**The weaponization of information is coming quietly**

**Author: Lu Jie**   
**Date: 2024-07-17**

**Editor's Note**   
The way humans produce is the way they fight. Since entering the information age, although the impact of information on human production and life has been widespread and profound, the "front-stage stars" of war are still various weapons and equipment. Compared with machinery and firepower, information is hidden in the "backstage", silently playing a guiding and controlling role. However, as information moves from the material use that supports production and life to directly affecting personal cognition and social orientation, the informatization of weapons will inevitably transform into the weaponization of information.

**Information weapons are the core tools of cognitive domain warfare**

Cognition refers to the process of processing information through thinking activities to understand and know objective things. Human beings have never stopped fighting in the cognitive domain since ancient times. However, for a long time, most of them have been manifested in self-recognition and guided cognition through social activities. Self-recognition is the self-acquisition of information about material and social activities, while cognitive guidance relies on traditional and standardized communication channels. In the information age, due to the qualitative changes in the content, methods and speed of information dissemination, the guiding role of information on individual and social cognition as a whole reflects the huge changes in initiative, full-time and all-round. Information itself has the characteristics of a weapon.

**The key to cognitive domain operations at the social level is the right to speak in information.** Cognitive domain operations at the social level are a confrontation process in which the enemy and us actively exert influence on the thinking of social groups to create cognitive tendencies that are beneficial to our own side. The most typical manifestation is the "color revolution". In the past 20 years, social unrest and chaos in some hot spots and countries in the world, such as the "Arab Spring" in the Middle East and the "color revolutions" in Eastern Europe, have the shadow of cognitive domain operations behind them. In cognitive domain operations, the role of information is no longer limited to the "catalyst" role of adding fuel to the flames, and sometimes it can even directly determine the final outcome of the development of events. In the information age, using the direct influence of information to shape the cognition of key personnel and public groups in the target country in a long-term and targeted manner is the most effective way and convenient way to implement cognitive domain operations at the social level. This requires mastering the right to speak in information in the global information environment, starting from the source of information, and intervening in the cognitive system of the target social group with our own advantages in information generation, transmission, and utilization, so as to minimize or suppress the enemy's information influence, thereby achieving the purpose of influencing the other party's social behavior.

**The key to battlefield-level cognitive domain operations is battlefield information control.**Battlefield-level cognitive domain operations are to influence the cognition of the combatants of the two warring parties, guide and disrupt the decision-making of the other commanders, weaken the resistance of the other combatants, and thus form a war situation and battlefield situation that is beneficial to one's own side. In traditional warfare, strategic deterrence, firepower strikes, and military assaults, while deterring and destroying the enemy, also indirectly convey information with rich connotations, changing the cognition of the two opposing parties until one party realizes that resistance is ineffective and then surrenders. However, this kind of information transmission and conversion is slow, and the effect of cognition has a certain lag, and the cost is high. In the era of information warfare, the command decisions and combat operations of the warring parties are highly dependent on information, making the seizure of battlefield information control a top priority in war. This struggle is essentially through the comprehensive use of various information, using information to counter information, suppress information with information, and destroy information with information, so that the influence of one's own information is stronger than that of the other party, making it difficult for the other party to perceive the battlefield situation, unable to make correct command decisions, and thus unable to carry out combat operations, and ultimately succumbing to one's own will.

**The core "equipment" of cognitive domain operations is weaponized information. Information is the "ammunition" of cognitive domain operations.**   
This kind of information is not a simple statement of facts or instructions, but weaponized information with strong purpose, targeting and destructiveness, that is, information weapons. According to the usual definition, weapons refer to the general term for equipment and devices that can be directly used to kill enemy manpower and destroy enemy equipment and facilities. From the perspective of the mechanism of action, information weapons can target the enemy's will to fight and fighting spirit, and can also destroy the enemy's information system, system and equipment, and affect the enemy's combat decisions and actions. Its essence is to weaken and reduce the enemy's combat effectiveness, which is in line with the value of the weapon. Compared with traditional weapons, information weapons have a deeper impact and a greater influence.

**Information weapons are the inevitable result of the development of information technology**   
  
For information to become a weapon, it must have the prerequisites for it to play a role. In the past social eras and war forms, the acquisition, transmission, processing and application of information were also involved, and fierce information struggles were also launched, but its role and influence are incomparable to those of today. The reason lies in the differences in science and technology, especially the constraints of information technology. At that time, the application of information in human society could not reach the level of "ization". After entering the 21st century, with the breakthrough and development of human information technology, information has gradually penetrated into all aspects of human society, established a "strong connection" with social activities such as politics, economy, military, and culture, and guided and controlled the orderly operation of social activities and infrastructure, becoming an important strategic resource. Human dependence on information and information technology has reached a high level. It is difficult to imagine what kind of scene will appear if human society loses the support of information technology and loses information resources. In a sense, the development of information technology has not only created the information age, but also provided the driving force and stage for the generation and use of information weapons.

**Internet technology has expanded the "power range" of information weapons.**   
The most important feature of the information age is the widespread use of Internet technology. The omnipresence of the Internet makes it possible for all things to be connected. The information barriers between people, between people and things, and between things are broken by network technology. People and things that were originally unrelated can establish relationships with the help of network platforms. This interconnected network environment provides convenient conditions for information weapons to spread their influence. Whether it is against people or things, as long as it is launched at a node in the network, it can quickly spread to every corner of the world and produce mapping effects and cascade reactions in the physical space. The most typical example is the network information hype and network virus attacks against individuals.

**Media communication technology has enriched the "firepower channel" of information weapons.** Traditional information dissemination mainly relies on radio and television media and paper media. Information dissemination is one-way, and the audience is often in a state of passive acceptance, which is not conducive to a comprehensive and detailed understanding of the truth of the matter. At this time, the use of information weapons is relatively limited, easy to be filtered, and difficult to achieve specific purposes. The development of modern media communication technology has changed this unfavorable factor. Various self-media platforms, social media, and video live broadcast software are widely installed on everyone's mobile communication devices. Everyone is a creator and transmitter of information, and can serve as a booster for the effectiveness of information weapons. Typically, information weapons such as false information and misinformation generated by face synthesis and audio and video forgery technology can be delivered with the help of media communication technology, causing public opinion to split, social contradictions to intensify, and even trigger street riots.

**Data processing technology improves the "strike accuracy" of information weapons.**   
Data processing technologies represented by big data, cloud computing, data mining, knowledge graphs and other technologies can achieve precise attacks of information weapons. With the support of these technologies, detailed personal data information can be widely collected, and people can be classified through correlation analysis and data collapse of information. When attempting to influence specific events, such as public voting and elections, information weapons can be accurately manufactured for different social groups and target individuals, and pushed centrally on their commonly used information interaction platforms, constantly strengthening or changing their original beliefs and attitudes, thereby achieving their specific goals.

**Information weapons are an objective requirement for changes in the war model**

Since the war entered the information age, although local wars have occurred frequently around the world, under the deterrence of the "terrorist nuclear balance", there has been no large-scale fighting between major powers, and the overall stability of the world has been basically maintained. In conflicts between countries, the main goal is to resolve international disputes through political means and non-military actions. Even if force is resorted to, efforts are made to resolve the problem in a short period of time and minimize collateral losses and casualties. In this international environment, the unlimited violence war model will be replaced by the limited violence or non-violent war model. Conquering the enemy without fighting is the best strategy, conquering the enemy with a small war is the middle strategy, and conquering the enemy with a large war is the worst strategy. Therefore, the world's military powers are exploring effective ways to achieve the best and middle strategies of war. The emergence of information weapons provides an effective option for achieving the above goals.

**The weaponization of information is conducive to directly achieving the purpose of war.**   
With the development of the information society and the deepening of military informatization, the impact of information on social activities and military operations will become increasingly greater. Information weapons can be used in three aspects to achieve the strategic goal of making the enemy surrender. First, cognitive attacks are carried out on the people of the hostile country to weaken their support for the ruling authorities; second, information attacks are carried out on the livelihood systems that support the operation of the enemy society to affect the normal life and consciousness of the people; third, information deterrence is carried out on the key information systems of the enemy's combat system to temporarily lose its combat capability. Without public support, unstable political situation, and weak equipment, the result can only be surrender.

**The weaponization of information is conducive to reducing battlefield risks.** When the enemy is determined to carry out military confrontation, information weapons are still an effective means to reduce casualties and weaken the enemy's combat capability. On the battlefield, electronic warfare and cyber warfare play the main role of information weapons, implementing information destruction and paralysis of the enemy's highly informationized military equipment and systems, and minimizing their combat effectiveness. Outside the battlefield, propaganda and psychological attacks play the leading role of information weapons, launching cognitive attacks on the enemy's military and civilians to reduce their will to resist. The coordinated efforts inside and outside the battlefield will achieve the purpose of war at the fastest speed and the lowest cost.

The future information warfare with intelligent characteristics is a transitional stage for information warfare to move to a higher level, and the reliance on information will be stronger.  
 The weaponization and use of information will have a strong driving force in implementing the national will and achieving war goals, and information weapons will become a powerful weapon to defeat the enemy in information warfare.