**Cognitive Domain The Commanding Heights of a New Round of Technological Innovation**

Publisher: Qiu Yunshu

Published: 2022-06-24

<https://ibd.fudan.edu.cn/e3/ef/c24057a451567/page.htm>

In the cognitive domain, who is the most "disruptive" and who can become the leader of a new round of changes? Through the "Cognitive Domain Science and Technology Innovation Series", we will gather the opinions of experts and scholars from all parties, focus on the paradigm change of cognitive domain engineering technology, and jointly discuss the strategic focus, development strategy, and implementation path of cognitive domain technology innovation, and make suggestions for national scientific and technological innovation.

The Russia-Ukraine conflict is a comprehensive conflict between a single world power and the proxies of multiple world powers, providing a new perspective for studying the form of war and understanding the characteristics of war. This conflict is considered to be "the first conflict to be broadcast live in short videos throughout the process", with a distinct feature of virtual-real integration. The conflict not only occurs in tangible physical space, where smart drones, precision-guided weapons, and information-based individual weapons have made their debut; it also occurs in virtual cyberspace, where Starlink, battlefield perception, and cyber warfare weapons have come to the fore; more noteworthy is that **this conflict is an unprecedented "cognitive war" between the United States, the Western world, and Russia** , which for the first time highlights the importance of cognitive space. The scope of cognitive domain operations has surpassed the traditional propaganda war, public opinion war, and psychological warfare, and may become an important way of future warfare.

Ren Kui, dean of the School of Cyberspace Security at Zhejiang University, believes that the cognitive warfare in the Russia-Ukraine conflict is likely to become a "new engine" driving the accelerated evolution of global high technology, just like the information warfare in the first Gulf War. More than 30 years ago, CNN successfully broadcast the first Gulf War live, and then more TV stations joined the ranks of real-time reporting, which also opened up a new paradigm of media warfare. Today, more than 30 years later, when digital platforms have become infrastructure that transcends time and space, social media and short videos have enabled everyone to become content makers and public opinion disseminators. Those who participate in the war are no longer just soldiers, but also "netizens". What affects the course of the war is no longer just weapons, but also a piece of "text". **The confrontation in the cognitive field is no longer limited to the bizarre public opinion field, but has also begun to play an increasingly complex role in military conflicts and international relations.**

Ren Kui believes that, unlike the telegraph and telephone in World War I, the newspapers and radio stations in World War II, and the live broadcast of local wars in modern times, the current Russia-Ukraine conflict has ushered in an era of segmented self-media and social platform live broadcasts, creating a global wide range of "synchronicity", "co-occurrence", "consensus" and "resonance". If the Iraq War brought cyber warfare into being, then the current **Russia-Ukraine conflict has officially made cyberspace the main battlefield of cognitive confrontation.** Cognitive warfare can be carried out intensively in wartime or subtly in peacetime; it involves public diplomacy, academic exchanges, culture and art, and international organizations, and can also be hidden in Twitter, TikTok , Facebook, and every seemingly harmless video, picture, topic or emoticon package on various platforms in China. Through "deep fakes" and "accelerationism", cognitive warfare can deliberately mobilize the emotions, perceptual experiences and collective unconsciousness of the target group, release extreme speech, create opposing emotions, hijack public opinion, and manipulate public opinion, thereby interfering with government decision-making and affecting the form and direction of war. From "air control" and "sea control" to "information control" and "network control" and then to "cognitive control", the trend of war evolution is gradually emerging, and a new military revolution is about to come.

Ren Kui believes that **military needs will inevitably drive the scientific and technological revolution.** It can be said that the military needs of the first Gulf War provided an important driving force for the information technology revolution at that time. In the 1990s, in order to maintain its development advantages in the field of high-tech, the United States launched the "Information Superhighway" plan to comprehensively promote the development and widespread application of technologies such as computers, the Internet, mobile communications, and integrated circuits. In November1993 , the Washington Post predicted: "A new era is coming, when news can be quickly transmitted on the so-called 'information superhighway'." Today, this prophecy has long been realized, and "seeing the world in the palm of your hand" has become a reality. Looking back on history is to better face the future. If the Gulf War highlights the power of the Internet to change the world, let precise strikes and efficient accusations become the trend, let data resources and information systems become the basic support, and let information technology become an important strategic game force for the country. Then in order to further seize opportunities, meet challenges, and do a good job in our scientific and technological innovation, what enlightenment does the current Russia-Ukraine conflict bring to me?

Ren Kui believes that **the cognitive domain will promote science and technology in all aspects.**

In the cognitive domain, we will see new communication technologies. **The core feature of cognitive domain game is the interweaving of the three domains of "physics-information-cognition", and its core foundation is ubiquitous interconnection.** The cognitive system composed of intelligent platforms under the condition of "connecting everything" will be more agile and adaptable than the Internet era. Communication comes from connection, and connection generates intelligence. Studies have shown that the tens of billions of neurons in the human brain do not just store information, but more importantly, they can inspire new information or "inspiration" while constantly transmitting information during the connection process. In the Russian-Ukrainian conflict, we saw that the "Starlink" system has been widely used. It is reported that the average download speed of "Starlink" in Ukraine is 136Mbps and the upload speed is 24Mbps5 times the local average Internet speed . In addition to providing convenient communication and high-speed Internet access, its satellite group operates in low orbit, has a short revisit cycle, and has low space transmission loss, which can ensure wider communication bandwidth, faster transmission speed and higher reconnaissance efficiency. It can provide support for face recognition, social network connection, multi-dimensional information dissemination, etc., and has significant military application value. New communication methods and new connection modes have reshaped the battlefield form - "conflicts are local, communications are in the sky, and data are in the West", and will also likely reshape the form of technology and applications.



The cognitive security confrontation model exhibited at the Cyber ​​Security Science and Technology Museum in Zhengzhou (Photo provided by Wang Danyu)

In the cognitive domain, we will see new intelligent technologies. In the Russian-Ukrainian conflict, we saw that the weapon system already has a certain cognitive ability, and with the empowerment of artificial intelligence technology, it can act more autonomously. For example, the mobilization of troops is like "Meituan taking orders" and "Didi sending cars". Some analysts say that the combat information system will autonomously calibrate targets according to the battlefield situation and combat needs, "distribute task orders" to the nearest combat unit according to the task, and link the strike platform and "crowdfunding" support forces. For another example, Western technology companies such as Apple, Google, and Facebook, relying on the digital media hegemony in their hands, use various AI robots to spread information, create public opinion, and shape the situation, making the speed and effect of "information load" far exceed the past. **Whether it is machine cognition or social cognition, big data and artificial intelligence technology are likely to make revolutionary progress.**

In the cognitive domain, we will see new computing technologies. **One of the core elements of cognitive warfare is still the competition of computing power.** Since the "man in the loop, man-machine collaboration" model has been formed, human decision-making, behavior and consciousness are all affected by machine computing, and "the one with the strongest computing power wins" may become an important law for winning the war. The existing human computing system not only consumes huge energy and has low efficiency, but also has difficulty in efficiently managing massive heterogeneous perception and computing resources, and cannot efficiently meet the needs of various scenarios. It is difficult to break through the constraints of parallel walls, memory walls, and resource locks, and it is impossible to achieve efficient collaboration in the virtual-real fusion environment of "man-machine-object" in the future cognitive domain. **In the future, people will be committed to transforming from simply pursuing "general computing power" to obtaining diversified and efficient "intelligent computing power", and it is possible to break through the constraints of the existing "von Neumann" architecture, create a new paradigm for the development of domain-specific software and hardware collaborative computing technology, and form new momentum in the process of accelerating "knowledge to wisdom".**

In the cognitive domain, we will see new security technologies. In the context of the interweaving of multiple domains in cyberspace, the generalized functional security issues of the cognitive domain have emerged. **Human cognition has "innate defects",** such as individual cognitive biases that cannot be eliminated, group cognitive polarization that is inevitable, and situational noise that is difficult to clean. At the same time, **big data and artificial intelligence technologies may also have some unpredictable new impacts on human cognition because they still have "endogenous insecurity" problems such as unexplainability, unpredictability, and unreasonability** . The various information generated by various intelligent systems is often difficult to distinguish between true and false. "Pictures may not necessarily indicate the truth" and "what you see may not be what you get". In the context of fragmented reading and viral transmission, "media reality" often replaces or covers the real situation. **The definability and resetability of the information environment, coupled with the characteristics that human cognitive defects can be exploited and manipulated, further highlight the security issues of the cognitive domain.**

In 2013 , the Center for a New American Security, a well-known American think tank, released a report titled "Game Changers: Disruptive Technologies and U.S. Defense Strategy", which discussed the global proliferation of advanced technologies and the challenges they pose to national defense technology advantages, and proposed that the focus of "next-generation technology" innovation should be placed on disruptive technologies, that is, focusing on "technologies or technology groups that solve problems in a way that quickly breaks the balance of military power with opponents." It can be said that **most military changes in the mid- 20th century were based on advances in the field of physics, and most new military changes in the early 21st century were triggered by breakthroughs in the field of information. In the next thirty years, the cognitive domain may become one of the new main trends in military change.** Driven by military needs, the engineering technology changes in the cognitive domain are also expected to become the "trendsetter" of scientific and technological innovation, and may open a new era similar to the information technology revolution.

**This article was first published on Guangming Daily client, by all-media reporter Cai Dongchen and correspondent Shang Yuting.**