the acceleration of the pace of intelligent development, intellectual power will become a new type of battlefield control that is growing rapidly and has a greater strategic influence on the overall situation of operations.

The essence of military intelligence is to use intelligent technology to establish diversified identification, decision-making and control models for the war system. These models are artificial intelligence (AI), which is the core of the intellectual property rights competition in the new era. Among them, the war system includes: equipment systems such as single equipment, clusters, manned and unmanned collaboration, multi-domain and cross-domain operations; combat forces such as individual soldiers, squads, teams, synthetic combat units, and theater joint command; combat links such as networked perception, mission planning and command, force coordination, and comprehensive support; professional systems such as network attack and defense, electronic countermeasures, public opinion control, and infrastructure management; military capabilities such as intelligent design, research and development, production, mobilization, and support. AI is embedded in various systems, levels, and links of the war system in the form of chips, algorithms, and software. It is a systematic brain. Although AI is a part of the war system, it will dominate the overall situation of future wars due to its increasingly powerful "brain-like" functions and "surpassing human limits."

**Reconstruction of battlefield ecology**

In traditional warfare, the elements of warfare are relatively independent and separated, and the battlefield ecosystem is relatively simple, mainly including people, equipment, and tactics. In the war of the intelligent era, the integration, association, and interaction between the various elements of warfare are obvious, and the battlefield ecosystem will undergo substantial changes, forming a combat system, cluster system, and human-machine system composed of AI brain systems, distributed clouds, communication networks, collaborative groups, and various virtual and real terminals, referred to as the "AI, cloud, network, group, terminal" intelligent ecosystem (see Figure 2). Among them, AI occupies a dominant position.



AI brain system. The AI ​​brain system of the intelligent battlefield is a networked and distributed system that is inseparable from the combat platform and combat missions. There are many ways to classify it. According to function and computing power, it mainly includes the cerebellum, group brain, midbrain, hybrid brain and cerebrum; according to combat missions and links, it mainly includes sensor AI, combat mission planning and decision-making AI, precision strike and controllable damage AI, network attack and defense AI, electronic countermeasures AI, intelligent defense AI and comprehensive support AI; according to form, it mainly includes embedded AI, cloud AI and parallel system AI.

The cerebellum mainly refers to the embedded AI of sensor platforms, combat platforms and support platforms, which mainly performs tasks such as battlefield environment detection, target identification, rapid maneuver, precision strike, controllable damage, equipment support, maintenance support and logistics support.

The swarm brain mainly refers to the AI ​​for intelligent control of unmanned swarm platforms on the ground, in the air, at sea, in water and in space. It mainly performs tasks such as collaborative perception of the battlefield environment, swarm maneuvers, swarm strikes and swarm defense. It focuses on algorithms for homogeneous swarm systems and algorithms for heterogeneous systems such as manned-unmanned collaboration.

The midbrain mainly refers to the AI ​​system of edge computing in the command center, data center, and command post of the front-line units on the battlefield. It mainly performs dynamic planning, autonomous decision-making, and auxiliary decision-making of tactical unit combat tasks under online and offline conditions.

The hybrid brain mainly refers to the collaborative command and hybrid decision-making system between commanders and machine AI during the operations of organized troops. Before the war, it mainly performs human-based combat mission planning. During the war, it mainly performs adaptive dynamic mission planning and adjustment based on machine AI. After the war, it mainly performs hybrid decision-making for counter-terrorism and defense.

The brain mainly refers to the model library, algorithm library, and tactics library of the theater command center and data center, which mainly provides auxiliary support for campaign and strategic decision-making. Due to sufficient data, various AI brain systems on the battlefield can be trained and modeled here, and then loaded into various task systems when they are mature.

In the future battlefield, there will be other AIs of different functions, types, and sizes, such as sensor AI, which mainly includes image recognition, electromagnetic spectrum recognition, sound recognition, voice recognition, human activity behavior recognition, etc. With the rapid development and widespread application of intelligence, AIs of all sizes will exist throughout society, serving the people and society in peacetime and the military in wartime.

Distributed cloud. Military cloud is different from civilian cloud. Generally speaking, the military cloud platform is a distributed resource management system that uses communication networks to search, collect, aggregate, analyze, calculate, store, and distribute combat information and data. By building a distributed system and multi-point fault-tolerant backup mechanism, the military cloud platform has strong intelligence sharing capabilities, data processing capabilities, anti-strike and self-repair capabilities, and can provide fixed and mobile, public and private cloud services, realizing "one point collection, everyone sharing", greatly reducing the information flow links, making the command process flat and fast, and avoiding repeated and decentralized construction at all levels.

From the perspective of future intelligent warfare needs, the military cloud needs to build at least four levels of tactical front-end cloud, troop cloud, theater cloud and strategic cloud. According to combat elements, it can also be divided into specialized cloud systems such as intelligence cloud, situation cloud, firepower cloud, information warfare cloud, support cloud and nebula.

1. Front-end cloud mainly refers to computing services such as information perception, target identification, battlefield environment analysis, autonomous action decision-making and auxiliary decision-making between teams, teams and platforms, as well as combat process and effect evaluation. The role of the front-end cloud is mainly reflected in two aspects. First, the mutual sharing and coordination of computing and storage resources between platforms, and the interactive integration of intelligent combat information. For example, once a platform or terminal is attacked, the relevant perception information, damage status and historical situation will be automatically backed up, automatically replaced, and automatically updated through the networked cloud platform, and the relevant information will be uploaded to the superior command post. The second is the online information service and intelligent software upgrade of offline terminals.

2. Troop cloud mainly refers to the cloud system built for battalion and brigade operations, with a focus on computing services such as intelligent perception, intelligent decision-making, autonomous action and intelligent support for different threats and environments. The goal of troop cloud construction is to establish a distributed cloud system that is networked, automatically backed up, and connected to multiple links at the upper level to meet the computing needs of different forces such as reconnaissance perception, mobile assault, command and control, firepower strike, and rear-end support, and to meet the computing needs of different combat tasks such as tactical joint operations, manned/unmanned coordination, and cluster attack and defense.

3. The theater cloud focuses on providing battlefield meteorological, geographical, electromagnetic, humanistic, social and other environmental factors and information data for the entire combat area, providing comprehensive information such as the deployment of forces, weapons and equipment, movement changes, and combat damage of both sides, and providing relevant information such as superiors, friendly forces and civilian support forces. The theater cloud should have networked, customized, and intelligent information service functions, and interconnect with various combat forces through military communication networks such as space-based, air-based, ground-based, sea-based and underwater, as well as civilian communication networks under confidentiality measures, to ensure the provision of efficient, timely and accurate information services.

4. Strategic cloud is mainly established by a country's national defense system and military command organs, focusing on military information, covering comprehensive information data such as relevant national defense science and technology, national defense industry, mobilization support, economic and social support capabilities, as well as politics, diplomacy, and public opinion. It provides core information such as war preparation, combat planning, combat plans, combat progress, battlefield situation, and combat situation analysis, as well as evaluation analysis and suggestions; it provides supporting data such as strategic intelligence, military strength of combat opponents, and war mobilization potential.

The above-mentioned clouds have relationships of size, top-to-bottom, as well as horizontal collaboration, mutual support, and mutual service. The military cloud platform has two core tasks: one is to provide data and computing support for building an AI brain system for intelligent combat; the other is to provide combat information, computing, and data assurance for various combat personnel and weapon platforms. In addition, from the perspective of terminal and group combat needs, some results, models, and algorithms of cloud computing need to be made into smart chips in advance and embedded in weapon platforms and group terminals. After that, they can be upgraded online or offline.

Communication network. Military communication and network information is a complex super network system. Since military forces mainly fight on land, sea, air, space, field mobile, urban and other environments, their communication networks include strategic communication and tactical communication, wired communication and wireless communication, confidential communication and civil communication. Among them, wireless, mobile and free space communication networks are the most important components of the military network system, and related integrated electronic information systems are also gradually established based on communication networks.

In the mechanized era, military communications mainly followed the platform, terminal and user, and the specialization was met, but there were too many chimneys and the interconnection and interoperability was extremely poor. In the information age, this situation began to change. At present, the military communication network is adopting a new technical system and development model, with two main characteristics: one is "network-number separation", the transmission of information does not rely on a specific network transmission method, "network access means access", as long as the network link is unobstructed, any required information can be delivered; the second is Internetization, based on IP addresses, routers, and servers to achieve "all roads lead to Beijing", that is, military networking or gridding. Of course, military communication networks are different from civilian ones. There are always strategic and special communication needs, such as nuclear button communications of nuclear weapons and command and control of strategic weapons, information transmission of satellite reconnaissance, remote sensing and strategic early warning, and even special communications under conditions such as single-soldier indoor and special operations. They may still adopt the mode of communication following the task. Even so, universalization and Internetization must be the development trend of military communication networks in the future. Otherwise, not only will there be more and more battlefield communication bands, radio stations and information exchange methods, causing self-disturbance, mutual interference and electromagnetic compatibility difficulties, but radio spectrum management will also become more and more complicated. More importantly, it will be difficult for platform users to implement automatic communication based on functions such as IP addresses and routing structures, just like e-mails on the Internet, where one-click commands can be sent to multiple users. Future combat platforms will definitely be both user terminals for communication and routers and servers.

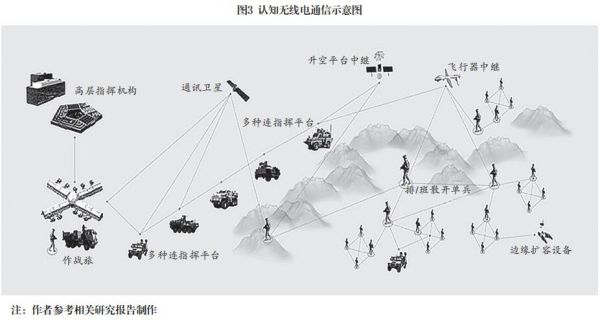
The military communication network system mainly includes space-based communication network, military mobile communication network, data link, new communication network, civilian communication network, etc.

1. Space-based information network. The United States is in a leading position in the construction of space-based information networks and the use of space-based information. Because more than half of the thousands of platforms and payloads in orbit in space are American. After the Gulf War, especially during the Iraq War, the U.S. military accelerated the application and advancement of space-based information networks through war practices. After the Iraq War, through the use of space-based information and the establishment of IP-based interconnection, nearly 140 vertical chimneys during the Gulf War were completely interconnected horizontally, greatly shortening the time of the "reconnaissance-judgment-decision-attack" (OODA) loop, and the time from space-based sensors to shooters was shortened from dozens of hours during the Gulf War to only about 20 seconds after the use of artificial intelligence recognition.

With the rapid development of small satellite technology, there are more and more low-cost, multifunctional small satellites. As the competition for commercial launches increases, the cost has begun to drop sharply, and a launch can carry several, dozens or even dozens of small satellites. If miniaturized electronic reconnaissance, visible light and infrared imaging, and even quantum dot micro-spectrometers are integrated on them, the integration of reconnaissance, communication, navigation, meteorology, mapping and other functions can be achieved, and the future world and battlefield will become more transparent.

2. Military mobile communication network. Military mobile communication network has three main uses. First, command and control between various military services and combat units in joint operations. This type of communication has a high confidentiality level and high reliability and security requirements. Second, communication between platforms and clusters requires anti-interference and high reliability. Third, the command and control and fire control of weapon systems are mostly solved through data links.

Traditional military mobile communication networks are mostly "centralized, vertically oriented, and tree-like in structure." With the acceleration of the informationization process, the trend of "decentralized, self-organizing, and Internet-based" is becoming more and more obvious. With the gradual maturity and promotion of cognitive radio technology (see Figure 3), future network communication systems will be able to automatically identify electromagnetic interference and communication obstacles in the battlefield, quickly find available spectrum resources, and conduct real-time communication through frequency hopping and other methods. At the same time, software and cognitive radio technology can also be compatible with different communication frequency bands and waveforms, which is convenient for compatible use in the transition from the old system to the new system.



3. Data link. Data link is a special communication technology that realizes the transmission of key information agreed in advance, regularly or irregularly, regularly or irregularly between various combat platforms through time division, frequency division, code division, etc. As long as it is not completely mastered or deciphered by the enemy, it is difficult to be interfered with. Data links are mainly divided into two categories: dedicated and general. Joint operations, formation coordination and cluster operations mainly use general data links. Satellite data links, drone data links, missile-borne data links, weapon fire control data links, etc., are mostly dedicated at present. In the future, generalization is a trend, and specialization will become less and less. In addition, from the perspective of the relationship between platform and communication, the information transmission and reception and internal information processing of platform sensors generally follow the mission system, with strong specialization characteristics, while communication and data transmission between platforms are becoming more and more general.

4. New communications. Traditional military communications are mainly based on microwave communications. Due to the large divergence angle and the large number of application platforms, the corresponding electronic interference and microwave attack methods have also developed rapidly, making it easy to implement interference and destruction at a long distance. Therefore, new communication methods such as millimeter waves, terahertz, laser communications, and free-space optical communications have become important choices that are both anti-interference and easy to implement high-speed, large-capacity, and high-bandwidth communications. Since high-frequency electromagnetic waves have a small divergence angle, although they have good anti-interference performance, it is still difficult to achieve point-to-point precision aiming and omnidirectional communication, especially under the conditions of high-speed maneuvering and rapid track change of combat platforms. How to achieve alignment and omnidirectional communication is still under technical exploration.

5. Civilian communication resources. The effective use of civil communication resources is a strategic issue that needs to be focused on and cannot be avoided in the era of intelligence. In the future, through civil communication networks, especially 5G/6G mobile communications, open source information mining and data correlation analysis will be carried out to provide battlefield environment, target and situation information, which will be very important for both combat and non-war military operations. In non-war military operations, especially overseas peacekeeping, rescue, counter-terrorism, disaster relief and other operations, the military's dedicated communication network can only be used in a limited range and region, and how to communicate and contact with the outside world becomes a problem. There are two main ways to use civil communication resources: one is to use civil satellites, especially small satellite communication resources; the other is to use civil mobile communications and Internet resources.

The core of the interactive use of military and civilian communication resources is to solve the problem of security and confidentiality. One way is to adopt firewalls and encryption, and directly use civilian satellite communications and global mobile communication facilities to command communications and contacts, but the risk of hackers and network attacks still exists. Another way is to use new technologies such as virtualization, intranet, semi-physical isolation, one-way transmission, mimicry defense, and blockchain developed in recent years to solve it.

Collaborative swarm. By simulating the behaviors of bee colonies, ant colonies, bird flocks, and fish schools in nature, studying the autonomous collaborative mechanism of cluster systems such as drones and intelligent ammunition, and completing combat tasks such as attacking or defending enemy targets, it can achieve a strike effect that is difficult to achieve with traditional combat means and methods. Collaborative swarms are an inevitable trend in the development of intelligence, and are also the main direction and key area of ​​intelligent construction. A single combat platform, no matter how high its combat performance and how powerful its functions are, cannot form an advantage in group and quantity scale. The simple accumulation of quantity and the expansion of scale, without autonomous, collaborative, and orderly intelligent elements, is also a mess.

The collaborative group mainly includes three aspects: first, the manned/unmanned collaborative group formed by the intelligent transformation of existing platforms, which is mainly constructed with large and medium-sized combat platforms; second, the low-cost, homogeneous, single-function, and different types of combat swarms, which are mainly constructed with small unmanned combat platforms and ammunition; third, the bionic swarm that integrates man and machine and has both biological and machine intelligence, which is mainly constructed with highly autonomous imitations of humans, reptiles, birds, and marine organisms. Using the collaborative group system to implement cluster warfare, especially swarm warfare, has many advantages and characteristics.

1. Scale advantage. A large unmanned system can disperse combat forces, increase the number of targets attacked by the enemy, and force the enemy to consume more weapons and ammunition. The survivability of the cluster is relatively flexible and has strong recovery capabilities due to its large number. The survivability of a single platform becomes irrelevant, and the overall advantage is more obvious. The scale of the number prevents the decline of combat effectiveness from fluctuating greatly, because the consumption of a low-cost unmanned platform is not like high-value manned combat platforms and complex weapon systems, such as B2 strategic bombers, F22, F35 advanced combat aircraft, once attacked or destroyed, the combat effectiveness will drop sharply. Cluster operations can launch attacks at the same time, making the enemy's defense line overwhelmed, because most defense systems have limited capabilities and can only handle a certain number of threats at a time. Even with dense artillery defense, a salvo can only hit a limited number of targets, and there will always be fish that slip through the net, so the cluster system has a strong penetration capability.

2. Cost advantage. Cluster warfare, especially swarm warfare, is mostly based on small and medium-sized drones, unmanned platforms and ammunition, with simple models, large quantities and the same quality and performance requirements, which are convenient for low-cost large-scale production. Although the speed of upgrading and replacement of modern weapons and equipment and combat platforms has significantly accelerated, the cost increase is also extremely alarming. After World War II, the research and development and procurement prices of weapons and equipment showed that the cost and price of equipment increased much faster than the performance improvement. The main battle tanks during the Gulf War were 40 times that of the World War II period, and combat aircraft and aircraft carriers were as high as 500 times. From the Gulf War to 2020, the prices of various main combat weapons and equipment have increased several times, dozens of times, and even dozens of times. In comparison, small and medium-sized drones, unmanned platforms and ammunition with simple models have obvious cost advantages.

3. Autonomous advantage. Under the unified space-time reference platform, through networked active and passive communication and intelligent perception of battlefield environment targets, individual platforms in the group can accurately perceive the distance, speed and position relationship between each other, and can also quickly identify the nature, size, priority and urgency of the target threat, as well as the distance between itself and friendly platforms. Under the premise of formulating combat rules in advance, one or several platforms can attack simultaneously and in waves according to the priority of the target threat, or they can attack simultaneously and multiple times in groups (see Figure 4). It can also clarify the priority replacement order of subsequent platforms once a platform is damaged, and finally achieve autonomous decision-making and autonomous action according to the combat rules agreed in advance. This intelligent combat action can be completely handed over to the group for autonomous action, or semi-autonomous action with human intervention, depending on the degree of human participation and the difficulty of controlling key nodes.



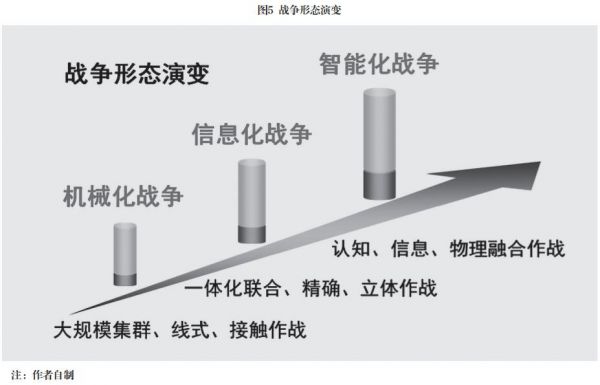
4. Decision-making advantage. The battlefield environment in the future is becoming increasingly complex, and the two sides of the war are competing in fierce games and confrontations. Therefore, with the rapidly changing environment and threats, it is too late to rely on people to participate in decision-making in a high-intensity confrontation environment, and the quality of decision-making is unreliable. Therefore, only by letting the collaborative group perform automatic environmental adaptation, automatic target and threat identification, autonomous decision-making and collaborative actions, can we quickly attack the opponent or implement effective defense and gain battlefield advantage and initiative.

Collaborative groups have brought new challenges to command and control. How to implement command and control of clusters is a new strategic issue. Control can be implemented by level and task, roughly including centralized control mode, hierarchical control mode, consistent collaborative mode, and spontaneous collaborative mode. [1] Various forms can be adopted to achieve human control and participation. Generally speaking, the smaller the tactical level of the action, the more autonomous action and human intervention are required; at the level of organized troop operations, since it involves the control of multiple combat groups, centralized planning and hierarchical control are required, and human participation is limited; at the higher strategic and campaign levels, clusters are only used as a platform weapon and combat style, requiring unified planning and layout, and the degree of human participation will be higher. From the nature of the task, the operation and use of strategic weapons, such as nuclear counterattacks, requires human operation and is not suitable for autonomous processing by weapon systems; when executing the attack and defense of important targets and high-value targets, such as decapitation operations, human participation and control are also required throughout the process, while giving full play to the autonomous functions of the weapon system; for the attack on tactical targets, if combat operations involving lethal strikes and destruction missions are required, limited human participation can be allowed, or after human confirmation, the coordinated group can be allowed to execute automatically; when performing non-strike tasks such as reconnaissance, surveillance, target identification, and investigation, or performing tasks such as air defense and anti-missile defense that are short in time and difficult for humans to participate, they are mainly handed over to the coordinated group to execute automatically, and humans do not need to participate and cannot participate. In addition, cluster warfare should also pay attention to the study of its countermeasures. Focus on the study of countermeasures such as electronic deception, electromagnetic interference, network attacks, high-power microwave weapons, electromagnetic pulse bombs, and artillery systems, whose related functions and effects are relatively obvious. At the same time, it is also necessary to study countermeasures such as laser weapons and swarms against swarms, and gradually establish a "firewall" that humans can effectively control to deal with the coordinated group.

Virtual and real end. Virtual and real end mainly refers to various terminals connected to "cloud and network", including various sensors, command and control platforms, weapon platforms, support platforms, related equipment and facilities, and combat personnel pre-installed with intelligent modules. In the future, various equipment and platforms will be cyber-physical systems CPS and human-computer interaction systems with diverse front-end functions, back-end cloud support, virtual-real interaction, and online and offline integration. In terms of simple environmental perception, path planning, platform mobility, weapon operation, etc., it mainly relies on front-end intelligence such as bionic intelligence and machine intelligence to achieve. Complex battlefield target identification, combat mission planning, networked coordinated strikes, combat situation analysis, advanced human-computer interaction, etc., need to rely on back-end cloud platforms and cloud AI to provide information data and algorithm support. The front-end intelligence of each equipment platform and the back-end cloud intelligence should be combined for overall planning and design to form a comprehensive advantage of front-end and back-end integrated intelligence. At the same time, virtual soldiers, virtual staff, virtual commanders and their intelligent interaction and efficient interaction with humans are also the focus and difficulty of future research and development.

**The qualitative change of war**

Since modern times, human society has mainly experienced large-scale mechanized wars and smaller-scale information-based local wars. The two world wars in the first half of the 20th century were typical mechanized wars. The Gulf War, Kosovo War, Afghanistan War, Iraq War and Syria War since the 1990s have fully demonstrated the form and characteristics of information warfare. In the new century and new stage, with the rapid development and widespread application of intelligent technology, the era of intelligent warfare with data and computing, models and algorithms as the main features is about to come (see Figure 5).



Mechanization is a product of the industrial age. It focuses on mechanical power and electrical technology. Weapons and equipment are mainly tanks, armored vehicles, artillery, aircraft, ships, etc., which correspond to mechanized warfare. Mechanized warfare is mainly based on classical physics represented by Newton's laws and socialized mass production. It is mainly based on large-scale cluster, linear, and contact operations. Tactically, it usually requires on-site reconnaissance, terrain survey, understanding of the opponent's frontier and deep deployment, and making up one's mind based on one's own capabilities, implementing offense or defense, and carrying out task division, combat coordination and support. It has obvious characteristics such as hierarchical command and control and serialization of time and space.

Informatization is a product of the information age. Technically, it focuses on information technology such as computers and network communications. The equipment forms are mainly radars, radio stations, satellites, missiles, computers, military software, command and control systems, network and electronic attack and defense systems, and integrated electronic information systems, which correspond to the form of informationized warfare. Informationized warfare is mainly based on the three laws of computers and networks (Moore's Law, Gilder's Law, and Metcalfe's Law), focusing on integrated joint, precise, and three-dimensional operations, establishing a "seamless and fast information link from sensor to shooter", seizing information control, and realizing the enemy's first discovery and attack. In terms of tactics, it is necessary to identify and catalog the battlefield and targets in detail, highlight the role of networked perception and command and control systems, and put forward new requirements for information functions such as platform interconnection. Due to the development of global information systems and diversified network communications, informationized warfare has diluted the boundaries between the front and rear, emphasizing the horizontal integration of "detection, control, attack, assessment, and protection" and the integration and flattening of strategy, campaign, and tactics.

Intelligence is a product of the knowledge economy era. Technically, it focuses on intelligent technologies such as artificial intelligence, big data, cloud computing, cognitive communication, the Internet of Things, biological intersection, hybrid enhancement, swarm intelligence, autonomous navigation and collaboration. The equipment forms are mainly manifested in unmanned platforms, intelligent ammunition, cluster systems, intelligent perception and database systems, adaptive mission planning and decision-making systems, combat simulation and parallel training systems, military cloud platforms and service systems, public opinion warning and guidance systems, smart wearable systems, etc., which correspond to the form of intelligent warfare.

Intelligent warfare is mainly based on the battlefield ecosystem of bionics, brain-like principles and AI. It is based on "energy mobility and information interconnection", supported by "network communication and distributed cloud", centered on "data calculation and model algorithm", and centered on "cognitive confrontation". It is a new combat form that integrates multiple domains, cross-domain offense and defense, is unmanned and clustered, and integrates the interaction of virtual and physical spaces.

Intelligent warfare aims to meet the needs of nuclear and conventional deterrence, joint operations, all-domain operations, and non-war military operations. It focuses on multi-domain integrated operations such as cognition, information, physics, society, and biology. It presents characteristics such as distributed deployment, networked links, flat structure, modular combination, adaptive reconstruction, parallel interaction, focused energy release, and nonlinear effects. The winning mechanism subverts the tradition, the organizational form undergoes qualitative changes, the combat efficiency is unprecedentedly improved, and the combat power generation mechanism has changed. Its substantial changes are mainly reflected in the following ten aspects.

AI-led winning mechanism. Under intelligent conditions, new combat elements represented by "AI, cloud, network, group, and terminal" will reconstruct the battlefield ecosystem, and the winning mechanism of war will be completely changed. Among them, the AI ​​system based on models and algorithms is the core combat capability, which runs through all aspects and links, and plays a multiplying, transcending and active role. The platform is controlled by AI, the cluster is guided by AI, and the system is decided by AI. The traditional human-based tactics are replaced by AI models and algorithms. Algorithmic warfare will play a decisive role in war. The combat system and process will eventually be dominated by AI, and the power of intelligence will become the core power of future wars.

In different eras and different war forms, the battlefield ecosystem is different, and the composition of combat elements and the winning mechanism are completely different. Mechanized warfare is a platform-centric warfare, with the core being "movement", the dominant forces being firepower and mobility, and the pursuit of carrying energy with objects and releasing energy with objects. The combat elements mainly include: people + mechanized equipment + tactics. The winning mechanism is based on the people-led decision-making of the combat use of mechanized equipment, winning with more, defeating with less, defeating with the big, defeating with the fast, and comprehensive, efficient, and sustainable mobilization capabilities, which play a decisive or important role respectively. Informationized warfare is a network-centric warfare, with the core being "connection", the dominant force being information power, and the pursuit of gathering energy with the network and releasing energy with the network. The combat elements and their interrelationships are mainly: "people + informationized equipment + tactics" based on network information. Information runs through people, equipment, and tactics, establishing a seamless information connection "from sensor to shooter", realizing systematic networked combat capabilities, using the system to defeat the local, the network to defeat the discrete, and the fast to defeat the slow, which has become an important mechanism for winning the war. Among them, information has played a multiplying role in equipment and combat systems, but the platform is still dominated by people. Information plays a role in assisting decision-making around people, but most decisions are still dominated by people. Intelligent warfare is cognitive-centered warfare, the core is "calculation", the dominant force is intelligence, and the weight of intelligence will exceed firepower, mobility and information power. The pursuit will be to control energy with intelligence, control energy with intelligence, control reality with virtuality, and win the battle with the weak. The more AI and smarter AI of the two combat parties, the greater the initiative on the battlefield. The combat elements and their mutual relationships are mainly: AI×(cloud+network+group+people+equipment+tactics), which can be simplified into an interconnected and integrated battlefield ecosystem composed of "AI, cloud, network, group, terminal" elements. In the future, the role of AI in war will become larger and stronger, and will eventually play a decisive and dominant role.

Emphasizing the leading role of AI does not deny the role of humans in war. On the one hand, human intelligence has been put in front and endowed to AI; on the other hand, AI cannot replace humans in the pre-war, backstage and strategic levels for quite a long time and in the foreseeable future.

The battlefield environment of modern warfare is becoming more and more complex, and the speed of combat confrontation is getting faster and faster. How to quickly identify and process massive amounts of information, quickly respond to battlefield situations, and quickly formulate decision-making plans is far beyond human capabilities and exceeds the limits of existing technical means (see Table 1 and Table 2). As AI is increasingly used in the war system and plays an increasingly important role, the combat process will be reshaped, the military kill chain will be accelerated and efficient, and fast perception, decision-making, action, and support will become important factors for winning future intelligent wars.





In the future, through intelligent recognition and pattern recognition of images, videos, electromagnetic spectrum, voice, etc., it will be possible to quickly and accurately identify targets for complex battlefield information of sky, land and sea sensor networks. By using big data technology, through multi-source and multi-dimensional directional search and intelligent correlation analysis, it is not only possible to accurately locate various strike targets, but also to accurately model human behavior, social activities, military operations and public opinion, and gradually improve the accuracy of early warning prediction. Based on accurate battlefield information, each theater and battlefield can adaptively implement task planning, autonomous decision-making and combat process control through a large number of parallel modeling and simulation training in virtual space in advance. The AI ​​of each combat platform and cluster system can autonomously and collaboratively perform tasks around combat objectives according to task planning, and can make active adjustments to changes that occur at any time. By establishing a distributed, networked, intelligent, and multi-mode support system and preset layout in advance, it is possible to quickly implement accurate logistics distribution, material supply, and intelligent maintenance. In short, through the extensive application of intelligent technology and the active role and evolutionary functions of various AI systems, the "simple, fast, efficient and controllable" combat process reengineering can be achieved in the entire combat process of planning, prediction, perception, decision-making, implementation, control and guarantee, which can gradually free humans from the heavy combat affairs. The reengineering of combat processes will accelerate the pace of future battlefields, compress time and shorten the process.

The winning mechanism dominated by AI is mainly manifested in combat capabilities, means, strategies and measures. It fully integrates human intelligence, approaches human intelligence, exceeds human limits, gives play to the advantages of machines, and embodies advancement, subversion and innovation. This advancement and innovation is not a simple extension and growth of previous wars, but a qualitative change and leap, a high-level feature. This high-level feature is reflected in the fact that intelligent warfare has "brain-like" functions that traditional warfare does not have and "capabilities that exceed human limits" in many aspects. With the continuous optimization and iteration of AI, it will one day surpass ordinary soldiers, staff officers, commanders and even elite and expert groups to become a "super brain" and "super brain group". This is the core and key of intelligent warfare, a technological revolution in the fields of epistemology and methodology, and a high-level combat capability that humans can currently foresee, realize and evolve.

The role of virtual space is rising. With the progress of the times and the development of science and technology, the combat space has gradually expanded from physical space to virtual space. The status and role of virtual space in the combat system have gradually increased and become more and more important, and have been deeply integrated and integrated with physical space and other fields. Virtual space is an information space based on network electromagnetics constructed by humans. It can reflect human society and the material world from multiple perspectives, and at the same time, it can be used beyond many limitations of the objective world. It is constructed by the information domain, connected by the physical domain, reflected by the social domain, and used by the cognitive domain. In a narrow sense, virtual space mainly refers to the civilian Internet, while in a broad sense, virtual space mainly refers to cyberspace, including virtual space composed of various Internet of Things, military networks and special networks. Cyberspace has the characteristics of being easy to attack and difficult to defend, using soft to fight hard, integrating peace and war, and being difficult to distinguish between the military and the civilians. It has become an important battlefield for military operations, strategic deterrence and cognitive confrontation.

The importance of virtual space is mainly reflected in three aspects: first, through the network information system, the scattered combat forces and combat elements are connected into a whole, forming a systematic networked combat capability, which becomes the foundation of information warfare; second, it becomes the main battlefield and basic support for cognitive confrontations such as network, intelligence, public opinion, psychology, and consciousness; third, it establishes a virtual battlefield, conducts combat experiments, realizes the interaction between the virtual and the real, and forms the core and key of parallel combat and the ability to control the real with the virtual.

In the future, with the accelerated upgrading of global interconnection and the Internet of Things, and with the establishment, improvement and widespread application of space-based networked reconnaissance, communications, navigation, mobile Internet, Wi-Fi and high-precision global space-time reference platforms, digital maps, industry big data and other systems, human society and global military activities will become increasingly "transparent", increasingly networked, perceived, analyzed, associated and controlled (see Figure 6), which will have a profound all-round and ubiquitous impact on military construction and operations. The combat system in the intelligent era will gradually expand from closed to open, from military-dominated to "open source and ubiquitous" direction of military-civilian integration.



In the era of intelligence, information data in the fields of physics, information, cognition, society, biology, etc. will gradually flow freely, combat elements will be deeply interconnected and connected, and various combat systems will develop from the primary "capability combination" to the advanced "information fusion, data cross-linking, integrated behavior interaction", with strong full-domain perception, multi-domain fusion, and cross-domain combat capabilities, and the ability to effectively control important targets, sensitive people, and critical infrastructure anytime and anywhere. A report from the U.S. Army Joint Arms Center believes that the world is entering an era of "global surveillance everywhere". Even if the world cannot track all activities, the spread of technology will undoubtedly increase potential sources of information exponentially.

At present, network-based software attacks have the ability to physically damage, and network attacks by militarily developed countries have the ability to invade, deceive, interfere, and destroy. Cyberspace has become another important battlefield for implementing military operations and strategic deterrence. The US's cyber attacks have been used in actual combat. Ben Ali of Tunisia, Gaddafi of Libya, and Saddam of Iraq have all been affected by the US's cyber attacks and WikiLeaks, causing public opinion to shift, psychological loss of control, social unrest, and the rapid collapse of the regime, which has had a subversive impact on the traditional form of warfare. Through the Snowden incident, the list of 49 "cyberspace" reconnaissance projects in 11 categories used by the United States has been exposed one after another. The "Stuxnet" virus destroyed Iran's nuclear facilities, the "Gauss" virus invaded relevant countries in the Middle East in groups, and the "Cuban Twitter" controlled public opinion. These events show that the United States has strong monitoring capabilities, soft and hard attacks, and psychological warfare capabilities for the Internet, closed networks, and mobile wireless networks.

Wars start with virtual space experiments. The U.S. military began exploring combat simulation, combat experiments and simulated training in the 1980s. Later, the U.S. military took the lead in using technologies such as virtual reality, war games, and digital twins in virtual battlefields and combat experiments. According to analysis, the U.S. military has conducted combat simulations in military operations such as the Gulf War, the Kosovo War, the Afghanistan War, and the Iraq War, trying to find the best combat and action plans. It is reported that before Russia sent troops to Syria, it conducted combat rehearsals in the war laboratory. Based on the experimental simulations, it formulated the "Central-2015" strategic exercise plan, and practiced "mobility and accessibility in unfamiliar areas" for the Syrian operations. After the exercise, Russian Chief of General Staff Gerasimov emphasized that the political, economic and public opinion psychological warfare should be mainly used, supplemented by long-range precision air strikes, special operations and other measures to ultimately achieve political and strategic goals. Practice has shown that the process of Russia's sending troops to Syria is basically consistent with experiments and exercises.

In the future, with the application and development of virtual simulation, mixed reality, big data, and intelligent software, by establishing a parallel military artificial system, the physical forces in the physical space and the virtual forces in the virtual space can be mapped and iterated with each other, which can solve the fast, high-intensity confrontation training and over-computing that are difficult to achieve in the physical space in the virtual space, and can confront and compete with the highly simulated "blue army system", continuously accumulate data, establish models and algorithms, so as to use the optimal solution to guide the construction and combat of physical forces, and achieve the purpose of virtual-real interaction, virtual-real, and virtual-victory. On January 25, 2019, Google's artificial intelligence team DeepMind and StarCraft developer Blizzard announced the results of the December 2018 match between AlphaSTAR and professional players TLO and MANA. In the end, in the best-of-five match, AlphaSTAR won 5:0. AlphaSTAR completed the training volume that human players need 200 years in just two weeks, demonstrating the great advantages and bright prospects of simulated confrontation training in virtual space.

Unmanned combat style. In the era of intelligence, unmanned combat will become the basic form, and the integrated development of artificial intelligence and related technologies will gradually push this form to an advanced stage. Unmanned systems are the full pre-placement of human wisdom in the combat system, and are the concentrated embodiment of the integrated development of intelligence, informatization, and mechanization. Unmanned equipment first appeared in the field of drones. In 1917, Britain built the world's first drone, but it was not used in actual combat. With the development of technology, drones are gradually used in target drones, reconnaissance, and integrated reconnaissance and attack. Since the beginning of the 21st century, unmanned technology and equipment have made great strides in exploration and application due to their advantages such as mission-centered design, no need to consider crew needs, and high combat cost-effectiveness. They have achieved major breakthroughs and shown a trend of rapid and all-round development. The scope of application has expanded rapidly, covering various fields such as air, surface, underwater, ground, and space.

In recent years, technologies such as artificial intelligence, bionic intelligence, human-machine fusion intelligence, and swarm intelligence have developed rapidly. With the help of satellite communication and navigation, and autonomous navigation, unmanned combat platforms can well achieve remote control, formation flight, and cluster coordination. At present, unmanned combat aircraft, underwater unmanned platforms, and space unmanned autonomous operation robots have been launched one after another. Bipedal, quadrupedal, multi-legged, and cloud-based intelligent robots are accelerating their development and have entered the fast lane of engineering and practical application. Military applications are not far away.

In general, unmanned warfare in the intelligent era will enter three stages of development. The first stage is the primary stage with humans as the main force and unmanned as the auxiliary force. Its main feature is "unmanned warfare under human control", that is, combat behavior is completely controlled and dominated by humans before, during, and after the event. The second stage is the intermediate stage with humans as the auxiliary force and unmanned as the main force. Its main feature is "unmanned warfare under limited control", that is, human control is limited, auxiliary but critical throughout the combat process, and most cases can rely on the platform's autonomous action capabilities. The third stage is the advanced stage with humans in the rules and unmanned actions. Its main feature is "unmanned warfare with human design and very little control". Humans make an overall design in advance, clarify the autonomous behavior and game rules under various combat environment conditions, and the action implementation stage is mainly handed over to unmanned platforms and unmanned troops for autonomous execution.

Autonomous behavior or autonomy is the essence of unmanned combat. It is a common and prominent feature of intelligent warfare and is reflected in many aspects.

The first is the autonomy of combat platforms, which mainly includes the autonomous capabilities and intelligence levels of drones, ground unmanned platforms, precision-guided weapons, underwater and space robots.

The second is the autonomy of the detection system, which mainly includes automatic search, tracking, association, aiming and intelligent recognition of information such as images, voice, video, and electronic signals.

The third is autonomous decision-making, the core of which is AI-based autonomous decision-making in the combat system, mainly including automatic analysis of battlefield situation, automatic planning of combat tasks, automated command and control, and human-computer intelligent interaction.

Fourth, the autonomous coordination of combat operations, which in the early stage includes the autonomous coordination of manned and unmanned systems, and in the later stage includes unmanned autonomous clusters, such as various combat formation clusters, bee swarms, ant colonies, fish schools and other combat behaviors.

The fifth is the autonomous behavior of network attack and defense, including automatic identification, automatic tracing, automatic protection, and autonomous counterattack of various viruses and network attack behaviors.

Sixth, cognitive electronic warfare, automatic identification of the power, frequency band, direction, etc. of electronic interference, automatic frequency hopping and autonomous networking, as well as active and automatic electronic interference against opponents.

Seven is other autonomous behaviors, including intelligent diagnosis, automatic repair, self-protection, etc.

In the future, with the continuous upgrading of the integration and development of artificial intelligence and related technologies, unmanned operations will rapidly develop in the direction of autonomy, bionics, clusters, and distributed collaboration, gradually pushing unmanned operations to an advanced stage, and significantly reducing direct confrontations between living forces on the battlefield. Although manned platforms will always exist in the future, bionic robots, humanoid robots, swarm weapons, robot troops, and unmanned system operations will become the norm in the era of intelligence. Since unmanned systems can be used to replace them in many combat fields and can be completed through autonomous behavior, humans must have unmanned combat systems to escort them before they are physically attacked and injured. Therefore, the unmanned combat system in the era of intelligence is the main protective barrier for humans, and it is amulet and shield for humans.

All-domain operations and cross-domain attack and defense. In the era of intelligence, all-domain operations and cross-domain attack and defense are also a basic combat style, which is reflected in many combat scenarios and many aspects. From land, sea, air, and space to multiple fields such as physics, information, cognition, society, and biology, as well as the integration and interaction of virtual and physical entities, from strategic deterrence in peacetime to high confrontation, high dynamics, and high response in wartime, the time and space span is very large. It not only faces cognitive confrontations such as physical space operations and virtual space network attack and defense, information confrontation, public opinion guidance, and psychological warfare, but also faces tasks such as global security governance, regional security cooperation, counterterrorism, and rescue, and faces the management and control of key infrastructure such as networks, communications, electricity, transportation, finance, and logistics.

Since 2010, supported by the achievements of information and intelligent technology, the US military has proposed concepts such as combat cloud, distributed lethality, multi-domain warfare, algorithmic warfare, mosaic warfare, and joint full-domain warfare, with the aim of maintaining battlefield and military advantages by using systems to defeat local forces, multiple capabilities to defeat simple capabilities, multiple domains to defeat single domains, integration to defeat discrete forces, and intelligence to defeat non-intelligence. The US military proposed multi-domain warfare in 2016 and the concept of joint full-domain warfare in 2020, with the aim of developing cross-service and cross-domain joint combat capabilities, achieving the support of the three services behind the operations of a single service, and having full-domain capabilities to defeat multiple domains and single domains.

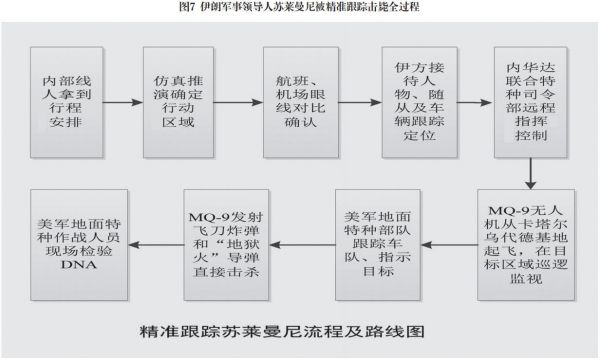
In the future, with the cross-integration of artificial intelligence and multiple disciplines, and breakthroughs in key cross-media attack and defense technology groups, multi-domain integration and cross-domain attack and defense based on AI and human-machine hybrid intelligence between functional domains such as physics, information, cognition, society, and biology, and between geographical domains such as land, sea, air, and space will become a distinctive feature of intelligent warfare.

In the intelligent era, multi-domain and cross-domain operations will expand from mission planning, physical jointness, and loose coordination to heterogeneous integration, data cross-linking, tactical inter-control, and cross-domain offensive and defensive integration.

First, multi-domain integration. According to different battlefields and opponents in a multi-domain environment, different combat styles, combat processes and tasks are planned in accordance with the requirements of joint operations, and they are unified as much as possible to achieve the coordination and integration of information, firepower, defense, support and command, and to achieve the integration of combat capabilities at strategic, campaign and tactical levels, forming the ability to fight in one domain and provide rapid joint support in multiple domains.

The second is cross-domain attack and defense. With the support of a unified network information system, through a unified battlefield situation and data information exchange based on unified standards, we can completely open up the cross-domain joint combat reconnaissance, control and attack evaluation information link, and achieve coordinated actions between services at the tactical and fire control levels, cross-domain command and interoperability, and seamless connection of combat elements and capabilities.

The third is full-process linkage. Take multi-domain integration and cross-domain attack and defense as a whole, coordinate the design, and link the whole process. Before the war, carry out intelligence collection and analysis, implement public opinion warfare, psychological warfare, propaganda warfare, and necessary network and electronic attacks. During the war, through special operations and cross-domain operations, implement decapitation, key point attacks, and precise and controllable strikes (see Figure 7). After the war, defend against information system network attacks, eliminate the impact of negative public opinion on the public, prevent infrastructure from being destroyed by the enemy, and implement post-war governance, public opinion control, and social order restoration in multiple fields.



Fourth, AI support. Through combat experiments, simulation training, necessary test verification, and actual combat testing, we will continuously accumulate data, optimize models, establish AI combat models and algorithms for different combat styles and opponents, and form an intelligent brain system to better support joint operations, multi-domain operations, and cross-domain offense and defense.

Human-AI hybrid decision-making. The continuous improvement, optimization, upgrading and perfection of the AI ​​brain system on the intelligent battlefield will enable it to surpass humans in many aspects. For thousands of years, the command, control and decision-making mode of human warfare, which has been dominated by humans, will be completely changed. Humans commanding AI, AI commanding humans, AI commanding AI, etc., may all appear in wars.

Distributed, networked, flat, and parallel are important features of intelligent combat systems. The centralized, human-dominated single decision-making model is gradually being changed by unmanned, autonomous clusters, manned-unmanned collaboration and other decentralized and weakly centralized models based on AI. Mixed compatibility has become a development trend. The lower the combat level and the simpler the task, the more prominent the role of unmanned and decentralized operations; the higher the level and the more complex the task, the more important the role of human decision-making and centralized operations. Before the war, human decision-making was the main method, supplemented by AI decision-making; during the war, AI decision-making was the main method, supplemented by human decision-making; after the war, both methods were used, with mixed decision-making being the main method (see Table 3).



In the future battlefield, the combat confrontation situation is highly complex, ever-changing, and extremely fierce. The intersection of multiple information forms massive data, which is difficult to process quickly and accurately by the human brain alone. Only by realizing the collaborative operation mode of "human brain + AI" and based on combat cloud, database, network communication, Internet of Things and other technical groups, can "commanders" cope with the ever-changing battlefield and complete command and control tasks. With the increase of the autonomous capabilities of unmanned systems and the enhancement of the AI ​​functions of clusters and systems, autonomous decision-making is gradually emerging. Once command and control achieve different degrees of intelligence, the reconnaissance-judgment-decision-attack (OODA) loop time will be greatly compressed and the efficiency will be significantly improved. In particular, pattern recognition for network sensor image processing, "optimization" algorithm for combat decision-making, particle swarm algorithm and bee colony algorithm for autonomous clusters, etc., will give the command and control system more advanced and complete decision-making capabilities, and gradually realize the "man out of the loop" combat cycle.

Nonlinear amplification and rapid convergence. Future intelligent warfare will no longer be the gradual release of energy and the linear superposition of combat effects, but the rapid amplification of multiple effects such as nonlinearity, emergence, self-growth, and self-focusing, and the rapid convergence of results.

Emergence mainly refers to the process in which each individual in a complex system follows local rules and continuously interacts, producing an overall qualitative change effect in a self-organizing manner. In the future, although battlefield information is complex and changeable, it will have the ability to "collect at one point and share with everyone" after being processed by intelligent recognition of images, voices, videos, etc. and military cloud systems. It will quickly associate with relevant information through big data technology and quickly link with various weapon fire control systems to implement distributed strikes, cluster strikes, and network psychological warfare, etc., and can achieve "discover and destroy", "attack in groups as soon as there is a situation", and "quantity advantage breeds psychological panic effect". These phenomena are the emergence effect.

The emergent effects of intelligent warfare are mainly reflected in three aspects: first, the acceleration of the kill chain caused by the rapidity of the AI ​​decision-making chain; second, the combat effect caused by the numerical advantage of manned and unmanned collaborative special swarm systems; third, the rapid group emergence behavior generated by network interconnection.

When military intelligence develops to a certain stage, under the joint action of advanced AI, quantum computing, IPV6, hypersonic technology, etc., the combat system will have nonlinear, asymmetric, self-growing, rapid confrontation, uncontrollable amplification effects and action effects, especially in unmanned, cluster, network public opinion, cognitive confrontation and other aspects. The group of fools will be wise, quantity will increase efficiency, nonlinear amplification, and emergence effects will become more and more prominent. The cognitive, information, and energy confrontations dominated by AI are intertwined and quickly focused around the target. Time is increasingly compressed and the confrontation speed is getting faster and faster, showing a sharp amplification of multiple effects and rapid convergence of results. Energy shock waves, confrontation speed wars, AI terminators, public opinion reversals, social unrest, psychological loss of control, and the chain effect of the Internet of Things will become the prominent characteristics of intelligent warfare.

In unmanned cluster attacks, when the platform performance of both sides is roughly the same, the Lanchester equation is followed, and the combat effectiveness is proportional to the square of the number, and the quantitative advantage is the qualitative advantage. Network attack and defense and psychological public opinion effects follow Metcalfe's law and are proportional to the square of the number of information interconnected users. The nonlinear and emergent effects are more obvious. The number of battlefield AIs and their IQs determine the overall level of intelligence of the combat system, which is related to the control of battlefield intellectual power and affects the outcome of the war. In the era of intelligence, how to deal with the relationship between energy, information, cognition, quantity, quality, virtuality, and entities, and how to cleverly design, control, use, and evaluate nonlinear effects are major new challenges and new requirements facing future wars.

In the future, whether it is public opinion reversal, psychological panic, swarm attacks, cluster actions, or autonomous combat by humans outside the loop, their emergence effects and strike effects will become relatively common phenomena and easy-to-implement actions, forming a capability that is compatible with deterrence and actual combat. It is also an act of war that human society must strictly manage and control.

An organically symbiotic relationship between people and equipment. In the era of intelligence, the relationship between people and weapons will undergo a fundamental change, becoming increasingly distant physically and increasingly close in thought. The equipment form and development management model will be completely changed, with people's thoughts and wisdom deeply linked to weapons and equipment through AI, fully advanced in the equipment development stage, optimized and iterated in the use and training stage, and further upgraded and improved after combat verification, and so on, in a repetitive and progressive manner.

First, with the rapid development of technologies such as network communications, mobile Internet, cloud computing, big data, machine learning and bionics and their widespread application in the military field, the structure and form of traditional weapons and equipment will be completely changed, presenting diversified functions such as front-end and back-end division of labor and collaboration, efficient interaction, and adaptive adjustment. It is a complex integrating machinery, information, network, data, and cognition.

Second, people and weapons are gradually separated physically, but they are gradually deeply integrated into an organic symbiosis in terms of thinking. As drones and robots gradually mature, they will shift from assisting people in combat to replacing people in combat, and people will retreat to the background. The combination of people and weapons will appear in a brand-new form. People's thoughts and wisdom will participate in the design, research and development, production, training, use and support processes throughout the life cycle. Unmanned combat systems will perfectly combine people's creativity and thinking with the accuracy, speed, reliability and fatigue resistance of machines.

Third, the equipment construction and management model has undergone profound changes. Mechanized equipment is getting older and older, information-based software is getting newer, and intelligent algorithms are getting more refined. Traditional mechanized equipment is delivered to troops in the mode of "pre-research-development-finalization", and its combat performance has been declining over time and motor hours; information-based equipment is the product of the compound development of mechanization and informatization. The platform remains unchanged, but the information system is constantly updated with the development of computer CPUs and storage devices, showing the step-by-step development characteristics of "information-led, soft-driven, fast replacement, and spiral rise"; intelligent equipment is based on mechanization and informatization. With the accumulation of data and experience, it continuously optimizes and improves training models and algorithms, showing an upward curve that becomes stronger and better with time and frequency of use. Therefore, the development and construction of intelligent equipment and the use of training and support models will undergo fundamental changes.

Evolution in learning and confrontation. Evolution must be a distinctive feature of future intelligent warfare and combat systems, and a commanding point in future strategic competition. The combat system in the intelligent era will gradually have the ability to adapt, self-learn, self-confront, self-repair, and self-evolve, becoming an evolvable ecological and game system.

The biggest feature and uniqueness of intelligent combat systems and systems lies in the combination of "human-like and human-like" intelligence and machine advantages to achieve "superhuman" combat capabilities. The core of this capability is that many models and algorithms become better and more refined with use, and have the function of evolution. If the future combat system is like the human body, the brain is the command and control center, the nervous system is the network, and the limbs are weapons and equipment controlled by the brain, just like a living organism, it has the ability to adapt, self-learn, self-confrontation, self-repair, and self-evolution. We believe that it has the ability and function of evolution. Since intelligent combat systems are not exactly the same as living organisms, a single intelligent system is similar to a living organism, but a multi-system combat system is more like an "ecosystem + confrontation game system", which is more complex than a single living organism, and more confrontational, social, collective, and emergent.

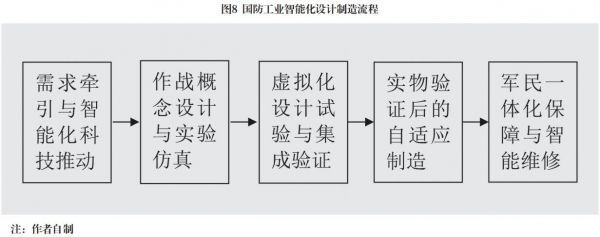
According to preliminary analysis and judgment, with the development and application of technologies such as combat simulation, virtual reality, digital twins, parallel training, intelligent software, brain-like chips, brain-like systems, bionic systems, natural energy collection and new machine learning, the future combat system can gradually evolve from a single function and partial system to a multi-function, multi-factor, multi-domain and multi-system evolution. Each system can quickly form a response strategy and take action according to the changes in the battlefield environment, the different threats faced, the different opponents faced, and its own strengths and capabilities, based on the accumulated experience and knowledge, a large number of simulation adversarial training and the model algorithm established by enhanced learning, and then continuously revise, optimize, improve and evolve itself in the practice of war. Single-task systems will have characteristics and functions similar to those of living organisms, and multi-task systems will have a cyclical function and evolutionary mechanism of mutual growth and mutual restraint, survival of the fittest, like species groups in the forest, and have the ability to compete and compete in complex environmental conditions, forming an evolvable ecological and game system.

The evolution of the combat system is mainly reflected in four aspects: First, the evolution of AI. With the accumulation of data and experience, it will be continuously optimized, upgraded and improved. This is relatively easy to understand. Second, the evolution of combat platforms and cluster systems, mainly from manned control to semi-autonomous and autonomous control. Since it not only involves the evolution of platform and cluster control AI, but also involves the optimization and improvement of related mechanical and information systems, it is relatively complicated. Third, the evolution of task systems. For example, the evolution of detection systems, strike systems, defense systems, and support systems, etc., because they involve multiple platforms and multiple tasks, the factors and elements involved in the evolution are much more complicated. Some may evolve quickly, and some may evolve slowly. Fourth, the evolution of the combat system, because it involves all elements, multiple tasks, cross-domains, and confrontations at all levels, its evolution process is very complicated. Whether the combat system can evolve cannot rely entirely on self-growth, but requires the active design of some environments and conditions, and needs to follow the principles of bionics, survival of the fittest, mutual promotion and mutual restraint, and full system and life cycle management to have the function and ability of continuous evolution.

Intelligent design and manufacturing. In the era of intelligence, the defense industry will transform from a relatively closed, physical-based, and long-cycle research and manufacturing model to an open source, intelligent design and manufacturing model that can quickly meet military needs.

The defense industry is a national strategic industry and a strong pillar of national security and national defense construction. It mainly provides the military with advanced, high-quality and reasonably priced weapons and equipment in peacetime. In wartime, it is an important force for implementing combat support and the core support for ensuring victory. The defense industry is a high-tech intensive industry. The research and development and manufacturing of modern weapons and equipment are technology-intensive, knowledge-intensive, system-complex and highly comprehensive. The research and development of large aircraft carriers, fighter jets, ballistic missiles, satellite systems, main battle tanks and other weapons and equipment generally takes ten, twenty years or even longer to be finalized and delivered to the troops. It requires large investment, long cycle and high cost. From the end of World War II to the end of the last century, the defense industry system and capability structure were the product of the mechanized era and war. Its scientific research, testing, production and manufacturing, and support focused on the needs of military services and the organization of scientific research and production in the industry system, mainly including weapons, ships, aviation, aerospace, nuclear and electronics industries, as well as civilian supporting and basic support industries. After the Cold War, the US defense industry has undergone strategic adjustments and mergers and reorganizations, and has generally formed a defense industry structure and layout that is compatible with the requirements of the information warfare system. The top six military giants in the United States can provide combat platforms and systems in professional fields for relevant military services, as well as overall solutions for joint operations. They are system integrators across military services and fields. Since the beginning of the 21st century, with the changes in the needs of systematic and informationized combat and the development of digital, networked, and intelligent manufacturing technologies, the development model of traditional weapons and equipment and scientific research and production capabilities have begun to change gradually, and they urgently need to be reshaped and adjusted in accordance with the requirements of informationized warfare, especially intelligent warfare.

In the future, the national defense science and technology industry will, in accordance with the requirements of joint operations, all-domain operations, mechanization, informationization and intelligentization, change from the traditional focus on military services and platform construction to cross-service and cross-domain system integration, and from relatively closed, self-contained, independent, fragmented, physical-based, and long-cycle research, design and manufacturing to open source, democratic crowdfunding, virtual design and integration verification, adaptive manufacturing, and rapid satisfaction of military needs (see Figure 8), and gradually form a new innovation system and intelligent manufacturing system that combines software and hardware, virtual and real interaction, intelligent interaction between man, machine, object and environment, effective connection of vertical industrial chain, horizontal distributed collaboration, and military-civilian integration. Joint demonstration and design by military and local parties, construction and use of joint research and development by both supply and demand parties, virtual and real iterative optimization based on parallel military systems, improvement and improvement through combat training and actual combat verification, and research, test, use and construction are the basic models for the development and construction of intelligent combat systems and the generation of combat effectiveness.



Wu Mingxi 8

Risk of losing control. Since intelligent combat systems theoretically have the ability to self-evolve and reach "superhuman" capabilities, if humans do not design control programs, control nodes, and "terminate buttons" in advance, the result is likely to bring destruction and disaster. What needs to be paid close attention to is that many hackers and "ill-intentioned" war maniacs will use intelligent technology to design uncontrollable war programs and combat methods, allowing many machine brain AIs and groups of robots to fight adaptively and self-evolvingly according to pre-set combat rules, invincible and moving forward, eventually leading to an uncontrollable situation and an unrecoverable endgame. This is a major challenge facing mankind in the process of intelligent warfare, and it is also a major issue that needs to be studied and resolved. It is necessary to recognize and attach importance to this issue from the perspective of a community with a shared future for all mankind and the sustainable development of human civilization, design war rules, formulate international conventions, regulate from technical, procedural, moral and legal perspectives, and implement mandatory constraints, inspections and management.

The mutations and leaps in the above ten aspects are the main contents of the new form of intelligent warfare. Of course, the development and maturity of intelligent warfare is not a castle in the air or a tree without roots, but is built on mechanization and informatization. Without mechanization and informatization, there is no intelligence. Mechanization, informatization, and intelligence are an organic whole, interconnected, mutually reinforcing, iteratively optimized, and leapfrog development. From the current perspective, mechanization is the foundation, informatization is the leading role, and intelligence is the direction. From the future perspective, mechanization is the foundation, informatization is the support, and intelligence is the leading role.

**A bright future**

In the space-time tunnel of the new century, we see that the train of intelligent warfare is running fast. Whether to allow human greed and the power of science and technology to move towards a more cruel darkness, or to move towards a more civilized and bright shore, this is a major philosophical proposition that mankind needs to think about. Intelligence is the future, but not everything. Intelligence can handle a variety of military tasks, but it is not omnipotent. Faced with sharp contradictions between civilizations, religions, countries, and classes, and extreme events such as thugs holding kitchen knives, suicide bombings, and mass riots, the role of intelligence is still limited. With global political imbalance, unequal rights, unfair trade, and unresolved social contradictions, wars and conflicts will be inevitable. The world ultimately depends on strength, and among them, scientific and technological strength, economic strength, and military strength are extremely important. Although military strength cannot determine politics, it can influence politics; it cannot determine the economy, but it can bring security to economic development. The stronger the intelligent combat capability, the stronger its function of deterring powerful enemies and curbing war, and the more hope there is for peace. Just like nuclear deterrence, it plays an important role in preventing large-scale wars to avoid terrible consequences and uncontrolled disasters.

The degree of intelligence of war, in a sense, reflects the progress of war civilization. The history of human war, from the initial struggle for food and living areas between ethnic groups to land occupation, resource plunder, expansion of political power, and domination of the spiritual world, is full of blood, violence and repression. As the ultimate means of resolving irreconcilable contradictions in human society, the ideal goal pursued by war is civilization: conquering the enemy without fighting, with the least resource investment, the least casualties, and the least damage to society... However, previous war practices often went against one's wishes due to political struggles, ethnic conflicts, competition for economic interests, and the cruelty of scientific and technological means of destruction, often destroying countries, cities and homes. Previous wars failed to achieve the above ideals, and in the future, intelligent wars will gradually give way to confrontations between robots and games between AIs, especially the confrontation of living forces will gradually give way to confrontations between robots and games between AIs. Casualties, material consumption, and collateral damage will become smaller and smaller. To a large extent, there is a possibility of achieving civilization, which brings hope to mankind. We expect that future wars will gradually transition from mutual slaughter in human society and great destruction of the material world to wars between unmanned systems and robots, and develop into deterrence and checks and balances limited to combat capabilities and comprehensive strength, confrontation between AI in the virtual world, and highly simulated war games... The consumption of human wars is limited to a certain scale of unmanned systems, simulated confrontations and simulation experiments, or even just the energy to play a war game. Humans have transformed from planners, designers, participants, leaders and victims of war to rational thinkers, organizers, controllers, bystanders and judges. Human bodies are no longer traumatized, spirits are no longer frightened, wealth is no longer destroyed, and homes are no longer destroyed. Although there may always be a gap between beautiful ideals and wishes and cruel reality, I sincerely hope that this day will come and come as soon as possible. This is the highest stage of the development of intelligent warfare, the author's greatest wish, and the beautiful vision of mankind!

(Thanks to my colleague Researcher Zhou Xumang for his support and help in writing the paper. He has unique ideas and insights in the development and construction of intelligence)

Notes

[1] Robert O. Walker et al., 20YY: War in the Age of Robots, translated by Zou Hui et al., Beijing: National Defense Industry Press, 2016, p. 148.

**The Era of Intelligent War Is Coming Rapidly**

**Wu Mingxi**

**Abstract:** Since the entry into the new century, the rapid development of intelligent technology with artificial intelligence (AI) at the core has accelerated the process of a new round of military revolution. The competition in the military field is going rapidly to the era of intelligent power. The operational elements represented by "AI, cloud, network, group and end" and their diverse combinations constitute a new battlefield ecosystem, and the winning mechanism of war has changed completely. multiplier, transcendence and active role. The platform has AI control, the cluster has AI guidance, and the system has AI decision-making. The traditional human-based combat method is replaced by AI models and algorithms, and intelligent dominance becomes the core of future war. The stronger the intelligent combat capability, the more hopeful the soldiers may win the war without firing a shot.