**The impact and enlightenment of cyberspace confrontation in the Ukrainian crisis**

Source: Russian, Eastern European and Central Asian Studies, Issue 3, 2023

Author: Wu Qiong

Editor: Li Xiang

2023-06-06

<https://www.cssn.cn/qygbx/202306/t20230606_5642969.shtml>

**Abstract:** After the outbreak of the Russian-Ukrainian conflict, the two sides launched a fierce contest in cyberspace. The cyberspace confrontation in the Russian-Ukrainian conflict is mainly reflected in two aspects: on the one hand, national cyber forces and non-state hacker organizations "take sides"; on the other hand, the control and competition around mainstream media and social platforms are becoming increasingly fierce. The Russian-Ukrainian cyberspace confrontation has three impacts: first, the strategic stability of both sides is impacted; second, it affects the form of war and combat style; third, the spillover effect forces countries to build a strong cyber security protection barrier. In the face of the cyberspace confrontation in the Russian-Ukrainian conflict, China should learn lessons from it and take the following four countermeasures: first, use big data technology to screen sensitive data from massive data and establish its own data advantage; second, promote the introduction and training of artificial intelligence talents; third, strengthen the construction of cognitive warfare forces; fourth, enhance cyberspace defense and deterrence capabilities and protect the security of critical information infrastructure.

**Keywords:** Russia-Ukraine conflict; cyber warfare; cognitive warfare; artificial intelligence; non-state actors

**About the author:** Wu Qiong, doctoral student at the Institute of International Relations, Nanjing University.

**Funding information:** This paper was supported by the “Nanjing University Outstanding Doctoral Student Innovation Ability Improvement Program B”.

　　[Citation Information] Wu Qiong: "The Impact and Implications of Cyberspace Confrontation in the Ukrainian Crisis", published in "Russian, Eastern European and Central Asian Studies" No. 3, 2023, pp. 84-104.

    On February 24, 2022, Russian President Vladimir Putin announced a special military operation, and the Ukrainian crisis escalated comprehensively. The two countries have launched a fierce competition in cyberspace, and its actual heat is no less than the smoke and rain of bullets on the battlefield. Existing research mainly focuses on the weaponization of cyberspace in the Russian-Ukrainian conflict, the use of deep fake technology, the competition for social platforms, and the impact on the global cybersecurity space. These research results have important implications for understanding the Russian-Ukrainian cyberspace confrontation and its impact, but there is still room for further supplementation and improvement: First, although existing research has paid attention to the global impact of the cyberspace confrontation in the Russian-Ukrainian conflict, the analysis of its impact at the international relations and international strategic levels (such as new forms of war and their impact) still needs to be strengthened; second, in the face of the Russian-Ukrainian cyberspace confrontation, the research on China's cybersecurity response strategy needs to be expanded. In view of this, this article first explores the main manifestations of the cyberspace confrontation in the Russian-Ukrainian conflict, then analyzes the main impact of the cyberspace confrontation in the Russian-Ukrainian conflict, and finally discusses the enlightenment brought by the Russian-Ukrainian cyberspace confrontation.

**I. Main manifestations of cyberspace confrontation in the Russia-Ukraine conflict**

　　As the fifth space alongside land, sea, air and space, cyberspace has become an important battlefield for Russia and Ukraine to engage in game and struggle. As the conflict continues, the cyberspace confrontation between the two countries has also entered a white-hot stage.

　　1. National cyber forces and non-national hacker groups “choose sides”

　　In recent years, major countries in the world have established cyberspace forces and accelerated the development of cyberspace combat equipment in order to seek strategic initiative. In the Russia-Ukraine conflict, national-level cyber forces have appeared one after another and launched a series of fierce confrontations in cyberspace.

　　First, the national cyber force from Russia. On April 12, 2022, the Ukrainian Computer Emergency Response Team (CERT-UA) and the cybersecurity company ESET issued an announcement that the hacker group "Sandworm" used a malware called "Industroyer2" to attack Ukrainian power facilities. "Industroyer2" is a fully modular platform with attack payloads for multiple industrial control system (ICS) protocols. It drives the operation of malware by hard-coding detailed information in the main body of the program. According to the Wall Street Journal, this malware is similar to the malware used in a power grid attack in 2016 and is believed to be the work of the hacker group "Sandworm" under the Russian General Staff Intelligence Directorate. Andy Greenberg believes that "Sandworm" actually serves the Russian military intelligence department and is a highly complex, technically sophisticated, state-supported cyber force with the most destructive malware that can carry out offensive cyber attacks on critical information infrastructure such as electricity, energy, and transportation. Although the Russian government has denied this, Western countries believe that "Sandworm", which belongs to the Russian military, is the mastermind behind the cyber attack on Ukraine.

　　Second, the national cyber forces from Ukraine and the United States. After the outbreak of the Russian-Ukrainian conflict, the Ukrainian cyber police force launched cyber attacks on the Russian Federal Investigation Committee, the Federal Security Service and state-owned banks, and achieved remarkable results. The Ukrainian "IT Army" actually also has a certain national hacker organization color. In the face of Russia's special military operations, the Ukrainian government called on civilians to join the Ukrainian "IT Army" to protect the critical information infrastructure in Ukraine and carry out cyber attack missions against Russia. On the surface, the Ukrainian "IT Army" is a civilian hacker organization, but Stephen Sosanto, a senior researcher at the Security Research Center of the Swiss Federal Institute of Technology, believes that the Ukrainian "IT Army" is a hacker army with clear goals, clear commands and strict organization. Its core members are closely related to Ukraine's defense and intelligence systems, or may be composed of personnel from its defense and intelligence systems. In an exclusive interview with a reporter, a senior manager within the Ukrainian "IT Army" once said that the core leadership of the organization is in the hands of Ukrainian "professionals"; although its members come from all over the world, most of them are Ukrainians. Some Chinese scholars also believe that some hacker organizations in the Russian-Ukrainian conflict seem to be civilian organizations, but they are obviously closely related to government departments in terms of organization and ideology. Soon after the Ukrainian "IT Army" was formed, it launched a cyber attack on Russia. According to data from Russian cybersecurity company Kaspersky, the duration of distributed denial of service (DDoS) attacks in the second quarter of 2022 was about 3,000 minutes, nearly 100 times the average of 30 minutes in the second quarter of 2021. The Russian Ministry of Foreign Affairs pointed out that hacker groups led by the Ukrainian "IT Army" regularly launch distributed denial of service attacks on Russia's critical information infrastructure.

　　In addition, the U.S. Cyber ​​Command and the National Security Agency are sending national-level cyber forces to intervene in the Russia-Ukraine conflict. On June 1, 2022, Admiral Paul Nakasone, commander of the U.S. Cyber ​​Command and director of the National Security Agency, said in an interview with reporters that the United States is sending cyber forces to carry out offensive cyber operations against Russia to support Ukraine. Although Nakasone did not explain the details, the remarks once sparked widespread heated discussions due to the sensitivity of offensive cyber operations. In fact, Nakasone also privately revealed that offensive cyber activities against Russia would prevent it from carrying out more effective cyber attacks. Gary Corn and Gary Brown, former legal advisers to the U.S. Cyber ​​Command, and others said that the offensive cyber operations mentioned by Nakasone should include a combination of reconnaissance and offensive activities. Even if the cyber operations taken by the United States against Russia are acts of armed attack, it will not provide an excuse for Russia to attack the United States.

　　The Russia-Ukraine conflict has spawned an unprecedented form of cyber guerrilla warfare: a large number of non-state actors can independently carry out cyber operations without the coordination of national military institutions, and their involvement in the war is astonishingly deep.

　　First, non-state hacker groups that support Russia, mainly including Conti, Zatoichi, Killnet, XakNet, etc. Take Killnet as an example. "Many Russians regard Killnet as a hero. The organization is good at using videos or images to publicize the results of the attack on social platforms, intending to make Europeans pay for their clear support for Ukraine and punish Western governments for their anti-Russian sentiment." In previous cyber attacks, Killnet mainly used distributed denial of service attacks to send a large number of requests, causing computer systems to overload or paralyze, making it unable to provide normal network services. On May 16, 2022, Killnet officially announced the launch of a cyber war against ten countries including the United States, Britain, Germany, Italy, Romania, Latvia, Estonia, Lithuania, Ukraine, and Poland on the grounds of "Russophobia." On August 10, 2022, Killnet announced the intrusion into the website of Lockheed Martin, causing the company's employee authorization system, NASA card and RSA authorization system to collapse, and the information of all job seekers in the company was hacked.

　　Second, non-state hacker groups that support Ukraine mainly include Anonymous, Ghostsec, Against the West (ATW), SHDWsec, etc. Take Anonymous as an example. According to statistics, it has attacked at least 2,500 Russian websites. The units attacked by it mainly include the military, central bank, aerospace departments, oil and gas companies, property management companies, broadcasting companies, IT companies, law firms, etc. The leaked data is quite large and may take years to verify. On June 4, 2022, Anonymous announced that it had invaded Rustam Kurmaev and Partners, a top Russian law firm, and stole a large amount of data such as emails, court documents, and client files. At present, the stolen data has been made public on DDoSecrets. Anonymous' cyber attacks on Russia are mainly divided into four categories: First, publicizing important data, attacking and publishing data obtained from entities such as the Russian State Space Corporation and Russian Energy Company. Second, attacking companies doing business in Russia and increasing the risk of companies operating in Russia by launching distributed denial of service attacks. The third is to hijack media services and undermine Russia's censorship system by hacking into Russian state television. The fourth is to carry out propaganda, such as sending anti-war and pro-Ukrainian messages through the Russian social networking site VK.

　　2. The competition for control over mainstream media and social platforms is becoming increasingly fierce

　　Mainstream media and social media platforms, with their huge user base, massive amounts of media data and extremely fast update speed, have become invisible tools for describing the course of war and influencing the direction of war. Based on this, the competition in this field is becoming increasingly fierce.

　　First, Western countries, national groups, and large Internet companies have issued a comprehensive "ban order" on Russian state-owned media. Western countries and national groups have used their digital technology advantages and media discourse power to completely block Russia's war propaganda. Western countries such as the United States, Australia, Spain, France, Germany, Canada, the United Kingdom, and Latvia have announced a blockade of Russian state-owned media, prohibiting Russia Today (RT) and Sputnik from broadcasting in their territories. The European Union requires EU countries not to broadcast programs of Russia Today and Sputnik TV channels and satellite operators. Large Internet companies are also actively cooperating with the United States and other Western countries in their sanctions against Russia. Companies such as Google and Meta followed the EU ban, banned access to Russia Today and Sputnik in Europe, closed their official accounts on YouTube, Facebook, and Instagram in Europe, and restricted advertising in Russian official media. Faced with the aggressive offensive posture of the United States and other Western countries, Russia has not been outdone and has taken a series of countermeasures: first, it blocked Facebook, stepped up censorship of information posted on YouTube and Telegram in Russia, listed "Meta" in the list of terrorist and extremist organizations, and fully recommended the Russian version of Facebook VK, the Russian version of YouTube Rutube, and the Russian version of TikTok Yappy; second, it signed the amendment to the Criminal Code of the Russian Federation, which stipulates that those who deliberately spread false information about the Russian army may be sentenced to up to 15 years in prison; third, it banned media such as Voice of America, BBC, Radio Free Europe, Latvian "Meduza" News Network, and Deutsche Welle, condemning these organizations for deliberately spreading false information about the Russia-Ukraine conflict; fourth, it cracked down on the use of VPNs and announced the establishment of a database to collect mobile phone IMEI codes.

　　Second, using mainstream media and social platforms to release mixed news. First, release relevant information through mainstream media. Russia mainly uses domestic mainstream media to expose the various war crimes committed by the "Azov Battalion" and the establishment of biological laboratories by the United States in Ukraine to promote the legitimacy of the war and win public support. According to the Russian Satellite News Agency, the "Azov Battalion" is a combat unit of the Ukrainian National Guard, directly led by the Ukrainian Ministry of Internal Affairs, and has neo-Nazism and white supremacist characteristics. Members of the "Azov Battalion" committed various shocking war crimes when fighting pro-Russian armed forces in the Donbas region, including imprisoning and persecuting local residents, so the existence of this unit is one of the main motivations for Russia to implement special military operations.

　　Second, they use social platforms to release various sympathetic or violent and terrifying information, such as a Ukrainian girl singing "Let It Go", the theme song of the movie "Frozen", in a bomb shelter in Kyiv, a large number of Ukrainian people taking refuge in subway stations, and the images of the Bucha incident. It should be pointed out that Zelensky is good at using social platforms to release "anti-Russian" and "anti-Russian" information. Zelensky once released a cleverly edited video. The beginning of this video partially shows the prosperous economic construction, social development and people's lives in Ukraine before the Russian-Ukrainian conflict. However, the picture immediately turned and switched to a war picture with a strong visual impact. The middle and latter half of this video records the scene of fire, smoke and explosions after the Russian army used missiles to attack Ukrainian cities, and shoots a large number of local civilians and displaced children injured by the war from different angles.

　　At the same time, a large amount of misleading and out-of-context false information is being widely spread on social platforms. For example, the "Thirteen Warriors of Snake Island" refused to surrender in the face of a large army, a Ukrainian man bid farewell to his wife and daughter in tears before going to the battlefield, and the Russian army broke into the US military laboratory in Ukraine and rescued thousands of children. A video of a Ukrainian man bidding farewell to his wife and daughter in tears and preparing to go to the front line to fight the Russian army went viral on social platforms, with 7 million views in just one day. But the fact is that the man is a pro-Russian person in the Donbas region. In order to ensure the safety of his family, he chose to send them to Russia, and he himself joined the battle with the Ukrainian army. Another example is a video of the Russian army breaking into the US military laboratory in Ukraine and rescuing thousands of children. But in fact, the video is an image of children injured in the Syrian civil war in 2018 being treated in a hospital, and has nothing to do with the Russian-Ukrainian conflict.

　　The third is to use high-tech means to create and spread false information. One is to use social robots to spread false information. Social robots refer to automated programs that imitate normal users to operate autonomously and publish text, pictures, audio, video and other content on social platforms. On March 28, 2022, the Ukrainian National Security Service reported that since Russia launched a special military operation, the Ukrainian National Security Service has discovered and closed five social robot farms. These robot farms with more than 100,000 social platform accounts mainly operate in the four regions of Kharkiv, Cherkasy, Ternopil and Zakarpattia, aiming to create panic by spreading false information and affect the stability of the social situation. On August 2, 2022, the Ukrainian National Security Service stated that it had closed robot farms operating in Kiev, Kharkiv and Vinnitsa. These robot farms rely on 1 million social platform accounts to spread false information, aiming to undermine the social and political situation in Ukraine.

　　The second is to spread false information with the help of video synthesis technology. Shortly after the outbreak of the Russian-Ukrainian conflict, a video about the "Ghost of Kiev" was widely circulated on social platforms. A Ukrainian Air Force pilot shot down 6 Russian fighter jets on the first day of the war, and set a "result" of shooting down 40 Russian aircraft alone, and was called the "Ghost of Kiev" by the outside world. Former Ukrainian President Poroshenko, the Ukrainian Ministry of Defense, the National Security Agency and the Air Force actively forwarded the relevant videos and continued to exaggerate their aerial "achievements". The Ukrainian Air Force Command even stated that the "Ghost of Kiev" is a "superhero legend" for Ukrainians and the "collective image" of all pilots of the 40th Tactical Aviation Brigade of the Ukrainian Army. However, Reuters and Deutsche Welle and other media found that the video of the "Ghost of Kiev" shooting down Russian fighter jets actually came from a computer game called "Digital Combat Simulator World" (DCS), and the clips were spliced ​​using video synthesis technology.

　　The third is to use deep fake technology to create fake videos. Deep fake technology refers to intelligent processing technology that tampers with original sounds, images, and videos through deep learning algorithms. After the Russian-Ukrainian conflict, fake videos about Putin and Zelensky went viral on social platforms. A fake video about Putin appeared on social platforms. In this fake video, Putin said that we will reach a peace agreement with Ukraine; Ukraine borders Donetsk and Luhansk, which are recognized borders by the world; we also signed a five-year roadmap to make Crimea an independent republic within Ukraine. At the same time, a fake video about Zelensky was also circulated on social platforms. The content of the video is to call on Ukrainian soldiers to lay down their arms, surrender to Russia, and return to their families. In fact, Putin and Zelensky never said these words. In the video, the audio and mouth movements of the two were completed using deep learning algorithms.

**II. The main impact of the cyberspace confrontation between Russia and Ukraine**

　　As important geostrategic players and geopolitical pillars on the Eurasian continent, the cyberspace confrontation in the Russia-Ukraine conflict has not only exacerbated the conflict between the two countries, but its impact on the global cyberspace security situation is also becoming increasingly apparent.

　　1. The strategic stability of both sides has been impacted

　　The concept of strategic stability originated from the interactive practice of mutual nuclear deterrence between the two superpowers, the United States and the Soviet Union, during the Cold War. After the end of the Cold War, the concept of strategic stability has shown a trend of continuous development and deepening. In a broad sense, strategic stability refers to the basic situation in which the interactive relationship in the international system is relatively stable, the behavior pattern is predictable, and it is difficult to have an offensive advantage. Among them, the strategic stability of cyberspace is very important, which is related to the national security and homeland security of various countries, and is also closely related to global peace and development. With the rapid development and continuous popularization of network information technology, cyberspace superpowers have influenced the situation and changed the behavior of their opponents by launching provocative cyber actions, preemptive cyber strikes, and even destructive cyber attacks, but at the same time, it will also weaken strategic stability and affect national and international security.

　　Before the outbreak of the Russia-Ukraine conflict, Russia continued to increase its strategic investment in offensive cyber forces, and its comprehensive cyber strength and cyber attack capabilities should not be underestimated. Russian military experts and senior generals believe that given the importance of cyberspace security, if one wants to gain a cyberspace advantage over competitors, taking a preemptive strike is an important part of it, and even the most likely way to win. Lieutenant General Alexander Rakhmanov, then deputy dean of the Russian Missile and Artillery Academy, once pointed out that the Russian army should adopt a "network-centric" war model in regional conflicts. Once a conflict occurs, it should preemptively suppress or destroy the enemy's network system to achieve information advantage. Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, believes that in order to cooperate with the offensive operations of ground forces, the Russian army should first adopt covert military means in regional conflicts, including offensive cyber attack operations and secret raids by special forces. Among them, conducting offensive cyber attack operations can help destroy important dual-use military and civilian infrastructure of the enemy in a short period of time and weaken its war potential. On the day the Russian-Ukrainian conflict broke out, Russia’s national cyber forces successfully deployed more destructive malware than the rest of the world’s cyber powers typically use in a given year, targeting key sectors such as the Ukrainian government and military, defense industry, energy, and electricity. Since then, Russia has continued to deploy destructive malware in cities such as Kiev and Kharkiv, backed by a arsenal of cyber tools. As the Russian-Ukrainian conflict continues, Russia’s national cyber forces will be in a permanent state of readiness and ready to support tactical and strategic objectives on the battlefield in Ukraine at any time according to notification from their superiors.

　　Facing cyber attacks from Russia, Ukraine alone cannot resist. In fact, Ukraine's cyber defense measures are quite backward. In order to enhance its cyber defense capabilities, the Ukrainian government has started cyberspace security cooperation with the United States and other Western countries since 2015. With the help of NATO, the U.S. European Command, the U.S. Army and the Navy, the cyber defense capabilities of important departments such as the Ministry of Defense and the Ministry of Internal Affairs of Ukraine have been substantially improved. The cyber technology support of the United States and other Western countries has played an irreplaceable role in protecting Ukraine's cyberspace security. After the outbreak of the Russian-Ukrainian conflict, although Western countries did not send large-scale ground troops to Ukraine to fight, in cyberspace, Western governments and technology and cybersecurity companies directly confronted Russia and were committed to taking measures to protect the critical information infrastructure and data security in Ukraine. According to Nick Beecroft's research, this is mainly reflected in the following six aspects: First, sending cybersecurity personnel to Ukraine, such as the US Cyber ​​Command's "hunt forward" operation and the EU's launch of a cyber rapid response team; second, conducting cybersecurity operations remotely, such as the United States and Britain funding the private sector to provide cybersecurity services to Ukraine, and cybersecurity companies providing security services to Ukrainian users; third, sharing intelligence such as attack activities, enemy tactics and strategic assessments, such as the US government departments sharing cyber intelligence with Ukraine, and cybersecurity companies establishing a mechanism for rapid intelligence sharing with Ukraine; fourth, providing training, institutional building and policy coordination, such as the United States and Ukraine conducting joint training and absorbing Ukraine into NATO's Cooperative Cyber ​​Defense Center of Excellence (CCDCOE); fifth, providing hardware and technical measures to address network vulnerabilities, such as Western governments donating hardware and SpaceX providing "Starlink" satellite communication equipment; sixth, enhancing robustness and resilience through cloud services, such as helping Ukraine migrate public and private institution data to the cloud.

　　The Russian military leaders initially expected the Russia-Ukraine conflict to be a short-term war that could be ended quickly with a "blitzkrieg" of unstoppable force, so Russia did not launch destructive cyber attacks on Ukraine, mainly hoping to keep Ukraine's critical information infrastructure intact for use after the conflict. However, as it fell into a protracted war and a war of attrition, Russia's national cyber forces are launching a full-scale offensive cyber attack on Ukraine's critical information infrastructure. A "full-scale cyberwar" is enveloping Ukraine. So far, the strategic stability of Russia and Ukraine in cyberspace has been seriously unbalanced, and is showing an increasingly intensified trend.

　　2. Impact on War Forms and Combat Styles

　　As human society enters the digital age, the far-reaching impact of the Russian-Ukrainian cyberspace confrontation on the international security field is changing the traditional war form and combat methods. The deep involvement of non-state actors, the extensive use of cognitive warfare, and the close integration of cyberspace and physical space will not only completely change the traditional war model, but also play an increasingly greater role in future wars.

　　First, the involvement of non-state actors in cyberspace is shaping a new style of warfare. Compared with state actors, non-state actors are not only not restricted by rules, but also have more diverse and rich strategic and tactical options. This means that non-state actors have the capital to win big with small and to defeat the strong with the weak. As the weaker party, non-state actors can confront state actors through provocation, mobilization, consumption, etc., which will lead to changes in the form of war. In the Russia-Ukraine conflict, non-state actors represented by large Internet companies, small technology companies and civilian hacker organizations not only significantly affect the battlefield process and change the comparative situation of national military forces, but also expand the space field of traditional war forms and create new war styles. Taking non-state hacker organizations as an example, in conventional military conflicts including cyber warfare, both sides of the war basically follow a combat style called "command-control", that is, commanders not only determine military targets when performing tasks, but also have supervision and command over combat troops. Without such a command structure, conflicts between countries may become a melee, because different units and even individuals will independently choose their targets. However, in the Russian-Ukrainian conflict, the cyber volunteers supporting Ukraine and the pro-Russian hacker groups will independently decide, plan and execute any attacks on the critical information infrastructure of the two countries. The cyber attacks of the Ukrainian cyber volunteers on Russia will prompt the pro-Russian hacker groups to retaliate. Similarly, the cyber attacks of the pro-Russian hacker groups on Ukraine will also prompt the Ukrainian cyber volunteers to launch revenge actions. The follow-up investigation of The Washington Post shows that these non-state hacker groups have three characteristics: first, they voluntarily carry out various cyber attacks without asking for any rewards; second, they provide the relevant infrastructure themselves and carry out various cyber attacks outside of work and family life; third, they do not receive guidance or help from Ukraine or other government agencies.

　　As far as the Russian-Ukrainian conflict is concerned, the widespread involvement of non-state hacker groups has become an important part of the cyberspace confrontation between Russia and Ukraine. Cybersecurity experts Joseph Max and Aaron Schaffer believe that most of the known cyber operations against Russia and Ukraine are carried out voluntarily by non-state hacker groups, rather than working directly for the two governments. According to the current development trend, non-state hacker groups will play a decisive role in future conflicts, especially when the public widely sympathizes with one side, so that a large number of hackers with network technology are willing to provide help. Gunnar Karlson, former director of the Swedish Military Intelligence Agency and retired Major General, predicts that more such free shadow wars will be seen in cyberspace in the future. Countries that cannot afford large-scale armed forces can wage wars at a low cost by calling on volunteers to join the shadow army. For the younger generation, this will become a natural way to participate. Unlike the traditional level, where countries mobilize overall forces and resources to coordinate and command military operations, non-state hacker groups with complex factions and loose organizational command structures are creating a new way of fighting: autonomously launching cyber attacks on targets at any time, any place, and any location, even if such attacks may violate international rules and domestic laws.

　　Second, cognitive warfare based on social platforms is affecting the course and key trends of war. With the rapid development and widespread use of new-generation information technologies such as 5G, big data, and artificial intelligence, the battle space is accelerating its transformation from the physical domain and information domain to the cognitive domain. Cognitive space is becoming the main battlefield for strategic competition among major powers. Unlike traditional military missions, "cognitive warfare uses people's minds as a battlefield, attempting not only to change people's ideas, but also to change their way of thinking and behavior patterns. Successful cognitive warfare will shape and influence the beliefs and behaviors of individuals and groups, thereby supporting the tactical and strategic goals of the attacker. In extreme cases, cognitive warfare may divide the entire society to weaken the enemy's will to resist."

　　Cognitive warfare in cyberspace has become an important part of the Russia-Ukraine conflict. Russia and Ukraine are using social platforms as a basis to interfere with each other's audiovisual, disrupt each other's thinking, and guide international public opinion, which can be regarded as a new form of warfare and an advanced combat style. During the Russia-Ukraine conflict, while all parties released real information to publicize their own positions and define the legitimacy of the war, they also released a large amount of false information to induce opponents to make strategic misjudgments and build an international public opinion environment that is favorable to them. Specifically, the creation and transmission of false information to opponents through pictures, videos, etc. can lead to the spread of rumors on social platforms, which helps to soft-kill the enemy's thinking, will, psychology and other intangible targets, and spread their own emotional attitudes and values, and shape a public opinion atmosphere that is favorable to them, so as to achieve the purpose of influencing the opponent's command decision-making and even interfering with the course or direction of the war. Especially with the rapid development of 5G networks and the widespread use of social platforms, these errors and false information will spread rapidly on various social platforms at an unprecedented speed. As Peter Singer and Emerson Brooking pointed out, social platforms used to be a place for people to connect with each other in a relaxed and pleasant way, but now they have evolved into a highly weaponized battlefield. Whether it is the world's most powerful sovereign states or the insignificant ordinary people, social platforms are becoming a weapon in their hands. To this end, they will spread and widely disseminate various false information including conspiracies and lies on social platforms in order to create a public opinion environment that is favorable to their own country and defeat their opponents with soft means.

　　From the widespread spread of fake videos such as "Ghost of Kiev", "Thirteen Warriors of Snake Island", and Ukrainian men being drafted into the battlefield and tearfully bidding farewell to their wives and daughters on social platforms, it can be found that Ukraine and Western countries are working together on the "battlefield without gunpowder smoke", using anti-Russian and pro-Ukrainian information as an important weapon to incite Ukrainians' hatred and anger towards Russia, so as to win the sympathy and support of the international community at the first time. Facts have proved that in the Russian-Ukrainian conflict, relying on the highly developed Western mainstream media and major social platforms, Ukraine has an advantage in the cognitive war, while "Russia is losing the cognitive war". The New York Times commented that since the outbreak of the Russian-Ukrainian conflict, Ukraine has continuously carried out a series of quite classic propaganda offensives, such as shaping battlefield heroes and publicizing the suffering of the people. This move can at least have four effects: first, it undermines Russia's international image; second, it shapes Ukraine's national image as a strong survivor standing on the moral high ground; third, unlike Russia's focus on influencing its own people, Ukraine wins the support of the domestic and international community by manipulating a large amount of false information and unverified information; fourth, it supports the Ukrainian army in fighting on the front line.

　　In addition, the extensive involvement of deep fake technology in the Russian-Ukrainian conflict through social platforms deserves great attention. Admittedly, due to technical limitations, the video of Zelensky persuading the Ukrainian army to surrender is of average quality and crude production, making it difficult to achieve a fake effect. However, deep fake expert Nina Schick said that although the video was very crudely produced, the situation will change in the near future. People will believe anyone or anything that is forged. This is a new weapon and an effective form of false information. American legal experts Robert Chesney and Daniel Citron pointed out that in the near future, not only will it become easier and easier to create videos tampered with using deep fake technology, but these videos will also achieve a convincing effect. Fueled by social platforms, users often do not verify the authenticity of this information, and the end result is that lies spread faster than ever. In view of this, as deep learning algorithms become increasingly optimized, political opponents or battlefield enemies can use deep fake technology to create highly realistic audio/video that is difficult for the outside world to distinguish, such as false command audio or violent action videos of national leaders or senior military generals, negative audio and video of government officials and leaders of political parties, etc. By then, whoever can master advanced deep fake technology will be able to interfere with and destroy the enemy's judgment and decision-making more quickly on the battlefield, disintegrate the enemy's will to resist, thereby causing decision-making errors, low morale, and a lack of morale, and ultimately achieve the strategic goal of winning hearts and minds.

　　Third, the close integration of cyberspace and physical space is giving rise to a new type of "hybrid warfare". With the rapid development of new technologies such as big data, artificial intelligence, the Internet of Things and cloud computing, cyberspace is in a stage of deep interaction with physical space. In the Russian-Ukrainian conflict, the rapid integration of cyberspace with traditional land, sea and air combat domains is surpassing the low-intensity and relatively single-purpose cyber warfare of the past. It is not only an integral part of the entire battlefield, but also a new type of "hybrid warfare" to help Ukraine's ground resistance. In fact, it is precisely relying on low-latency and highly stable network information services that Russia and Ukraine can deploy and use intelligent command systems and unmanned combat systems in a targeted manner on the battlefield, so as to quickly locate important targets and carry out precision strikes on them.

　　First, the intelligent command system is used to improve battlefield decision-making capabilities. To some extent, the intelligent command system exists in the form of software, and the normal operation of the software is inseparable from continuous and stable network services. After the outbreak of the Russian-Ukrainian conflict, the two countries used the "Automatic Control System" (ACS) and the "Delta System" (Delta) to analyze and process the massive combat data collected from the battlefield, and convert it into valuable intelligence, so as to assist commanders to get out of the "data ocean" and quickly formulate scientific and reasonable decision-making plans. The "Automatic Control System" used by the Russian army mainly uses intelligent algorithms to autonomously analyze and process the massive raw data obtained from the battlefield to mine key military intelligence from it, thereby shortening the decision-making cycle of Russian commanders and helping to formulate plans, such as autonomously prioritizing attack targets or determining the military equipment needed to strike enemy targets. Ukraine mainly uses the "Delta System" to process raw combat data. The system can be logged in and used from a laptop, and the "situational awareness" intelligent software is installed to build an interactive map combined with images from drones and satellites to track the enemy. According to the changes in battlefield situation awareness, Ukrainian commanders can determine the best ambush site, the best attack route, and the location of their own and enemy forces based on important military intelligence, so as to accurately command and coordinate the control of front-line combat forces. It should be pointed out that Western countries led by the United States are using artificial intelligence systems to analyze and process massive battlefield data and transmit it to Ukrainian military units to help the Ukrainian army establish battlefield advantages. U.S. intelligence officials said that after Russia launched a special military operation, the U.S. Department of Defense promptly provided Ukraine with detailed intelligence on the Russian military's operations, including the Russian military's strategic deployment and the main targets, exact times and specific locations of missile and bomb attacks, the Russian military command posts, ammunition depots and marching routes, and Russian military movements collected from Russia's secret combat plans. For confidentiality reasons, U.S. officials did not disclose the specific details of intelligence sharing. Lauren Kahn, a researcher at the Council on Foreign Relations, said that the United States is using artificial intelligence systems to analyze massive data and generate Russian tactical and strategic models to support Ukraine's operations.

　　The second is to use unmanned combat systems to strike important military targets. In the Russian-Ukrainian conflict, the two countries mainly used unmanned combat systems such as drones and precision-guided missiles to strike the enemy. Take drones as an example. Drones are favored by major powers because of their easy operation, strong maneuverability, high combat efficiency, and outstanding concealment performance. However, if drones want to perform frontier reconnaissance, high-altitude surveillance, and firepower strikes on the battlefield, they need reliable and stable network communication services. Russia mainly uses drones represented by "Orion", "Forpost-R", and "Geranium 2" on the battlefield. On March 4 and 13, 2022, Russia used "Orion" and "Forpost-R" drones to strike the Ukrainian "Aidar" battalion observation command post and multiple rocket system respectively. On September 17, 2022, Rodion Kulagin, commander of the artillery of the 92nd Mechanized Brigade of Ukraine, pointed out that in the past week, Russia used the "Geranium-2" drone to carry out a "swarm" attack on the Ukrainian armored and artillery positions in the northeast of the Kharkiv region. This is the first time that the Russian army has deployed suicide drones on a large scale on the battlefield, causing serious damage to the Ukrainian army. Ukraine mainly uses drones such as "Bayraktar-TB2", "Switchblade-300", and "Phoenix Ghost" on the battlefield to attack important targets of the Russian army. On April 14, 2022, the Russian Ministry of Defense stated that the "Moscow" missile cruiser was damaged by the explosion of ammunition due to a fire, and then lost stability while being towed back to the port and sank in the Black Sea in strong winds and waves. However, Ukrainian officials and military experts said that the "Vanguard-TB2" drone used its miniature laser-guided missiles to launch the first attack, hitting the ship's air defense system, and then assisted the "Neptune" anti-ship missile to hit the ship.

　　3. Spillover effects force countries to build a strong cybersecurity protection barrier

　　Since cyberspace breaks the traditional geographical boundaries, local and even global hazards caused by cyber attacks between countries have long been common. In order to cope with the spillover effects caused by the cyberspace confrontation between Russia and Ukraine, countries and international organizations have raised their security levels. As the largest international military action taken by Russia after the end of the Cold War, the cyberspace confrontation between Russia and Ukraine has had obvious spillover effects on NATO countries. David Cutler, NATO Assistant Secretary-General for Intelligence and Security, and Daniel Black, Chief Analyst of NATO Cyber ​​Threat Analysis Department, believe that after the outbreak of the Russian-Ukrainian conflict, Russia's cyber attack has had obvious spillover effects on NATO countries, thereby affecting the normal operation of key departments and civilian Internet connections. For example, on the day when the Russian-Ukrainian conflict broke out, hacker groups launched a cyber attack on satellite communications company Viasat. Although the target of this attack should be mainly military targets in Ukraine, it also caused network service interruptions for about 13,000 Internet users in NATO countries such as Germany, France, Hungary, Greece, Italy, and Poland, and caused the modems of about 5,800 wind turbines in Germany and other countries to go offline. Major General Michel Friedling, commander of the French Space Command, confirmed that thousands of terminals on Viasat, a satellite network covering Europe, were inoperable after a cyber attack.

　　In the face of the spillover risks brought about by the cyberspace confrontation between Russia and Ukraine, NATO is enhancing the cyberspace combat capabilities of NATO countries by conducting cybersecurity exercises, holding cybersecurity meetings, and establishing cyberspace support forces. From April 19 to 22, 2022, 32 countries, including NATO countries and Ukraine, participated in the "Locked Shields" exercise organized by the NATO Cooperative Cyber ​​Defense Center of Excellence. Jaak Tarien, head of the NATO Cooperative Cyber ​​Defense Center of Excellence, said that the specific details of the "Locked Shields" exercise are not convenient to be made public, but some of the scenarios reflect concerns related to the Russian-Ukrainian conflict. For example, the first exercise rehearsed the situation of the power grid being attacked. On May 18, NATO senior cyber coordinators held their first meeting in Brussels, mainly discussing the strategic environment after the Russian-Ukrainian conflict and its impact on cyberspace security, as well as further strengthening NATO's cyberspace combat capabilities. On June 29, NATO officials revealed that as the spillover effects of the Russian-Ukrainian conflict become increasingly apparent, NATO plans to establish a joint cybersecurity team to quickly deploy in the event of a large-scale cyber attack on its member states and protect the cybersecurity of each member state.

　　It should be noted that the United States is the main leader of NATO. Once NATO countries are subject to social unrest or political instability due to large-scale cyber attacks, it will directly undermine the strategic interests of the United States in Europe. Therefore, the United States is using its organized cyberspace combat forces and systematic offensive cyber weapons and equipment to help NATO countries achieve "weakness becomes stronger, strong stronger" in cyberspace. On the one hand, after the outbreak of the Russian-Ukrainian conflict, the US Cyber ​​Command continued to carry out "hunting forward" operations in NATO countries such as Lithuania and Croatia, aiming to enhance the cyber defense capabilities of critical information infrastructure by identifying malicious network activities. On the other hand, the United States continues to provide offensive cyber weapons to close allies within NATO. Before the outbreak of the Russian-Ukrainian conflict, the United States had already delivered cyber attack weapons to the United Kingdom, Canada and other countries for use. After the outbreak of the Russian-Ukrainian conflict, the United States and other Western countries continued to exaggerate the threat of Russia in cyberspace. Therefore, the United States may continue to provide offensive cyber weapons to close allies within NATO. The United States and NATO, which it leads, are accelerating the construction of cyberspace combat forces and enhancing cyberspace combat capabilities. This move will intensify the militarization of global cyberspace and have a huge negative impact on the regional and even global security landscape.

　　Although some countries are far away from the European continent, they are still highly vigilant about the spillover effects caused by the cyberspace confrontation between Russia and Ukraine, and have taken countermeasures. On the one hand, domestic enterprises are required to take necessary measures to protect critical information infrastructure from attacks and damage. After the outbreak of the Russian-Ukrainian conflict, the Australian Cyber ​​Security Center (ACSC), the US Cybersecurity and Infrastructure Security Agency (CISA), the Singapore Cybersecurity Agency (CSA) and other institutions have required domestic enterprises to upgrade the level of cyberspace security protection to protect critical information infrastructure from interference and damage. The Australian Cyber ​​Security Center stated that after the outbreak of the Russian-Ukrainian conflict, the risk of cyber attacks faced by Australia is increasing rapidly. Major operators should be prepared for potential cyber threats such as destructive malware, ransomware, and spear phishing. On the other hand, it is to strengthen cybersecurity cooperation with countries or international organizations. The most representative is that South Korea and Japan joined the NATO Cooperative Cyber ​​Defense Center of Excellence in May and November 2022 respectively. When the Russian-Ukrainian conflict was in full swing, South Korea and Japan, two Northeast Asian countries, announced their high-profile joining of the NATO Cooperative Cyber ​​Defense Center of Excellence, which once attracted great attention from the outside world. Shortly after South Korea joined NATO's Cooperative Cyber ​​Defense Center of Excellence, the center immediately stated that the Russia-Ukraine conflict highlighted the importance of guarding against threats in cyberspace, and strengthening technical cooperation and intelligence sharing among member states including South Korea is crucial to dealing with the increasingly severe cyberspace security situation.

**III. Lessons from Cyberspace Conflict in the Ukrainian Crisis**

　　The cyberspace confrontation during the Russia-Ukraine crisis has given countries around the world a real-life lesson in cyber warfare. Against the backdrop of the rapid advancement of the world's unprecedented changes in a century, cyberspace security threats have become one of the main challenges facing China. Based on this, we should sum up experience and draw lessons from the cyberspace confrontation between Russia and Ukraine, and take timely cybersecurity measures to prevent problems before they occur.

　　1. Using big data technology to filter out sensitive data from massive amounts of data and establish your own data advantage

　　The continuous data leakage incidents in the Russia-Ukraine conflict highlight the importance of data security protection. The core of network security is data security. Data security is related to national security, national economic development and social harmony and stability, and its strategic value is constantly increasing. At the same time, data security issues represented by data theft, data leakage and illegal use of data are becoming increasingly prominent. Personal identity information, facial recognition data, key geographical location data and other data are all sensitive data. After obtaining this data, other countries can use deep learning algorithms to analyze and process it, find weak links in social and economic development and military strategic policies, and formulate targeted combat plans. Therefore, relevant departments should use big data technology to mine sensitive data related to defense and military industry, core technologies, important geographical locations and other fields from massive data, and make every effort to ensure its storage and management in China to prevent it from being secretly carried out of the country.

　　2. Promoting the introduction and training of AI talents

　　At present, there is an overall shortage of artificial intelligence talents. Take deep fake technology as an example. During the Russian-Ukrainian conflict, various deep fake videos continued to rage on various social platforms, but the number of analysts responsible for detection was extremely scarce. According to Hany Farid, a professor of computer science at Dartmouth University, as deep fake videos quickly develop to a highly realistic level, defenders will be helpless in this situation. The number of people developing false content may be 100 to 1,000 times more than the number of people responsible for detecting and identifying deep fake videos. Therefore, it is urgent to introduce and cultivate artificial intelligence talents. On the one hand, we must vigorously introduce international high-end talents, young leading talents and top innovation teams related to neural networks, machine learning, natural language processing and other fields, strengthen the major research efforts on original, forward-looking and leading scientific research results, and comprehensively improve the level of innovation in artificial intelligence technology. On the other hand, we must establish a multi-level artificial intelligence talent training system covering primary education, secondary education and higher education. In primary and secondary schools, introduce popular education on artificial intelligence, set up corresponding artificial intelligence courses, and focus on cultivating students' computational thinking, design thinking and innovative thinking. At the college level, a complete AI core knowledge curriculum system should be created to ensure that students master the basic theories of AI. At the same time, cross-disciplinary integration should be achieved to generate personalized and efficient learning plans for students.

　　3. Strengthening cognitive warfare capabilities

　　In the Russian-Ukrainian conflict, from using intelligent robots to spread various false information, to the so-called "Ghost of Kiev" edited by the "Digital Combat Simulator World" game, to the fake videos of Russian and Ukrainian leaders' speeches tampered with by deep fake technology, it shows that cognitive warfare has already started in cyberspace and has become an important factor affecting the direction of the Russian-Ukrainian conflict. In order to avoid being at a disadvantage in cognitive warfare, the following two aspects can be carried out.

　　First, use cutting-edge technologies such as big data and artificial intelligence to empower cognitive warfare capabilities and comprehensively enhance soft lethality. Joseph Nye, former dean of the Kennedy School of Government at Harvard University, believes that in the information age, success depends not only on whose army has strong combat effectiveness, but also on whose story is more convincing. In the digital age, if you want to maximize the combat effectiveness of cognitive space, the best way is to use cutting-edge technologies such as big data and artificial intelligence to provide strong technical support for commanders and frontline combatants. Some studies have pointed out that the application of advanced technologies such as big data and artificial intelligence in cognitive warfare can help optimize the combat concept of cognitive warfare and give full play to the maximum combat power. Based on this, intelligent algorithms can be used to quickly extract high-value intelligence from massive raw data to reduce the cognitive load of combatants; big data technology can be used to draw cognitive scene maps of target objects in terms of psychological characteristics and thinking habits; virtual reality technology can be used to build a realistic digital battlefield environment, increase the psychological resilience training of combatants, and improve the psychological quality of the battlefield.

　　Second, build a number of social platforms with international influence to enhance China's influence in the international public opinion field. In recent years, the overseas influence of mainstream media such as Xinhua News Agency, People's Daily, and China Central Radio and Television has been increasing. In contrast, social platforms are the weak link in China's overseas propaganda. Social platforms are an important platform for creating an external public opinion environment and enhancing China's national image. Take Tik Tok as an example. As a Chinese technology company that has fully opened up the US market, the key to Tik Tok's success is that "it can use powerful intelligent algorithms to actively push relaxed and lively short videos to users, and establish a user-made video dissemination network like a butterfly effect, which is rarely achieved by other large Internet companies." In the future, Chinese Internet companies can follow the Tik Tok model and make conveying China's voice and telling China's stories a top priority in external communication to help China improve its positive image in the international public opinion field.

　　4. Enhance cyberspace defense and deterrence capabilities and protect the security of critical information infrastructure

　　During the Russia-Ukraine conflict, hacker groups launched a series of cyber attacks on critical information infrastructure in the financial, telecommunications and other fields in order to weaken the other side's resistance. Critical information infrastructure is an important carrier for maintaining national cyberspace security, ensuring the stable operation of the national economy and high-quality social development. Once it is attacked on a large scale or severely damaged, it will trigger a chain reaction in the financial, transportation, electricity, energy and other fields, and then have a serious impact on national security, national economy, people's livelihood and public interests. In view of this, China can advance from the following two aspects.

　　First, use artificial intelligence to enhance cyberspace defense capabilities. Cyberspace defense force construction is an important part of China's national defense and military modernization, and follows the consistent active defense military strategic policy. Therefore, China should use artificial intelligence technology as a backing to accelerate the construction of an all-weather, all-round, and full-coverage cyberspace defense system, enhance the construction of real-time network security monitoring, joint disposal, and tracking and tracing capabilities, and prevent and contain system vulnerabilities, hacker attacks, network intrusions, information destruction and other network security risk events. For example, use deep learning to build a "cyber attack chain" model to promptly discover possible network intrusions that attackers may implement, and quickly form a network counterattack plan; at the same time, use massive data to train deep neural network models, use the trained models to improve the detection accuracy and response speed of new malicious Trojan programs and advanced persistent threat (APT) attacks, and continuously accelerate the upgrading of models based on real-time data, thereby strengthening cyberspace defense capabilities and protecting critical information infrastructure from malicious intrusions and destruction.

　　Second, develop "killer mace" weapons to enhance the deterrence capability in cyberspace. Pure passive defense will undoubtedly provide cyber intruders with an opportunity to take advantage. In cyberspace, we must adhere to active defense, seize network control through deterrence and defense, and include cyber deterrence in the category of active defense. Zhang Shibo: "New High Ground of War", National Defense University Press, 2016 edition, pp. 67-85. Therefore, China should strengthen the enabling role of artificial intelligence in network security, and develop asymmetric "killer mace" weapons with greater strategic deterrence by leveraging the role of artificial intelligence in situational awareness, threat detection and continuous monitoring. As a new type of combat force to safeguard national security, the Strategic Support Force should accelerate the development of "killer mace" network weapons and equipment that are strategic, targeted and deterrent, and use them as a multiplier to enhance the deterrence capability in cyberspace.