Journal of Global Economy, Business and Finance (JGEBF) ISSN: 2141-5595
DOI: 10.53469/jgebf.2024.06(07).02

Preventing Security Risks in Government Information Disclosure: A Mosaic Theory Perspective

Ling Chen

College of Economics and Management, Nanning Normal University, Nanning 530001, Guangxi, China
991094@nnnu.edu.cn

Abstract: ***The security risks in government information disclosure are directly related to the effective operation of the information society and have significant theoretical and practical value for information security governance and the improvement of the national security strategy system. This article uses mosaic theory's "information synergy effect" and life cycle theory to examine the stages of information collection, embedding, and utilization, focusing on key aspects such as risk source formation, risk transmission, and social amplification of risks. It analyzes the security risks and related typical events in government information disclosure and proposes prevention measures. The results show that security risks generally follow the logic of "internal and external factors trigger—direct information damage—secondary information loss of control—imbalance of information ecology." Therefore, the full-process governance of security risks in government information disclosure is a continuous project that involves building security barriers and adjusting the scope of disclosure in the information collection phase before the risk source is formally generated to prevent the formation of risk sources. In the information embedding phase, illegal processing should be prevented, emergency plans established, and all-around and multiangle prevention warnings and overall treatment carried out to ensure national security.***

Keywords: Government information disclosure, Security risks, Mosaic theory.

1. Introduction

With the gradual popularization of the internet and the continuous opening up of government data [1], open source data have become an important source of information for the intelligence community. It is estimated that intelligence obtained from open source data accounts for more than 80% of the total intelligence gathered [2]. Massive amounts of information generate significant intelligence value through collection and analysis. Information that was previously meaningless on an individual level can produce unique intelligence value through multiple analyses and inlays and can penetrate various aspects of China's politics, economy, military, etc [3]. China has always attached great importance to the security of government information disclosures. The "Guiding Opinions on Strengthening the Construction of Digital Government" issued in 2022 mentioned the need to accelerate the integration and open sharing of information resources to effectively safeguard national data security. In the United States, mosaic theory has been widely applied in the field of national security, and it became a powerful tool for the CIA to withhold information from public disclosure in the late 1970s. Especially since the 9/11 attacks, intelligence collection and analysis have become the most important strategic asset in the national security field. The role of mosaic theory in controlling information has become increasingly prominent, and its strategic significance to the government continues to grow [4]. The theory is increasingly relied on to assert national security privileges for classified information [5].

To reconcile the contradiction between government information disclosure and national security, it is necessary to first clarify the security risks in government information disclosure. Currently, explicit information security risks have received much attention both domestically and internationally, but potential implicit security risks in the era of big data have not received enough attention. Therefore, based on mosaic theory, this article analyzes the types of security risks in government information disclosure and related typical events, aiming to identify different types of security risks, expand the research perspective on government information disclosure and contribute to the construction of a contemporary national security system.

2. Methodological Approach: Literature Review

2.1 Literature Review

As the pace of government information disclosure has accelerated, security issues have become a focus of researchers' attention, including emphasizing the types of security risks and obtaining a comprehensive understanding of countermeasures for security issues.

First are the types of security risks in government information disclosure. The industry and academia have reached a consensus on the inevitable security risks associated with government information disclosure, such as information leakage, tampering, and destruction, and have discussed the security risks in government information disclosure from the perspectives of information security, economic security, and social security. A large amount of research has shown that government information disclosure can lead to information security risks at both the national and individual levels (Yan Qian, 2018). It may not only affect economic security (Kucera J, 2014; Zhao Longwen, 2019) and social security (Zhang Feng, 2020; Zhang Xinbao, 2022; Yang Xiaobo, 2022) but also lead to personal privacy breaches (Zuiderwijk A, 2014; Meijer R, 2014; Du Hehua, 2020; Ding Hongfa, 2019). Xiao Dongmei (2022) divides the security risks of government information disclosure into explicit and implicit security risks, where explicit security risks include external risks at the

technical level and internal risks related to personnel, while implicit security risks are mainly confidential information leakage due to secondary processing of information.

Second are preventive measures and the effectiveness of security risks in government information disclosure. In line with the practical research on security risks in government information disclosure, the academic community is also greatly concerned about countermeasures against security risks. Zhao Jiyang (2016) and Chen Mei (2018) mainly propose suggestions regarding core technology, while Frederik Zuiderveen Borgesius (2015) and Zou Dongsheng (2018) construct a balanced framework that includes "risk categories, types of government information disclosure, and factors affecting government information disclosure." Xiao Dongmei (2022), Chen Chaobing (2019), Yuan Hong (2022) and others focus on the construction of the policy and regulatory system and the establishment of an information security evaluation mechanism to support a strict crackdown on illegal activities using open data. In addition, the government should be aware of security risks and improve the security literacy of management personnel.

Analysis shows that current research focuses mainly on the types of security risks and corresponding solutions in government information disclosure, with little attention paid to the logic of security risk generation. Early identification and management of risk sources are crucial in addressing security risks. In the context of big data and globalization, the breadth and depth of government information disclosure and dissemination in China have increased, resulting in significant information synergy effects and internal diversity and external extension of security risks. Furthermore, as the information related to national security becomes increasingly heterogeneous and the international ecological environment for information disclosure becomes more complex, the conflict between government information disclosure and national security is becoming more acute. Therefore, academia, industry, and government agencies should pay close attention to this issue and propose new solutions using relevant theories and technological approaches to promote optimization and improvement of security measures. Against this background, this paper draws on successful theoretical research and practical experiences in China and abroad, summarizes the security risks of government information disclosure in China from the perspective of mosaic theory, and uses case analysis to explore the logic of security risk generation in government information disclosure under information synergy effects. Furthermore, the paper studies potential security risks in government information disclosure, establishes an information security protection mechanism based on mosaic theory, and proposes suggestions and solutions, thus developing the research in a linear manner.

2.2 Research Framework

As a classic analysis theory for the protection of national security in the government information disclosure process, mosaic theory, which first appeared in the Fourth Amendment of the Constitution of the United States, has been widely applied to the US government's information disclosure, especially in the protection of national security information. From the 1980s to the 1990s, mosaic theory rapidly developed in the national security precedent law of the US Freedom of Information Act [6]. Based on this theory, the US government chooses to adopt a conservative approach to some information, choosing not to disclose it to avoid the combination of government-publicized information with certain specific information that may harm national security. Essentially, mosaic theory is a theory of the information synergy effect that holds that individual information items have limited or no effect on their owners, but the value generated by combining these items far exceeds the sum of their values. Government agencies have consistently cited mosaic theory to justify the legitimacy of their nondisclosure of information [7]. Based on this theory, although some information may not be classified as state secrets, due to the special correlation between items of data, criminals can connect seemingly unrelated information through organized professional research and further speculate and verify it. It cannot be guaranteed that such connections will not pose a potential threat to national security, even if this possibility cannot be fully proven. In short, mosaic theory reflects the information collection rule of "information 1 + information 2 + information 3 +…+ information N > the sum of partial values"; that is, the overall value of information is greater than the sum of partial values. Therefore, potentially hostile elements can infer important information from seemingly harmless information and then use it for malicious purposes. The information synergy effect does exist, and hostile elements can use it to harm national security. To determine the security risks of a given document being made public, the possibility that it is embedded must be considered.

The coordination of information disclosure and national security emphasizes the correct understanding and scientific handling of the relationship between security and openness in government information disclosure. The aim is to form a pattern of ensuring security in openness and promoting openness in security. The main question is how to deal with the relationship between the two in the era of informatization and carry out corresponding information sharing. Mosaic theory describes a basic rule for the formation of intelligence information: a single piece of information may not have security risks, but when combined with other information, it will produce a synergistic effect that is more valuable than the sum of the values of multiple pieces of information, thereby threatening national security. This rule has strong reference significance for analyzing and responding to the security risks of government information disclosure. Some intelligence information is formed on the basis of aggregated fragmentary information, and it produces obvious synergistic effects after being embedded in a single piece of information, becoming a factor that affects national security. Combining the concept and connotations of mosaic theory, an analytical framework of "information synergy—synergistic effect—security guarantee" can be constructed to study three dimensions of the security risks of government information disclosure: the logic of risk generation (information synergy), risk types (synergistic effect), and risk prevention (security guarantee). The results provide a theoretical reference for risk identification, early warning, prevention, and resolution (as shown in Figure 1).

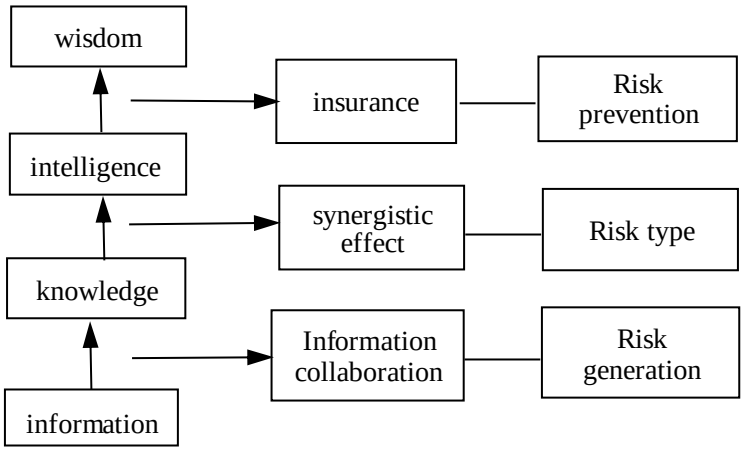

Figure 1: Analytical framework

3. Security Risks of Government Information Disclosure

With the increasing amount of information collected on the government information disclosure platform, previously dispersed, isolated, and low-value information has created an aggregation effect, dramatically increasing its value and inevitably attracting more external attacks and internal threats. As a result, security risks in government information disclosure events occur frequently (see Table 1). According to statistics, from January to October 2022, 16.1% of major data security incidents in global political and enterprise institutions occurred in government institutions and public service units, 14.4% were in the IT information technology industry, and 11.7% were in the internet industry. As the government holds important national information and data, its security directly affects national security and social stability. The connotations and extension of national security in the information age continue to expand in time and space, and risk factors are becoming increasingly complex and changeable, increasingly blurring security risk boundaries and rendering them uncertain. The information synergy effect generated by information embedding has become an important security risk factor. Many scholars (Wang Yizhou, 2004; Yu Xiaofeng, 2008; Liu Yuejin, 2021) divide national security into traditional security and nontraditional security, with traditional security issues including political security, military security, and territorial security and nontraditional security issues including ecological security, information security, cultural security, and social security. Therefore, it is believed that the security risks in government information disclosure are mainly the information security, political security, social security, and economic security risks caused by the integration of individual information. They include both traditional and nontraditional security issues, demonstrating diversity and complexity.

Table 1: Typical security risk event cases of government information disclosure

Time	Event	Public information	Risk type
1964	China's "photo leak case"	Photo of Wang Jinxi	Economic security
2007	The United States releases the internal handbook of the Chinese Navy 2007	The White Paper on China's National Defense, the Naval Dictionary and other public documents published in China and abroad	Information security
2014	Bellingcat Malaysia Airlines MH17 air crash incident intelligence analysis case	Twitter, YouTube, Google and other public data	Political security
2017	Equifax company "Superdatabase" event	Names, social security numbers, dates of birth, addresses, etc.	Information security
2017	Photo of the DF-41 ballistic missile carrier	Missile photo	Political security
2022	Information leakage in Britain and Ukraine	Photos of Ukrainian forces unloading weapons	Information security
2022	Russia-Ukraine war	Network platform to open information	Community security

3.1 Information Security Risk

First is the infringement of citizens' privacy rights. The information security risk of citizens refers to the security status of personal information, such as citizenship and property [8]. The risk under mosaic theory is mainly the "mosaicization" of citizens' information, which threatens personal privacy. In today's network era, personal information is basically digitized, and the boundary between personal information and personal privacy is gradually becoming blurred. Although the information disclosed by the government is only a part of personal information, under the assumption of mosaic theory, when these pieces of information are put together, a complete personal information image can be formed, which involves the issue of personal privacy. Malicious analysts, based on mosaic theory, constantly explore hidden special relationships in various network interactive activities, such as email communication, information retrieval, and online transactions, by combining mining methods (such as online information analysis and micropattern recognition) to extract hidden potentially valuable information that was previously unknown. A study by the famous American computer scientist Latanya Sweeney shows that "combining postal codes, birth dates, and genders

can basically determine a person's identity, with a probability of up to 87%." [9]

The Columbia Circuit Court of Appeals, citing mosaic theory, pointed out that even though individual pieces of personal private information may be protected, the accumulation of a large amount of information still poses a significant threat to individual privacy [10]. In 2017, the personal information of approximately 145 million Americans and 100,000 British people, including names, social security numbers, birth dates, addresses, and driver's license numbers, was stolen from the Equifax global credit rating agency database [11]. Hackers were able to obtain more information by integrating the information they collected. The combination of personal contact information, ID numbers, marital status, residence permits, and property rights certificates is like combining small individual tiles to form a mosaic that can reveal a person's economic situation. Under specific usage, this may endanger the personal safety and property of the information subject and can easily lead to damage to personal reputation, harm to physical and mental health, or discrimination. Although individuals may not subjectively feel that their privacy rights have been violated by fragmented information, the accumulation of a large amount of information can still pose a serious threat to individual privacy. The cost of collecting and matching information is decreasing, and once individual, isolated, and publicized personal information is collected, extracted, and synthesized, complete, detailed, and accurate overall information about a specific individual can be obtained. Once this comprehensive and systematic overall information is leaked and spread, privacy will be greatly threatened.

Second is military intelligence leaks. Any facts, processes, states, and methods related to national defense, military, weapons, and war as well as various descriptions of facts, processes, states, and methods related to military affairs can be considered military intelligence [12]. Photos of military units and strategic locations may seem ordinary to the average person, but they are extremely valuable to intelligence analysts. For example, a photograph of the Yangtze River Bridge may appear "majestic and spectacular" to most people, but intelligence experts can calculate the most deadly strike points of the bridge based on its proportions and estimate the amount of materials needed to destroy it by examining the quality of the building materials in close-up photos [13]. In March 2007, the US Navy's intelligence agency released an internal manual called "China's Navy 2007," which drew mainly from Chinese and international public sources, such as "China's Maritime Strategy," "The Great Wall at Sea: China's Navy Enters the Twenty-First Century," "China's Defense White Paper," "China's Naval Encyclopedia," and "Naval Dictionary." The 144-page manual is divided into 16 chapters. Compared with traditional US Navy combat manuals, the manual does not list or illustrate specific ships, but it does provide detailed introductions to China's naval organizational structure, leadership, political work system, naval military academies, recruitment system, troop training, foreign exchanges, weapons and equipment, and other content [14]. Based on the analysis of photographs of weapons unloaded by the Ukrainian side, the British "Defense Brief" speculated on the types of weapons and combining this analysis with public information from multiple sources, estimated the quantity of equipment [15]. In the process of the Russo-Ukrainian conflict, the US used public information to investigate whether Russia was using cluster munitions in civilian areas and to track military infrastructure, evaluate on-site events, and assess casualty numbers. Based on mosaic theory, although certain information itself may not be considered a state secret, because of the special nature of some data, if illegal elements organize professional researchers to connect these data with other data for inference and verification, it is difficult to guarantee that they will not pose a potential threat to national security. However, this possibility is often difficult to prove.

3.2 Political Security Risk

Political security risks are mainly risks to sovereignty security, territorial security, political regime and political system security, and ideological security that are characterized by fundamental, strategic, comprehensive, and long-term values [16]. Against the background of mosaic theory, security risks are the integration of fragments of government information, which threatens the security and stability of the government regime. Whether government information in China is open depends on the consideration of documents rather than individual pieces of information. Occasionally, the consideration of individual pieces of information is limited to whether they will pose a threat to national security, and the potential risks to national security brought by the mosaic of individual pieces of information are not considered, resulting in the disclosure of any information that has no security risks. Based on mosaic theory, malicious analysts can use a combination of various data mining techniques to explore special correlations hidden in various network interactions and extract potentially valuable, previously unknown information. These information fragments may contain sensitive information, such as the internal organization and business information of government agencies. Attackers can investigate more sensitive information by collecting relevant organizational fragments and using social networks, creating false information about government activities, or using government agency business process and work detail fragments to gain a deeper understanding of the operational mode and weaknesses of government agencies. Then, they can conduct attacks and infiltrations, which may lead to disorder in government operations, interruption of public services, and social unrest.

The intelligence analysis of the MH17 plane crash by the Bellingcat team in 2014 is a typical case. After the air disaster, the Bellingcat team quickly found that the plane had been shot down by a Russian-made "Buk" missile and accurately determined the transportation route and time of the missile launcher as well as the fact that the launcher had eventually entered Russian territory after the accident. Using public data such as Twitter tweets, Instagram photos, YouTube videos, and Google Maps from the crash site, they achieved an information collection and confirmation speed that was comparable to those of intelligence agencies. On January 24, 2017, a photograph of a "Dongfeng-41" ballistic missile transport vehicle appearing on the streets of Heilongjiang caused widespread discussion on the internet. Once relevant public information such as reports, photos, videos, and maps are aggregated for intelligence analysis, as in the case of the

MH17 plane crash, some classified information and important intelligence will inevitably be leaked [17]. In addition, using public information to create false information is a "cancer" that worsens the relationship between the government and the people. If this problem is not resolved, the interests of the public will be violated, and all services provided by the government will be in vain. Since the beginning of the military conflict between Russia and Ukraine, Western countries have launched a comprehensive information war against Russia, causing false messages to spread. Russian Foreign Ministry spokesperson Zakharova said on the "Russia-24" TV program, "A large number of false messages are filling our news space [18]. Behind all of this is the intelligence agency, and NATO is leading and manipulating it." False information and leaks will seriously affect the credibility of the government and lead to a "Tacitus trap," which should be taken seriously.

3.3 Economic Security Risk

Economic security risk refers to potential threats to the development of a country's national economy and economic strength [19]. When information is obtained about a country's trends, including decisions, resource allocation, internal policy adjustments, and changes in procedures, significant changes in that country can often be inferred through integrated analysis of the information. Some companies and organizations in Western countries have used information publicly released by the Chinese government, such as geographic information, statistical data, and scientific research results, for commercial espionage and intellectual property infringement activities, posing a threat to China's economic interests and security. China's most famous "photo leak case" was an early example of intelligence discovered through correlated analysis of public data. In the photo, Wang Jinxi, the "Iron Man" of the Daqing Oilfield, wore a large fur hat and a thick cotton coat and looked into the distance, holding a drilling machine handle, with tall oil derricks scattered behind him in the snow. Japanese intelligence experts deciphered the secret of the Daqing Oilfield through this photo. Based on Wang Jinxi's clothing in the photo, they deduced that only in the region between 46 and 48 degrees north latitude would someone wear such clothes in winter; therefore, they inferred that the Daqing Oilfield was located between Qiqihar and Harbin. They also inferred the diameter of the oil well from the position of the handle in Wang Jinxi's hand and roughly estimated the reserves and production of the oilfield based on the distance between the drilling rig, the oilfield behind Wang Jinxi, and the density of the derricks. With so much accurate intelligence, the Japanese quickly designed petroleum equipment suitable for the development of the Daqing Oilfield. When the Chinese government solicited design proposals for the development of the Daqing Oilfield from countries around the world, the Japanese won the bid with their design. Fortunately, at that time, Japan was driven by economic motives, and based on the results of its intelligence analysis, it sold refining facilities to China at a high price rather than using them for military strategic purposes [20].

3.4 Social Security Risks

Social security risks refer to unsafe factors that affect the benign operation and coordinated development of the social system [21]. Mosaic theory emphasizes that the main social security risk is the threat of terrorists. After 9/11, the Bush administration extensively cited mosaic theory, portraying seemingly ordinary information as intelligence-related. Terrorists often scrutinize public information sources to piece together government activities [22]. Publicly available statistical data, along with other information in the public domain [23], allows terrorists to draw maps of government research, outline investigation processes, and develop investigation methods to interfere with law enforcement procedures [24]. Terrorists use the synergistic effect to transform harmless information, such as city maps and traffic routes, which the government publicly posts on social media [25], into useful materials for attacking targets and planning schemes. In the ACLU v. Department of Justice case, the government relied on mosaic theory to detain summary statistical data on the implementation of certain provisions of the USA PATRIOT Act, arguing that publishing such statistical data in the public domain, combined with other information, could allow terrorists to understand the FBI's investigative work [26].

In the era of big data, the construction of digital government enables more information to be openly shared without national boundaries, and these sources can easily be searched for information related to national security. Such searches are supported by various data mining, processing, and analytical technologies and software. Thus, the risk of leaking national security information is increasing. Unilateral information disclosure by government departments may meet the requirements of departmental responsibilities, but the integration and mining of information from various departments may reveal secrets related to national security, personal privacy, and government. If this information is controlled by competitors, criminal organizations, or even hostile countries, it will provide an opportunity for foreign hostile forces to interfere in a country's internal affairs, attack its political system, incite social unrest, and undermine its political stability. The security risks are self-evident.

4. Analysis

Mosaic theory describes a process of collecting, combining, and compiling information [27], that is, the process of information synergy through which government public information is transformed into open-source intelligence [28]. This has long been associated with the intelligence collection process. In the context of mosaic theory, security risks in government information disclosure mainly involve the integration and analysis of information fragments. Any organization or individual can collect and process government information, and further excavation of some information may endanger national security and public interests. This is mainly attributed to external and internal factors. First, external organizations or individuals process public information to serve economic, political, and other interests. Information warfare has become an important component of competition among countries. When information flows into government systems through different channels, the government, as an information field, must converge different directions, categories, and types of information vectors and use appropriate methods to analyze, encode, and abstract

information. Through correlation analysis and cluster analysis of information, fragmented information can be pieced together to extract valuable new information and adjust its behavior in a timely manner to achieve predetermined goals. Second, the underlying security mechanisms of the internal network are not sound. First, various information on the internet has not been encrypted, and all information is transmitted and stored in plain text, which can be easily captured, read, and analyzed. Second, users and devices on the network have not been authenticated, as an authentication and management system is lacking. When a user logs on to the internet, the interacting device and user do not know each other's identity, whether the device can log in, and whether there are security risks. In recent years, security risk events induced by external factors have occurred frequently, exposing many internal security factors. This article aims to analyze the generation logic and evolution characteristics of security risks in government information disclosure at different stages.

This study uses life cycle theory and focuses on the three key stages, information collection, embedding, and utilization, in order to explore the evolution and development of risk, including the formation of risk sources, the transmission of risk, and the social amplification of risk. These three stages interact and influence each other, collectively constituting the process of the formation and development of security risks (see Figure 2). The information collection stage represents the risk source, the embedding stage is the key stage for risk generation, and the utilization stage amplifies the risk socially. The evolution process of security risks will be further discussed in terms of these three aspects.

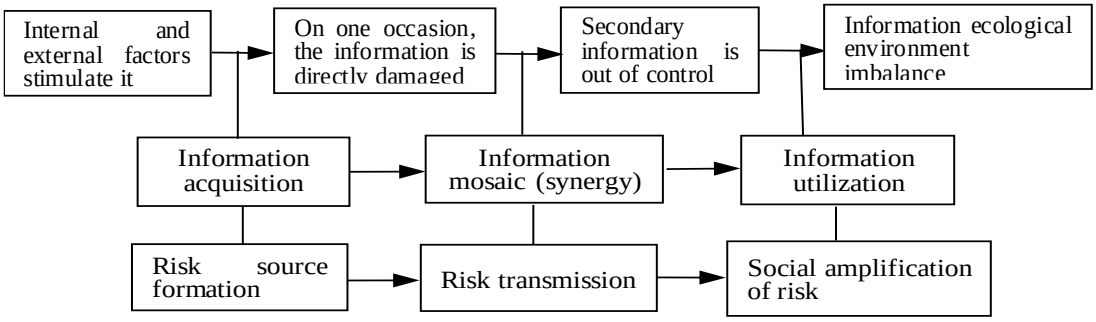

Figure 2: Generation process of security risks

(1) Formation of risk sources. Risk sources are the starting point of safety risks, which are usually caused by various uncertainty factors, including internal and external factors. The information collection stage is a risk source because individuals or organizations can collect and obtain target information through various means at this stage. This information may involve countries, government agencies, enterprises, or individuals, including personal identity information, business secrets, and politically sensitive information. This information is usually unprocessed, and a piece of information has three characteristics: comprehensiveness, i.e., the information volume is sufficient to be valuable and can support relevant analysis needs; multidimensionality, i.e., the information is flexible and can be customized quickly, with various types meeting different target needs; and efficiency, i.e., the efficient and timely analysis and satisfaction of information needs. Due to the openness of government information, the collection channels are extensive, including information from various departments, real-time monitoring information, and network data. Under normal information conditions, information collection occurs mainly through formal information channels, and the embedded scope is relatively small, while under big data information conditions, information collection occurs through informal informational channels such as the internet and social media, and the embedded scope expands accordingly. Driven by external interests, especially in the context of globalization, economic, political, and military competition between different countries has become increasingly frequent and intense, and information power directly determines international discourse power. The lack of sound internal security mechanisms leads to extremely low information collection costs, and both internal and external factors jointly cause direct damage to a piece of information, forming a risk source.

(2) Risk transfer refers to the process in which security risks spread from the source to the outside. After the information collection stage, information is usually transmitted and processed, and the information is then transformed into secondary information, forming the process of risk transfer. In this study, the key link of risk transfer is called the "embedding stage," during which information is integrated, processed, stored, and transmitted. Through different management activities, useless information can be organized and processed to transform it from unavailable to available, from low availability to high availability, and from low value to high value, thus improving information quality, improving information utilization, and promoting information added value. This process relies on information technology to manage individual government information resources, classify and organize individual useless information, and enable this information to be effectively counted and analyzed. Thus, the overall value of information is greater than the sum of its parts, as it becomes intelligence that is helpful to the country, government and individuals. Information embedding tools are mainly technical tools (system platform construction, information communication technology, network mining technology, data processing technology) and management tools (administrative command promotion, mechanism and system construction, mutual assistance agreements, outsourcing and crowdsourcing). During the embedding stage, secondary information may become out of control, and the risk may be amplified. Criminals can mine weak relationships between information sets from massive, complex, seemingly unrelated and scattered information and, through spatiotemporal puzzles, turn fragmented static unit information into networked dynamic module information, and further transform public information into open source intelligence, thus tracing individuals' personal whereabouts, enterprise research and development or business trajectory,

and even national strategic actions. This may threaten personal privacy, government secrets, and national secrets and have varying degrees of impact on society.

(3) The social amplification of risk refers to the final stage of security risks, which occurs during the utilization of information after it has been embedded. This stage is characterized by a severe imbalance in information ecology, and it significantly expands the scope of security risks. Government information contains both explicit and implicit intelligence, and the latter plays a crucial role in decision-making. As information is disseminated, communicated, released, transferred, and transformed, its value increases and it provides a knowledge base and experiential background for solving problems. However, it can also lead to hidden security risks, such as economic losses, political crises, and social instability, thereby further expanding the influence of security risks. At this stage, the social amplification effect of risk is enhanced, as in the case of information warfare between countries, which can lead to information powerhouses controlling information and causing one-sided international public opinion, leading to injustice. In a sense, an imbalanced information ecology that fails to serve society impartially can become a disaster for humankind. The traditional and nontraditional security risks described here are examples of the social amplification of risk. Only by managing security risks in the first two stages can the creation of these risks be avoided.

5. Discussion

5.1 Implications for Research

By applying mosaic theory to analyze security risks and the logic of how they are generated in government information disclosure, the following conclusions can be drawn. First, the security risks in government information disclosure include both traditional and nontraditional risks, with information security being the main risk, followed by political, economic, and social security risks. Second, the logic behind the generation of security risks is similar to life cycle theory, and three stages of the process of generating security risks can be analyzed: information collection, information embedding, and information utilization. The generation logic roughly follows the process of "internal and external factors triggering—direct information damage—secondary information loss of control—imbalance of information ecological environment." Third, the main source of security risks is driven by external interests and internal security mechanisms that are not sound. Therefore, the internal environment should be the focus to prevent security risks caused by the external environment.

Public information can be used as a national security strategy by other countries, posing a threat to national security. Mosaic theory can help us understand the risks of public and nonpublic information [29]. Mosaic theory provides a new perspective for preventing security risks in government information disclosure.

5.2 Implications for Practice

First, in the information collection stage, it is important to strengthen security measures, limit public access, and prevent potential risks. Starting from the foundational architecture, security mechanisms should be established to monitor information collection activities. According to China's Personal Information Protection Law, data handlers must obtain user consent before collecting, storing, transmitting, or reusing personal data. Transmitted information should be encrypted to minimize the risk of leakage and increase the cost of unauthorized access. Security authentication and warning systems should be established for devices, users, and organizations operating on the network. Blacklists should also be created for accounts that maliciously manipulate and spread false information, with measures such as account suspension or banning[30]. Network security technologies such as access control, identity verification, authorization, system integrity checks, encryption, intrusion detection, and defense should be comprehensively applied to track and control potential risks, thereby eliminating security risks in the early stages. Second, the information classification management system should be improved to prioritize reasonable information that should not be made public. The Data Security Law of 2021 clearly states in Chapter Three, "Data Security System," that public data attributes should be classified and protected. Mosaic theory requires organizations to classify information that may be harmless when isolated but could be harmful to national security when combined with other information [31]. This theory is a theoretical tool to help the government reasonably disclose content and support the retention of classified information. It is essential to establish and improve the classification standards for important information in political, military, economic, technological, and other relevant fields. Based on the processability and value of information, important information should be distinguished from general information. Mosaic theory should be regarded as a legitimate reason for government secrecy and expanded to allow the government to retain information under existing laws. However, the potential harm to the integrity of the government system and excessive secrecy caused by mosaic theory should be carefully evaluated, and using mosaic theory to refuse to disclose useful and harmless information to the public should be forbidden [32]. If public access in electronic form to disputed information is requested, organizations can consider providing a hard disk copy or encrypted version instead of using mosaic theory to refuse to disclose all versions [33]. Finally, national security reviews of mobile information should be strengthened. Article 24 of China's Data Security Law clearly states that "the state establishes a data security review system to conduct national security reviews of data processing activities that affect or may affect national security," and the "Network Security Review Measures (Draft for Soliciting Opinions)" further strengthens data security reviews. Regulatory authorities should conduct security reviews of public information flows, and sensitive and important data containing national or citizen information should be submitted for security evaluation before leaving the country to prevent government information from becoming a tool for illegal organizations or individuals to analyze and harm China. In addition, the cross-border circulation of core national data should be prohibited.

Second, in the information embedding stage, it is necessary to crack down on illegal processing, establish emergency plans, and block risk transmission. First, legislation should be strengthened to strictly control information processing

behaviors. Article 111 and Article 1038 of China's Civil Code specifically prohibit the "illegal" processing of individuals' personal information. Therefore, "what types of information can and cannot be publicly collected and processed by organizations or individuals" should be clarified in all relevant laws, and organizations and individuals engaged in illegal processing should be punished according to the harm caused by the information processing. Furthermore, countermeasures should be established, the scope of network security reviews should be expanded, and foreign organizations collecting and processing information that is publicly available from the Chinese government should be subjected to national security reviews with the power to access data and examine devices when necessary [34]. Second, awareness should be deepened, and literacy should be improved. In terms of risk awareness, government information disclosure reviewers should be aware of intelligence, risk, compliance, security, collaboration, and embedding and use intelligence concepts to guide their work; they should have a clear understanding of the security risks of information embedding and always operate in compliance with safety guidelines. In terms of information embedding skills, the US National Intelligence Director's Office has established an Open Source Center (OSC) and launched the National Open Source Enterprise (NOSE) program, which focuses on collecting, sharing, and analyzing publicly available information, establishing open source intelligence training standards, and including open source intelligence training in leadership and management training. China can learn from the US approach and establish a comprehensive information embedding skills education system that includes professional education, skills training, and knowledge dissemination. Only by improving the information embedding skills of government personnel can external embedding behaviors be precisely identified. In terms of emergency plan establishment, various types of information embedding incidents can be summarized, and information sources, processing methods, consequences and impacts, involved units, resolution methods, bottlenecks, and other aspects can be listed to gradually identify the embedding relationships, forming a multidimensional risk identification and processing case library for information security, political security, social security, etc. Solving security risks in the first two stages can avoid the expansion of risks in the final stage.

5.3 Limitations and Future Research

Because this study is limited by the mosaic theory perspective in the analysis, the security risks in government information disclosure cannot be traversed, so in the subsequent study, we will further sort out each subdivision of risks and conduct in-depth excavation and targeted exploration.

References

[1] Libor B. OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm[J]. Journal of Strategic Security, 2013, 6 (3):22-37.

[2] Jiang Changqing. Risk assessment of big data for national cyber security[J]. Information security in China. 2015, (05):53-54.

[3] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 635-652.

[4] Christina E. Wells. CIA v. Sims: Mosaic Theory and Government Attitude[J]. Administrative Law Review, 2006, 58: 864.

[5] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 643.

[6] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 630.

[7] Ning Yuan. Personal Information Protection Regulation in the Application of Health Code[J]. Law Comments. 2020, 38 (06):111-121.

[8] Zhang Minan. Research on Information Privacy Rights[M]. Guangzhou: Zhongshan University Press, 2014.

[9] United States v. Maynard,615 F.3d 544 (D.C. Cir. 2010).

[10] Sohu.com: The United States sues China on the grounds of "cyber attacks" for stealing 145 million citizens' data. [EB/OL].[2020-02-11].https://www.sohu.com/a/372226016_354899.

[11] Zhou Lin. Military informatics[M]. Beijing: National Defense University Presss, 2003.

[12] People's Daily Online: Revealing the secrets of China's most famous "photo leak case". [EB/OL]. [2014-05-12]. http://military.people.com.cn/n/2014/0512/c1011-25007286.html.

[13] Secretariat Administration Department of the National Bureau of Secrets: The risk of data leakage in the era of big data when public data is disclosed. [EB/OL].[2023-02-21].http://www.gjbmj.gov.cn/n1/2018/1218/c411145-30474566.html.

[14] Xinhua News: Information Leakage, UK Admits Providing Weapons to Ukraine. [EB/OL]. [2022-01-27]. http://www.news.cn/mil/2022-01/27/c_1211543170.htm.

[15] Li Haoqing. Hong Libo,. Risk analysis and prevention strategy of network rumors for political security[J]. Modern intelligence. 2019, 39 (05):156-165.

[16] Secretary of the Administrative Department of the National Administration for the Protection of State Secrets: The Risk of Data Leakage in the Era of Big Data Open Data. [EB/OL].[2018-12-18]. http://www.gjbmj.gov.cn/n1/2018/1218/c411145-30474566.html.

[17] Sui Xin. Liu Zhi. Russia comprehensively back the information war between Ukraine and the West[N]. Global Times. 2022-03-03.

[18] Zheng Xiuxiu. Liu Qing. Zhao Zhongxiu. Technical barriers to trade with China and National economic security [J]. International Economic Review. 2023 (01): 131-151+7-8.

[19] People's Daily Online. Revealing the secrets of China's most famous "photo leak case" [EB/OL]. [2014-05-12]. http://military.people.com.cn/n/2014/0512/c1011-25007286.html.

[20] Wang Long. Huo Guoqing. Empirical study on the original influencing factors and their mechanism of social security[J]. Management Review, 2019, 31 (11): 255-266.

[21] Christina E. Wells. CIA v. Sims: Mosaic Theory and Government Attitude[J]. Administrative Law Review, 2006, 58: 867.
[22] Christina E. Wells. CIA v. Sims: Mosaic Theory and Government Attitude[J]. Administrative Law Review, 2006, 58: 863.
[23] United States Court of Appeals, District of Columbia Circuit. Center for National Security Studies v. Department of Justice [EB /OL] [2023-01-15]. https://caselaw.findlaw.com/us-dc-circuit/1046947.html .
[24] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 633.
[25] United States District Court for The District of Columbia. Electronic Privacy Information Center v. United States Department Of Justice [EB/OL]. [2023-01-15]. https://www.aclu.Org/sites/default/files/field_document /aclu_v_doj_gov_msj. pdf.
[26] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 633.
[27] Christina E. Wells. CIA v. Sims: Mosaic Theory and Government Attitude[J]. Administrative Law Review, 2006, 58: 853.
[28] Jameel Jaffer. The Mosaic Theory. Social Research, Vol. 77, No. 3, Limiting Knowledge in a Democracy (FALL 2010), pp. 881.
[29] Gao Yandong. Use the weapon of law to deal with information warfare[N]. Global Times.2022-03-31.
[30] Taylor v. Dep't of the Army, 684 F.2d 99, 102-05 (D.C. Cir. 1982).
[31] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 673.
[32] David E. Pozen. The Mosaic Theory, National Security, and the Freedom of Information Act[J]. The Yale Law Journal, 2005, 115(3): 676-677.
[33] Gao Yandong. China needs to fully defend its data sovereignty[N]. Global Times. 2021-07-14.