Constructing a New Framework for Digital-Intelligence Security to Safeguard the New Development Pattern Postprint

Authors: Yang Xiaoguang, Wu Yang, Zhang Xingwei, Zheng Xiaolong

Date: 2024-03-27T00:00:00+00:00

Abstract

With China' s entry into a new development era following the 20th National Congress of the Communist Party of China, the rapid development and widespread application of digital-intelligent technologies have unleashed new potential for economic growth while also introducing novel security challenges to economic and social development. The article first analyzes the characteristics of the new development pattern under the new international and domestic circumstances, and examines the digital-intelligent security risks and challenges within this new development pattern, encompassing technical security and personal security at the micro level, as well as economic security, social security, and cultural security at the macro level. Building upon this foundation, the article proposes a fundamental methodology for constructing a new pattern of digital-intelligent security, presenting a basic framework for this new pattern that covers three dimensions: the security of digital-intelligent technology itself, digital-intelligent technologies for ensuring digital-intelligent security, and the laws, regulations, and policies governing digital-intelligent security. Finally, the article explores the dialectical and spiral-shaped co-evolutionary relationship between the new pattern of digital-intelligent security and the new development pattern, providing guidance for ensuring the healthy and sustainable development of the economy and society in the new era.

Full Text

Building a New Paradigm of Digital Intelligence Security for New Development Pattern

YANG Xiaoguang[12], **WU Yang**[4], **ZHANG Xingwei**[4], **ZHENG Xiaolong**[34]*

[1] Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[2] School of Economics and Management, University of Chinese Academy of Sciences, Beijing 100190, China
[3] School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100190, China
[4] State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China

Abstract

Following the 20th National Congress of the Communist Party of China, China has entered a new era of development. The rapid advancement and extensive application of digital intelligence technologies have unlocked new waves of economic potential while simultaneously introducing novel security challenges to socioeconomic development. This article first analyzes the characteristics of the new development pattern under evolving international and domestic contexts, and examines the digital intelligence security risks and challenges within this framework. These challenges span five dimensions: technological security and personal security at the micro level, and economic security, social security, and cultural security at the macro level. Building upon this analysis, the article proposes a fundamental methodology for constructing a new paradigm of digital intelligence security, presenting a comprehensive architecture that encompasses three core components: the security of digital intelligence technologies themselves, digital intelligence technologies that safeguard security, and the legal and policy frameworks governing digital intelligence security. Finally, the article explores the dialectical and spiral co-evolutionary relationship between the new paradigm of digital intelligence security and the new development pattern, offering guidance for ensuring the healthy and sustainable development of the economy and society in this new era.

Keywords: digital intelligence security, new paradigm of digital intelligence security, new development pattern, security and development

---

1. Characteristics of the New Development Pattern

Digital technology has become deeply integrated into all aspects of social development. By the end of 2022, China' s digital economy had reached 50.2 trillion RMB, accounting for 41.5% of GDP, marking China' s entry into a digital era of national economic and social development. With the rapid development of artificial intelligence technologies such as big data and deep learning, digital technologies represented by computers, information, and communications are gradually evolving into digital intelligence technologies dominated by next-generation internet, generative AI, virtual reality, and digital twins. Data and intelligence have become core drivers of social progress, new engines for eco-

nomic and social development, and new focal points for government and social governance. Currently, generative AI exemplified by ChatGPT is triggering a new wave of intelligence through large model empowerment, with some scholars suggesting that the singularity of new-generation AI may be approaching [1]. However, while driving technological progress, the development of digital intelligence technologies also poses unprecedented challenges to national security systems. The report of the 20th Party Congress strategically deploys the modernization of national security systems and capabilities, emphasizing the need to safeguard national security and social stability, and proposes using a new security pattern to guarantee the new development pattern. At a time of profound social transformation, coordinating development and security is undoubtedly a complex systematic endeavor [2,3]. As digital intelligence technologies become deeply coupled with various functional structural modules of social and economic systems across multiple temporal and spatial scales [4], they have triggered a series of complex social security governance issues such as data misuse, algorithmic discrimination, and labor market fluctuations [5,6]. Facing these difficulties and challenges, it is crucial to thoroughly analyze the internal mechanisms of digital intelligence development risks—including data security and privacy leakage, algorithmic discrimination and unfairness, technological barriers and digital divide, and false information and information manipulation [7]—and to comprehensively understand the profound implications of coordinating development and security. Advancing the construction of a new digital intelligence security paradigm in key areas such as economy, society, and culture is essential for safeguarding the new development pattern. Based on the overall national security concept, this article examines the new characteristics of digital intelligence security risks under the new development pattern from both international and domestic perspectives, proposes a comprehensive framework for building a new digital intelligence security paradigm, and discusses the dialectical relationship between this new security paradigm and the new development pattern, offering policy recommendations for coordinating development and security in the digital intelligence era.

1.1 International Perspective

First, following the Industrial Revolution, the capitalist modernization model greatly advanced productivity and transformed lifestyles. However, the inherent contradictions of capitalism have continuously pushed the entire human modernization process toward extreme materialization and imbalance. In contrast, China' s path to modernization, through building a community with a shared future for mankind, connects its own modernization with global development, representing an innovation in human development models that will profoundly influence the world' s modernization process.

Second, the international trend of anti-globalization is intensifying, undermining the global division of labor and cooperation that had formed over the past decades. The Russia-Ukraine conflict and the Palestine-Israel conflict are re-

shaping the geopolitical landscape, creating enormous uncertainty for global prospects. Since 2017, the United States has imposed multiple rounds of sanctions on China, and China has responded with countermeasures, leading to difficulties in political, economic, and security exchanges between the two countries. These factors pose severe challenges to China' s external development environment from multiple angles including technology, capital, and markets.

Third, the COVID-19 pandemic triggered declining demand, production contraction, trade disruptions, logistics interruptions, and surging unemployment, pushing the global economy into recession. To combat the pandemic, massive U.S. fiscal stimulus policies exacerbated global inflation, prompting the Federal Reserve to initiate interest rate hikes that tightened global liquidity and increased external financing costs for Chinese enterprises and the government. The severe supply-side shock manifested directly in large-scale business shutdowns, worker unemployment, and widespread disruption of industrial and supply chains across multiple countries. Survey data from August 2023 shows that global unemployment surged from 192 million in 2019 to 235 million in 2020 due to the pandemic. Although the figure gradually recovered to 205 million in 2022, it remained nearly 13 million higher than pre-pandemic levels, with further increases projected for 2023.

1.2 Domestic Perspective

First, China' s economy has shifted from high-speed growth to high-quality development. The 19th Party Congress report stated that China' s principal social contradiction has transformed into the contradiction between the people' s ever-growing needs for a better life and unbalanced and inadequate development. In this new era, economic development must transition from pursuing quantity to pursuing higher quality. On the supply side, high-quality development requires enterprises to optimize their industrial systems and structures, achieving sustainable development through innovation-driven growth, though this transition may cause pain and significant operational pressure. On the demand side, high-quality development demands more balanced and equitable growth, requiring improved distribution systems, reduced urban-rural and wealth gaps, and enhanced people' s well-being [8].

Second, following the pandemic, China' s economy urgently needs to return to normalcy. The pandemic, combined with the complex international environment, has shifted public motivation from profit maximization to debt minimization, creating strong expectations for economic and social development to return to the right track. At this stage, ensuring stable economic development is crucial for people' s livelihoods and social harmony.

2. Digital Intelligence Security Risks Under the New Development Pattern

As the representative of advanced productive forces, digital intelligence technology plays an extremely important role in the new development pattern. Therefore, further advancing the secure and controllable development of digital intelligence technology is particularly vital for promoting stable and high-quality economic and social development [9]. Based on the overall national security concept, we categorize digital intelligence security risks into five domains: technological security and personal security at the micro level, and economic security, social security, and cultural security at the macro level (Figure 1 [Figure 1: see original paper]). Micro-level security issues may emerge as macro-level problems as system scales expand, or may trigger cascading effects through propagation and feedback, rapidly impacting various aspects of the system.

2.1 Technological Security

First, infrastructure security. Digital intelligence technology operation relies heavily on infrastructure such as servers, data centers, and IoT devices. Failures, attacks, or disasters affecting data infrastructure may cause business disruptions, data loss, and service unavailability, leading to enormous economic losses and even affecting social stability and security. For example, on December 18, 2022, a large-scale service outage at Alibaba Cloud' s Hong Kong data center directly rendered the Monetary Authority of Macao, numerous local food delivery platforms, and media applications such as *Macao Daily* unusable, significantly impacting the smooth operation of Macao society.

Second, data security. With technological development and increasing human societal data volume, data security and leakage risks have attracted growing attention. From 2005 to 2022, the number of data breach incidents in the United States showed an overall upward trend, with 1,802 incidents in 2022 alone (Figure 2 [Figure 2: see original paper]). During data storage, hacker attacks or employee negligence may lead to leakage of sensitive customer information, financial records, and other data. During data usage, employees or others with data access privileges may abuse their authority by selling sensitive data to competitors or using data illegally. In 2018, Cambridge Analytica in the UK used personal information from millions of Facebook users without authorization for voter behavior analysis and promotional activities, subjecting both companies to severe public pressure, legal investigations, and regulatory restrictions. Cambridge Analytica declared bankruptcy later that year.

Third, model security. As deep learning has become mainstream for AI models, security issues arising from the black-box nature of deep neural networks have gradually become a focus of attention. Additionally, as large-scale language models like ChatGPT rapidly penetrate numerous industries and deeply integrate into people' s lives, the misinformation they generate poses significant security risks. First, deep learning models are vulnerable to adversarial sample

attacks. These specially designed input data can deceive models and cause erroneous outputs, potentially causing severe losses in scenarios such as autonomous driving and medical diagnosis. Second, large language models exhibit bias issues [5]. Limitations in training methods and datasets may cause models to exhibit unfair or unbalanced behaviors or decision-making results toward certain groups or matters. Third, large language models suffer from hallucination problems [6]. The text generated by current large models still contains plausible but fabricated or incorrect information, which can easily lead users to form mistaken perceptions.

2.2 Personal Security

First, privacy security. Privacy security refers to the harm to individuals' social lives when their private data is leaked. Leaked sensitive information (such as ID numbers, bank account numbers) may lead to identity theft, fraudulent activities, and economic losses. Additionally, personal information leakage may result in rumors, insults, harassment, and other malicious behaviors, causing psychological stress and social distress. For instance, family information leakage may lead to extortion and personal safety threats. A survey of UK adults showed that 21% worry about privacy data being passed to third parties by companies, 16% fear becoming fraud targets, and only 9% see no need for concern (Figure 3 [Figure 3: see original paper]). Similarly, a 2022 survey of Chinese netizens found that 31% frequently reject website cookie requests, and 25.5% express concern about how technology companies use their online data (Figure 4 [Figure 4: see original paper]).

Second, mental security. With the development of digital intelligence technology, people' s mental states may also be affected by environmental and technological factors. For example, excessive social media use may lead to time waste, feelings of social isolation, anxiety, and depression; information overload and attention fragmentation may cause concentration difficulties, memory decline, and mental confusion; the anonymity and widespread dissemination channels online make bullying and harassment more convenient, causing psychological harm and self-esteem issues for victims. Furthermore, digital intelligence technology may cause alienation of human subjectivity, capabilities, and communication patterns, depriving people of choice rights [10], weakening human capabilities [11], triggering mental crises and loss of human dignity, while also causing cognitive polarization [12] and various social problems.

2.3 Economic Security

First, technological stability risk. As digital intelligence technology penetrates various economic sectors, its micro-level technological security issues may trigger risks in the macroeconomic system. Whether in financial sector blockchain and intelligent risk control models or manufacturing supply chain management systems, failures or attacks may cause cascading reactions, leading to paralysis

of entire trading or supply chain systems and resulting in enormous economic losses.

Second, technological monopoly risk. When a few large technology companies monopolize a certain intelligent technology market, they may weaken the competitiveness of other entrepreneurs and small enterprises, suppress industry innovation, and hinder market development and progress. Additionally, the massive user data controlled by monopolistic enterprises may infringe on personal privacy rights, while the public lacks corresponding supervision and intervention capabilities.

Third, development imbalance risk. In the digital intelligence wave, if certain regions, groups, or industries fail to seize first-mover opportunities, they will likely lag behind other regions due to lack of technological capabilities and resources. Research reports show that China' s eastern region' s digital economy development level significantly leads that of the central, western, and northeastern regions, exhibiting obvious imbalance characteristics [13]. This unbalanced development of digital intelligence technology, combined with unequal distribution of resources, wealth, and opportunities, may cause economic fluctuations, rising unemployment, population outflow, widening wealth gaps, and affect social stability and harmony [14,15].

Fourth, systemic unemployment risk. The automation capabilities of digital intelligence technology enable many traditional labor tasks to be replaced by machines and software, leading to large-scale unemployment risks in traditional positions in manufacturing, retail, online customer service, financial services, logistics, and other industries. Although emerging positions such as machine learning engineers and large language model prompt engineers will see increased demand, the mismatch and lag between worker skills and market demands during the technological transition may still cause phased shocks in the labor market.

2.4 Social Security

First, false information risk. The popularization of the internet and social media has greatly increased people' s daily exposure to false information. Deepfake technology can generate highly realistic face-swapped images or videos for manufacturing political rumors, fake news, or online fraud. Additionally, malicious users can use generative AI like ChatGPT to automatically produce large volumes of false text, then use bot accounts and other means to mislead values in online communities. A 2020 study by the Cornell University Alliance for Science showed that among 38 million English-language articles about the pandemic published by global media, over 1.1 million contained false information [7].

Second, virtual social risk. As digital intelligence technology profoundly reshapes contemporary social interaction, platforms such as social media and instant messaging tools enable people to communicate and interact with family,

friends, and even strangers worldwide in virtual spaces anytime, anywhere. However, excessive virtual social interaction not only easily leads to addiction and wasted energy but may also reduce face-to-face social interaction, exacerbating real-world social loneliness. Meanwhile, malicious actors can easily hide their true identities online and publish false information, causing misleading and deceptive problems that inflict psychological harm on others.

Third, online violence and bullying. Digital intelligence technology has significantly lowered the threshold for violent behaviors such as verbal abuse, malicious comments, threats, and discriminatory remarks in online social interactions. Malicious users may obtain, publish, or disseminate others' private information such as addresses and photos through public or illegal means, altering photos through obscene processing and dissemination to insult others. These behaviors may cause bullying victims to develop inferiority complexes, anxiety, depression, suicidal tendencies, and other psychological problems, or may cause them to self-censor or remain silent in future expression, creating a vicious cycle. A January 2021 survey of 2,251 U.S. adults found that 41% of respondents had personally experienced some form of online harassment (Figure 5 [Figure 5: see original paper]). The *Analysis and Forecast of China' s Social Situation 2019* (Social Blue Book) published by the Chinese Academy of Social Sciences shows that 28.89% of Chinese youth encountered violent and abusive information online. Among these, violent abuse mainly consisted of "online ridicule and sarcasm" (74.71%) and "insults or use of humiliating vocabulary" (77.01%), followed by "malicious images or GIFs" (53.87%) and "verbal or textual intimidation" (45.49%) [8].

2.5 Cultural Security

First, consumerism. In highly developed market economies, "consumerism"refers to the mindset and attitude of individuals pursuing satisfaction and happiness through purchasing goods and services. Various convenient shopping platforms and advertising algorithms based on digital intelligence technology lower consumption thresholds while making people' s consumption decisions more easily manipulated and influenced, leading them into excessive consumption traps. Driven by this cultural inertia, social resources are easily wasted, and individual happiness is eroded in the eternal cycle of "earning-spending-earning." A questionnaire survey on the consumption status and subjective well-being of Chinese youth shows that consumerism has a significant inhibitory effect on the subjective well-being of the younger generation born between 1995 and 2009 [16].

Second, cultural fragmentation. While digital intelligence recommendation systems and personalized customization technologies improve information search efficiency, they also cause individuals to often only receive homogeneous and one-sided information and viewpoints, forming so-called "information cocoons." Individuals within these "cocoons" repeatedly reinforce their own cognition, exclude other viewpoints, form numerous homogeneous small online communities, and generate large amounts of subcultures. When individuals from different cul-

tural backgrounds collide online, especially on sensitive topics involving freedom of speech, social morality, and religious beliefs, cultural conflicts and confrontations may arise, exacerbating social tensions.

Third, cultural nihilism. Under the influence and impact of emerging popular culture, industrial culture, and modern scientific pragmatism, the living space of many traditional cultures has been squeezed, giving rise to cultural nihilism. Culture is the foundation of national and ethnic cohesion. Blindly negating one' s own culture and history can greatly reduce people' s sense of collective identity, thereby affecting ideological stability. In today' s era of digital intelligence technology continuously accelerating cultural evolution, how to maintain spiritual footing in the tide of the times and guard against cultural nihilism has become an important proposition.

3. Building a New Paradigm for Digital Intelligence Security

The report of the 20th Party Congress emphasizes that "national security is the foundation of national rejuvenation, and social stability is the prerequisite for national prosperity." Therefore, facing various security risks in the digital intelligence era, using systematic concepts to build a new paradigm for digital intelligence security (Figure 6 [Figure 6: see original paper]) is a necessary measure to ensure healthy economic and social development and stable social operation.

3.1 Enhancing the Security of Digital Intelligence Technology Itself

Facing challenges brought by digital intelligence technology, we should not blindly reject technological progress but should strive to enhance the security of technology itself.

First, encryption algorithms and blockchain can protect information security. During information transmission, symmetric or asymmetric encryption algorithms such as DEA (Data Encryption Algorithm) and RSA, as well as emerging quantum entanglement-based communication methods, can reduce risks of illegal data access, tampering, and theft. The decentralization and immutability of blockchain technology enhance the reliability of digital financial transactions and help prevent systemic technological stability risks.

Second, federated learning can protect data privacy. For machine learning data security, federated learning technology [17] proposes training models locally and distributedly at multiple locations, then aggregating parameters at a central server, thereby ensuring local data privacy.

Third, adversarial robustness technology can improve deep learning model reliability. Addressing adversarial sample risks in deep learning models, adversarial robustness technology [18] enables models to correctly process perturbed adversarial samples by incorporating them into the training process or designing

mechanisms to detect them.

Fourth, optimizing training processes can mitigate bias and hallucination problems in large models. By artificially balancing dataset distributions during training, introducing fairness constraints or additional optimization objectives, we can guide large language models to generate safer, more reliable, and diverse content, thereby avoiding cultural conflicts caused by biased or false content.

3.2 Using Digital Intelligence Technology to Safeguard Digital Intelligence Security

Simultaneously, certain digital intelligence technologies can be employed to solve public problems, promote individual development, and reduce economic, social, and cultural risks brought by digital intelligence technology.

First, digital media promotion technology can help the public better adapt to new changes in the digital intelligence era. For example, relevant departments or public welfare organizations can share actual cases of privacy leakage on social media to raise privacy security awareness; by introducing hybrid recommendation strategies in recommendation systems, platforms can expose users to more diverse and heterogeneous content, thereby breaking "information cocoons" and optimizing community atmosphere; by creating higher-quality cultural works and intensifying promotion efforts, the state can promote the formation of excellent and advanced cultures, safeguard the living space of traditional culture, and reduce the harm of cultural nihilism.

Second, social computing technology provides an automated solution for preventing digital intelligence risks. Rumor detection algorithms [9] can identify false information on social media, helping platforms and relevant departments organize the spread of rumors and strengthen social trust and consensus; text sentiment recognition technology [19] can help online community managers promptly detect users' emotional fluctuations, reduce the possibility of online violence incidents, and provide timely psychological intervention for those in need; fraud detection algorithms [20] can promptly detect potential fraud risks, alert victims, or assist police in investigation and analysis.

Third, digital intelligence service technology can promote social equity and healthy sustainable development. Digital government, smart cities, smart education, and other digital intelligence technologies significantly improve public service efficiency, promote equitable social distribution, and can also improve the imbalance in digital intelligence economic development between regions to a certain extent.

3.3 Formulating Laws, Regulations, and Policies for Digital Intelligence Security

First, relevant laws provide the legal foundation for digital intelligence security. Laws and regulations are necessary tools for maintaining social order and sta-

bility, safeguarding citizens' rights and freedoms, promoting social justice and equality, protecting social security and public interests, and ensuring economic and social development, and are also important means for promoting digital intelligence security construction [21]. Internationally, the EU General Data Protection Regulation (GDPR) provides detailed provisions on personal data protection and privacy for EU member states, including data subjects' right to know and right to consent. Many international organizations and industry associations are also actively developing ethical guidelines and behavioral norms applicable to artificial intelligence, such as UNESCO' s *Recommendation on the Ethics of Artificial Intelligence*. Domestically, the *Personal Information Protection Law of the People' s Republic of China* passed in 2021 clarifies principles for personal information processing, individuals' rights in information processing activities, and personal information processors' obligations, and proposes explicit regulations on personal information collection, use, storage, and transmission, prohibiting "big data-based price discrimination" and regulating automated decision-making while strengthening supervision and penalties by relevant institutions.

Second, social policies provide practical support for digital intelligence security. Addressing individual-level mental health issues and social-level development imbalance and systemic unemployment problems in the digital intelligence wave, the government can ensure smooth social transition through relevant policies. On one hand, the government can increase investment in mental health services, establish mental health hotlines, and open psychological counseling centers to help people cope with psychological pressure and problems brought by the intelligent wave. On the other hand, the government can encourage relatively underdeveloped regions to increase investment in digital and intelligent development through fiscal fund allocation, preferential policies, and establishment of talent training bases, thereby narrowing development gaps between regions. For unemployed individuals, the government can increase investment in skills training or provide more entrepreneurship support policies to help them adapt to new demands in the intelligent era.

4. Using the New Paradigm of Digital Intelligence Security to Safeguard the New Development Pattern

Security is the prerequisite for development, and development is the guarantee of security. The report of the 20th Party Congress emphasizes "using the new security pattern to safeguard the new development pattern." In an era where digital intelligence technology drives development, it is necessary to grasp the dialectical relationship between digital intelligence security and economic and social development, using the new paradigm of digital intelligence security to safeguard the new development pattern.

4.1 The New Paradigm of Digital Intelligence Security as a Safeguard for the New Development Pattern

The mechanism by which the new paradigm of digital intelligence security promotes economic and social development can be elaborated from four dimensions: ensuring stability, stimulating innovation, accelerating production, and enhancing resilience. First, ensuring stability: the new paradigm of digital intelligence security ensures the long-term stable operation of social and economic systems, contributing to national long-term development and people' s peaceful lives. Second, stimulating innovation: the need for digital intelligence security can stimulate innovation-driven development, enhance public and enterprise trust in government-promoted innovation, promote multi-stakeholder participation in digital intelligence construction, and increase market vitality. Third, accelerating production: the need for digital intelligence security helps improve total factor productivity growth, transforming basic core industries and fields through digital intelligence transformation, thereby driving the development of the entire national economic production network. Fourth, enhancing resilience: secure digital intelligence technology provides data, technical, and infrastructure support for enhancing industrial chain resilience, fully utilizing the multiplier effect of data to improve dynamic understanding and risk response capabilities of industrial chains. Simultaneously, constructing the new paradigm of digital intelligence security promotes the development of information communication networks and computing infrastructure, providing a solid foundation for industrial internet and digital transformation, and ensuring the independent controllability of industrial chains.

4.2 The New Development Pattern as the Goal of the New Paradigm of Digital Intelligence Security

Development and security are two wings of one body and two wheels of a driving force, complementing each other and neither dispensable. Technological progress and economic and social development provide the material foundation and means for digital intelligence security construction. First, the state needs to find a balance between security and innovation. Overemphasizing security may suppress innovation, limit development, and bring adverse consequences. Additionally, excessive focus on security may lead to over-concentration of resources in the digital intelligence security field, thereby reducing investment in other areas and limiting comprehensive economic development. Therefore, with limited resources, the state needs to determine resource allocation based on risk assessment and priority ranking. Second, the state needs to dynamically adjust the balance and formulate scientific and reasonable security strategies. In practice, completely eliminating all security hazards in complex social systems is unrealistic. Therefore, while ensuring basic security, the state needs to dynamically adjust the balance between security and innovation, establish flexible security strategies and resource allocation mechanisms to face various complex situations, and enhance the robustness of the entire social system.

4.3 Spiral Co-evolution Between Digital Intelligence Security and Socioeconomic Development

By achieving equilibrium between the new paradigm of digital intelligence security and the new development pattern, security and development can form a spiral co-evolutionary relationship model. The development of digital intelligence security needs to be built upon a stable economic and social environment, while economic and social development also requires support and guarantee from digital intelligence technology. Driven by technology and innovation, advances in digital intelligence technology can provide more security guarantees for society, such as improving technology' s inherent security and promoting individual development, while also providing new opportunities for economic development and driving industrial upgrading and innovation. In achieving this goal, it is necessary to focus on the balance between security and development, avoiding overemphasis on one side while neglecting the importance of the other. Only through balanced development can the new paradigm of digital intelligence security and the new development pattern achieve a virtuous cycle of mutual promotion and common progress.

5. Conclusions and Outlook

Driven by digital intelligence technology, both the international environment and domestic society are undergoing profound structural and functional changes, with governance complexity far exceeding the scope of traditional development and security theories. Addressing new risks brought by digital intelligence technology, constructing a new paradigm of digital intelligence security from multiple perspectives including technology, culture, law, and policy, is of great significance for national economic stability and development. In the digital intelligence era full of opportunities and challenges, security and development should be regarded as an integrated whole. Only by correctly balancing and coordinating the relationship between security and development can we achieve long-term prosperity and stability of the economy and society in the digital intelligence era.

References

[1] Teubner T, Flath C M, Weinhardt C, et al. Welcome to the era of ChatGPT et al.—The prospects of large language models. *Business & Information Systems Engineering*, 2023, 65(2): 95-101.

[2] Yang Xiaoguang, Gao Ziyou, Sheng Zhaohan, et al. Complex Systems Management is an Important Component of the Management System with Chinese Characteristics. *Management World*, 2022, 38(10): 1-24.

[3] Wang Fang, Guo Lei. Research on System Complexity of Digital Society. *Management World*, 2022, 38(9): 208-221.

[4] Chen Guoqing, Zeng Dajun, Wei Qiang, et al. Decision Paradigm Shift and Enabling Innovation in Big Data Environment. *Management World*, 2020, 36(2): 95-105.

[5] Yang Xiaoguang, Chen Kaihua, Zheng Xiaolong, et al. Digital Technology Empowering the Modernization of National Governance: Challenges and Responses. *State Governance*, 2023, (5): 52-55.

[6] Zhang Quan, Lei Huamei. Social Impact and Governance Path of Internet Platforms. *National Modernization Construction Research*, 2022, 1(2): 108-123.

[7] Xiao Hongjun. Algorithmic Responsibility: Theoretical Justification, Panoramic Portrait, and Governance Paradigm. *Management World*, 2022, 38(4): 200-226.

[8] Ren Baoping. China's Economic Transition from High-Speed Growth to High-Quality Development in the New Era: Theoretical Interpretation and Practical Orientation. *Academic Monthly*, 2018, 50(3): 66-74.

[9] Hu Jian. Mechanism and Path of Policy-Based Development Finance Supporting the Construction of a New Development Pattern. *China Development Observation*, 2022, (10): 82-86.

[10] Xu Yuan. Governance of Artificial Intelligence Technology from the Perspective of Marx' s "Fragment on Machines" . *Journal of Shandong University (Philosophy and Social Sciences Edition)*, 2022, (5): 145-153.

[11] Xu Zhixiang, Luo Dongxia. Political Economy Analysis of Artificial Intelligence Promoting Common Prosperity. *Contemporary Economic Research*, 2022, (7): 34-44.

[12] Yan Kunru, Cao Yanna. Subjectivity Alienation and Its Resolution Path in the Era of Artificial Intelligence. *Journal of South China University of Technology (Social Science Edition)*, 2020, 22(4): 25-32.

[13] Sun Xiaoqiang, Wang Yanni, Wang Yumei. China' s Digital Economy Development Level: Indicator System, Regional Gaps, and Spatio-Temporal Evolution. *Journal of Dalian University of Technology (Social Sciences Edition)*, 2023, 44(6): 1-10.

[14] Cattaneo A, Nelson A, McMenomy T. Global mapping of urban-rural catchment areas reveals unequal access to services. *PNAS*, 2021, 118(2): e2011990118.

[15] Jackman J A, Gentile D A, Cho N J, et al. Addressing the digital skills gap for future education. *Nature Human Behaviour*, 2021, 5: 542-545.

[16] Tian Xiaowen, Dai Yan, Bo Le. "Happy Shopping" yet "Exquisitely Poor" : The Impact of Consumerism on the Subjective Well-Being of Generation Z. *Consumer Economics*, 2023, 39(4): 81-93.

[17] Yang Qiang. AI and Data Privacy Protection: The Solution of Federated Learning. *Information Security Research*, 2019, 5(11): 961-965.

[18] Zhang X W, Zheng X L, Mao W J. Adversarial perturbation defense on deep neural networks. *ACM Computing Surveys*, 2021, 54(8): 159.

[19] Cao J, Guo J, Li X, et al. Automatic rumor detection on microblogs: A survey. (2018-07-10). https://arxiv.org/abs/

[20] Singh Yadav A K, Sora M. Fraud detection in financial statements using text mining methods: A review. *IOP Conference Series: Materials Science and Engineering*, 2021, 1020(1): 012012.

[21] Xie Lincan. Latest Developments in EU Digital Legislation and Their Implications. *China Reform*, 2022, (6): 79-82.

Note: Figure translations are in progress. See original paper for figures.