**Virtual social warfare from the perspective of cognitive domain warfare**

Source: China Social Sciences Network

Author: Gao Ya & Yu Yuan Lai

Editor: Xie De

Date: 2023-03-28

Link(not secure): <https://www.cssn.cn/jsx/jsx_xxqj/202303/t20230328_5616582.shtml>

With the advent of the era of mobility, intelligence, and socialization, cognitive domain warfare has become a focus of attention for countries around the world. Cognitive domain warfare is not only an important strategic means of coordinating armed operations in wartime, but also an important strategic tool for major power political games in peacetime. It plays an extremely important role in guiding the cognition of the international community and shaping a favorable strategic situation. In 2019, the internationally renowned think tank RAND Corporation released a research report entitled "New Risks of Virtual Social Warfare - Social Manipulation in a Changing Information Environment", which first proposed the concept of "virtual social warfare" and attracted international attention.

　　Virtual social warfare refers to the systematic generation and dissemination of specific information through the application of technologies such as computational propaganda, false information, deep fakes, artificial intelligence, augmented reality, etc., to manipulate social information in target countries and regions in order to influence the beliefs, attitudes and behaviors of their people, interfere with the normal operation of their society, politics and economy and bring adverse consequences. It has become a new style of cognitive domain warfare.

**The essence of virtual social warfare is to manipulate social cognition**

　　"Manipulation" comes from the Latin word "manus" (hand), which means "to treat an object with intent and purpose." Russian scholar She. Kara-Murza pointed out in his book On the Manipulation of Consciousness that "magicians with flexible techniques use the psychological paradigms of the audience to divert, shift and focus their attention, influence their imagination, and create illusions when they are accepted. When these principles become operational techniques for controlling people's behavior, the modern meaning of the metaphor of manipulation is generated, that is, programming the opinions, interests, emotions, and even psychological states of the public, with the purpose of manipulating the desired behavior." It can be seen from this that manipulation is a potential influence that conceals the facts from the manipulated object, and is a form of influence from the spiritual, psychological, and cognitive aspects. Human cognition is the target of the manipulator.

　　Virtual social warfare is a cognitive warfare action that uses various emerging technologies such as artificial intelligence, virtual reality, and deep fakes to create and change people's basic social reality. Its essence is a form of social manipulation. It manipulates social cognition through information based on people's cognitive characteristics, causing them to undergo cognitive changes in the direction of their preset reactions, thereby creating a social reality that is in line with their interests.

　　The rapid development of technologies such as big data and artificial intelligence has profoundly changed the social information environment in which people live, and the trend of the "post-truth era" has gradually intensified. For individuals, it will become increasingly difficult to achieve a balance and reconciliation between social truth and social cognition under the flood of information brought about by communication technology. Former British Prime Minister Theresa May once proposed the concept of "weaponizing information", believing that using information as a weapon can weaken and subvert a country's democracy and regime from within. The development of information technology has accelerated the potential impact of information weaponization and broadened new ways to achieve effectiveness in cognitive domain operations. Human social cognition follows the "cognitive stinginess" or "frugality principle", and often relies on obvious surface information and simple and effective strategy evaluation to make judgments on information in order to reduce cognitive burden. In other words, it is to produce those behaviors that can best improve reproductive fitness with the least information processing energy loss, so people will use a variety of techniques to integrate information into their own worldview and accept information from information sources they believe to be reliable, including the social psychology of conformity.

　　Virtual social warfare is an attempt to use various information technologies to achieve cognitive manipulation of the target audience, so that under the flooding of information, the precise attack of computational propaganda, and the influence and penetration of false information, a "float effect" of social cognition is produced, that is, when the subject cannot judge the authenticity of relevant information based on his own cognitive ability, he often makes judgments based on the social mainstream opinions preset by the manipulation, just like randomly jumping on a seemingly fancy float when participating in a float parade. Under information manipulation, cognitive subjects often reduce information processing costs by "borrowing brains" from the mainstream society or relevant authorities, and then become the "silent majority" under the influence of information waterfalls, and are thus influenced by some false, fragmented, aggressive, and machine-controlled "mainstream social opinions" and fall into cognitive traps.

**Emerging technologies help virtual social warfare to move to the real world**

　　Although technology cannot directly bring about the combat effectiveness of virtual social warfare, it can enable and enhance cognitive domain warfare. Virtual social warfare in the "smart +" era, spawned by information and intelligent technology, is showing a trend of virtual-real interaction and synergistic symbiosis between physical, network and social systems, and is fully integrated into all levels and fields of cognitive domain warfare. The Rand Corporation's report lists nine emerging technologies for social manipulation and virtual social warfare: precise positioning of influence, artificial intelligence, algorithmic decision-making, virtual reality and augmented reality technology, the Internet of Things, intelligent voice, blockchain, deep fakes and monitoring systems. These technologies will quickly promote the "realization" of virtual social warfare, deeply change people's social cognition in a changing information environment, and greatly enrich the strategic means and tool selection of cognitive domain warfare.

　　How does the application of emerging technologies affect human cognition? Currently, the following five technologies are widely used in the field of cognitive domain operations.

　　First, use big data technology to accurately draw the cognitive landscape of key groups. With the emergence of big data technology, by mastering the target's online traces, shopping experience, smart car travel, social media use, etc., we can more accurately understand their personality characteristics and cognitive thinking habits, and accurately draw the cognitive landscape of key groups, making specific cognitive attacks and targeted information isolation possible.

　　The second is to use algorithmic technology to continuously influence the cognitive thinking of the target object. Google widely uses algorithms to shape search results based on prior patterns, while Amazon uses algorithms to evaluate other products that customers may be interested in. Facebook has established detailed psychological profiles for its 2.2 billion users, carefully screens the pushed content based on algorithms, and then adjusts the algorithm or changes the user's information flow through effect evaluation, filters the content shared by users, selectively allows users to see certain content, analyzes the impact on users, and then specifically influences users' emotions to influence their cognitive thinking.

　　The third is to use artificial intelligence technology to carry out saturated cognitive attacks on specific audiences. Artificial intelligence technology involves the use of computers to simulate intelligent responses to information input and processing, covering areas such as pattern and voice recognition, strategy selection, visual perception and translation. Through deep learning of machines, it can even surpass human intelligence, and has affected the nature of daily activities of every industry and individual in the physical environment and cyberspace. For example, chatbots and water army robots are used to carry out saturated cognitive attacks on specific audiences on social media, making it impossible for specific audiences to correctly judge the current situation under such information attacks, and it is difficult for them to think independently and draw correct conclusions. Instead, they are more likely to be infected by emotions and fall into a preset "cognitive trap."

　　Fourth, use deep fake technology to interfere with the enemy's decision-making cognition. The current typical application forms of deep fakes mainly include: face replacement, face reproduction, face synthesis, and voice synthesis. In the future, deep fakes will develop in the direction of full body synthesis, audio, video and image synthesis. Once widely used in the field of cognitive domain operations, it will increase the prevalence of false information, covertly interfere with the cognitive judgment of the target audience, and even affect the decision-making cognition of the enemy.

　　The fifth is to use augmented reality technology to simulate cognitive scenarios. This technology, combined with the Internet of Things, blockchain and other technologies, can build a "metaverse" that connects the digital world and the real world, providing users with an immersive virtual space. With the help of this augmented reality technology, it is possible to tailor cognitive scenarios for specific target groups and implement purposeful manipulation, such as guiding audience cognition through typical propaganda and positive guidance, creating pressure and distorting results to make the audience feel frustrated, and sending specific information to spread specific views or interference to users, making cognitive domain operations more embodied, precise and situational.

**Prospective planning and suggestions for coping with virtual social war**

　　Virtual social warfare describes a reality that has already arrived and is a typical scenario for the use of cognitive domain warfare. Everyone lives in an information society. This combat style, which is based on information, uses technology as a means, and targets social cognition, has a very important impact on consolidating the cognitive defense line, ensuring social security, and maintaining national stability in the future. We must respond and plan early to firmly grasp the discourse power and initiative of cognitive confrontation.

　　The most common method of social manipulation in virtual social warfare is that hostile forces use information manipulation technology extensively to deliberately hype up hot and sensitive issues in domestic society, put in preset conceptual frameworks such as "despotism" and "authoritarianism", and create labeling effects, float effects, cocoon effects, etc. to manipulate social cognition, guide the public to attack the government and divide public opinion. In the face of the flood of information, only a few smart people have the ability to think and judge independently, and the public can easily become a "mob" like puppets.

　　On the one hand, we must increase the intensity of theoretical research, institutional construction and technological development to counter virtual social warfare, coordinate the resources of military and civilian universities, think tanks, media organizations and professional groups, build and improve the relevant institutional mechanisms for cognitive domain operations, establish theoretical research and technical development teams, and carry out collective research on the strategies, methods, and technical applications of powerful enemies' cognitive domain operations against our social information attacks. We must attract social forces such as Internet companies and technology companies to deeply participate in social information activities, jointly participate in the governance of network information, develop emerging technologies such as counter-deep fake technology, robot water army, false information, and public opinion warning, and effectively control the gateway of cognitive information attacks from the source.

　　On the other hand, we must strengthen the cultivation and training of the entire population's online media literacy, increase propaganda efforts to counter virtual social warfare, accelerate the network deployment of fact-checking and rumor-refuting platforms, raise the public's awareness of anti-China forces' social manipulation through online information, clarify the legal and social responsibilities of platforms and individuals for producing, forwarding, and spreading false information, and work with companies to proactively provide the public with some simple and reliable technical support, detect false information in real time, monitor the direction of computer propaganda, and promptly publish relevant evidence to the public, effectively improve the public's media literacy and prevention awareness, consolidate the social cognitive defense line, and ensure that people are not led astray or fall into traps.

**(Author’s unit: School of Sociology and Population, Renmin University of China; Political Science Academy, National Defense University)**