zeitgeschichte
ZEITGESCHICHTE
ISSN / eISSN 0256-5250 / 2569-5304
Publisher BRILL DEUTSCHLAND GMBH,
VIENNA UNIV PRESS, ROBERT BOSCH BREITE 6,
GOTTINGEN, GERMANY, D-37079
Tel No:+49 05241 2151 1000
Volume 25-Issue 1 -(2025)

Practical trends and evaluation of Russia's information security strategy since the Russia-Ukraine conflict
——Based on the perspective of strategic inertia

Wenjin Fan*

PhD, Shanghai Academy of Global Governance & Area Studies, Shanghai International Studies University，Shanghai 201620, China

Corresponding author：Wenjin Fan
Corresponding email：fanwenjin729548732@gmail.com

Abstract：The theoretical structure of "strategic inertia" is consistent with the current development of Russia's information security strategy. Under the force of inertia, the established path of Russia's information security strategy follows strategic inertia. The reason is that the power system is solidified, and the inertial thinking of decision-making elites and the passive defense-oriented strategic model are difficult to break the inertia. However, due to the increase in external threats and internal security risks and the adjustment of strategic means, Russia has gradually adjusted its information security strategic means to cope with information security threats, and its strategic means have shown new characteristics. In the face of the intensification of international information security threats and the complexity and variability of information warfare means, especially under the influence of the continued fermentation and spillover of the Ukrainian crisis, the development trend of Russia's information security strategy deserves great attention.

Keywords: strategic inertia; information security strategy; information warfare; Russia-Ukraine conflict

In recent decades, a series of local conflicts have occurred in the field of Russia's historical responsibility. There are two types of local crises and wars. One is a conflict between two or more countries at the local or regional level, which indirectly affects the international situation. The other is a local conflict caused by confrontation at the global level, which reflects the struggle to redistribute spheres of influence between the world's power centers. In an era of globalization and increasing universal human values, these local conflicts are considered to be institutionalized forms of hybrid

warfare such as information warfare, that is, wars that use various soft powers to achieve their strategic goals. After the Ukrainian crisis in 2014, the technological "revolution" in the information field actually promoted the process of non-military forms of power. Hybrid warfare such as information warfare has become the most common form of confrontation between countries today as an increasingly mature military strategy. The 2022 Russia-Ukraine conflict is a hot war between highly informationized and digitalized countries. Behind the military conflict, the information space has become a battlefield with real global and global confrontation. The United States and the West have launched an all-out attack on Russia at the psychological and technical levels of information warfare, and Russia's response and measures in this information war are worthy of attention. More importantly, new changes have begun to appear at the level of Russia's information security strategy. In 2016, the Russian Federation Information Security Doctrine extended national sovereignty to information space for the first time, making information space an important part of national sovereignty. While emphasizing traditional information threats, it also considered new challenges brought about by factors such as "color revolutions", information warfare and cyber terrorism, which reflects the development and changes of Russia's information security strategy in the new era. This strategic change not only shows that Russia's information security situation is facing threats, but also means that the face of war has changed, posing new challenges to international security.

Cyber operations attributed to Moscow are not carried out in a strategic vacuum, but are based on broader geopolitical factors and the institutional culture of Russia's military, intelligence and policy leadership. To understand the motivations and means behind them, it is necessary to delve into existing policies and mechanisms. This study finds that Russia's information warfare stance is rooted in its strategic culture. Due to the solidification of the power system, the "paternalistic" style of information supervision, and the passive prevention-oriented strategic model, it is difficult for information security strategy to break the inertial thinking of decision-making elites, resulting in the practical logic of information warfare following strategic inertia.

Although it is impossible to break free from the constraints of strategic inertia, under the influence of internal and external situations, Russia's interest in developing information weapons continues to increase, and adjusting strategic means in conflicts may drive changes in Russia's future information security policies and strategies

一、 Strategic inertia and Russia’s information security strategy

（一）Strategic Inertia Theory

As a complex system, strategic adjustments are subject to multiple factors. Russia generally makes concrete strategic adjustments only after a major sudden crisis or setback in strategic goals. These adjustments are often small and slightly passive. This phenomenon is strongly related to strategic inertia. The concept of inertia comes from the field of physics. It refers to the characteristic of an object itself to maintain its original state of rest or uniform linear motion. It is the fundamental attribute of all objects. It essentially reflects the stability of the object, and also reflects its inability to change its own state and its tendency to resist any change.[①]In the 1980s, inertia was introduced into the field of social sciences. The theoretical basis includes organizational inertia theory and environmental determinism, which are mainly divided into the Stanford School, the Population School and the Mellon School, all of which recognize that under the influence of multiple factors, strategies may maintain the status quo. From the perspective of organizational ecology, Michael Hannan and John Freeman believe that strategic inertia is a characteristic of organizations that tend to maintain their original strategies and behavior patterns when facing environmental changes, which stems from the constraints of the internal structure of the organization and the external system.[②]Miller and Friesen emphasize that strategic inertia is the relative stability of the strategic decision-making model and resource allocation mode formed by the enterprise over a long period of time. This stability makes the enterprise resist strategic change to a certain extent. Therefore, strategic inertia can be understood as: the role and state in which the organization is difficult to change its

① Liu Guozhu, Yang Nan: "The Evolution of American Grand Strategy in the Post-Cold War Period: From the Perspective of Strategic Inertia", Journal of Zhejiang University (Humanities and Social Sciences), No. 4, 2019, pp. 38-39.

② Michael T. Hannan, John Freeman.Organizational Ecology.Harvard University Press.1993.pp57-68.

original posture under the influence of various factors, which may induce negative reactions.[①]From the perspective of national strategy, strategic inertia refers to the path-dependent characteristics that organizations or countries exhibit in the process of strategic selection and implementation based on past experience, traditions, and established procedures. Just as an object maintains its original state of motion when not acted upon by external forces, strategic inertia enables strategic behavior to maintain consistency and stability over a certain period of time, and even tends to stick to existing policies in the face of changes in the international landscape.

The formation of strategic inertia is not achieved overnight, but rather a slow and continuous process. The driving force of this process may come from the strategic goals that the actors have long followed, or from the path dependence derived from the established operating model of many domestic government organizations,[②]or from the constraints of the strategic culture within the government organization.[③]Most of the time, this force works alternately or simultaneously, affecting its own strategic behavior. This article believes that the strategic inertia theory can fully explain Russia's information security strategy. The main reasons are: First, Russia's information security strategy shows remarkable stability and continuity, which is highly consistent with the strategic inertia theory. From a historical perspective, since the disintegration of the Soviet Union, Russia's information security strategy has always centered on protecting national information sovereignty and safeguarding national interests in the information field. This long-term and stable strategic orientation is precisely the embodiment of strategic inertia that maintains the consistency of strategic behavior based on past experience and tradition. Especially in the face of emerging information security threats and technological changes, Russia's information security strategy is relatively slow to adjust, which can be explained by the formation mechanism in the strategic inertia theory. Second, Russia's behavior in

① Wang Ruixuan, Wu Shaozhong, Han Mengyang, and Zhang Xuanyi: "Analysis and Inspiration of the Biden Administration's National Cybersecurity Strategy—Based on the Perspective of Strategic Inertia", Intelligence Magazine, No. 12, 2023, p. 11.

② Hoffmain F.G.Neuhard R.Avoiding Strategic Inertia:Enablinh the National Security Council. Orbis, vol.60, No.2 2016,pp.217-236.

③ Polsky A.Staying the Course:Presidential leadership,Military Stalemate,and Stratedic Inertia.Perstives on politics,Vol.8,No.1,2010,pp.127-139.

international information security cooperation is also affected by strategic inertia. Russia has long adhered to the concept of independent information security. Under the influence of strategic inertia, this concept has caused it to have many concerns in international cooperation. When sharing information and technology with other countries, Russia overemphasizes the protection of its own information sovereignty, fearing that cooperation will pose a potential threat to sovereignty. Under the framework of international organizations and multilateral cooperation, Russia has difficulty reaching a consensus with other countries in the discussion of information security rule-making due to strategic inertia. Therefore, the theory of strategic inertia can precisely explain Russia's behavior pattern in international cooperation. Third, based on the theory of strategic inertia, the future development trend of Russia's information security strategy can be predicted to a certain extent. Due to the existence of strategic inertia, Russia may continue some of its existing strategic patterns and behaviors in the short term. When the external environment changes, Russia may have to adjust its strategic means, which provides a theoretical basis for analyzing the dynamic changes in this strategic development.

（二）Characteristics of the formation mechanism of Russia's information security strategy

The formation mechanism of strategic inertia is affected by many factors: First, the organizational structure. Complex organizational structures are often accompanied by cumbersome processes and established divisions of labor, which hinder strategic adjustments. Different departments may resist strategic changes in order to protect their own interests and responsibilities. Second, cognitive factors. Decision-makers in organizations or countries are influenced by past successful experiences and tend to form fixed cognitive patterns. The success of past strategies makes them firmly believe in the effectiveness of existing models and resist change. Third, resource allocation. Resource allocation tends to be in the direction of existing strategies. The resource dependence or resource-oriented model formed by long-term investment makes it difficult to reallocate resources.

1.Path dependence in the operation of the power system

Russia has a large information operations organization to support the operation of information strategic means and thereby achieve its domestic and international strategic goals.[①]During the Soviet era, information technology and information psychology operations were conducted by state security agencies, with the KGB being the main security and intelligence agency of the Soviet Union. By the late 1970s, the Kremlin had established an institutionalized system for conducting secret and overt military and non-military information operations. With the advent of the digital age in the late 1990s, Russia had to adjust its Soviet-era strategy and establish a presidential responsibility system in the field of information security, stipulating that the main structure of the information security system is determined by the president, which is the organizational basis for information security assurance (see Figure 1).[②]It can be seen that Russia prefers to ensure information security by concentrating its efforts and strengthening state control: in terms of strategic orientation and concept, compared with the United States and the West, which focus on the free flow of information and the mechanism of pursuing a balance between security and freedom in the market, Russia's information security strategy emphasizes the state's absolute control over information security, regards information sovereignty as the core, and focuses on preventing external information infiltration and maintaining domestic information stability, aiming to build an autonomous and controllable information space. In terms of organizational structure and responsibilities, the Russian President, the National Security Council, and the Federal Security Council are in a core decision-making position, comprehensively coordinating and guiding the information security strategy. Government departments perform specific tasks under their leadership, and each department has a clear division of labor and cooperates with each other, forming a centralized organizational structure with state power as the core. Obviously, Russia's organizational structure in the field of information security is completely opposite to the European and American countries' focus on multi-departmental collaboration and

① Lesley Kucharski. “Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe.” Lawrence Livermore National Lab. (LLNL), Livermore, CA (United States). 2019. https://www.osti.gov/biblio/1635758

② You Xian Ju, Gao Shangbao: "Interpretation of the Russian Federation Information Security Doctrine (2016)", Confidentiality Science and Technology, No. 2, 2016, pp. 37-39.

close cooperation with private enterprises. In terms of technology research and development and industrial development, the Russian government plays a leading role in information security technology research and development and industrial development, rather than a market-driven model, and will concentrate resources to support key technology research and development and the development of state-owned information security enterprises. In summary, although the organizational structure of Russia's information security strategy seems independent and has a clear division of labor, it actually serves the national information security strategy in a unified manner, and the deep power system and core organizational structure are almost unaffected. Therefore, the formulation and implementation process of the information security strategy cannot escape the control of this system.

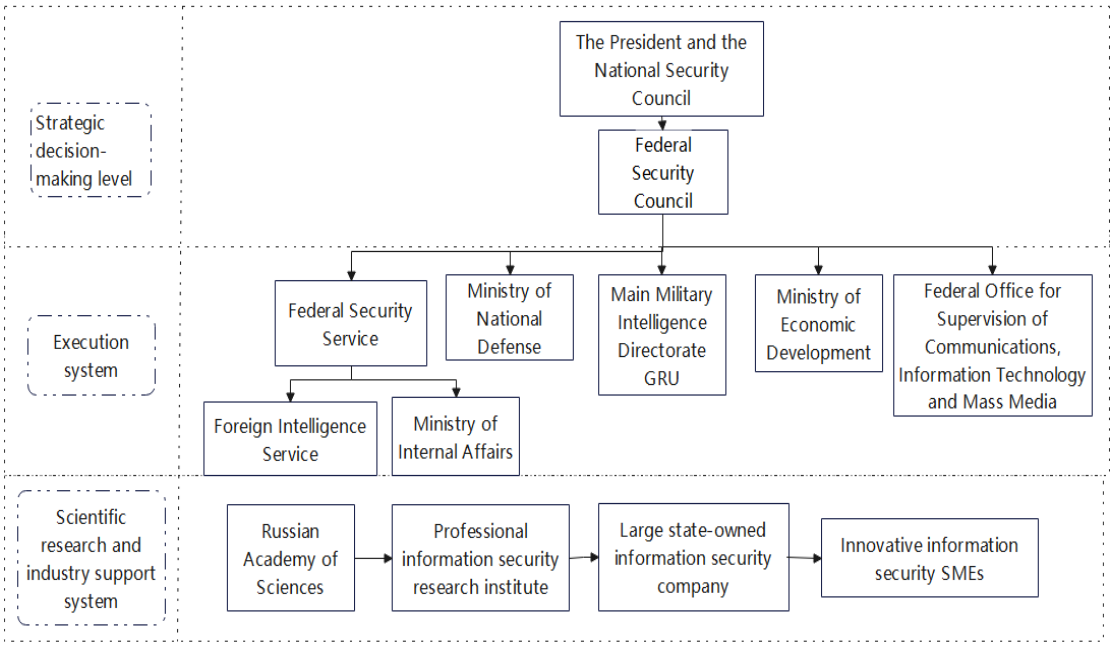

Figure 1 Basic framework of Russian information security organizational structure

2.The shackles of the political elite's inertial thinking

Historically, Russia has a long tradition of autocratic rule. This historical background may lead some political elites to have strong authoritarian tendencies in their thinking. In the decision-making process, it tends to concentrate power to a large extent and emphasizes top-down decision-making, which to a certain extent restricts the development of democratic participation and pluralistic decision-making, and makes it difficult to fully mobilize the enthusiasm and creativity of all social classes.

In terms of information security construction, Russia's new national security concept requires it to choose between integration and protectionism, multipolarity and unipolarity, that is, Russia will seek to integrate into the international community, but only within the scope and conditions it deems appropriate, rather than following the route set by other countries.[①]Frequent references by political elites to "foreign agents," in particular those regarding threats of "information-psychological operations" targeting collective public consciousness, and the determination to establish complete control over parts of the Russian Internet and deprive private companies of their remnants of freedom all highlight the many fears that Russia's corrupt and aging population has about information technology and its internal upheavals (such as the "Twitter Revolution").[②]

Under this circumstance, in order to avoid risks, the Russian information security policy-making group often adheres to empiricism, solidifies their thinking, and forms cognitive inertia in order to promote national information security construction and their own interests. In the Russian information security organizational structure, President Putin has also served as the director of the Federal Security Service. Most officials in various security intelligence departments have worked in cyber intelligence or come from the KGB, and are important influencing factors in the strategic decision-making process. These elites have long-term work and practical experience in cyber security and intelligence work, and are more inclined to make strategic repairs. Under the domination of the "stability" mentality and limited rationality, the policy-making group will exert inertia and weaken the innovation of strategic adjustments.

3.Passive prevention/response-oriented strategic model

George Kennan laid out the dual nature of information threats to the state—playing both a destabilizing and a legitimizing role—in his famous 1947 essay, "The Sources of Soviet Conduct." He wrote: "Serious or widespread opposition to the

① Nikolai Sokov. Russia′s new concept of national security. EastEuropean Constitutional Review,2000,PP.83—87.

② Sergey Sukhankin.Russia′s New Information Security Doctrine: Fencing Russia from the "Outside World"?Eurasia Daily Monitor Volume: 13,p. 198.
https://jamestown.org/program/russias-new-information-security-doctrine-fencing-russia-outside-world/

Kremlin may arise spontaneously in Russia, and as the masses are liberated from its authority, it may become necessary to justify the dictatorship by emphasizing the threat of capitalism abroad."[①]Kennan seemed to imply that the Soviet description of the foreign information threat was real, that the elites did consider any information that contradicted the state narrative to be a foreign attack, and that labeling anti-regime narratives as foreign threats was an effective method. In 1998, U.S. Army analyst Timothy L. Thomas, comparing key differences between Russian and American approaches to information operations, noted that Russia's focus on "information psychology" was intended to protect its society from foreign manipulation operations by various means.[②]The Soviet Union has long recognized the importance of information in domestic security and control, foreign armed conflicts, and broader geopolitical competition. This is prevalent in Soviet theory and practice. On the one hand, in terms of security threat cognition, Russia regards Western information infiltration, cyber attacks, and potential threats to its information infrastructure as major security challenges. It also pays attention to ideological struggles in the information field, believing that external forces are trying to subvert its social system and values through information dissemination. On the other hand, at the policy level, the core of Russia's entire security legislation system is its key goal of information security, namely, responding to external threats and overcoming international "discrimination" against Russian media. Although Russia is good at using "information manipulation" to achieve national goals and safeguard national interests, it is not difficult to find from a review of its information security strategy that the information strategy emphasizes the national security risks of the Russian Federation related to information warfare. Strategies including "information warfare" are defensive concepts. This is Russia's "mentality", and this decision-making thinking has prompted Russia to form and solidify a "passive prevention/

① George F. Kennan, "The Sources of Soviet Conduct," Foreign Affairs, 1947, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct.

② Timothy L. Thomas. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations." Journal of Slavic Military Studies, 1998, Vol.11, No.1, pp. 40-62. https://community.apan.org/cfs-file/__key/docpreview-s/00-00-08-56-53/1998_2D00_03_2D00_01-Dialectical-Versus-Empirical-Thinking-_2800_Thomas_2900_.pdf

response-oriented" strategic model. Therefore, in the actions to protect information security, in order to take defensive measures, Russia often takes the initiative, which shows how deep its strategic inertia is.

（三）Characteristics of Russian information security strategy under the mechanism of strategic inertia

Russia's information security strategy is subject to the influence of strategic inertia, which can ensure the continuity of Russia's information security policy. At the level of legislation and strategic inheritance, the policies have always reflected Russia's emphasis on information security, and the content of relevant policies has been continuously enriched and improved. At the level of institutional and functional stability, the presidential responsibility system enables all departments to serve the national information security strategy in a unified manner. At the same time, it ensures that the functions of information security management and assurance are relatively stable, and also ensures that information security policies can be effectively implemented and implemented.

Although the inertial thinking of Russia's information security strategy has certain positive significance, it also has some drawbacks, which are mainly manifested in the following aspects: First, strategic lag. The technology in the field of information security is rapidly updated, and new threats and risks continue to emerge, such as security issues brought about by the development of artificial intelligence and the Internet of Things. Due to strategic inertia, Russia may rely on past experience and models, and it is difficult to quickly adapt to these new changes. It may be unprepared when dealing with new network attack methods and technologies, resulting in delayed response and increasing the risk of being attacked. Second, unbalanced resource allocation. Due to strategic inertia, Russia may continue to invest a lot of resources in traditional information security fields, such as military and critical infrastructure protection. However, the investment in emerging information security fields, such as cloud computing security and big data security, is relatively insufficient, resulting in the lagging development of these fields, unable to meet the needs of national digital transformation, and affecting the overall information security

situation of the country. Third, insufficient innovation motivation. Russia relies on existing technical routes and solutions in the research and development of information security technology, and lacks exploration and experimentation of new technologies and new methods. This will inhibit the vitality of domestic information security technology innovation, causing Russia to gradually lag behind in the global information security technology competition and find it difficult to master core technologies and key discourse power. Fourth, the talent training model is rigid. The training of information security talents may follow the traditional model, focusing on the imparting of existing knowledge and skills, while neglecting the training of innovative thinking and interdisciplinary capabilities. This will make it difficult for the trained talents to adapt to the ever-changing needs in the field of information security and lack the innovative ability to cope with complex and changing security challenges. Fifth, the institutional mechanism is rigid. The decision-making mechanism of Russia's information security policy is rigid, and the decision-making process is cumbersome and slow. When faced with urgent information security incidents or when policy adjustments need to be made quickly, it is difficult to respond quickly, especially when dealing with cross-departmental and cross-field information security issues. Problems such as poor coordination and unclear responsibilities may occur, resulting in missing the best time to respond and aggravating the degree of harm caused by information security incidents.

Due to Russia's traditional great power consciousness and the values of collectivism, national authority and order, as well as deep-rooted power mechanisms, its information security strategy remains highly vigilant and defensive, making it difficult to get rid of the drawbacks of the inertial strategy.

二.Adjustment of Russian Information Strategy in the Context of the Russian-Ukrainian Conflict

The drawbacks brought by strategic inertia make it impossible for Russia to respond in time when facing security threats, resulting in strategic sluggishness. However, in the context of the Russia-Ukraine conflict, a series of highly targeted and innovative practices have been carried out to ensure Russia's information security.

First, in terms of technological empowerment, Russia has demonstrated innovative use of emerging technologies. During the conflict, Russia made full use of modern information technology to accurately control and guide the dissemination of public opinion, presenting the real situation on the battlefield to global audiences in a timely and intuitive manner, breaking the information monopoly of Western media and effectively shaping its own international public opinion image. Secondly, in terms of information supervision, Russia has elevated it to the core position of national strategy, formulated a series of policies and regulations that keep pace with the times, and increased the crackdown on false and harmful information. In the process of policy implementation, the Russian government has strengthened the supervision of various media platforms and curbed the spread of bad information from the source. Finally, network defense at the "whole society" level has also shown a new development trend. Russia actively promotes the coordinated participation of various forces such as government agencies and hacker organizations in network defense, forming a solid network defense barrier and effectively responding to external network threats and challenges.

（一）Technology empowers public opinion control

Russia is engaging in an asymmetric cognitive game around the world, aiming to protect the core of its civilization and maintain national identity. In terms of strategic narrative, the Russian National Security Strategy points out that the international situation under modern conditions is increasingly affected by the growing confrontation in the global information space, which is due to the desire of some countries to use information and communication technologies to achieve their geopolitical goals, with the goal of manipulating public consciousness and falsifying history.[①]The theoretical basis of Russia's information security strategy is to respond to information attacks from the United States and Western countries, conduct large-scale government propaganda, and protect Russia's national interests. Through propaganda and information campaigns, it demonstrates its economic stability, social development,

[①] Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 № 683. –[Электронный ресурс]. URL:URL: http://kremlin.ru/acts/news/51129

and international authority as an argument against the negative impact of false information and hybrid threats. In terms of strategic measures, in order to safeguard national security, a space designated by the concept of "national culture" is formed, based on the recognition of the significance and value of national culture by all citizens of the country. This is why "rewriting history" in crises is used as the main means of information confrontation to adapt to geopolitical interests. Compared with traditional public opinion propaganda, technology has become a powerful driving force for Russia's information security strategic measures in recent years.

Especially in the cognitive warfare of the Russia-Ukraine conflict, a large number of advanced technologies such as machine learning, image recognition, knowledge graphs, and deep fakes have been applied, providing powerful technical empowerment for actions such as public opinion propaganda, psychological guidance, and cognitive intervention, enriching the combat style and triggering a major change in the evolution of cognitive warfare equipment.[①]This is mainly reflected in Russia's strategic means of cognitive manipulation. For example, in the first two weeks of the EU sanctions on Russian media, the Kremlin took several temporary measures aimed at circumventing the ban. The Android version of the RT application was available for direct download, thus circumventing the ban on the Google Store, while social media accounts promoted high-quality RT live links provided through network proxy services, using the infrastructure of mirror accounts to share the latest links and expand propaganda. These temporary measures have brought about systematic changes in the Kremlin's propaganda methods. Among them, the focus has shifted to Telegram, which is less familiar to Western users, as the main social media platform for public opinion in both Russia and Ukraine. Telegram provides an alternative infrastructure for influence, using trolls to guide other social media users on a large scale to the Russian-controlled Internet, and the relevant network rules and content are manipulated by Russia. During the conflict, Telegram, as a broader digital diplomatic channel infrastructure, supplemented by the accounts of well-known

① An Zidong, Hao Zhichao: "Analysis of Cyber Confrontation in the Russia-Ukraine Conflict", "Information Security and Communications Confidentiality", Issue 11, 2022, pp. 2-8.

state-related figures, became the main source of Kremlin propaganda within the EU.[①]It is worth noting that social robots have played an important role in the Russia-Ukraine public opinion war. AI robots can independently run accounts, engage in social interactions, build social networks, effectively manipulate public opinion, and promote "cyber terrorism", playing a huge inciting role in the war.[②]A study by New York University in the United States shows that more than half of the Russian-language tweets related to Russian politics are from robots.[③]At the same time, advanced persistent manipulation teams associated with government agencies also operate through social media and digital platforms, pre-deploying false narratives in a manner similar to the pre-deployment of malware and other software codes. They then "report" these narratives extensively and simultaneously from websites managed and influenced by the government, and amplify the narratives through technical tools designed to exploit social media services. As part of Microsoft's new plan, Microsoft is using artificial intelligence, new analytical tools, a wider data set, and a growing team of experts to track and predict this cyber threat. Judging from the public opinion trends in Russia, Russia's means of controlling public opinion are effective, and the influence of technological factors in cognitive public opinion has greatly increased compared to the past.

（二）Information regulation becomes a national public policy priority

"Information" confrontation is not new, but a country that cannot resist "information" threats will face security threats in the modern world, which requires early and rapid regulation of this situation. For a long time, due to the inertia of the vertical power system, conservatism has become a characteristic of the Russian political system, which means that government agencies have extensive powers, including in the field of information, which is characterized by strict government control and supervision.

---

① James Pamment.How the Kremlin circumvented EU sanctions on Russian state media in the frst weeks of the illegal invasion of Ukraine.Place Branding and Public Diplomacy，No19, 2023,pp.200－205.

② Li Shu: "Prevention of Extreme Risks on the Internet and Game among Great Powers", Journal of Tongji University (Social Sciences Edition), No. 4, 2022, pp. 48-57.

③ Li Shu: "Prevention of Extreme Risks on the Internet and Game among Great Powers", Journal of Tongji University (Social Sciences Edition), No. 4, 2022, pp. 48-57.

According to the Russian political tradition, the production and consumption of personal information resources are restricted, state control is strengthened, and it is equally important to use information resources to protect state sovereignty. In the information security strategy, Russia has taken this into account, and in recent years, the process of developing a national strategy required for the implementation of this task has been significantly strengthened. Under the influence of the information revolution, the Russian political leadership is strengthening control in the information field. The main policy is to focus on the content of information transmitted through telecommunications networks. Data published and transmitted on the Internet must comply with legislative norms, including established national standards. The data localization norms formulated by Russia show that the understanding of the "information" phenomenon by national law does not take into account the characteristics of this resource, but regards it as a physical phenomenon under the jurisdiction of state sovereignty. In fact, in most theoretical documents, state interests and citizen interests are opposed. In particular, the newly revised "Information Security Doctrine" retains the principle of the trinity of personal, social and national interests adopted in the 2000 version, but the rules involving personal interests disappear, and only the content involving national interests is retained. It can be seen that Russia's information supervision principle is that national information security is more important than personal information freedom, which is exactly the opposite of the "net neutrality" principle pursued by the United States and Western countries. It has become the root cause of the information struggle between Russia and the United States and the West, and has also led to the Russian national security agencies being criticized at home and abroad for ignoring the legal procedures for obtaining Russian private information. Critics believe that Russia's information supervision policy is similar to the "Iron Curtain" during the Cold War.[①]

Earlier, after Telegram refused to provide encryption keys to national security agencies, Russia's national communications regulator blocked all Internet addresses of

[①] П.Ш.Натадия.Степанова подходы США,ЕС и России к проблеме информационной политики современная Европа,No2,2019,p.73-81.

the social network. The relevant actions resulted in the blocking of 20 million Internet addresses, including addresses providing services such as Amazon and Google. In the 2022 Russian-Ukrainian conflict, in order to resist the policy squeeze of the United States and the West in the information space, Russia has formulated a stricter regulatory framework. Blocking Russian citizens from accessing Facebook and Twitter, shutting down access to the Russian-language news broadcasts of Radio Freedom in the United States, shutting down the independent Russian news service Meduza (designated as a "foreign agent media" by the Russian authorities), and blocking two well-known independent media websites Echo Moscow and Dozhd. Earlier, Dmitry Peskov said that in response to the information war launched against the country, it is necessary to impose criminal penalties for the spread of false information about the behavior of the Russian armed forces. To this end, Russia has passed a law that criminalizes the spread of "fake news", which is punishable by up to 15 years in prison.[①]At the same time, Russia took public censorship actions against the social network Twitter for the first time. These events further prove the strictness of Russian government agencies in regulating information exchange.

In essence, the information blockade strategy is almost the same as the confrontation strategy, clearly recognizing the existence of the "other". The difference is that this strategy is inward-looking and protective, in the sense that it aims to maintain the national strategic narrative but not to promote it to foreign audiences. This can be described as a defensive strategy, verifying the passive prevention-oriented strategic model influenced by inertia and denying the public access to the narrative projected by the "other". In recent years, influenced by the inherent "paternalistic" regulatory policy and the threat of public opinion in the Russian-Ukrainian conflict, the Russian authorities have been working to tighten their information policy. This politically motivated policy approach may lead to the regulatory system becoming permanent.

（三）Cyber defense at the “whole of society” level

① Todd C. Helmus ,Andrew Radin.Keeping Russians Informed About Ukraine Could Help End This War. URL:https://www.rand.org/blog/2022/03/keeping-russians-informed-about-ukraine-could-help.html

After the Ukrainian crisis, the task facing the Russian armed forces is to enhance their ability to prepare for war and resolve armed conflicts by adopting classical and asymmetric actions. In 2019, Gerasimov published a report that believed that Russia's military development was faster than that of its enemies, and that it relied on a military strategy of "surpassing the enemy" to activate Russia's dominance in information warfare.[①]To this end, Russian decision-makers regard information as the core of security policy and "hybrid warfare" or "full spectrum conflict", using a combination of subversive strategies at multiple levels, from conventional military means to secret special forces, intelligence systems, economic threats and political influence, to ensure national security.

First, the Russian military has raised the prevention and confrontation of cyber information aggression to the national strategic level and strengthened its cyber warfare capabilities. The thinking of the Russian military elite has changed significantly since the Russian-Ukrainian conflict. At the level of strategic planning and policies and regulations, Russia emphasizes the strategic position of information security. In the 2021 National Security Strategy, it is proposed that "the purpose of information security is to strengthen the sovereignty of the Russian Federation in the information field". After 2022, this strategic guiding ideology continues to deepen, providing strategic guidance for preventing and confronting cyber information aggression. In terms of cyber warfare capabilities, Russia has established special information forces to implement cyber information warfare offensive and defensive operations, enhance combat capabilities in cyberspace, respond to cyber information aggression threats with professional forces, and perform network reconnaissance, attack, defense and other tasks. In terms of information infrastructure construction, based on the Sovereign Internet Law, Russia continues to promote RuNet network isolation exercises and improve network infrastructure, develop independent network communication technologies, such as realizing the autonomy of the Russian national domain name (DNS), reduce dependence on external networks, and enhance the

① Доклад Валерия Герасимова «Вектора развития военной стратегии». 01.03 2019 г. https://bmpd.livejournal.com/3557155.html

autonomy and security of the network. In terms of cyber security practice, the Russian military actively carries out cyber warfare operations to attack and interfere with the enemy's network systems, such as launching network paralysis attacks on Ukrainian government and media websites. At the same time, it regularly holds various cyber security exercises to enhance the actual combat capability and coordination and cooperation ability of the military and relevant departments to deal with network information invasion, test and improve cyber security strategies and tactics, and enhance defense and counterattack capabilities in cyberspace.

Secondly, Russia reorganized its intelligence agencies to improve the network coordination capabilities of the intelligence system. After the Russian-Ukrainian conflict, the Russian intelligence agencies, together with the Federal Security Service and the General Staff Intelligence Department, took joint actions to break the traditional division of labor and strengthen information sharing and coordinated actions. In addition, more funds, equipment and facilities resources were invested in intelligence work to strengthen satellite reconnaissance, electronic monitoring, network intelligence collection and other capabilities. At the same time, a strategic shift in intelligence activities was achieved, including expanding the scope of overseas intelligence activities, especially increasing activities in Europe and neighboring countries, using foreign citizens to bypass restrictions on Russians, carrying out operations such as monitoring the West and tracking weapons shipped to Ukraine, and exerting pressure on Russian exiles and opponents of the Putin regime who fled abroad after the outbreak of the war.

Finally, from the perspective of tactics research, the high degree of integration of national power and civilian hacker corps can effectively combat all-round cyber threats. The national cyberspace combat force includes two levels: government and military. The government level is led by the Federal Security Service, including the Federal Ministry of Internal Affairs K Bureau, the Federal Security Protection Service, and the Foreign Intelligence Service. Its main tasks are to protect Russia from foreign network attacks and monitor domestic hackers, and to detect and monitor domestic and foreign cyber criminal gangs; the military level includes the General Staff

Operations Directorate, the General Staff Intelligence Directorate, the Cyber Command, the Information Operations Force, etc., with a scale of more than 7,000 people. The civilian hacker team includes Group 26165, Group 74455, the Internet Research Institute, etc., and coordinates with the Federal Security Service Information Security Center and the Ministry of Internal Affairs to carry out cyber attack operations.[①]Other civilian hackers have launched their own operations, especially the Russian hacker group Killnet, which has been active since January 2022. Its attack method is mainly DDOS, and its targets are Ukraine and countries that support Ukraine, mainly including the United States, Germany, Italy, Norway, Poland, Romania, the three Baltic countries and Japan. Unlike hacker groups such as FancyBear that are suspected to be affiliated with Russian intelligence agencies, Killnet does not seem to have anything to do with the Russian government and military.[②]These civilian hacker forces have participated in many cyber operations against US and European government targets, achieving coordinated operations among government, military and civilian forces. This approach strengthens the interaction between national forces, and national intelligence agencies, relevant departments and hacker organizations maintain strategic goals, focus on key attack areas, and improve organizational cooperation and coordination.

It is worth noting that in the international situation, when a country faces severe security threats, its strategy often shows a trend of breaking inertia. This kind of breaking inertia usually means bold innovation and transformation of past strategic models to adapt to the new and challenging security environment. In the complex and high-profile geopolitical event of the Russia-Ukraine conflict, Russia's cybersecurity operations have always been under the unified leadership of the authorities, and the relevant departments have cooperated very closely to form an efficient and coordinated organic whole. In the actual operation process, Russia can flexibly and quickly adjust the means of network attack and defense according to the dynamic

① Cao Weidong, Song Liuyong, Zeng Xiangwei: "Analysis of Cyber Warfare Tactics in the Ukrainian Crisis", Information Security and Communications Confidentiality, No. 7, 2023, pp. 22-29.

②Luo Dongsen, He Junwei, and Lv Wei: "Overview of Active Hacker Groups in 2022", Information Security and Communications Confidentiality, No. 4, 2023, pp. 2-11.

changes of the battlefield situation. In the fierce cyberspace game with the United States and Western countries, it maintains national security and steadily moves towards achieving strategic goals. In this process, it is not oriented towards breaking strategic inertia and pursuing radical change. However, Russia's use of technology to strengthen public opinion control, information supervision and the extensive participation of hackers shows the "inward" tendency of its security strategy. The strategy itself focuses more on adhering to established principles within the existing power system, further deepening strategic inertia.

三、The force of inertia: An assessment of Russia's information security strategy

（一）Strategic continuity and stability

In recent years, the information warfare between Russia and the United States and the West in Eurasia has caused countries to rethink the forms and means of warfare. The focus of competition between major powers in the information field is shifting to the use of political, economic, information, humanitarian and other non-military measures, including the implementation of information warfare initiatives and special operations forces operations, to comprehensively suppress Russia.[①]On the contrary, Western information strategic means and deterrence have not had an impact on Russia's political decision-making. Under the influence of inertia, Russia's information security strategy has shown remarkable continuity and stability in strategic goals, strategic means, and emphasis on key areas.

First, the continuity of strategic goals. The international information security situation is becoming increasingly complex, and the external information security challenges facing Russia are increasing. However, the core connotation of its strategic goals has remained unchanged. In the latest international information security strategy approved by Russian President Vladimir Putin in 2021, it is clearly stated that the country's technological sovereignty in the field of information and communication technology should be ensured and information inequality between developed and developing countries should be overcome. This goal is highly consistent with the

[①] Сотрудничество в противодействии гибридным угрозам. 23.11.2018. [Электронный ресурс]. URL: https://www.nato.int/docu/review/2018/Alsoin-2018/cooperating-to-counter-hybrid-threats/RU/index.htm

early emphasis on protecting the country's interests in the information field and maintaining information sovereignty. It is a continuation and deepening of traditional strategic goals under new historical conditions, reflecting the consistency and stability of Russia's information security strategy.

Secondly, the continuity of strategic means. On the one hand, strengthening domestic information security construction is an important measure for Russia. Promoting the localization of information technology and equipment and achieving "independent control of key and core technologies" is the direction that the country has long adhered to. Through a series of policy support and capital investment, the country can reduce its dependence on foreign technology and ensure national information security. This domestic construction method has been continuously used in the development of Russia's information security strategy and has become an important cornerstone for ensuring information security. On the other hand, actively carrying out international cooperation is also an important part of Russia's information security strategy. With the help of platforms such as the Shanghai Cooperation Organization and the Collective Security Organization, Russia has joined hands with partner countries to do a good job in "in-circle" information security protection. In these regional cooperation organizations, Russia and member states jointly carry out information security technology exchanges, joint exercises and other activities to enhance the overall regional information security protection capabilities. This combination of internal and external strategic means has existed since Russia's early participation in international information security affairs, and has been continuously developed and improved with changes in the international situation, reflecting significant continuity.

Finally, the continuity of the emphasis on key areas. In terms of cyberspace security, Russia continues to invest resources to strengthen the construction of cyber defense forces. From the establishment of professional cyber warfare forces to the development of advanced cyber defense technologies, it continuously improves its combat capabilities in cyberspace. By strengthening the construction of a cyber security monitoring and early warning system, Russia can grasp the cyber security

situation in real time and detect and respond to cyber attacks in a timely manner. In the field of ideology, Russia closely links information security with ideological struggle and fights back against Western infiltration in various ways. For example, it popularizes patriotic education in the country, strengthens the promotion of its own culture and values, and enhances the people's national identity and national pride. At the same time, it strengthens the management of media and network information to prevent the spread of bad Western information. Russia also actively carries out external propaganda to spread its own voice and values and strive for more voice in the international public opinion field. This emphasis on information security in the ideological field has existed since the formation of Russia's information security strategy, and corresponding measures have been taken at different times to strengthen it.

However, the potential for action in the field of information warfare could drive Russia’s future security policy and strategy. The Russian leadership may choose to formally incorporate the research, development, and use of cyber weapons into its information strategy doctrine as an official line. However, this scenario seems unlikely, given the defensive nature of the current Russian information warfare doctrine, which could strengthen its claims of plausible deniability. On the other hand, due to the strategic mutual suspicion and structural contradictions between Russia and the United States and the West, the Russian military will undoubtedly continue to value conventional assets and invest in modern combat tactics, while unconventional means (especially cyber offense and defense) are becoming increasingly prominent in Russia’s ongoing competition with the West.

（二）Strategic constraints and bottlenecks

As the international information security landscape continues to evolve, Russia's information security strategy is deeply influenced by inertia, encountering many difficulties in the development process and facing significant bottlenecks and constraints.

First, the lag in strategic adjustment. Traditional strategic thinking focuses on responding to obvious external information security threats, such as external network

attacks and information theft, but lacks sufficient foresight and innovative thinking for potential and indirect information security risks, such as the impact of changes in the international information and public opinion environment on national information security, the unknown security risks brought about by the application of emerging technologies and external sanctions. In the era of social media, the rapidity and extensiveness of information dissemination have made information and public opinion warfare an important part of information security. However, due to the rigidification of strategic thinking, Russia has failed to timely incorporate information and public opinion warfare into the core category of information security strategy at the strategic level. It has been slow to respond to emerging security threats and technological changes, and it is difficult to quickly adjust the strategic layout and formulate effective response strategies, which puts it at a disadvantage in the international information and public opinion competition, restricting the comprehensive development of information security strategy.

Second, insufficient resource investment. Although Russia's investment in information security continues to grow, the total amount of funds is still insufficient compared with Western countries such as the United States. In some key technology research and development projects, the research and development progress is slow due to lack of funds. For example, in the development of high-end chips, it is difficult for Russia to make major breakthroughs in the short term and it still needs to rely on imports. Although Russia has a high combat capability, it still faces major challenges in the field of information warfare, especially cyber warfare. Like other government agencies, Russian security departments face the challenge of recruiting professionals. The private sector and competitors compete for talent, which often leads to Russian security departments outsourcing their business to civilian hackers. In 2013, more than 100 universities in Russia trained experts in the field of information security in accordance with the six national higher vocational education standards. There were about 150,000 people working in the industry in the country, and the actual demand

exceeded 500,000 people.[①]Especially in the 2022 Russia-Ukraine conflict, Russia's best experts (including those dealing with cybercrime) have been involved in offensive cyber activities. Due to personal sanctions from the United States and the West, Russian cybersecurity experts (perhaps even a quarter of them) are planning to leave Russia. The authorities need to find a solution, perhaps introducing more stringent restrictions rather than incentives to retain professionals.

Third, capacity building is lagging behind. Especially in terms of technology research and development and innovation, in order to accelerate the development and innovation of information technology and reduce dependence on foreign technology products, Russia's information society development strategy must have the mechanisms and technologies required to solve this task. On the one hand, Russia lists information and communication technology as the main direction of development to provide sufficient technical foundation and guarantee for national security construction. The "Russian Information Security Doctrine" clearly stipulates that the scientific and technological potential in the field of information space construction is mainly related to innovation and independent control, so as to enhance Russia's competitiveness in the field of information and communication technology. On the other hand, in order not to lag behind in the information space and not be subject to other countries, Russia will accelerate the implementation of import substitution in the field of information technology. Especially after the Ukrainian crisis, Western sanctions promoted the Russian government's import substitution process. In 2014, Russia began to study and formulate a list of import substitution plan projects, and information and communication technology became a priority development area for import substitution.[②]Russia has promulgated the "Implementation Plan of the (National Outline of the Russian Federation's 'Digital Economy') in the Field of Information Security", which will significantly reduce the share of Internet traffic using overseas routers (to 10% in 2024), significantly reduce the proportion of

① Kravcov A.A. Podgotovka kvalificirovannyh kadrov po discipline «Konkurentnaja razvedka» v Rossii i drugih stranah. Internet-zhurnal <<Naukovedenie>> (VAK).No2 ,2013,p.15.

② You Xianju: "Ideas and Practices in Building Russia's Information Space", "Russian, Eastern European and Central Asian Studies", Issue 5, 2017, p. 58.

imported computers, network communication equipment and software products used by government departments and state-owned institutions, and steadily increase the proportion of government agencies, research institutes and state-owned institutions that use secure interaction protocols for information exchange (to 90% in 2024), etc.[①]At the St. Petersburg International Economic Forum in 2022, the Russian government proposed to attach importance to the implementation of the software import substitution plan and the domestic microelectronics development plan. These measures are aimed at enhancing the competitiveness of Russian industry and the level of nationalization of related products, and reducing the heavy dependence on foreign technology and industrial products.

In fact, Russia's national strength is still in the recovery stage, and its economy and society are also in a period of transformation. Its information infrastructure is still underdeveloped and the way of using information is not perfect, which hinders Russia's construction of an information security system.[②]At the same time, the United States dominates the global economic system and uses sanctions to put pressure on Russia. Once economic development is affected, the corresponding investment in information infrastructure construction, the development and research of information technology, the training of scientific and technological talents, etc. will inevitably be affected, thus affecting the country's overall networking and informatization development level.[③]Therefore, in the short term, economic sanctions and development issues will remain key factors hindering Russia's scientific and technological research and innovation.

四、Conclusion

The Russian-Ukrainian military conflict will not fundamentally change the original information space pattern. The information warfare and cyber attacks that come with the conflict are increasingly becoming new means of inter-state gaming,

① You Xian Ju, Jie Jing, and Tian Sumei: "A Review of Russia's Information Security Construction in 2018", Confidentiality Science and Technology, No. 2, 2019, pp. 43-48.

② Xiao Jun: "Construction and Enlightenment of Russia's Information Security System", "Intelligence Magazine", Issue 12, 2019, pp. 134-137.

③ Ban Jie, Lu Chuanying, "The Adjustment of Russia's Cyberspace Strategy from the Perspective of the Federal Government's Information Security Theory", Information Security and Communications Confidentiality, No. 2, 2017, pp. 82-85.

especially with the involvement of non-state actors, making the confrontation situation in the global information space more complicated and the consequences of actions difficult to predict.[①]Through the above research, Russia regards external threats as the main threat to information security. Due to the solidification of the power system, the limited rationality of decision-making elites and the passive prevention resource orientation, Russia's information security strategy is affected by inertial thinking. In addition to the threats of internal and external situations, even if the strategic practice means are adjusted, it still maintains or even deepens the strategic inertia. At the same time, the Russian-Ukrainian conflict further promotes Russia's information strategy to deepen its organizational and regulatory capabilities, driving Russia's future network policies and strategies. In the future, it may continue to consolidate the role of network and information operations and strengthen investment in unconventional means such as digital. The confrontation in the information field may continue.

Information warfare is not a new thing, but its widely used information space has a transformative impact on the international order as a new field of great power game. The problem of global information network security governance needs to be solved. It is necessary to continuously combine information security strategy with information space governance practice, and straighten out practical logic and game thinking to ensure that the dual goals of regulation and development, competition and security are achieved between major powers.

① Zhang Zaitian and Gong Hanqing: "Looking at Malicious Data Wiping Software Attacks from the Perspective of the Russian-Ukrainian Military Conflict", Information Security and Communications Confidentiality, No. 11, 2022, pp. 22-27.