· Article ·

Global Cyberspace Governance Crisis and Response in the Digital Age

Xinyang Lyu[1,*]

[1] School of Public Administration, Jilin University, Changchun, China

* Corresponding Authors: Xinyang Lyu. Email: lvxinyang61@163.com

Received: 19 October 2024 Accepted: 31 October 2024 Published: 25 November 2024

Abstract: In the digital age, cyberspace has emerged as a new frontier for major power exploration and competition. Initially considered an auxiliary means of traditional combat, cyber warfare has evolved into an independent mode with significant impact, extending the nature and forms of conflict. It is imperative that nations recognize cyber warfare as an inseparable component of modern warfare and deeply understand the importance of strengthening data sovereignty in cyberspace. This concerns the fundamental aspects of national security and is crucial for maintaining the health of the global internet ecosystem. Furthermore, it is key to fostering peace and stability within our "global village". By strengthening international cooperation to jointly address cybersecurity threats, humanity can take steps toward a safer and more prosperous digital future.

Keywords: Cybersecurity; Cyberspace Governance; Global Digital Governance

1. Introduction

Digital technology has developed at an unprecedented pace, fostering societal advancement and economic growth. However, the rapid pace of technological advancement, along with its inherent uncertainties, has led to new security threats and challenges. As a result, frequent incidents like cyber-attacks, data breaches, and privacy infringements now pose serious risks to national security, social stability, and individual privacy. Consequently, strengthening international cooperation in cybersecurity to build a collaborative framework based on mutual trust, cooperation, and shared benefit is not only an active response to current cybersecurity challenges but also a necessary path toward a more just and reasonable global cyberspace governance structure. In existing literature, research on global cyberspace governance primarily focuses on three areas. Firstly, the complex and volatile state of global cyberspace security. As noted by Yi Shen and Yiyun Sun (2019), the broad application and perception of "omnipresent security" in information and communication technology have heightened cybersecurity risks. This has widened the cybersecurity deficit. Secondly, the prevalence of cyber warfare, which disrupts global cyberspace order. As pointed out by Jianping Ruan

and Dongxu Zhang (2024), the international community has not yet reached a consensus on norms of behavior in cyberspace, and existing international laws lack effective constraints, leaving cyberspace disorder fundamentally institutionalized. Thirdly, the differing attitudes of countries toward global cyberspace governance, marked by intense competition and governance divergences among major powers. Mark Manulis (2021) observed that advancements in technology and investments are reshaping the space environment, enabling greater accessibility for an increasing number of countries and political entities. Similarly, Yu Dahao and Cai Cuihong (2024) noted the opportunity for China and India to advance cooperation in cyberspace security, though significant obstacles remain due to limited consensus and implementation challenges. Addressing why a global cyberspace governance crisis exists and accelerating governance efforts are urgent priorities that require immediate solutions.

1.1 Cyber Information Warfare and Sovereignty in Cyberspace

Cyberspace has become a critical channel for information flow and is gradually evolving into a new arena for interstate competition. Issues surrounding cyber information warfare and cyber sovereignty are increasingly prominent, with the strategic contest among nations in cyberspace intensifying. A thorough understanding of the dynamics of cyber information warfare and the boundaries of cyber sovereignty is essential to safeguarding national cybersecurity.

1.1.1 Cyberspace and Cyber Information Warfare

With the rapid development and application of digital technology, the Internet has increasingly become an integral part of daily life, cyberspace has consequently emerged as the "fifth domain" following land, sea, air, and universe. The Internet is not only a battlefield, but has also evolved into a tool for conquering the real-world dominance. Within the Internet and cyberspace, a new type of warfare exists, leaving no one untouched. This form of warfare, termed "cyber information warfare" or "cyberwar", refers to the strategy of pressuring and paralyzing an adversary's essential infrastructure, such as governmental and financial websites, even before direct combat. By disrupting an adversary's computer networks and systems, this approach seeks to gather confidential information to achieve specific political objectives.

The concept of cyberwarfare did not originate from reality. It was born in the soil of science fiction. It can be traced back to John Brunner's 1975 novel, *The Shockwave Rider*. In this visionary work, Brunner not only foresaw the birth of computer viruses but also depicted virtual threats that later inspired the term "worm virus", foreshadowing the turbulent undercurrents of the digital world. Scholarly discussions on the topic of cyberwar emerged formally in the early 1990s as information technology developed at a rapid pace, bringing security and conflict in cyberspace to the forefront. However, it was not until the early 21st century that a real-world example of cyberwarfare struck the world: the 2007 "Bronze Night" cyber-attack on Estonia, widely regarded as the first clear instance of cyberwarfare, marking cyberspace as a new battlefield for inter-state confrontations. Moreover, the 2011 Stuxnet virus attack on Iran's Natanz uranium enrichment facility propelled the power of

cyberwarfare into global focus. This incident not only conclusively demonstrated the unprecedented destructive potential of cyber weapons but also revealed the multifaceted complexities of cyberwarfare, transcending traditional war boundaries and intertwining political maneuvering, strategic planning, and military action into a critical area demanding close attention. The success of Stuxnet undoubtedly sounded an alarm globally, prompting nations to reassess and enhance their cyber defense and strategic preparedness.

1.1.2 Sovereignty in Cyberspace

Cyberwarfare rampant in cyberspace not only jeopardizes the interests of countries globally but also disrupts the order within cyberspace. In this environment, nations must prioritize their internal cybersecurity and data sovereignty, gaining worldwide attention.

Defining the concept of "cyberspace sovereignty", we observe that "sovereignty" within the international community is inherently dynamic, open, and developmental, evolving with shifts in time, advancements in productivity, and changes in production relations. The progress in digital technology has expanded the territorial reach of states, broadening the exercise of cyberspace sovereignty, while data sovereignty represents a novel extension of national sovereignty theory in the digital age. Cyber sovereignty and data sovereignty are intertwined, with data sovereignty representing a subset of cyber sovereignty. Within cyberspace, a country's network infrastructure, including but not limited to self-built network stations, fiber optic and cable installations, is undoubtedly within its sovereign jurisdiction. Going beyond these physical boundaries, data flows transmitted within national territories, the complex logic structures embedded within data, and the various forms in which this data manifests — such as audiovisual material, images, and written content — constitute extensions of national sovereignty in cyberspace. We can collectively refer to this concept as the "network territory" domain. This concept profoundly impacts the core domain of information data, underscoring the nation's strong commitment to securing and maintaining data sovereignty in the era of cyberspace.

Overseas scholars have categorized the power in cyberspace into four forms, namely, "compulsory network power", "institutional network power", "structural network power", and "interpretative network power", "structural network rights", and "interpretative network rights". Specifically, coercive cyber power refers to "the power to carry out coercive activities against other countries through cyberspace and information technology". For example, Ira's nuclear equipment was attacked by the "Stuxnet" virus, Israel suffered a large-scale DDoS attack, and the Russian-Ukrainian conflict carried out in the network war are all real cases of the implementation of coercive cyber power in the international community; institutional cyber power is through certain formal or informal institutions to obtain legitimacy, to the international community, and to the international community, to the international community. Institutional cyber power is "the power to manage international cyberspace through certain formal or informal institutions to gain legitimacy". For example, the U.S. has gained control of the Internet Corporation for Assigned Names and Numbers (ICANN) to manage the root servers and assign domain names in international cyberspace. Therefore, in order to avoid

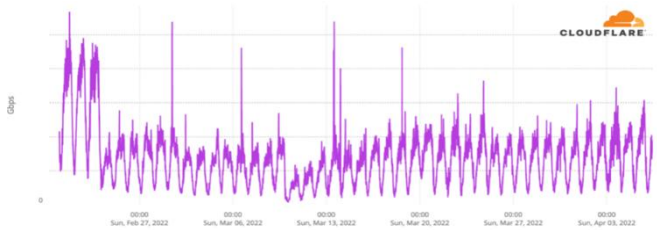
being controlled by ICANN and the U.S., Russia has implemented the "disconnection law" to safeguard its national security and interests; structural cyber power is a system of power that includes both state and non-state actors. That is, under the leadership of the national government, through the participation of non-state actors, such as individuals, enterprises, academics, non-governmental organizations, so that the cyberspace is more open and more dynamic; Finally, "the interpretive network rights" refers to the cultural level, the right to interpret ideology, political events, which is usually part of the power to the state. There were countries that hid their actual hegemony under slogans of justice, a hypocritical model of utopianism. Especially in developing and underdeveloped countries, which are themselves weak in information and digital technology, if national governments simply relinquish their sovereignty in cyberspace, the hegemonic powers will be in no man's land, reducing them to neo-colonies in the cyber age.

However, in real practice, the United States, Europe and other developed countries can deprive other countries of the power they have in cyberspace through multi-stakeholder, and at the same time control the cyberspace of other countries by virtue of their own technological advantages and the ICANN, thus eroding the cyberspace sovereignty of other countries.

2. Global Cybersecurity Governance Crisis and Its Diffusion

The cybersecurity crisis within the Russia-Ukraine conflict epitomizes the broader global cybersecurity governance crisis. During the conflict, Ukrainian government websites and financial institutions experienced temporary shutdowns, and similar "cyberwar" challenges surfaced for Russia. In February 2022, Ukraine faced a large-scale DDoS attack, severely impacting critical sectors such as military command, government agencies, the education system, and financial services, leading to significant disrupts. Information warfare has become an effective means of realizing geopolitical goals. The Russian-Ukrainian conflict has been broadcast live to the world from numerous "first views", and if there are devices that can access the Internet, anyone in any part of the world can be the first to see live broadcasts of the Russian-Ukrainian conflict from different perspectives. Key equipment provided by the United States and other Western countries supports Ukraine's cyberwarfare at the basic level. For example, at the beginning of the Russia-Ukraine conflict, all levels of the Ukrainian government moved their databases and operations to the cloud, and then succeeded in keeping the Ukrainian government running stably through the "Starlink" satellite system and foreign servers.

Table 1: Hacked Ukrainian Service Providers Experiencing Unscheduled Brief Traffic



Source: Cloudflare.

2.1 Cyberwar's Impact on Data Security

The state of global cybersecurity is increasingly complex. Countries, driven by varying interests, demonstrate divergent approaches to cybersecurity governance, as seen in strategies that hinder the technological advancement of other nations, particularly by Western countries like the United States. At the same time, the friction in cyberspace is constant, and high intensity cyberattacks against critical infrastructure between different countries occur frequently, such as in January 2020, a domestic airline's information system was suddenly abnormal, attacked by cyberweapons, and key information was stolen by the network of foreign espionage and intelligence agencies, and China's national security organs immediately carried out a technical inspection and found that a number of important servers and network equipment had been implanted with special Trojan horse programs. In May 2021, an overseas consulting and investigation company frequently contacted the management of my large shipping enterprises and agency service companies through the Internet and telephone, and established "cooperation" with dozens of people in my territory in the name of hiring industry consulting experts with high remuneration. and instructed them to widely collect and provide me with basic shipping data, specific ship cargo information, etc. The relevant overseas consulting and investigation companies have close relations with the espionage and intelligence agencies of their countries, undertake a large number of intelligence collection and analysis operations, and provide all the key data collected by the domestic personnel to the espionage and intelligence agencies of their countries to carry out espionage and intelligence work, and turn a blind eye to privacy issues, which extremely jeopardizes the data security of the country and individuals. The strategic position of cyberspace as an important battlefield for great power games is deepening day by day. Chinese scholar Chuanying Lu summarized the impact of cyberspace on global strategic stability, including the change of cyber science and technology on the traditional military form and mode of combat as well as the difficulty of existing international institutional arrangements to effectively respond to the challenges of cyberspace and so on. In addition, overseas cyberattacks have also appeared in the military command system, government agencies, education system and financial services and other key sectors, this series of attacks is not only a serious test of cybersecurity defenses, but also a direct threat to the national security of all countries, which highlights the fact that cyberspace has become a new battlefield for the game between countries. Such incidents have also profoundly challenged the data sovereignty authority of countries in cyberspace, prompting the international community to pay more attention to building a security order in cyberspace and protecting the core interests and data assets of countries in the cyber era.

2.2 Cyberwar and Ideological Security

Social media, now as an indispensable part of modern society, has become a vital platform for disseminating principles of justice and national values, while also establishing an arena of significant ideological influence. Cognitive cyberwar is especially fierce, utilizing psychological tactics such as deception, inducement, and deterrence to weaken an adversary's psychological defenses and core

values, potentially shaking their foundational decision-making and resilience. This invisible competition has profoundly demonstrated the complexity and urgency of the interweaving of information warfare and psychological warfare in the network era.

At the same time, the tentacles of cyberwarfare have also penetrated into the legal framework at the social level, posing unprecedented challenges to the traditional legal mechanism. Especially in the digital age, the protection of human rights has become a particularly prominent issue in the context of cyberwarfare. The misuse of cyberweapons, such as surveillance, tampering and even deletion of citizens' personal information, not only violates individual privacy rights, but also touches the core of digital human rights. The U.S. Prism program and the Snowden incident are typical examples of this issue, which not only expose the widespread existence of cyber surveillance, but also trigger a profound reflection on human rights protection and legal regulation in the digital era worldwide.

2.3 Diffusion of the Global Cybersecurity Governance Crisis

The frequent occurrence of international cyber-related fraud resulting from telecom scams signifies a growing burden for countering cyber-fraud. Widening this view globally, cyberterrorism, cybercrime, and cyber-fraud have spread amid the substantial cybersecurity governance deficit worldwide, threatening anyone connected to the Internet.

Under such conditions, the need for data sovereignty protection strategies within cyberwarfare becomes urgent. Despite there is still much room for progress in the understanding and constraints of the existing international law on cyber warfare, but the United States and other cyber powers of the arms race and China bias thinking for a long time, in the future, the shape of cyber war between the countries "before the troops move, the network first" will also become the norm. Chinese scholars, such as Cuihong Cai, believe that "camping", "securitization", and "fragmentation" in governance have a tendency to jointly shape the systemic dilemma, exposing the mismatch between the existing cyberspace governance mechanism and the reality of governance. This exposes the mismatch between the existing cyberspace governance mechanism and the reality of governance. At the same time, due to the large differences between different countries in terms of legal and social systems and the level of development of network technology, it is difficult to reach agreement and make progress in transnational cooperation on cybersecurity in the short term.

3. Vision for Global Cyberspace Governance and China's Role

Driven by globalization and digitalization, cyberspace governance has become a central focus of global attention. In the face of increasingly complex cybersecurity threats, nations urgently need to strengthen cooperation and build consensus in cyberspace governance. This is essential to ensuring the stability and sustainability of global cybersecurity. As a key participant in global cyberspace governance, China is committed to promoting multilateral cooperation and fostering innovation in governance, playing an increasingly significant role in the development of cyberspace governance.

3.1 Russia-Ukraine Conflict Accelerates Global Cyberspace Governance

The cyberwarfare and information warfare triggered by the Russia-Ukraine conflict have posed challenges not only to the cyber capabilities of the nations involved but also to the governance capacity of international internet organizations.

First, cybersecurity research has become a national strategic priority. Nations should integrate cybersecurity into their strategic priorities, allocate more resources to enhance their cybersecurity defenses, establish comprehensive regulatory frameworks, build specialized cybersecurity teams, and work closely with the private sector to address security challenges in cyberspace collectively. On this foundation, strengthening international collaboration is essential for addressing cyber threats together. Subsequently, the governance model of multilateralism is crucial to maintaining the stability of cyberspace. It embodies government-led multi-stakeholder participation and is conducive to the full mobilization of resources and the rapid implementation of policies. The decision-making mode of multilateralism is conducive to the promotion of global public interests and enables relevant international organizations to resist unilateral decision-making. The principle of multilateralism is conducive to the role played by various actors, such as governments, international organizations, Internet enterprises, technology communities, civil society institutions and individual citizens, and reflects fairness and justice in cyberspace governance. The international community should, on the basis of mutual respect and trust, strengthen dialogue and cooperation and adhere to the concept of global governance based on common cause and sharing, so as to maintain the unity, openness, security and stability of the global Internet. All of the nations and regions in the world should actively participate in international cyberspace governance mechanisms, jointly formulate a code of conduct for cyberspace, share intelligence information and coordinate responses to transnational cyberthreats. Through international cooperation, the overall security level of global cyberspace will be enhanced. Finally, promote the improvement of the cyberspace governance system. International organizations should maintain a neutral attitude in it and play the role of leading sheep of international organizations in governance. As technical coordinators in the field of the Internet, international organizations such as The ICANN can ensure that the operation of the Internet is not politicized only if they remain neutral in conflicts and disputes. As an independent technical organization, ICANN goal is to create a single, unique, global, and interoperable Internet. If international Internet organizations are oriented by ideology and values and have a tendency in relevant disputes, the normal operation of the Internet will be affected. On the first anniversary of the outbreak of the Russian-Ukrainian crisis, global attention is once again focused on the United Nations headquarters in New York. On February 23rd local time, the 11th Emergency Special Session of the UN General Assembly adopted a new resolution calling for a comprehensive, just and lasting peace in Ukraine, demanding Russia's immediate, complete and unconditional withdrawal of all its military forces from the territory of Ukraine within its internationally recognized borders and calling for a cessation of hostilities. In the context of the Russian-Ukrainian conflict, the Russian people have the right to access the Internet and

cannot be denied the right to connect to it. It would be lacking in strategic foresight to try to isolate or marginalize Russia from the digital space. The Internet is a global infrastructure. International Internet organizations, led by the Internet Society (ISOC), have always adhered to the principle that the Internet is for the people, insisting that the Internet is for everyone in the world and that everyone has the right to access the Internet. If an international Internet organization restricts a country's the access to the Internet, the trust and effectiveness of the global Internet system will be adversely affected.

The draft resolution, jointly submitted by 57 countries, including Ukraine, the United States, Germany, Japan, and Guatemala, ultimately received 141 votes in favor, with UN Secretary-General Guterres emphasizing in his UNGA message that "war is not the solution, war is the problem". He reiterated his call for all parties to stop the conflict and respect the Charter of the United Nations.

3.2 Envisioning Practical Global Cyberspace Governance

Before formulating governance policies, it is crucial to recognize that states are the primary actors in cyberwarfare. As sovereign entities, states play an irreplaceable role in cyberspace, exercising sovereignty, safeguarding security, and fostering cooperation.

After affirming states as the sole responsible entities in cyberwarfare, one can apply constructivist theories to analyze national behavior within the international political culture and system. According to constructivism, culture influences not only the various motives of state actors, but also the basic characteristic of the state, "national identity". The culture of international politics can change the international system. Alexander Winter proposed three cultures of international politics: Hobbesian, Lockean and Kantian. Some scholars believe that the cultural environment that can make the system of cyberspace sovereignty better maintained and prolonged is the Kantian culture, which is based on friendship, and the maintenance function of cyberspace sovereignty requires a deeper Kantian culture, where countries identify with each other and have a high degree of trust. Countries are closely interconnected, forming a holistic pattern of intertwined interests and shared prosperity, in which each country plays an indispensable part of the collective. In this context, cyberspace, as a strategic high ground in the new era, the construction of its community of destiny is particularly important. The formation of a community of destiny in cyberspace builds a cultural environment based on the principles of mutual trust and mutual benefit. In such an environment, cyberspace sovereignty is not only a natural extension of a country's sovereignty, but also a key element in maintaining national security and promoting economic development. States need to strengthen international cooperation to jointly address security challenges in cyberspace and promote the building of a community of destiny in cyberspace.

3.3 China's Proposal for Global Cyberspace Governance

The transnational and anonymous nature of cyberspace makes it challenging for individual nations to effectively address cyber threats independently. As a responsible major power, China prioritizes the healthy development of cyberspace and actively participates in cyber governance

activities within regional and multilateral organizational frameworks. It also deepens collaboration with other nations and non-state actors in global cyberspace governance. China advocates for enhanced international cooperation to jointly confront cyber threats, encouraging countries to engage actively in international cyberspace governance mechanisms, jointly establish norms of conduct, share intelligence, and coordinate responses to transnational cyber threats. Through international collaboration, countries can elevate the overall security level of global cyberspace and advance the improvement of cyberspace governance systems.

From a historical point of view, China has always been a responsible power that "takes peace as its value", supports the weak and does not easily provoke disputes. We should pay attention to the issue of governance in cyberspace, actively exercise data sovereignty in cyberspace, and take multiple measures to safeguard cybersecurity and national security, from the top-level design of strategies to specific means of attack and defense. Firstly, China supports the United Nations' initiatives in cyberspace governance. Secondly, China promotes the establishment of a cyberspace community with a shared future, advocating this concept in various multilateral settings and releasing "concept papers" and "action initiatives" at the World Internet Conference to contribute China's insights. Global cyberspace governance is a continuous process, and the "China solution" seeks to serve both domestic and international communities, shaped by external circumstances and pressures. Moreover, as the world's largest developing country, China actively assists other developing and less developed countries in advancing technological progress, enhancing global digital connectivity, and striving to close the digital divide. China promotes global information infrastructure development and supports internet access in African regions. However, emerging technologies, such as artificial intelligence, introduce new challenges to cyberspace governance, suggesting that China's approach to global cyberspace governance must evolve with the times, embodying a forward-looking adaptability that not only serves domestic development but also contributes to global cyberspace governance.

4. Conclusion

In the tides of globalization and digitalization, cyberspace governance has become a vital part of national governance, with increasingly prominent complexity and multi-dimensional challenges. Security issues such as cybercrime and cyber warfare are directly linked to the dynamics and competition between nations. Emerging concepts like the metaverse and the rapid development of streaming have deeply influenced the strategic positioning and future development plans of nations. In facing these new issues of the digital era, the central role of state governance and the concept of sovereignty in cyberspace have garnered unprecedented attention. If a country cannot uphold its sovereignty in cyberspace, it risks the possibility of digital colonization by hegemonic powers, thereby losing its initiative and opportunities in the digital age. Therefore, nations must take active steps to establish a robust legal framework for cyberspace, clearly defining the specific scope of state sovereignty. This not only helps regulate domestic cyber behavior and protect citizens' legitimate rights but also provides robust support for international cyberspace governance. Implementing

cybersecurity strategies and plans is an essential path to enhance national equality and independence in cyberspace. Through international cooperation and exchange, countries can jointly establish international rules and standards in cyberspace, effectively combating cybercrime and promoting the healthy and positive development of cyberspace.

Acknowledgement

None.

Funding Statement

None.

Author Contributions

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

Availability of Data and Materials

The data for this study are derived from publicly available literature and news reports, which have been listed in the references.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1]. Singer, P. W., & Brooking, E. T. (2019). *Like war: Weaponization of social media.* HarperCollins.

[2]. Shen, Y., & Sun, Y. (2019). Reconstructing Threat Perception and Rebuilding Strategic Mutual Trust - National Cyberspace Governance Capacity Building in the Context of the Fourth Industrial Revolution. *Journal of the Central Academy of Socialism,* (05), 101-109.

[3]. Ruan, J., & Zhang, D. (2024). U.S. Layered Cyber Deterrence Strategy and China's Response. *Socialist Studies*, (03), 162-172.

[4]. Manulis, M., Bridges, C. P., Harrison, R., Sekar, V. & Davis, A. (2021). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, *20*, 287-311.

[5]. Yu, D., & Cai, C. (2024). China-India Cyberspace Security Cooperation: Opportunities, Challenges and Responses. *Journal of International Relations*, (05), 116-135+158-159.

[6]. Liu, Y., & Wei, Y. (2023). Multiple Risks of Data Sovereignty Security under the Perspective of Cyberwarfare and Response Strategies. *Journal of Intelligence*, (05), 54-60.

[7]. Luo, Y. (2022). *Research on Cyberspace Sovereignty from the Perspective of Structural Functionalism*. [Master dissertation, West China Normal University].

[8]. Xu, F. (2022). The establishment and maintenance of network sovereignty and data sover eignty. *Beijing Social Science*, (07), 55-64.

[9]. Fang, B. (2017). *Research on Cyberspace Sovereignty*. China Science Publishing.

[10]. Lee, H. (2022). Cyber Confrontation in the Russia-Ukraine Conflict and Its Impact on C yberspace Security. *China Information Security*, (06), 83-86.

[11]. Xinhua Official Website (2021). *Ministry of National Security Announces Three Cases of Endangering Important Data Security*. http://www.news.cn/legal/2021-10/31/c_1128014674. htm

[12]. Lu, C. (2020). The Evolution of Great Power Relations in Cyberspace and the Construct ion of Strategic Stabilization Mechanism. *Foreign Social Sciences*, (02), 96-105.

[13]. Yang, C. (2023). On the Risk and Governance of Military Application of Artificial Intell igence under the Threshold of National Security - Taking the Russia-Ukraine Conflict as an Example. *International Forum*, (02), 61-82+157.

[14]. Cai, C., & Zhang, L. (2023). Systemic Dilemma and Direction Choice: Analyzing the R eality and Way Forward of Global Cyberspace Governance. *Contemporary China and the World*, (04), 25-34+123.

[15]. Chu, D. (2023). Geopolitics and beyond borders: an analysis based on Russian think tan ks' perception of the Ukrainian crisis. *Russian East European Central Asian Studies*, (0 2), 122-137+157-158.

[16]. Liu, Y. (1998). Western neorealist theory and constructivist criticism. *World Economy an d Politics*, (11), 26-30.

[17]. Qin, Y. (2001). The Anarchy of the International System: A Reading of Alexander Wen dt's Social Theory of International Politics. *The Chinese Journal of American Studies*, *15* (2), 135-145.

[18]. World Internet Conference (2023). *Collection of practical cases on Joining hands to buil d a community of destiny in cyberspace*. https://cn.wicinternet.org/2023-11/07/content_3695 3570.htm

[19]. Xu, L. (2023). Global cyberspace governance: core issues, Chinese programs and future directions. *Chinese Journal of European Studies*, (06), 58-79+6.

[20]. Tyler Baum (2022). *Twitter Brings out Fake News Policy as Elon Musk Panics over Bo ts and Deal Remains "on Hold"*. https://www.thesun.co.uk/tech/18637838/twitter-brings-out -fake-news-policy/

[21]. Alex Friedland (2022). *AI and the invasion of Ukraine, how an Nvidia hack could help China, tech talk in the SOTU, and the ODNI's annual threat assessment.* https://cset.geor getown.edu/newsletter/march-10-2022/

[22]. Jane Wakefield (2022). *Deepfake Presidents Used in Russia-Ukraine War*. https://www.bbc.com/news/technology-60780142

[23]. Hunter, R. (2022). The Ukraine Crisis: Why and What now? *Survival*, *64*(1), 7-28.