Algorithmic Risks and Their Regulation in Intelligent Intelligence Analysis (Postprint)

Authors: Zhang Tao, Ma Haiqun

Date: 2023-04-01T16:02:51+00:00

Abstract

[Purpose/Significance] In recent years, artificial intelligence has brought about transformations in thinking, concepts, and methodological techniques to national intelligence work, making intelligent intelligence analysis gradually become one of the important tasks serving the innovative development of the national intelligence enterprise. Research on algorithmic risks and their regulation in intelligent intelligence analysis can help avoid security risks posed by artificial intelligence algorithms and reduce risk-related factors that constrain the development of intelligence work. [Method/Process] Based on an elucidation of core algorithms and research issues in intelligent intelligence analysis, and in conjunction with practical application scenarios, this study analyzes the causes of algorithmic risk formation, the resulting consequences, and the interactive relationships among various factors of algorithmic risk. A progressive regulatory framework for intelligent intelligence analysis algorithms is established through ex-ante assessment, in-process supervision, and ex-post accountability mechanisms. [Results/Conclusion] By analyzing the formation mechanism of the "intelligence cocoon," and addressing risks such as algorithmic black boxes, algorithmic defects, and algorithmic manipulation in intelligent intelligence analysis, this study proposes recommendations for a virtuous cycle and coordinated development of algorithmic regulation across ex-ante, in-process, and ex-post stages. It further contends that acknowledging the dual nature of algorithms constitutes an effective pathway for preventing and mitigating algorithmic risks.

Full Text

Research on Algorithm Risk and Regulation in Intelligent Intelligence Analysis

Zhang Tao[1], **Ma Haiqun**[2] [1]School of Information Management, Heilongjiang University, Harbin 150080 [2]Research Center of Information Resource Management, Heilongjiang University, Harbin 150080

Abstract: [Purpose/Significance] In recent years, artificial intelligence has brought transformative changes in thinking, concepts, and methodologies to national intelligence work, making intelligent intelligence analysis an increasingly important task serving the innovative development of national intelligence endeavors. Research on algorithmic risk and its regulation in intelligent intelligence analysis can help avoid security risks posed by AI algorithms and reduce factors that limit intelligence development. [Method/Process] Based on an interpretation of core algorithms and research issues in intelligent intelligence analysis, this study analyzes the causes and consequences of algorithmic risk and the interactive relationships among various risk factors in practical application scenarios. A progressive regulatory framework for intelligent intelligence analysis algorithms is established through ex-ante assessment, ongoing supervision, and ex-post accountability. [Result/Conclusion] This article analyzes the formation mechanism of the "intelligence cocoon" phenomenon and proposes recommendations for a virtuous cycle and coordinated development of algorithmic regulation before, during, and after the occurrence of risks such as algorithmic black boxes, algorithmic defects, and algorithmic manipulation. It argues that confronting the dual nature of algorithms is also an effective approach to preventing and mitigating algorithmic risk.

Keywords: Intelligent intelligence analysis; Algorithmic risk; Algorithmic regulation; Intelligent algorithms; "Intelligence cocoon"

With the rapid development of emerging technologies such as artificial intelligence, big data, and blockchain, intelligence work serving national security and development has been entrusted with new historical missions, while its functions and roles in national governance and decision-making have also evolved. The overarching goal of intelligence work is to provide users with relatively comprehensive and scientific decision-making support [1]. Following the introduction of the "Intelligent+" concept in the 2019 Government Work Report, China embarked on a path of large-scale AI implementation, giving rise to "Intelligent+" intelligence analysis—defined as the process of using artificial intelligence technology, relying on intelligence big data, and combining intelligence work norms and methods to reasonably provide users with objective and precise intelligence analysis. In the era of artificial intelligence, intelligence analysts face massive, heterogeneous, and multimodal data in complex and dynamic decision-making environments, where algorithms play a crucial role. While algorithms can assist users in completing intelligent analysis processes and improving intelligence analysis efficiency, they are also a double-edged sword that triggers a series of security risks such as algorithmic black boxes, algorithmic defects, and algorithmic manipulation, gradually becoming one of the main factors limiting intelligence work development. Algorithmic risk was not prominent in traditional intelligence analysis; it is unique to intelligence analysis from the perspective of artificial intelligence. China's institutional construction for AI algorithms is relatively weak, especially in the intelligence work field. If algorithmic risks are

not prevented and resolved in a timely manner, they will not only lead to inaccurate intelligence analysis but also have far-reaching impacts on social stability and even national security.

1 Related Research

1.1 Theoretical Research

Theoretical research forms the foundation of intelligent intelligence analysis. In recent years, academia has produced a series of theoretical achievements on the integration of artificial intelligence and intelligence work: (1) Computational intelligence research: Computational intelligence uses AI, brain science, and cognitive technologies to compute intelligence and support decision-making. Li Guangjian et al. [4-5] proposed theories, methods, technologies, systems, and practical applications for computational intelligence analysis; Chen Xuefei et al. [6] explored implementation pathways for computational intelligence through an "evidence chain model"; (2) Data-driven intelligence research: Hu Changping et al. [7] analyzed frontiers in intelligence theory research under data intelligence environments; Li Lin et al. [8] studied the transformation and development of the entire intelligence process driven by data intelligence technology; Qiu Yunfei et al. [9] examined the application and integrated development of data-driven and knowledge-driven methods in intelligent intelligence analysis; (3) Intelligent intelligence analysis systems: Hua Bolin et al. [10] researched architecture design and key technologies for intelligent intelligence analysis systems; Zeng Wen et al. [11] proposed and constructed an intelligent intelligence analysis decision model from a data engineering perspective; (4) Intelligence-AI integration research: Sun Jianjun et al. [12] discussed "intelligent" elements in intelligence work development from perspectives of thinking, resources, technology, education, and pathways; Feng Qiuyan et al. [13] constructed a new intelligence work system and elaborated on the integrated development of AI and intelligence work at their core levels; Niu Haibo et al. [14] envisioned future intelligence work in the intelligent era.

1.2 Applied Research

Applied research represents the goal of intelligent intelligence analysis. In recent years, scholars have combined AI technologies with intelligence work in different fields, producing numerous applied research achievements: (1) Counter-terrorism intelligence: Zeng Qinghua et al. [15] constructed a human-machine integrated, human-centered intelligent counter-terrorism intelligence analysis system; (2) Financial intelligence: Ding Xiaowei et al. [16] proposed new concepts for financial intelligence analysis based on blockchain-enabled trustworthy big data and trustworthy AI; (3) Military intelligence: Wang Tianyao et al. [17] analyzed the application status, characteristics, and implications of AI in military intelligence work; (4) Security intelligence: Huang Yunfang et al. [18] proposed ideas for constructing intelligent security intelligence analysis models; (5) Competitive intelligence: Tang Xiaobo et al. [19] built enterprise competitive

intelligence system models based on AI technology; (6) Emergency intelligence: Zeng Ziming et al. [20] constructed an emergency incident intelligent intelligence service system and explored its specific application in the Shanghai Bund stampede incident.

Although academia has conducted extensive research on intelligent intelligence analysis, studies on security risks—particularly those posed by algorithms—remain insufficient. In contrast, scholars in law, public administration, and other social science fields have already discussed algorithmic risk issues. Domestically, Jia Kai [21] early proposed that while intelligent algorithms improve social operation efficiency, they also bring risks and challenges of unexplainable concerns, self-reinforcement dilemmas, and subjectivity issues; Zhang Aijun et al. [22] comprehensively analyzed the logic, risks, and regulation of algorithmic power in the AI era; Xu Feng [23] elaborated on legal regulation issues of AI algorithmic black boxes; Chen Si [24] proposed the risk of technological alienation and discussed reasonable and effective AI algorithm governance solutions from technical and value perspectives. Internationally, J. Yang [25] analyzed the impact and patterns of AI algorithm bias and opacity on legal decision-making; H.W. Liu et al. [26] examined the risks of "algorithmization" through a detailed analysis of the "Wisconsin v. Loomis" case and proposed methods for improving AI decision-making accountability; I. Giuffrida [27] studied legal and ethical responsibilities arising from AI algorithms; A. Simoncini [28] depicted the inherent tension between AI algorithms and law, reviewed and criticized standards formulated for democratic policies to protect fundamental freedoms, and proposed "preventive constitutionalism" theory; F.J.Z. Borgesius [29] assessed current European legal protection against discriminatory algorithmic decisions and proposed improvements to existing document enforcement rules. In summary, scholars in the library and information science field have paid limited attention to security risks posed by algorithms, particularly lacking achievements highlighting intelligence domain characteristics. Therefore, this paper, based on interpreting core algorithms and research issues in intelligent intelligence analysis and combining practical application scenarios, analyzes algorithmic risks and the interactive relationships among risk factors, ultimately proposing forward-looking prevention and regulation recommendations for algorithmic risk.

2 Core Algorithms and Research Issues in Intelligent Intelligence Analysis

Intelligence analysis is the process of aggregating, processing, evaluating, and analyzing multi-source data to transform results into intelligence. Traditional methods primarily relied on manual analysis and retrieval-based analysis [30]. With rapid emerging technology development, AI's powerful self-learning capabilities have greatly enhanced intelligence analysis capacity when facing massive data, gradually shifting intelligence analysis toward integrated knowledge-driven and data-driven development [31]. Consequently, intelligent intelligence analysis has been widely applied in counter-terrorism, financial, military, security,

competitive, and emergency intelligence fields, with core algorithms and main research issues sharing common characteristics that help us understand algorithmic risks in intelligent intelligence analysis.

2.1 Core Algorithms in Intelligent Intelligence Analysis

Intelligence is a hybrid product of human and artificial intelligence [32], and intelligent intelligence analysis is an intelligent computing program formed by algorithms and data based on intelligence domain experts' knowledge and experience. Algorithms in intelligent intelligence analysis possess strong self-learning, self-correcting, and self-improving capabilities. This paper categorizes them into five types [33]: machine learning, deep learning, knowledge graphs, natural language processing, and computer vision [Figure 1: see original paper].

(1) **Machine Learning** is the most fundamental algorithm in intelligent intelligence analysis applications. Based on statistical theory, it enables machines to simulate human self-learning, summarize patterns and features, and continuously optimize iterations to mine intelligence from massive data. It mainly includes classification algorithms, regression algorithms, clustering algorithms, dimensionality reduction algorithms, probabilistic graphical model algorithms, and optimization algorithms.

(2) **Deep Learning** represents advanced research on machine learning algorithms. By establishing classification model structures similar to the human brain, it extracts features from low-level to high-level hierarchically from input data to establish semantic mapping relationships. Its back-propagation neural networks, convolutional neural networks, deep neural networks, recurrent neural networks, and long short-term memory networks are core algorithms for intelligence mining and prediction, often combined with computer vision and natural language processing. Such algorithms feature high complexity and low transparency.

(3) **Knowledge Graph Algorithms** have unique advantages in information aggregation, knowledge representation, and automatic inference. They can identify, discover, and infer complex relationships between entities from data to construct knowledge systems in intelligence. Extraction algorithms, path-finding algorithms, centrality algorithms, and graph algorithms are core algorithms in intelligent intelligence correlation and visualization applications.

(4) **Natural Language Processing Algorithms** transform human language into computer-recognizable language and enable human-computer communication in natural language. They create artificial neural networks that simulate human brain structures to achieve semantic understanding and transformation by processing symbolic information. They include syntactic analysis, parsing, text vectorization, and semantic analysis, with semantic analysis being a core algorithm in many domain-specific intelligent intelligence analysis applications. Its accuracy has important

implications for practical applications.

(5) **Computer Vision Algorithms** represent the process of intelligence perception and expression, enabling machines to extract, understand, and analyze massive image data. They demonstrate significant advantages in identifying, tracking, measuring, and processing image and video intelligence. Image classification algorithms, object detection algorithms, target tracking algorithms, semantic segmentation algorithms, and instance segmentation algorithms are widely applied in image- and video-based big data intelligent intelligence analysis.

These algorithms have complex interactive relationships and are often mixed in practical intelligent intelligence analysis applications, making them smarter yet more difficult to understand. This is particularly true for semantic analysis algorithms in natural language processing that form functions like intent recognition, fuzzy association, and reasoning judgment, as well as deep learning neural network algorithms with characteristics of multi-neurons, distributed parallel computing, and multi-layer deep feedback adjustment—all of which intensify algorithmic complexity and opacity.

2.2 Research Issues in Intelligent Intelligence Analysis

Intelligent intelligence analysis can simplify data processing workflows, allowing intelligence analysts more time and energy to learn and apply professional knowledge to provide users with high-level, rapid, and valuable analysis results [34]. Although AI cannot simplify all complexities of intelligence analysis, it can intelligently improve key analysis links and provide bases for analytical judgment [35]. Building upon Zhao Zhiyun et al.'s model-based intelligence analysis [36] and Hua Bolin et al.'s intelligent intelligence analysis system functional structure [10], this paper identifies six main research areas: intelligent intelligence perception, intelligent data collection, intelligent intelligence recommendation, intelligent intelligence correlation, intelligent intelligence prediction, and intelligent intelligence interpretation [Figure 2: see original paper].

(1) **Intelligent Intelligence Perception** addresses real-time user demand perception in response to application scenario changes. It uses machine learning algorithms to optimize data flow, filter invalid data within short timeframes, achieve transformation from data construction to data intelligence perception, and provide early warning and monitoring for potential demands.

(2) **Intelligent Data Collection** utilizes deep learning, knowledge graphs, and natural language processing algorithms for real-time multi-channel data collection. Based on knowledge representation, it provides exploratory collection modes supporting semantic analysis and intent understanding, thereby achieving intelligent identification of data source characteristics, adaptive collection rules, dynamic adjustment of collection strategies, and data screening and verification.

(3) **Intelligent Intelligence Recommendation** is an important means of intelligence acquisition. In addition to intelligently collected information, the process requires identifying strongly correlated intelligence from professional intelligence databases. Intelligent recommendation thus plays a crucial role, using deep learning and natural language processing algorithms to intelligently perceive intelligence needs and push relevant intelligence to analysts, with knowledge graphs introducing more semantic relationships to achieve recommendation accuracy.

(4) **Intelligent Intelligence Correlation** discovers and reveals hidden intelligence in data by strengthening knowledge associations [37]. Based on knowledge graphs and natural language processing algorithms, it combines different data to support semantic retrieval and dynamic expansion mechanisms for single entities, forming mapping associations and achieving progressive and personalized visual intelligence analysis.

(5) **Intelligent Intelligence Prediction** involves intelligent predictive analysis of intelligence. Through intelligence data comparison and historical measurement, it achieves intelligence evolution analysis, development path analysis, and trend prediction based on knowledge graphs, natural language processing, and neural network algorithms.

(6) **Intelligent Intelligence Interpretation** provides intelligent interpretation and judgment of intelligence analysis results. It uses deep learning algorithms to discover data patterns, explore relevant factors, analyze data phenomena and their underlying causes, and form intelligent intelligence interpretation solutions through continuous accumulation of intelligence data, industry rules, and analysis patterns. Natural language processing semantic analysis algorithms assist analysts in generating intelligence reports, with different reports influencing intelligence demands that in turn affect intelligent intelligence perception, forming a cyclical research process.

As data grows exponentially and deep learning multi-layer neural network structures become more complex, security risks hidden behind algorithms have been continuously exposed in recent intelligent intelligence analysis application cases, raising public concerns and questions.

3 Algorithmic Risk Research in Intelligent Intelligence Analysis

Algorithm-based intelligent intelligence analysis is both a powerful driver for national intelligence development and a weapon in AI-era intelligence competition. However, it cannot remain confined to formal logical frameworks of national security; it must achieve full-process analysis combining subjective and objective elements. In reality, algorithm-caused limitations, subjectivity, and security issues in intelligent intelligence analysis are prominent, inconsistent

with the holistic principles of national security. Over time, various algorithm-induced risks emerge. Knowledge, data, algorithms, and computing power are indispensable elements of AI, with algorithm security and robustness being core concerns. To truly leverage intelligent intelligence analysis in intelligence work, we must understand algorithmic risk, analyze its causes, and recognize its serious consequences. This article dissects algorithmic risk based on recent practical application scenarios.

3.1 Algorithmic Black Boxes: Opaque Intelligence Analysis

3.1.1 Understanding Algorithmic Black Boxes Algorithmic black boxes refer to situations where only input and output stages are visible and understandable, while internal processing remains completely opaque and undisclosed, preventing users from knowing algorithms' ultimate goals and intentions. Black boxes mean not only unobservable processes but also that even when computers attempt to explain, users cannot understand. Intelligent investment advisory is an important application in financial intelligence analysis, using deep learning, knowledge graphs, and automated management technologies to analyze financial markets and generate personalized portfolio recommendations by obtaining users' risk preferences and expected return indicators [38]. Throughout this process, algorithms remain completely opaque. Many users do not understand how investment advice is formed, nor do they realize that the premise of intelligent advisory automation is replacing human thinking with technical rationality, meaning "algorithms" will largely become the basic logic followed by intelligent advisors. Professors Tom Baker of the University of Pennsylvania Law School and Benedict Dellært of Erasmus University Rotterdam argue that the public cannot presume intelligent advisory robots lack the impure motives humans possess [39]. Thus, algorithms' lack of transparency or explanatory mechanisms poses enormous security risks for intelligent advisory services.

3.1.2 Causes of Algorithmic Black Boxes Analysis of intelligent advisory services reveals two causes: (1) **Technical factors**: Algorithmic complexity leads to black box formation. Recent deep learning developments enable algorithms to bypass traditional machine learning explanation processes, with computers automatically learning from raw data to produce advanced intelligence results, making the entire intelligent advisory process lack transparency or explanatory mechanisms—even analysts cannot explain it, thus forming algorithmic black boxes. The rise and application of deep neural networks particularly highlight technical barriers caused by black box phenomena, making algorithms increasingly difficult to identify. (2) **Social factors**: Interest-driven black box formation. In intelligent advisory services, technology companies deliberately conceal algorithmic operation processes, leaving users and the public almost completely outside the black box. Typically, these are interest-induced black boxes: transparency could damage companies' economic interests—first, by risking intellectual property infringement, as algorithm R&D has long been confidential in intelligence work, and transparency could enable competitors to

copy core concepts; second, by risking intelligence leakage, as algorithm transparency could make the entire intelligent advisory analysis process transparent, potentially causing severe intelligence leakage consequences.

3.1.3 Risks of Algorithmic Black Boxes Algorithmic black boxes pose severe challenges to the healthy development of intelligent intelligence analysis, making analysis behaviors lack effective explanatory power. Once algorithms become "black boxes," users and intelligence analysts face extreme uncertainty, opacity, and high risk. In intelligent advisory services, black box risks include: (1) User profiling relies on algorithms to collect, filter, and model behavioral data, social situations, transaction records, and financial status. This process not only inadvertently infringes on user privacy but also, if based on partial or discriminatory indicators, fails to address financial resource allocation inequality and instead creates 固化 discrimination and exclusion at the technical level. (2) Overly complex algorithmic execution lacking transparency can mask potential financial investment risks. Once analysts and users become lost in the fog of macro market trends, forming excessive investment expectations and taking aggressive risk-taking actions, financial market imbalances affecting social stability can occur. Throughout this process, they neither understand algorithmic execution nor can distinguish what is safe versus risky, making truth verification difficult.

3.2 Algorithmic Defects: Falling into the "Intelligence Cocoon"

3.2.1 Understanding Algorithmic Defects Algorithmic discrimination causing inequality and algorithmic bias causing injustice fall under algorithmic defects, which refer to inherent deficiencies or incompleteness in algorithms themselves [40] and represent primary manifestations of algorithmic non-robustness. The Wisconsin v. Loomis case introduced COMPAS to assist judicial decision-making, sparking heated debate. COMPAS uses deep learning and knowledge graph algorithms to predict recidivism risk based on criminal interviews and judicial intelligence, aiming to help judges make intelligent decisions. In this case, COMPAS analysis showed Loomis had "high violence risk, high recidivism risk, and high pretrial risk," leading the court to identify him as high-risk to the community and sentence him to six years imprisonment and five years extended supervision. Society widely questioned COMPAS's inclusion of discriminatory factors like race and gender, seriously violating Loomis's due process rights. Although the court clarified the case, social debate continues, reflecting complex issues of algorithmic discrimination and procedural justice [41]. Current applications in corporate recruitment [42] and intelligent recommendation [43] also demonstrate varying degrees of unfairness and injustice caused by algorithms. A 2018 Pew Research Center report showed approximately 60% of Americans believe algorithms are always biased [44], indicating that algorithmic bias and discrimination have attracted social attention and public skepticism.

3.2.2 Causes of Algorithmic Defects Analysis reveals two causes: (1) **Non-subjective algorithmic defects**: Limited programmer experience creates non-subjective defects. AI algorithms' high complexity demands high professional competence, but some programmers focus solely on results without recognizing potential risks. In cases like Loomis and corporate recruitment, programmers included race, gender, and other factors based on historical data without realizing results would carry discrimination and bias, forming non-subjective defects. (2) **Subjective algorithmic defects**: Driven by political and economic interests, developers or designers may embed their own discrimination or bias into algorithms, which then perpetuates these issues. In intelligent recommendation scenarios, recommendation algorithms essentially use past experiences for prediction and push, but past experiences inherently contain discrimination or bias that becomes 固化 and amplified in algorithms, forming subjective defects.

3.2.3 Risks of Algorithmic Defects Algorithmic complexity and black boxes cause transparency deficits, preventing users from knowing whether internal defects exist. Algorithmic defects cause deviations in analysis result security, accuracy, and comprehensiveness, potentially triggering major social security risks of discrimination or bias. Algorithms in Loomis, corporate recruitment, and intelligent recommendation applications already reflect analysts' preconceptions about gender, race, and other factors. Such defects can trap decision-makers in "intelligence cocoons," catalyzing extreme tendencies through over-reliance on algorithmic convenience, with particularly severe security risks. This article explains the "intelligence cocoon" phenomenon as follows [Figure 3: see original paper]: Based on Maslow's hierarchy of needs [45], under continuous intelligent recommendation algorithm influence, intelligence personnel's information acquisition shifts from multi-source to single-source. If intelligence personnel depend on defective single-source information in a positive feedback loop, they gradually fall into an information-deficient "cocoon." Since intelligence represents an advanced stage of information—reprocessed and refined—intelligence personnel's focus areas become habitually guided by their subjective consciousness, confining their thinking within silkworm-cocoon-like "cocoons." The "intelligence cocoon" causes intelligence personnel's preconceptions to become entrenched, ultimately leading to inaccurate and biased intelligence analysis results and difficulty forming consensus in management decisions [47].

3.3 Algorithmic Manipulation: Uncontrolled Decision-Making Behavior

3.3.1 Understanding Algorithmic Manipulation Algorithmic manipulation refers to algorithms being manipulated by humans or humans being manipulated by algorithms after algorithmic alienation. Users must recognize and guard against any form of algorithmic manipulation in domain-specific intelligent intelligence analysis. Cambridge Analytica gained notoriety between 2016-2018 for using precision marketing to influence voter political attitudes in the

U.S. election and Brexit [48]. Based on user behavioral data, Cambridge Analytica used deep learning algorithms to model and analyze different user groups' personality traits, potential needs, character, and negative emotions, rapidly identifying users' private information through social media evaluation tendencies to establish user profiles as important bases for more accurate behavioral assessment and prediction. During this process, voter users did not recognize algorithms' potential risks, but Cambridge Analytica precisely delivered political marketing ads and manufactured bot accounts to spread political ideas based on voters' personalities and cognitive characteristics, directly influencing political attitudes and voting results. Such algorithmic manipulation not only exacerbates new social inequality risks but also endangers national political security.

3.3.2 Causes of Algorithmic Manipulation Analysis reveals two causes: (1) **Algorithms manipulated by humans**: Risk from interest group manipulation is subjective, as algorithms depend on programmers' judgments and choices. As T.J. Dunning wrote in *Trades' Unions and Strikes*: "Capital will take 20% profits, and with 50% it becomes adventurous; at 100% it tramples all human laws; at 300% it commits any crime, even at the risk of the gallows" [49]. Cambridge Analytica's manipulation of algorithms for profit directly influenced voting results, causing a public outcry and leading to its bankruptcy after the scandal. (2) **Humans manipulated by algorithms**: Algorithmic alienation plus the "intelligence cocoon" is an important cause of humans being manipulated by algorithms. Algorithmic alienation refers to algorithms created by humans becoming alien, hostile forces that harm society and counteract humanity. Algorithms can achieve self-learning, self-training, and self-generation through big data, and according to human personality traits, customize and deliver information matching specific audiences' views and preferences to guide and manipulate human behavior. Although humans remain involved, algorithms have transcended limitations of human expression capacity, greatly enhancing algorithmic capabilities and expanding application scope.

3.3.3 Risks of Algorithmic Manipulation Risks from algorithmic manipulation of humans are more terrifying than human manipulation of algorithms. (1) **Human manipulation of algorithms**: Futurist Alvin Toffler proposed in *PowerShift* that global corporations' data monopolies in the AI era will weaken national political cohesion and central consciousness, potentially enabling a few technological superhumans to manipulate global economy and politics [50]. Cambridge Analytica's manipulation caused severe security risks: first, exacerbating new social inequality risks—the "digital divide" continuously widens, evolving into new political hegemony (algorithmic power); second, citizens losing trust in government as they become elements in algorithmic operation, dissolving their subjectivity and value, gradually losing trust in government and society; third, seriously endangering national political security, as algorithmic manipulation directly affects political justice, a political foundation that must be safeguarded. Once this balance breaks, national political security is endan-

gered. (2) **Algorithmic manipulation of humans**: Algorithmic alienation belongs to algorithmic defects in principle but may cause more severe social consequences. Current rapid algorithmic development and self-evolution have initially verified Jacques Ellul's prophecy in *The Technological Society* that "technology typically develops beyond human control" [51]. Future algorithmic alienation combined with "intelligence cocoon" constraints will manipulate intelligence analysts' and decision-makers' thinking, causing decision-making behavior to be controlled. More terrifyingly, humans cannot recognize behavior manipulated by algorithms. Such unpredictable consequences endanger social stability and national security, even opening a "Pandora's box" threatening world peace—seriously deviating from the holistic national security concept.

3.4 Interactive Relationships Among Algorithmic Risks

Research on practical intelligent intelligence analysis application scenarios reveals complex interactive relationships among algorithmic black boxes, defects, and manipulation, with mutual influence [Figure 4: see original paper]. Algorithmic black boxes are the root cause of algorithmic risk. Algorithmic complexity and interests are main inducements for black box formation, providing space and conditions for invisible algorithmic power operation. Algorithmic defects and manipulation are also risks derived from black boxes—manipulation essentially belongs to defects, and using algorithms to manipulate others also leads to algorithmic power. Algorithmic power is interest-oriented and inherently discriminatory and biased. Political and economic interests cause algorithmic manipulation, which inevitably creates defects, while defects easily trap intelligence personnel in cocoons. Once "intelligence cocoons" combine with algorithmic alienation, security risks of humans being manipulated by algorithms may emerge. The bold path in [Figure 4: see original paper] clearly traces this risk line: black boxes → defects → alienation ("intelligence cocoon") → manipulated by algorithms, representing the most concerning algorithmic risk pathway.

4 Algorithmic Regulation Research in Intelligent Intelligence Analysis

Beyond the aforementioned scenarios, many intelligence fields face catastrophic consequences if security incidents occur, such as national security intelligence, military intelligence, and counter-terrorism intelligence. Therefore, particular attention must be paid to algorithmic risk in intelligent intelligence analysis, especially in fields severely impacting national security and development. The *New Generation Artificial Intelligence Development Plan* proposes that "while vigorously developing AI, we must attach great importance to potential security risk challenges, strengthen forward-looking prevention and constraint guidance, minimize risks to the greatest extent, and ensure safe, reliable, and controllable AI development" [52]. Algorithmic risk is both a technical and social issue; healthy algorithmic development depends not only on self-innovation but also on correct social constraints. Algorithmic regulation is an important means to

prevent and resolve algorithmic risks in intelligent intelligence analysis. Addressing algorithmic risks requires establishing a progressive regulatory framework through ex-ante assessment, ongoing supervision, and ex-post accountability to achieve virtuous cycles and coordinated development from an overall security perspective, providing policy recommendations for government and intelligence agencies [Figure 5: see original paper].

4.1 Ex-ante: Algorithmic Assessment and Institutional Expansion

Algorithmic assessment systematically evaluates algorithm security, robustness, portability, efficiency, and other aspects, serving as an effective means to predict and identify algorithmic risk. In July 2018, the China Electronics Standardization Institute, together with multiple industry-academia-research units, compiled the *Artificial Intelligence Deep Learning Algorithm Assessment Specification* (hereinafter "Specification"), proposing assessment indicator systems, processes, and content for AI deep learning algorithms, including assessments of requirements, design, implementation, and operation phases. The Specification is a pioneering system for intelligent algorithm assessment in China, providing important guidance for algorithm policy formulation in other fields. Currently, China's intelligence work field lacks algorithm assessment systems. Future national intelligence agencies should, based on intelligence work characteristics and referring to the Specification, expand algorithm assessment institutions: (1) **Classify algorithm application domains**: Financial, military, security, counter-terrorism, emergency, and other intelligence fields should have differentiated assessment content and focus, with domain-specific mechanisms; (2) **Classify algorithm security levels**: Subdivide security levels according to algorithmic complexity and potential negative social impacts; (3) **Establish algorithm standard libraries**: Create databases with "application domain-security level-optimal algorithm" correspondences, removing unnecessary complexity and replacing overly complex, unexplainable methods with more understandable ones; (4) **Establish assessment norms**: Promote establishment of beneficial assessment norms across domains and stages for intelligence agencies and related organizations.

4.2 Ongoing: Algorithmic Supervision and Institutional Improvement

Lack of effective algorithmic supervision is a thorny problem. Supervision should include monitoring, early warning, and guarantee components, with paramount importance on using policies and regulations to ensure algorithmic transparency and avoid overly broad exemptions for developers' information disclosure obligations [53]. Since 2018, China's cyberspace administration has emphasized algorithmic supervision, initially strengthening application of existing laws to better protect user rights and cybersecurity, focusing on algorithm distribution rules and ethics. However, as deep learning algorithms' self-learning capabilities continuously improve, supervision should be further strengthened. Although China has not yet issued specialized algorithm supervision regulations, the *E-commerce*

Law and *Cybersecurity Law* contain algorithm-related provisions, preliminarily incorporating algorithm rules into the legal supervision system at the national level. Based on China's currently scattered algorithm supervision policies, three improvements are recommended for the intelligence field: (1) **Establish automated intelligence analysis system inventories**: National intelligence work administrative departments should include inventoried systems in ex-ante assessment impact and ongoing monitoring review scopes, granting regulators investigation authority to access relevant information; (2) **Strengthen third-party professional supervision**: Support academic and non-profit organizations that understand intelligence work to participate, expand professional supervision through establishing intelligent algorithm research committees in intelligence fields, and coordinate interests to strengthen industry self-discipline; (3) **Implement hierarchical supervision by security level**: Given that most intelligence analysis algorithms have certain confidentiality levels, regulators or industry organizations should require obligators to file algorithms or algorithmic logic, especially strictly supervising algorithms with significant negative impacts.

4.3 Ex-post: Algorithmic Accountability and Institutional Innovation

Algorithmic accountability refers to the process where intelligence agencies or individuals bear responsibility for adverse impacts on the nation and society during algorithm application and take corresponding remedial measures [54]. Strengthening accountability for algorithmic results helps promote open, fair, and value-oriented analysis, ensuring that algorithm-caused analysis errors cannot evade responsibility, with increased accountability for algorithmic manipulation. In 2019, the EU introduced the *Algorithmic Accountability and Transparency Governance Framework* focusing on transparency and accountability; the U.S. Congress introduced the *Algorithmic Accountability Act* making transparency an important accountability factor; Germany's Data Ethics Commission released recommendations emphasizing algorithmic supervision and responsibility, advocating human-centered design aligned with core social values and focusing on sustainability, stability, and security. China's 2018 *E-commerce Law* stipulates consumer protection obligations for personalized recommendation results, with penalties for violations. However, China still lacks systematic algorithmic accountability systems, especially in intelligent intelligence analysis. Drawing on European and American measures, China should strengthen institutional innovation from three aspects: (1) **Implement responsibility stratification**: Leverage roles of societies and committees in intelligence agencies to identify special risk points in assessment and supervision processes and clarify responsibility standards for different algorithmic risks; (2) **Strengthen algorithmic auditing**: Algorithmic assessment and auditing are closely related, with auditing efficiency and quality being important accountability concerns; (3) **Establish intelligence-characteristic accountability systems**: The state should timely consider formulating an *Algorithm Law*, while national intelligence agencies should formulate *Artificial Intelligence Algorithm Review Specifications* and

Algorithmic Responsibility Frameworks applicable to intelligence fields based on existing regulations, strengthening legal effects of accountability while guiding intelligence work across domains.

Although algorithmic challenges to intelligent intelligence analysis are evident, simply attributing algorithmic risk issues to AI is unobjective, as algorithms themselves are harmless. Removing political and economic interest factors, the key lies in how to reasonably use intelligent algorithms to assist intelligence analysis. In intelligent intelligence analysis, algorithmic value and risk constitute a complex problem requiring synergy for common development. What is certain is that AI will always assist rather than replace human analysis, requiring intelligence personnel to possess high data and intelligence literacy to effectively use intelligent analysis tools and methods and explain processes and results to users. Currently, humanity is committed to creating AI brains and promoting multi-dimensional robot learning, especially improving robots' emotional levels. When machine subjects possess cognitive abilities, autonomy, and human emotions, human attitudes toward algorithmic manipulation may shift, with respecting objective facts potentially becoming mainstream. Therefore, confronting the dual nature of intelligent algorithms is also an effective way to prevent and mitigate algorithmic risk. Due to intelligence analysis's distinctive characteristics differing from other information and data analysis fields, this paper provides an initial exploration of algorithmic risk and regulation in intelligent intelligence analysis to produce research highlighting intelligence characteristics and discourse power. As intelligent algorithms become widely applied in intelligence work, algorithmic risk issues will inevitably become more prominent, and future research teams will continue in-depth studies on algorithmic risk identification and governance through technical and institutional means.

References

[1] Wang Zhongjun, Yu Wei, Yang Qing. Expert Interview on Practical Innovation and Development of Scientific and Technical Intelligence Agencies [2] Tu Yuanji. Qian Xuesen's Letters: August 8, 1993 Letter to Dai Ruwei [3] Wang Feiyue. From Laser to Activation: Qian Xuesen's Intelligence Philosophy and Parallel Intelligence Systems [4] Li Guangjian, Luo Liqun. Progress in Computational Intelligence Analysis [5] Li Guangjian, Jiang Xinyu. On Computational Intelligence Analysis [6] Chen Xuefei, Li Hui, Jin Xiaohong, et al. Preliminary Exploration of Computational Intelligence [7] Hu Changping, Lü Meijiao. Frontier Development of Intelligence Theory in Big Data and Intelligent Environments [8] Li Lin, Sun Min. Transformation and Development of the Entire Intelligence Process Driven by Data Intelligence Technology [9] Qiu Yunfei, Li Chunwang. Intelligent Intelligence Analysis Models: Data-Driven and Knowledge-Driven [10] Hua Bolin, Li Guangjian. Architecture Design and Key Technology Research for Intelligent Intelligence Analysis Systems [11] Zeng Wen, Li Hui, Li Rong, et al. Exploration of Intelligent Intelligence Analysis and Application from a Data Engineering Perspective [12] Sun Jianjun, Li Yang. Several

Issues on the "Intelligent" Development of Intelligence Science and Intelligence Work [13] Feng Qiuyan, Zhu Xuefang. Research on AI Application in Intelligence Work [14] Niu Haibo, Li Lin. Prospects for Intelligence Work in the Intelligent Era [15] Zeng Qinghua, Chen Chengxin. Construction of an Intelligent Counter-Terrorism Intelligence Analysis System Based on Comprehensive Integration Methods [16] Ding Xiaowei, Su Xinning. Financial Security Intelligence Analysis Based on Blockchain Trusted Big Data and AI [17] Wang Tianyao, Wu Subin. Application Status, Characteristics, and Implications of AI in Military Intelligence Work [18] Huang Yunfang, Wang Bing. Construction of an Intelligent Security Intelligence Analysis Model [19] Tang Xiaobo, Zheng Du, Tan Mingliang. Enterprise Competitive Intelligence System Model Construction Integrating Intelligence Methodology and AI Technology [20] Zeng Ziming, Wang Jing. Research on Emergency Incident Intelligent Intelligence Services from a Social Computing Perspective—Taking the Shanghai Bund Stampede as an Example [21] Jia Kai. Research on AI and Algorithmic Governance [22] Zhang Aijun, Li Yuan. Algorithmic Power in the AI Era: Logic, Risks, and Regulation [23] Xu Feng. Legal Regulation of AI Algorithm Black Boxes—Taking Intelligent Advisory as an Example [24] Chen Si. Algorithmic Governance: Risks and Responses to Technological Alienation in Intelligent Society [25] Yang J. Effects of Bias and Opacity of AI Algorithms on Legal Decision-Making and Its Discipline [26] Liu HW, Lin CF, Chen YJ, et al. Loomis: Artificial Intelligence, Governmental Algorithmization, and Accountability [27] Giuffrida I. Liability for AI Decision-Making: Some Legal and Ethical Considerations [28] Simoncini A. The Constitutional Algorithm: Artificial Intelligence and the Future of Liberties [29] Borgesius FJZ. Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence [30] Liu Xudong, Su Majing, Zhu Guangyu. Research and Design of a Multi-Source Intelligence Analysis System Based on Natural Language Processing [31] Zhang Bo, Zhu Jun, Su Hang. Toward the Third Generation of Artificial Intelligence [32] Hayles NK. How We Become Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics [33] Gao Hang, Yu Xuekang, Wang Maolu. Blockchain and AI: The New Era of Digital Economy [34] Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis [35] Clark RM. Intelligence Analysis: A Target-Centric Approach [36] Zhao Zhiyun, Sun Xingkai, Wang Xiao, et al. Organizational Intelligence and System Intelligence: From Scenario-Based to Model-Based Intelligence [37] Wang Junping, Zhang Wensheng, Wang Yongfei, et al. Event Cognitive Graph Construction and Inference Analysis for Big Data [38] Jiang Huiyu. On Institutional Prevention of Technical Risks in Intelligent Advisory Services [39] Liu Yuanxing. The "Algorithmic Explainability" Issue in Intelligent Finance [40] Li Yuke. Research on Information System Quality Improvement Based on Defect Analysis [41] Jiang Su. Automated Decision-Making, Criminal Justice, and Algorithmic Regulation—Reflections on the Loomis Case [42] Why It's Totally Unsurprising That Amazon's Recruitment AI Was Biased Against Women [43] Discrimination in Online Ad Delivery [44] Public Attitudes Toward Computer Algorithms [45] Hu Wanzhong. On Human Value and Self-Worth from Maslow's Needs Theory [46] Wang Yicheng, Wang Ping, Wang Meiyue, et

al. Strategies for Content Intelligent Distribution Platforms to Break Through "Information Cocoons" from an Information Movement Perspective [47] Peng Lan. Illusions, Algorithmic Prisoners, and Rights Concession: New Risks in the Data and Algorithm Era [48] Mu Lin. Analysis of the "Algorithm Black Box" Issue in the Cambridge Analytica Incident [49] Dunning TJ. Trades' Unions and Strikes [50] Toffler. PowerShift [51] Ellul J. The Technological Society [52] Zhang Tao, Ma Haiqun. Comparative Study of China's AI Policies Based on Text Similarity Calculation [53] Lucero K. American Algorithmic Governance Policy and Implementation Approach [54] Dilia. Research on Accountability and Countermeasures for Big Data Algorithmic Decision-Making

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