**Overview of Overseas Cognitive Warfare Combat Forces and Technical Equipment**

**Authors: Xiao Ning & Zeng Huasheng**

**Date: 2024-07-17**

Taking the United States, Russia and other countries as well as China's Taiwan region as research objects, this paper sorted out their combat forces and main technical equipment, and summarized the evolution process of their combat forces in the past 10 years.

**summary**

The Western world, led by the United States, has used cognitive warfare as the main means of ideological infiltration and color revolution in other countries, with the characteristics of diverse force composition, advanced technical means, and complete equipment spectrum. In order to better understand and master the overseas cognitive combat system, this paper takes the United States, Russia and other countries and Taiwan as the research objects, sorts out their combat forces and main technical equipment, summarizes the evolution process of their combat forces in the past 10 years, and provides reference for my country's active defense in the cognitive domain.

Contents:

1 The Evolution of Cognitive Warfare

2 Combat Force  
 2.1 United States  
 2.2 Russia  
 2.3 United Kingdom   
2.4 Taiwan, China   
  
3 Main technical equipment   
3.1 Situational Awareness Equipment   
3.2 Identification equipment   
3.3 Content Creation Equipment   
3.4 Guidance intervention equipment   
3.5 Simulation and evaluation equipment

4 Conclusion

As the old saying goes, "If you want to do your work well, you must first sharpen your tools." The trend of a war is not only closely related to the combat forces involved in the war, but also inseparable from the advancement of their weapons and equipment. Understanding the composition and functional changes of the opponent's combat forces can indirectly reflect the changing trends of the target country's combat form and war situation.

Since its birth, cognitive confrontation has undergone many rounds of evolution, from the earliest rumor spreading and leaflet delivery in physical space to the current video image forgery and synthesis, false news dissemination, and information cocoon construction in cyberspace, which fully reflects the major changes brought about by technologies such as machine learning and big data. After the popularization of the Internet, Western countries led by the United States gradually transformed cognitive operations from physical space to cyberspace. Due to the low cost, low price, and anti-tracing characteristics, in just a few decades, some Western countries have caused regime changes in many countries with only money without spending a single soldier. Therefore, understanding the composition of the target cognitive combat force, mastering its key technologies and main equipment systems, and comprehensively analyzing development trends will help my country actively prevent cognitive domain attacks.

1 The Evolution of Cognitive Warfare

German military theorist Clausewitz said, "The ultimate goal of war is to make the enemy submit to one's will. This submission ultimately comes from an extremely pessimistic understanding of the battlefield situation. Understanding not only fundamentally determines the outcome of the war, but also runs through the entire war."

Since the 1980s, with the rapid development of information technology, battlefield cognitive tools, cognitive objects, cognitive space, cognitive patterns, etc. have undergone revolutionary changes, and have shown new characteristics such as an increase in cognitive objects, a large number of cognitive raw materials, and increasingly complex cognitive activities. As the war process continues to accelerate, battlefield cognitive confrontation is becoming increasingly fierce, and the dependence on information-based cognitive tools is also becoming stronger. The cognitive function of "pre-practice" of war is highlighted, and advanced cognition has become a key link in battlefield cognition. Cognitive activities have broken through the scope of war guidance and become a special field of confrontation between the enemy and us.

From the perspective of propaganda concepts and strategies, Western countries, led by the United States, regard propaganda (called influence warfare by the U.S. military) as part of their information warfare, and organically combine cognitive domains with physical domains and cyber domains to conduct joint operations as information environments. In 2018, the U.S. military released the "Joint Concept of Operations in the Information Environment", proposing research on propaganda strategies and tactics, which covers both state actions and some non-governmental actions.

To sum up, the broad concept of cognitive warfare can be expressed as carrying out actions at the physical domain, information domain, and cognitive domain levels to influence cognitive factors such as the concepts, psychology, and will of the people in the target country or region, weaken the target's decision-making ability, and at the same time prevent it from performing the same behavior, protect one's own cognitive and decision-making capabilities, and conduct battlefield operations for this purpose.

Looking at the history of color revolutions in Western countries, whether it is the Orange Revolution and the Tulip Revolution that were nurtured and developed in traditional spaces in the past, or the Jasmine Revolution and the Libyan Civil War that used the Internet as a new medium for information dissemination, the West’s idea of ​​using hot events to guide the process of color revolutions has never changed.

The "Crimea Independence" event in 2014 is a classic example of winning a national political game by controlling hot events. Russia used its strong technical strength in cognitive information collection, intelligence analysis and prediction, and political election intervention to conduct comprehensive information, detailed analysis, and accurate prediction of Crimea's referendum on leaving Ukraine and joining Russia, and formulated a detailed action plan based on this decision. It promoted the common origin of Russia and Ukraine to build momentum in advance, released the recording of the phone call between the Ukrainian president and Putin before the referendum, and controlled the social platform Vkontakte after the referendum to cut off the Western media's voice channels and consolidate the victory. This series of well-planned and detailed operations realized the grand plan of "Crimea Independence".

During the 2019 Hong Kong Amendment Storm, Western anti-China forces provided the Hong Kong opposition and some radical forces with a series of tools based on artificial intelligence and big data, which were used to plan, organize and connect the protests through various unregulated Internet media, such as more than a dozen group management, chat and propaganda robots, enabling a small number of people to control the "cyber public opinion" environment of nearly one million groups, seriously endangering my country's national security.

In the 2022 "Russia-Ukraine conflict" incident, Western countries led by the United States have mastered the right to speak on mainstream social platforms. Governments, organizations, and individuals have made full use of social media such as Facebook, Twitter, Telegram, YouTube, and TikTok to spread various rumors, ban Russian accounts and speeches, prevent them from speaking out in international media, portray Russia as an aggressor, isolate it globally, and form an asymmetric cognitive game. Russia used evidence of the United States' development of biological and chemical weapons in Ukraine to successfully shift the focus of international public opinion. In addition, Russian and Ukrainian people have made full use of social media such as TikTok to upload a large number of real battlefield videos in real time, spontaneously acting as disseminators of war information, boosting their own morale and weakening the enemy's will.

It can be seen that cognitive warfare can be carried out intensively in wartime or subtly in peacetime; it involves social, military, political, economic, cultural and other fields, and can also be hidden in Twitter, Facebook, TikTok, Instagram, Weibo and other seemingly harmless videos, pictures, topics or emoticons to continuously infiltrate us. Through the empowerment of technology and the application of equipment, it can effectively mobilize the target's emotions, release extreme speech, create oppositional behavior, manipulate international public opinion, thereby interfering with government decision-making and affecting the direction of war.

**2 Combat Force**

**The United States, Russia, the United Kingdom and other countries, as well as China's Taiwan region, have established corresponding cognitive warfare command organizations and cognitive warfare forces, each with its own unique functions, and can effectively conduct joint operations with other services and arms.**

**2.1   
United States The U.S. military has the highest level of informatization among all the armies in the world. It has always regarded cognitive warfare as the core combat style in the information age, and its related team building is also at the forefront of the world. As early as 2006, the U.S. military completed the establishment of the network media warfare force. Its members not only have superb computer skills, but also have profound media propaganda skills; they can not only quickly respond to "unfavorable" reports, but also "hack" those "unfavorable" contents when necessary. Its purpose is to control the network propaganda channels and thus seize the commanding heights of cognitive warfare. In May 2010, the U.S. military established the Cyber ​​Warfare Command to integrate the cyber warfare command organizations scattered in the various arms of the U.S. military, and made the network media warfare force one of its important combat forces, which was upgraded to the 10th Joint Operations Command in 2018. Taking the U.S. Navy as an example, its network media warfare force occupies 3 of the 5 core comprehensive capabilities of information construction, namely electronic warfare, cyber warfare, psychological warfare, military fraud and operational security, which fully reflects its emphasis on cognitive warfare.**

2.2 Russia  
The Russian military has been committed to building a professional and complete information warfare force. In February 2013, the General Operations Directorate and the General Mobilization Directorate of the Russian General Staff began to establish the Cyberspace Command. Its main responsibility is to destroy the enemy's command system and create favorable social public opinion by invading the enemy's Internet, television, media, etc. In February 2017, the Russian military announced that it had established an information warfare force, whose main function is to protect private computer networks and military command and communication systems from cyber attacks. In addition, the information warfare force is also responsible for conducting public opinion warfare to enhance the Russian military's ability to control network public opinion. The size of the force is about 1,000 people. In 2018, Russia established the General Directorate of Military and Political Management to enhance the Russian military's psychological warfare, public opinion warfare, and information warfare capabilities by reshaping the military's political culture and strengthening the information dissemination function.

In addition to the above-mentioned official combat forces, the Russian army also conducts psychological warfare, public opinion warfare, and information warfare through "Operation Troll" and botnets (the Kremlin's "Troll Army"). Each "troll" has 6 Facebook accounts and 10 Twitter accounts, and can post 50 tweets a day. In addition, it can also publish 50 news reports a day.

2.3 United Kingdom   
As the first country to conduct psychological warfare, the United Kingdom has long maintained a team engaged in psychological warfare abroad. This team played a significant role in the process of Brexit. The British Army established the 15th Psychological Operations Group, which is positioned as a support force for joint operations at home and abroad, and assists in conducting battlefield psychological warfare activities by supporting regional and local combat missions.

The British Army divides its cognitive warfare forces into strategic, campaign, and tactical levels. Among them, the 15th Psychological Operations Group belongs to the strategic level, mainly responsible for recruitment, training, guidance, planning and other activities. The psychological operations support detachment and tactical psychological operations team under it belong to the campaign and tactical levels respectively.

2.4 Taiwan, China   
Taiwan believes that psychological warfare under high-tech conditions in the future is different from physical warfare in the traditional sense. It is a new combat style that integrates military behavior, political offensives, and electronic interference. It must rely on a sound and professional psychological warfare combat organization to organize, coordinate and implement. To this end, the "Information Warfare Strategy Planning Committee" was established in the "Taiwan Region Defense Affairs Authority" to be responsible for the overall guidance of information warfare, including psychological warfare. In imitation of the US military's practice, a psychological warfare research institution, the "Army Psychological Warfare Equipment Center", was established. It has three divisions under it, namely "Information Psychological Warfare", "Planning Guidance" and "Logistics Support", which are affiliated to the "Army Headquarters Political Warfare Department". The purpose of the Taiwan military taking these measures is to attempt to launch a powerful psychological offensive through various media channels in order to win without fighting.

Most of the intelligence units in Taiwan originated from the Kuomintang's "Military Intelligence" and "Central Intelligence" during the period of the mainland. After years of reorganization and evolution, they are currently mainly composed of the "Taiwan Security Bureau", "Taiwan Military Intelligence Authority", "Taiwan Legal Affairs Authority Investigation Bureau", "Taiwan Internal Affairs Authority Police Bureau", etc. In addition, the "Coast Guard Command" and "Military Police Command" in Taiwan also undertake part of the intelligence collection work. The psychological warfare of the Taiwan military is directly led by the "Taiwan Defense Affairs Authority", the director of the "General Political Warfare Bureau" coordinates the planning, and a deputy director of the "General Political Warfare Bureau" supervises the implementation. The "General Political Warfare Bureau" has institutions such as the "Psychological Warfare Corps", "Psychological Warfare TV Station", "Psychological Warfare Broadcasting Battalion", and "Psychological Warfare Intelligence Battalion". The "Psychological Warfare Corps" has three psychological warfare battalions under its jurisdiction, each of which contains three squadrons.

In addition, the Taiwan authorities also used civilian forces to form the "1450" troll army. The organization cooperated with the Democratic Progressive Party to promote various policies issued by the Green Camp, suppress opponents such as the Kuomintang and the People's Party, and discredit the mainland's economic, political, and diplomatic systems. In the "Hong Kong Amendment Storm", the "1450" figure can be seen everywhere; "1450" also launched cyber attacks on the service trade agreement, Taiwan-friendly policies, and Taiwanese businessmen and students; hyped up topics such as Lithuania's establishment of a "Taiwan Representative Office" and Taiwan's participation in the Tokyo Olympics; and created the topic of "Ukraine today, Taiwan tomorrow" in an attempt to create panic on the island and alienate the feelings of compatriots on both sides of the Taiwan Strait.

**3 Main technical equipment**

The United States has always regarded the development of advanced weapons and equipment as the key to maintaining its position as the world's number one military power. As the scope of traditional weapons expands from the physical domain to the cognitive domain, the US military has also invested a lot of money and manpower in the development of cognitive combat equipment. In recent years, the Defense Advanced Research Projects Agency (DARPA) has continued to support a series of projects, including the Social Media in Strategic Communication (SMISC) project, the Data-Driven Discovery of Models (D3M) project, the Culturally-Aware IO Defense (CLAID) project, the Computational Culture Understand (CCU) project, and the Deep Green (DG) project. It has conducted systematic research on social network battlefields, weapon countermeasures, and combat simulations, and provided a series of equipment support for US military operations.

From a business perspective, cyberspace cognitive combat equipment can be divided into situational awareness equipment, identification and recognition equipment, content creation equipment, guidance and intervention equipment, and simulation and evaluation equipment.

3.1 Situational Awareness Equipment  
Foreign militaries have developed a variety of situational awareness and strategic warning tools. By real-time monitoring of global news media, social media and other targets, they have comprehensively acquired Internet information, used big data technology to analyze and mine hot events and sensitive information, and achieved real-time monitoring of global hot network situations and real-time warning of hot conflicts.

3.1.1 US Army Psychological Operations Automation Management System  
The U.S. military's psychological warfare automated management system mainly provides various information required for the formulation of psychological warfare plans, implementation of psychological warfare, and evaluation of psychological warfare effects. It has functions such as information storage, information analysis, information processing, and information distribution. The system includes three systems: foreign media analysis, foreign region data for psychological warfare, and psychological warfare effect analysis. The foreign media analysis system mainly collects network media information in the target area and provides detailed analysis reports on important events and public figures in the area. The psychological warfare foreign region data system can process information data from more than 1,600 regions and supports dynamic automatic updates. The system not only provides foreign region data for the U.S. Department of Defense's psychological warfare organization, but also provides auxiliary decision-making for the Chairman of the Joint Chiefs of Staff and the psychological warfare command. The psychological warfare effect analysis system mainly provides the ability to analyze and evaluate the effects of psychological warfare.

3.1.2 “Social Media Strategic Communication” Project   
The "Social Media Strategic Communication" project was initiated by DARPA. By studying social network information acquisition based on new technologies, it helps the US military to grasp hot events on the Internet in real time, track the entire process of event generation, development, and evolution, explore the patterns of events, and support the US military in strategic propaganda.

3.1.3 “Data-driven Model Discovery” Initiative   
The purpose of the "Data-Driven Model Discovery" program is to learn how machine learning can be modeled through data-driven. Research on efficient simulation acceleration computing architecture and support platform, develop independent simulation processing systems designed for evolutionary computing of large and complex systems, and provide social simulation computing capabilities; research on deep media data mining capabilities such as intelligent image analysis and reverse image search, and provide decision support for cognitive domain analysis of institutions such as the National Security Agency (NSA) of the United States.

3.1.4 “Open Source Indicator” Project   
The Open Source Indicator (OSI) project was initiated by the Intelligence Advanced Research Projects Activity (IARPA) of the United States. It aims to develop methods for continuous and automatic analysis of open source data to detect and predict major social events such as political crises, humanitarian crises, large-scale violent riots, large-scale migrations, and disease outbreaks. Researchers evaluate and analyze real-world events by integrating early indicators from multiple public data sources and types of events.

3.1.5 “X Critical Score” Program   
The "XKeyScore" program was initiated by the NSA, which was the most extensive network information theft program in 2013. The NSA monitors all online behaviors of ordinary users (such as email content, network access and search records, etc.) by setting up more than 700 servers in 150 regions around the world. NSA personnel only need to enter the target's email address to monitor their online behavior in real time.

3.1.6 “Hybrid Forecasting Competition” Project   
The Hybrid Forecasting Competition (HFC) research project was launched by IARPA in August 2017. The project aims to improve the accuracy of geopolitical forecasts around the world by leveraging the strengths of both human and computer systems. During the competition, HFC will try various human-machine hybrid strategies to combine traditional news reports, social media, financial data and other information sources with human judgment in a series of scenarios involving real-world events such as political elections, national conflicts, and major epidemics, and conduct a comprehensive analysis of the forecast results to improve accuracy.

3.1.7 Maltego   
Maltego is an interactive social network topology intelligence mining tool developed by Paterva. It only needs a domain name to search resources on the Internet from top to bottom. It can enumerate network and domain information, including Domain Name System (DNS), Internet Protocol Address (IP), etc. It can collect target emails, websites, phone numbers, organizations, companies and other information.

3.2 Identification equipment   
Identification and recognition equipment helps foreign militaries detect and identify sensitive information they monitor, and provides references such as local culture and language to help them correctly understand events.

3.2.1 “Culturally Aware Information Operations Defense” Project   
The "Culturally Aware Information Operations Defense" project is a key AI project proposed by DARPA, which aims to develop human language capabilities so that machines can understand cultural, social and emotional backgrounds, thereby deepening situational awareness of emergencies. The project can help combatants quickly understand changing battlefield situations.

The project has three plans for 2022: first, introduce a social and cultural context model framework, including shared values, social norms, and differences in cross-cultural emotional expressions; second, develop methods for new natural language processing (NLP) capabilities, such as interpreting localized references to entities, emotions, and urgency, as well as the cultural significance of narratives and events; third, build cultural expertise to understand the types of emergencies commonly encountered in stabilization operations.

3.2.2 “Computational Cultural Understanding” Program  
In May 2021, DARPA launched the "Computational Cultural Understanding Program" project, which aims to use artificial intelligence technology to achieve a natural language processing technology that can communicate across cultures to assist the U.S. Department of Defense in overseas operations. The technology must not only read language, but also be able to understand and interpret cultural clues and provide combat advice.

This work is divided into two main research areas: one is to address a series of challenges that currently limit the application of human language and communication technologies, including the discovery of sociocultural norms, emotion recognition and detection of emotional changes; the other is to develop a conversation assistance service that can automatically detect sociocultural context and detect misunderstandings.

3.3 Content Creation Equipment  
 Foreign militaries use a combination of technologies such as virtual reality and artificial intelligence to develop content creation equipment and generate multimodal propaganda products to provide "ammunition" support for information guidance.

3.3.1 Motion Capture System  
 In recent years, virtual reality and augmented reality technologies have been widely used to simulate various extreme and harsh environments and improve the realism of military training environments. The behavioral interaction with the system is realized by various motion capture systems, among which Facerig software can read the user's facial expressions and movements as well as audio input in real time; somatosensory controllers include Leap Motion, Kinect, etc.; Valve Index handles, Noitom Hi5 gloves, etc. can realize hand motion capture; full body motion capture includes Xsens MVN inertial motion capture system, Noitom Perception Neuron motion capture system, etc.

3.3.2 Deep Fake System  
 During the 2022 Russia-Ukraine conflict, a video produced using the DeepFake platform in which Ukrainian President Zelensky called on Ukrainian soldiers to lay down their weapons caused an uproar. This was the first time that DeepFake was used in military activities. As AI technology matures, including the rapid development of Generative Adversarial Networks (GAN) and the open source of various deep fake project algorithms on the Internet, various face-changing apps of all sizes are emerging on the market, which can achieve the effect of making the fake look real.

3.3.3 Intelligent Dialogue System Based on Large Language Model  
 The large language model dialogue system represented by ChatGPT is the most powerful text automatic generation tool at present. With its powerful language understanding ability, it can not only learn and understand human language for contextual interactive chat, but also continue writing articles based on the context, and perform logical reasoning based on the chat content to complete tasks such as email writing, code writing, paper output, and image generation. In addition to OpenAI's ChatGPT, the current mainstream large language models include Google's T5, Microsoft and NVIDIA's MT-NLG, Meta's RoBERTa and LLaMA, BigScience's BLOOM, DeepMind's Chinchilla, etc.

3.4 Guidance intervention equipment  
 Based on the target identity positioning, foreign militaries use guidance and intervention equipment to deliver customized "ammunition" to specific target groups, achieving the precise release of cognitive "ammunition".

3.4.1 Social network opinion publishing system  
 The social network opinion publishing system was developed by the U.S. Central Command and can publish information on social media with multiple virtual identities. By forging IP addresses to log in to social networking sites, it creates the illusion that virtual netizens are logging in and posting in different countries and regions, and then uses these fake identities to publish information, inducing extremists to accept them into chat rooms and forums, thereby infiltrating some organizations (such as al-Qaeda and the Taliban) to spread false information and interfere with their actions.

3.4.2 “Advanced Concept Technology Demonstration” Program  
 The Advanced Concept Technology Display (ACTD) program of the U.S. Special Operations Command proposed the development of a comprehensive information push system to solve the problem of distributing psychological warfare products in restricted areas. One of the important research contents is the development of an information push system based on different communication facilities, including satellite communications, mobile phones, other wireless devices and the international Internet.

3.4.3 Cambridge Analytica’s Political Campaign System  
 Cambridge Analytica incorporates psychological theories and influence models into its actual operations, and makes personalized recommendations for different user groups, thereby quietly influencing user election behavior. By analyzing user network traces and posting information obtained from social media, analyzing user behavior, integrating user group portraits, and analyzing each person's gender, age, religious beliefs, hobbies, personality traits, political ideas, and supported political parties, etc.

In the 2015 U.S. presidential election, Cambridge Analytica used data models to identify middle-class voters, create "resonant information," achieve precise advertising delivery, and push specific biased content to users' social media over a long period of time, thereby influencing their voting results.

3.5 Simulation and evaluation equipment  
 Simulation and evaluation equipment uses intelligent simulation technology to simulate combat environments and scenarios, and evaluate the effects of various decisions to help commanders make decisions.

3.5.1 “Deep Green” Plan  
 "Deep Green" is a combat decision support system developed by DARPA that integrates pre-war and in-war planning, analysis and evaluation. The technical essence of the "Deep Green" program is dynamic simulation based on real-time situation.

The substantive work of the plan mainly includes three items: First, provide an intelligent human-machine interface. It can automatically transform the commander's or staff's freehand sketches and intentions into brigade-level action plans, and fully realize the goal of "making decisions based on sketches". Second, simulate battlefield decisions. Identify each decision branch point, simulate each decision plan, and predict the possible results and probability of different decisions to generate possible future battlefield situations. Third, develop a "deep green" simulation control system. It can build a parallel simulation battlefield environment that runs in parallel with the real battlefield environment. The simulated battlefield environment can be dynamically updated according to real-time battlefield data to achieve ultra-real-time simulation of future battlefield situations. Through battlefield decision simulation and ultra-real-time simulation of future battlefield situations, the system can help commanders make targeted and advanced decisions.

3.5.2 Psychological Operations Effect Analysis System  
 The psychological warfare effect analysis system is part of the U.S. military's psychological warfare automation management system. By analyzing the sample survey data of information receivers, it can evaluate information products and combat plans.

**4 Conclusion**

The evolution of combat forces and the development of technical equipment are all processes of continuous improvement of cognitive combat systems. With the development of new technologies such as artificial intelligence, social sciences, virtual reality, and ChatGPT, technical equipment is also moving towards intelligence, human-machine collaboration, and unmanned operations. This article summarizes the comprehensive situation of cognitive confrontation abroad, hoping to provide reference and reference for the construction of my country's cognitive defense system.

Citation format: Xiao Ning, Zeng Huasheng. Overview of overseas cognitive warfare combat forces and technical equipment[J]. Information Security and Communication Confidentiality, 2023(5):8-16.

*Selected from "Information Security and Communication Confidentiality" 2023 Issue 5 (for the convenience of typesetting, the original references have been omitted)*