Analysis of the Characteristics of the "Hybrid War" between Russia and Ukraine and Its Enlightenment to China

Wang Wei
Northwest University of Political Science and Law, Xi'an, Shaanxi, China

Abstract: The Russian-Ukrainian war has not yet settled, and news reports, online new media reviews, and academic reviews about the Russian-Ukrainian war are also constantly being updated. This war is not limited to the traditional armed conflict, accompanied by the addition of new elements such as artificial intelligence technology, network information dissemination, and online public opinion attacks, and it presents a situation of "hybrid warfare". Based on this background, starting from the basic theory of "hybrid warfare", combined with the "hybrid warfare" adopted by the United States during the Cold War and the "hybrid warfare" implemented by Russia during the Russia-Ukraine conflict, this paper analyzes the basic characteristics of "hybrid warfare" in the Russian-Ukrainian war in the intelligent era, and tries to provide experience for China to deal with "hybrid warfare" in the future, so as to consolidate and maintain China's military security and national security.

Keywords: "Hybrid Warfare"; Cyber Warfare; Public Opinion Warfare; Artificial Intelligence

1. The Theory of "Hybrid Warfare" Was Proposed and First Applied

The Russia-Ukraine conflict is the first real cyber era war since the birth of the Internet, which reconstructs the rules of war, rewrites the key factors that determine the outcome of war, and marks a fundamental change in the form and mode of human war. With the gradual advancement of the Russian-Ukrainian war, "hybrid warfare" has increasingly become a hot word in the field of warfare in the intelligent era, but "hybrid warfare" is not indiscriminate, and the predecessor of the theory of "hybrid warfare" is the "hybrid threat" constructed by the United States in reflection.

1.1 Sources of "Hybrid Warfare".

In the wars in Afghanistan in 2001 and Iraq in 2003, the United States maintained its battlefield superiority, but it was at a disadvantage in the wars. While the power of the United States has been greatly weakened by the war, its national soft power and international image have been greatly damaged, and terrorism, extremism, and separatism have become more rampant. This made the United States change its war mentality and gradually realize that winning the hearts and minds of the people is the foundation of victory rather than conquering cities. [1]

With this in mind, the 2005 edition of the U.S. National Defense Strategy was the first to introduce the idea of a "hybrid threat": the most powerful adversary of the future may combine destructive capabilities with traditional, unconventional, and disastrous forms of warfare. The 2006 fighting between Allah Lebanon and Israel further bankrupted the "Kosovo" model of operations. After that, the US Navy recognized that the "hybrid threat" became a new form of threat in modern warfare. The theory of "hybrid warfare" was systematically discussed for the first time in the book "Conflict in the 21st Century: The Rise of Hybrid Warfare" compiled by American military scholar Frank Hoffman.[2] Based on the research results of their predecessors, Chinese scholars have further clarified the basic concept of "hybrid warfare", that is, with the expansion of globalization and information technology, traditional large-scale conventional warfare and small-scale unconventional warfare are gradually evolving into a hybrid warfare with more blurred war boundaries and more integrated combat patterns. [3]

1.2 The Use of "Hybrid Warfare" in the

United States During the Cold War

The collapse of the Soviet Union was an appearance of the "hybrid war" of the United States, and Professor Wang Xiangsui also pointed out in the article that the United States had carried out "hybrid warfare", and the disintegration of the Soviet Union was one of the practices. A book published by the CIA details how the Reagan administration brought down the Soviet Union, the superpower of the time. In the preface to the book, it is mentioned that the Soviet Union, as a world power, could not have completely collapsed by suicide, but was more likely to have been murdered en masse, because the murder was a silent battle. Then, in the author's discussion, the whole process of the Reagan administration's attack on its system (A system to realize the ownership of the country by the people, its basic elements include public ownership; Planned economy; democracy) is shown from seven angles. [4]

The seven-point plan is not limited to the traditional arms race, but involves multiple dimensions such as economic sanctions, diplomatic strategies, and intelligence attacks. For example, in foreign policy, the United States has given strong financial and military support to the Afghan resistance, cooperated with Saudi Arabia to lower oil prices, thereby reducing the Soviet Union's foreign exchange earnings, and engaged in secret diplomacy. At the spiritual level, a "slick" spiritual warfare was waged in order to intervene forcefully in the decision-making bodies of the Soviet Union; In terms of intelligence, it deliberately sent false high-tech intelligence information to the Soviet Union to undermine the Soviet economy (The Soviet Union wanted to build an oil pipeline from Siberia to Europe, and the blades of the pressurized stations in the pipeline depended on American imports.); Under these circumstances, the United States deliberately leaked technical information about the blades of the pressurized station, and mixed false information on the angular parameters of the blades in most of the true information, resulting in the failure of the pressurized station developed by the Soviet Union and obstacles to the transmission and export of oil. In the field of defense construction, taking an offensive and high-tech path is aimed at plunging the adversary into an expensive arms race, leading to economic weakness.

The "hybrid war" of the Cold War period of the United States did inflict heavy losses on the Soviet Union, which is instructive for the development of "hybrid war" today. However, compared with the two "hybrid wars" discussed below, the "hybrid warfare" of this period did not involve as much breadth and depth in terms of dimensions and domains as the latter.

2. Theoretical Expansion and Practical Application of "Hybrid Warfare"

2.1 A New Understanding of "Hybrid War" During the Crimean Crisis

In 2013, Russia began to pay attention to the study of "hybrid warfare", and it is surprising that, compared with the United States, Russia, which started late, showed a trend of latecomers catching up. Subsequently, in the Crimean crisis, the principle of "hybrid warfare" was fully applied and a phased victory was achieved.

In 2013, Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, published an article arguing that the boundaries of war have become blurred, it is becoming more and more difficult to determine the state of war, and conventional military means need the support of political, economic, informational, humanitarian and other non-military means, and in 2015, he published a report entitled ""Hybrid Warfare" Needs High-tech Weapons and Scientific Demonstration", which systematically expounded the Russian army's understanding of "hybrid warfare" for the first time, pointing out that the focus of the methods used in modern warfare is increasingly towards the comprehensive use of politics, Economic, informational, and other non-military measures are shifted. [5]

Subsequently, senior generals and military theorists of the Russian army conducted in-depth analysis from the political, strategic and tactical levels, based on the actual situation of the Russian army, and used it as a program for Russia's military operations in Ukraine to conduct actual combat exercises, creating a Russian-style "hybrid war" with distinctive characteristics. [6] In other words, future warfare is a mixture of the main body of war, such as the state, non-state actors (terrorist organizations) and individuals, a mixture of conventional warfare and unconventional warfare, a mixture of military operations such as operations, stability maintenance, and reconstruction, a mixture of political, military, economic, and people's livelihood and other fields, and a mixture of various operational objectives such as defeating enemy forces and winning the hearts and minds of the people. The field of operations has expanded from the military field to the fields of politics, economy, culture, and people's livelihood. The core essence of the mode of warfare is to "take advantage of chaos" and the main purpose of the war is to win by skill.

2.2 The Practice of the Russian-style Theory of "Hybrid Warfare"

The ability of the Russian military to coordinate and coordinate in the Crimean crisis is a "masterpiece" of the Russian "hybrid war" that is superb. During this period, Russia mainly "mixed" four combat methods, namely proxy warfare, information warfare, cyber warfare, and special warfare. These four new forms of warfare, combined with traditional conventional warfare, constitute the main body of the Russian version of "hybrid warfare".

2.2.1 Proxy Wars

The so-called proxy war refers to Russia's cultivation and support of pro-Russian proxies in Ukraine, fostering pro-Russian political parties and political leaders, shaping political legitimacy, and expanding Moscow's political influence in the region. Before the outbreak of the Ukraine crisis in 2014, Russia had vigorously operated in Ukraine, cultivating pro-Russian forces and setting up intelligence networks. On March 1, 2014, it sent troops to take control of Crimea and participated in the military conflict in eastern Ukraine, which achieved good results.

2.2.2 Information warfare

The purpose of information warfare is to control and guide the direction of public opinion, weaken people's ability to make judgments, and cause confusion in the enemy's thinking. During the Ukraine crisis, Russia invested huge resources, applied globalization tools, combined online and offline, carried out large-scale propaganda activities, and created all kinds of true and false information to cover up the fact that the Russian army intervened in Ukraine, hit the prestige of the Ukrainian government and political leaders, suppress the fighting spirit of Ukrainians, and control and guide world public opinion. For example, when secretly transporting armed forces to Crimea, the Russian army implemented a strict radio silence system, which made it impossible for NATO's intelligence services to detect the movements of the Russian army in time, thus gaining valuable military opportunities.

2.2.3 Cyber warfare

In recent years, with the advent of the intelligent era, network security has attracted attention, and various countries have invested a lot of capital to maintain network security, but they are still inevitably suffering from unknown attacks at home and abroad. The main institutions engaged in cyber warfare in Russia are the Foreign Intelligence Service and the Military Intelligence Directorate of the General Staff "GRU". Since 2014, highly organized Russian "hacker legions" have attacked all areas of Ukraine: including media, finance, transportation, energy, military and political network systems, stealing and deleting data, destroying computers, and paralyzing basic functions. [7] For example, when Russia sent troops to Crimea, Russia carried out a high-intensity cyber attack on Ukraine, resulting in almost all webcams in Crimea and its ports being cut off, news websites in the port of Feodosia being paralyzed by the attack, and the Ukrainian government's official communications network being attacked by a new cyber virus.

2.2.4 Special Operations

The "special" in special warfare does not refer to the special nature of the main body of operations in the traditional sense, but refers specifically to special strategic and tactical arrangements. The "little green men" are the most typical example. Early in the morning of February 27, 2014, a large number of masked armed men dressed in uniforms of green uniforms without any markings, dubbed "little green men" by the international media, appeared on the streets of Crimea. In addition, since April 2014, a large number of unidentified armed men have entered eastern Ukraine, disguised as locals, participating in demonstrations, storming government institutions, and blocking military institutions. NATO's Supreme Allied Commander Breedlove called it an "invisible soldier."

It is undeniable that Russia's "hybrid war" in Ukraine has achieved certain successes, mainly in three aspects: first, backed by military deterrence, at a very small cost, almost without firing a shot, quickly seized Crimea. Second, through the secret dispatch of troops and the support of proxies, it basically controlled the Donbas region. Third, through large-scale information warfare, it has influenced Ukrainian and world public opinion and delayed the decision-making of Ukraine, the EU and NATO. There are two sides to everything, and while Russia has achieved certain successes, anti-Russian and Russophobic sentiments are rising in Central and Eastern European countries.

3. A New Interpretation of the "Hybrid War" between Russia and Ukraine

The most striking aspect of previous wars has been the use of new weapons and the subtle strategic and tactical coordination, but what has attracted attention in the 2022 Russia-Ukraine war is the hybrid of cyber and reality, which is a creative change from the traditional way of warfare. This war can be roughly divided into two typical asymmetric wars at two levels: one is a real-world ground military war between Russia and Ukraine, which mainly takes place within the borders of the Ukrainian state; The other is a new type of war in cyberspace, a new type of cyber warfare and public opinion warfare led by the United States and the West against Russia. The former is an asymmetric war with a huge disparity in military strength and a crushing advantage in Russia's strength, and the latter is an "war" in which the United States and the West are mobilized and mobilized against Russia on a global scale, and it has also formed an asymmetric war with a clear situation.

The author believes that the Russia-Ukraine conflict can be described as the first "hybrid war" in the true sense of the word, with a high degree of integration of "guns" and "pens" and game linkage. That is, there is a high degree of coordination, overall planning, and real-time linkage between the top-down traditional military warfare based on national strength and the bottom-up cyber warfare on a global scale. Compared with the basic form of the "hybrid war" presented before, this "hybrid war" is superior in terms of network participation, public opinion guidance, and scientific and technological integration. At the same time, Russia, which prevailed in the Crimean crisis, at this time no longer seems to be in the posture of a winner.

3.1 The Internet Has Become a New Field for Warfare

The characteristics of low cost, large effect, and difficult traceability give cyber warfare strong stealth and lethality. Before the start of modern warfare, cyber warfare was used to sabotage the target's domestic key information systems, steal intelligence, and even paralyze key infrastructure such as transportation, energy, and finance, and attack military capabilities became the top option. More importantly, this is a mode of warfare in which offensive and defensive resources are extremely asymmetrical. In the digital era, the network defines everything, and any node may become a springboard for attack, which can lead to serious consequences for the whole body.

The cyber warfare of the Russia-Ukraine conflict has the following characteristics: First, cyber attacks occur intensively with the war. In line with the traditional war, Russia has launched three rounds of large-scale and high-level cyber attacks on Ukraine (First round of attacks around January 14, 2022 - WhisperGate Data Eraser; Around February 15, the second round of attacks - DDoS attacks; Around February 21-23, the third round of attacks - HermeticWiper data wiper, malicious document spearphishing attacks, and DDoS attacks.); Second, the use of virtual information to influence psychological cognition. As the conflict between Russia and Ukraine continues to escalate, true and false information on the Internet is spreading overwhelmingly on different language platforms in countries around the world. To this day, most people do not know what the situation of the Russia-Ukraine conflict is; Third, more forces are involved in the cyber battlefield. Under the leadership of the United States, the EU has set up a cyber rapid response team, whose members are cyber experts from the EU and other countries, to help Ukraine carry out cyber attacks against Russia. U.S. intelligence agencies have also recommended that the Biden administration launch a "massive cyberattack" against Russia, including cutting off internet connections throughout Russia, blackouts, and interfering with the operation of railway turnouts. According to reports, many Russian websites, including the Russian Kremlin, the federal government and the Ministry of Defense, have been forced offline due to suspected cyberattacks.

3.2 Public Opinion Warfare Has Become the Main Battlefield of Ideological Conquest

Public opinion warfare refers to the behavior of one side that has the right to speak to attack the opposite side and cause it to suffer damage, the main purpose is to spread false information, attack and destroy the opposite side's ideology, and greatly reduce the opponent's self-confidence in winning the war; Publicizing one's own superiority and the legitimacy of war to promote one's own strong cohesion and win international support and sympathy. For example, in the Russia-Ukraine conflict, Russia tried to deny the legitimacy of the Ukrainian state from a historical perspective, while Ukrainian President Volodymyr Zelensky made better use of social media performances to create a "narrative of difference" and seize the "moral high ground".[8] In addition, the United States and Europe are the "masters" of online public opinion warfare, and in the current Russia-Ukraine conflict, through public opinion warfare, with maximum pressure, economic sanctions, and arms assistance, the role of public opinion has been vividly and vividly expressed.

Drawing on the analysis of relevant scholars on the public opinion war in the Russia-Ukraine conflict, the public opinion war can be divided into the hidden truth before the official outbreak of the war, the preemptive strike in the early stage of the war, and the information monopoly in the stalemate stage of the war. [9] In the three stages, the manifestations of public opinion warfare include, but are not limited to, the following:

First, public opinion attacks are carried out in accordance with the "first cause effect". The first cause effect in psychology refers to the fact that the information that people receive for the first time can have a strong impact on their later cognition and behavior about things, which is often referred to as "preconceived ideas". In a state of war, it is necessary to strengthen the offensive awareness of public opinion, and gather the advantages of network communication to seize the high ground of public opinion. In the Russia-Ukraine conflict, a large number of media controlled by the United States and Western countries and enjoying international discourse rights have automatically hugged together and become a public opinion war machine with Russia as the main target in one fell swoop. Many of the reporting frameworks and rhetoric are the same: seizing the commanding heights of conflict definition and moral criticism, describing Russia's series of military operations as "invasions" and agitating "anti-Russian" and "anti-war" voices. In short, the United States and Western countries have made full use of their own advantages in media discourse to label Russia as an "invader". [10]

Second, use rumors to cause social unrest. In The Psychology of Rumors, G. Allport and L. Postman proposed a formula for interpreting rumors: *Rumor = Importance × Ambiguity*. If the importance of what is said is equal to zero, or if the event itself is clear and the evidence is conclusive, the rumor will not arise. That is to say, the greater the importance and ambiguity of the event, the wider and deeper the rumors will spread. [11] During the Russia-Ukraine war, rumors and disinformation were rife in the online world. Due to the high level of world attention to the Russia-Ukraine conflict, supplemented by the rapidly changing battlefield winds, and the true and false strategies and tactics of Russia and Ukraine, rumors have been mixed with public opinion warfare. The purpose of public opinion warfare is to spread disinformation on a large scale, cause panic in society, and undermine the morale of the military.

Third, public opinion promotes ideological struggle, and even brings the danger of subversion to the ideology of the other side. In the conflict between Russia and Ukraine, the camp of Western countries, led by the United States, maliciously tied China and Russia together, trying to split China's domestic public opinion field in an attempt to slander China while attacking Russia. The United States and other countries have carefully fabricated traps through various Internet platforms, exaggerated the atmosphere of "China's knowledge theory", and spread rumors that China has provided all kinds of help to Russia. At the same time, it generalizes issues, exerts political influence, deliberately releases confrontational and conflicting rhetoric, translates domestic discussions on the Russia-Ukraine conflict into multiple languages and disseminates them on overseas platforms, and undermines China's international image in the field of overseas public opinion. [12]

3.3 Artificial Intelligence Technology Has Become a New Type of Combat Tool

The Russia-Ukraine war is inseparable from the development of artificial intelligence in the widespread development of public opinion warfare and ground warfare. Artificial intelligence is becoming a "new track" in the arms race of major military powers, and intelligent warfare is beginning to take shape. War will help the further development of artificial intelligence in the military field, and the Russia-Ukraine war is such an opportunity, a training ground for artificial intelligence technology. By leveraging information technology from NATO and EU countries, especially the United States, Ukraine is clearly superior to Russia in the use of artificial intelligence in warfare.

First of all, the Ukrainian military has incubated a digital command system-driven "order-taking" combat model. The joint operations command center of the Ukrainian army and the intelligence center of the US military are in the rear, directly controlling and directing the operations of hundreds of Ukrainian battalions, companies and platoons on the front line. The combat of the troops is very flexible and changeable, and the combat mode is similar to the current "order-taking" mode of China's takeaway platform. The combat information platform system will intelligently "send orders" to the appropriate combat units, and the special operations squad of the Ukrainian army relies on digital terminals to obtain battlefield information, and once a target appears on the navigation map, the nearby Ukrainian combat units can judge whether to take the order or not, whether to fight by themselves or jointly with other units. After receiving the order, an ambush war was launched against Russian targets. After destroying the target and completing the task, take a photo with the drone and upload it to the platform, and the platform will reward you according to the results.

Second, the Ukrainian military uses AI to extrapolate the war situation. NATO sends all the collected intelligence and information to the big data center for analysis, and calculates the composition of the Russian army through AI intelligent calculation, such as the number of troops, personnel quality and military equipment, etc., and analyzes the composition of the logistics supply system through big data such as military trade and military orders over the years, and uses this to calculate the offensive route and logistics support route of the Russian army. The Ukrainian army used the best solution given by the AI intelligent staff system to match personnel and equipment to attack the Russian army, destroy the logistics support of the Russian army, and achieve good combat results.

Finally, the Ukrainian military used AI to carry out precision attacks. AI facial recognition technology was used for the first time in the Russian-Ukrainian war, and Lieutenant General Mordvicho, commander of the 8th Russian Guards Army, was the first Russian lieutenant general-level officer to be killed in the Russian-Ukrainian battlefield, and the first senior Russian general to be killed by AI technology. Lieutenant General Moldviggio's location was discovered and located by the opposing side, so he was killed by a long-range attack by precision-guided munitions.

In addition, Ukraine collects information on Russian combatants through drones, roadside surveillance systems, mobile phone users, etc., and then transmits the data to the Ukrainian military command platform in real time for analysis, and then uses AI face recognition technology to determine the identity of prisoners of war in turn, even if they are not wearing combat uniforms, they can be accurately identified. Subsequently, combined with the latest GPS and other geolocation technologies of European and American intelligence departments, it quickly and accurately located and carried out precision strikes.

Russia also uses its own AI system to carry out precise strikes on the Ukrainian army, such as the selfie video sent by the soldiers of the Azov Battalion was discovered by the Russian army, and the AI system was used to calculate the specific location and launch missiles to eliminate it. [13]

4. The Enlightenment of the new Characteristics of the "Hybrid War" between Russia and Ukraine to China's Military Security

The course and final outcome of the Russia-Ukraine conflict have affected the attitude of Western countries led by the United States towards China. As far as China is concerned, from the perspective of the highest national interests and strategy, even in the face of a highly tense international environment and a highly complex domestic public opinion situation, our neutral attitude and position on this conflict are clear, firm, and unshakable, and so far appropriate. The most urgent task for China at present is to take precautions, that is, to analyze the current situation of the latest "hybrid war" and to prepare for a possible war in the future.

The author believes that the battlefield domain between the two sides in the Russia-Ukraine conflict stage is concentrated in the network, public opinion, artificial intelligence technology, etc., showing a development trend of unmanned and bloodless warfare in the future. With the horizontal and vertical development of high and new technology, the emergence of unmanned fighters, unmanned warships, and unmanned submarines is only a matter of time. Bloodless refers to the development of information warfare and public opinion warfare, which aims to attack and reverse the ideology of the enemy, and with the addition of multiple subjects in public opinion warfare, it is no longer difficult to destroy the enemy's will and subvert the ideology.

4.1 Responding to the New Situation - Accelerating the Transformation and Development of China's Military Forces

The Russia-Ukraine conflict is essentially a contest between major powers, with the United States behind the scenes, and even occasionally going to the front of the curtain to engage in a direct confrontation with Russia in terms of scientific and technological strength. From the perspective of suppression and containment, in addition to Russia, China is also a "target" of the United States. In recent years, Western countries, led by the United States, have spared no effort to spread the "China threat theory" in the international community, and even called China "the most severe long-term challenge to the international order." The Russia-Ukraine conflict can be regarded as a rehearsal, allowing us to see our own capacity shortcomings, institutional shortcomings, and practical dilemmas in dealing with the real ideological international game. In other words, the greatest significance and enlightenment of this conflict for China is mainly aimed at the changes in the form and mode of warfare under the new situation, the need to gain insight into the new laws and characteristics, and to deeply reflect on the military security issues caused by it. In the face of severe threats and challenges, we must make the whole society clearly understand the reality and essence of international competition, and while strengthening military deterrence, we should upgrade the strategy, tactics, methods, and means of dealing with hybrid warfare with the mentality of "preparing for war."

Tremendous changes have taken place in the combat objects, combat means, and battlefield environment of "hybrid warfare," which will inevitably lead to the future transformation of China's military strength. First of all, in the use of military force, it is necessary to attach importance to the use of conventional military forces and traditional strategic resources and means, as well as to the use of irregular military forces, information, networks, and other non-traditional resources and means. Second, in the area of army building, more attention should be paid to building a joint force that can adapt to a variety of tasks and is balanced and multi-capable. The building of the armed forces should develop in the direction of high efficiency and multi-functionalization, and the military forces are faced with the practical needs of transforming and upgrading from general-task units to multi-task forces. By increasing the proportion of unconventional military forces such as special operations and information operations, our military forces will be able to better cope with "mixed threats" and adapt to "full-spectrum operations." Finally, in terms of capacity building, guided by the theory of "hybrid warfare," the armed forces should be strengthened in their ability to adapt, react, attack, and survive in ordinary military training and military exercises, to strengthen operational coordination and the flexible use of tactics, and to enhance their rapid reaction capability and irregular combat capability.

4.2 Dealing with Unmanned: Strengthen the Practical Practice of Cyber Warfare and Public Opinion Warfare

The research, judgment and strategic deployment of network warfare and public opinion warfare cannot stop at the theoretical level, but need the development of high and new technologies and the shaping of military public opinion platforms.

First, the effectiveness of cyber warfare is inseparable from high technology and artificial intelligence. Through the analysis of the specific situation of the Russia-Ukraine conflict, it can be clear that self-reliance and self-improvement in science and technology are the strategic support for national development. Focusing on the shortcomings of key core technologies related to public opinion warfare and information warfare, especially the foundation of chips, operating systems, databases, industrial software, and other foundations, we should coordinate resources such as national science and technology plans and national laboratories, and pool the superior forces of key enterprises, institutions of higher learning, and research institutions to jointly tackle key problems and break through bottlenecks as soon as possible. At the same time, we will expand the supply chain of short-board technology products in the international market to ensure that there are alternatives under extreme conditions. Implement actions to improve the capacity of critical information infrastructure, improve security protections for financial, energy, electric power, communications, transportation, and other facilities by level and category, establish emergency control over new Internet technologies and applications with strong mobilization capabilities, and accelerate the construction of a safe and controllable autonomous domain name resolution system with China as the mainstay, to ensure the normal operation of the Internet within the territory.

Second, China must build a distinctive military public opinion propaganda platform. The development of the public opinion war between Russia and Ukraine has further made us realize the importance of grasping the international discourse in the new type of war. In wartime, the influence of the mainstream media can be translated directly and quickly into effective war mobilization and political advocacy. China's mainstream media exists and the people's trust is high, what needs to be done is: first, face the world, pay attention to the construction of a global communication platform, carefully study the laws of public opinion warfare, constantly strengthen and reform communication methods, tell Chinese stories well, and win the hearts of the people. Only by taking precautions and actively preparing for the war of public opinion in a high-tech war that may occur in the future can we be invincible. [14] Second, it is necessary to strengthen international exchanges and cooperation, establish stable distribution channels in the global media, actively convey their own voices, and break the monopoly of the Western media. In order to meet the needs of wartime in the future, we should establish a complete wartime public opinion dissemination system in peacetime, so that it can be quickly put into operation when war breaks out.

4.3 Dealing with Bloodlessness–Winning the People's War of Ideology

In the Russia-Ukraine conflict, the most serious mode of combat against ideology is cognitive domain warfare. Cognitive warfare is to destroy the sense of belief of other armies in the country, to undermine the self-confidence of other armies in victory, and to make other armies and all citizens doubt the rationality of waging war.

In order to win the cognitive domain war, China needs to do the following two things:

First, we must recognize the importance of new infrastructure. Warfare in the era of intelligence needs to be built on new infrastructure, such as the world's leading basic software and hardware, global social media platforms, and real-time situational awareness monitoring systems. Future warfare is based on a series of normalized infrastructure construction, and infrastructure is a support system and capability system, which should be based on a long-term perspective, laid out in advance, carefully planned, and continuously established. In addition to traditional mass media platforms, the guidance and influence of the world's top influencers, opinion leaders and mass user groups should also be regarded as daily infrastructure construction work.

Second, the importance of ideology must be clarified. [15] Ideological and political work in the ideological field is the lifeline of our organization and the army, and it is a matter of life and death. First of all, persisting in guiding the whole army and arming officers and men with scientific theory is the basic experience of building and administering the army. The members in the military must build a solid foundation of faith, replenish spiritual calcium, and stabilize the ideological rudder. Second, we should always rely on the leader's strong ideological leadership to strengthen the cultivation of the military soul. Integrate the education of the military soul into major military activities such as emergency rescue and disaster relief, stability maintenance and emergency handling, joint training and joint exercises, and integrate it into the political life and core organization of our country's spirit training within the organization, so as to protect the "lifeblood" of the organization's absolute leadership over the army, and achieve absolute loyalty, absolute purity, and absolute reliability. Finally, we will carry out the educational activities of "studying and implementing our country's Constitution and carrying forward the fine style" and the country's mass line education and practice activities. Strengthen the unity between the military and the government and the army and the people, gather the majestic force of "the army and the people are united as one person, and try to see who can be the enemy in the world," and trap the enemy in the vast sea of the people's war.

5. Conclusion

The "hybrid war" between Russia and Ukraine has sounded the alarm for countries around the world, fully demonstrating that the form of war is no longer confined to the traditional and physical strategic and tactical coordination, the dimension of war has been expanded, and new terms such as network warfare, public opinion warfare, and information warfare have entered the field of vision of military doers and theorists, and China's war theory has not surprisingly been impacted.

In the face of "hybrid war", we must summarize and analyze the experience and lessons of the Russia-Ukraine conflict, and prepare for the future war that China will face.

References:

[1] Gao Kai, Zhao Lin. "Hybrid warfare"—Russia's new strategic game means. Military Digest, 2019, (13): 10-13.

[2] Duan Junze. The Practice of Russian-style "Hybrid Warfare" and Its Impact. Contemporary International Relations, 2017, (03): 31-36.

[3] Wang Xiangsui. Hybrid warfare is an important tool in the current international political game. Economic Tribune, 2018, (11): 10-14.

[4] Peter Schweizer, trans. Yin Xiong. How did the Reagan administration bring down the Soviet Union. Beijing: Xinhua Publishing House, 2001.

[5] Anwen. The forerunner of hybrid warfare: General Gerasimov, Chief of the General Staff of the Russian Armed Forces. Military Digest, 2021, (13): 74-79.

[6] Liu Jiwei, Zhang Chang. Analysis of Russian Military Strategy Adjustment from the Perspective of "Hybrid War" Theory. Journal of Jiangnan Social University, 2019, 21 (02): 47-52.

[7] Han Kedi. Russia's hybrid war in Ukraine. Strategic Decision Research, 2021, 12 (06): 51-80+101-102.

[8] Fang Xingdong, Zhong Xiangming. Algorithmic Cognitive Warfare: Paradigm Shift of Public Opinion Warfare in the Context of Russia-Ukraine Conflict. Media Observer, 2022, (04): 5-15.

[9] Wang Lin. The war of public opinion in the Russo - Ukrainian War and its enlightenment. Academic Exploration, 2022, (09): 73-79.

[10]Zhang Xuekui. Under the new crown epidemic, 11 golden rules of public opinion communication. (2020-5-15) [2022-10-4]. https://China.chinadaily.com.cn/a/202005/15/WS5ebe3373a310eec9c72b92c1.html.

[11]Ding Xiaohang, Ding Hui, Liu Yupeng, Xiao Yawen. Russia-Ukraine information war, the war behind the war. Global Times, 2022-02-28 (007).

[12]Li Long, Ma Lu Yao, Miao Lina. Shift of contest fields: war of public opinion on fifth-dimension field in Ukraine-Russia

conflict. Media Observation, 2022, (09): 65-72.

[13]Geng Haijun. AI war game behind Russia-Ukraine conflict. China Reading News .2022-07-13 (018).

[14]Liang Wei. Media war of public opinion: the strategic measure of modern warfare. Strategic Decision Research, 2010, 1 (04): 46-49.

[15]An Ziqian. Past Practices and Present Revelation of Political Works in Soviet and Russian Military. Military History, 2020, (06): 83-92.