Frontiers in Business, Economics and Management
ISSN: 2766-824X | Vol. 5, No. 3, 2022

The Study on National Security in Big Data Era

Xuan Liu

Emilio Aguinaldo College, Manila, Philippines

Abstract: Over the past decade, " big data " has become an ubiquitous buzzword in academia, the professional world and the media. Some commentators have hailed big data as " the new oil of the 21st century " and " the world's most valuable resource ". As technology advances and data becomes more readily available, processing power is increasing, as predicted by Moore's Law in the 1970s. The rapid development of instruments and sensors, digital storage and computing, communications and networks has driven an inevitable " big data revolution ", generating and providing ever more data. This has huge implications for national governance, political and military strategy, national security, corporate decisions and individual lifestyles. In the face of the surging flood of big data, existing national security management methods can no longer meet the security requirements of the era of big data, and national security is facing severe challenges. The exposure to PRISM shows that European and American countries have carried out large-scale development and research on big data, constantly mining big data, analyzing the connection between data information, in order to serve the national security strategy. Therefore, the arrival of the era of big data has brought both opportunities and challenges to China's national security management. In this context, only by closely tracking the development trend of big data can we grasp the trend of The Times, safeguard political security and regime security, and comprehensively improve China's future security strategic advantages.

Keywords: Big data, National security, National security strategy, International strategic pattern, Information security.

1. Introduction

With the development of science and technology and the continuing spread of COVID-19, data-centered digital technology has gradually become a new driving force for economic development, generating new momentum for the further development of the digital economy. For example, innovations driven by new modes of mobility, personalized medicine, telecommuting and more have benefited more people. At the same time, increasing data resources and changes in their storage and processing technologies will gradually become a potentially growing and sustainable accumulation of social resources.

According to the well-known consultancy IDC, the global data volume will reach 163ZB in 2025. Among them, China's data volume is expected to increase to 48.6ZB in 2025, accounting for 27.8% of the global data circle. (https://www.sohu.com/a/139853369_380891) The average annual growth rate is 3% faster than the global data circle, and China will become the largest data circle in the world.Big data is another disruptive technological revolution in the IT industry following cloud computing and the Internet, which will have a huge impact on national governance model, political and military strategy, national security, enterprise decision-making, and personal life style. The mining and application of big data can not only create a value of more than a trillion DOLLARS, which can be called another industrial revolution, but also may have a huge impact on government management, national security, especially political security and regime security. Therefore, at the critical moment when the world is moving towards the era of data and big data, China, which is the smallest distance from the world in reform and development, is facing significant historical opportunities and challenges.

In the face of the surging flood of big data, the existing national security management methods have been unable to meet the security needs of the era of big data, and national security is facing severe challenges. The exposure of PRISM reflects that European and American countries have developed corresponding national security management strategies in the era of big data, and invested in research and development on a large scale. Through the mining of big data, these information and connection information are analyzed to obtain relevant intelligence, serving for the government's anti-terrorism and national security work. Therefore, the advent of the big data era has put forward new requirements for the formulation of national security management methods in China. In this context, only by closely tracking the development trend of big data can we grasp the trend of The Times, safeguard political security and regime security, and comprehensively improve China's future security strategy.

From the perspective of national security, the formulation of national security management policies in the era of big data has become an urgent and realistic major problem. This article through to the big data definition, connotations and era characteristics analysis of the concept of big data leak case of threats to national security, and with the United States and Europe in recent years, in view of the large data in national security management measures taken and scheme were analyzed, and on the problems faced by China's national security management and impact study, and provide some Suggestions.

2. Literature References

The futurist school, represented by Alvin Toffler, has seen the transformative effect of the development of a series of new technologies such as microelectronics, computers and communication on human society since the 1970s. He predicted the coming of the information society and its political, economic, social and cultural consequences. In a series of books, Future Shock (1970), Third Wave (1980), Power Transfer (1990) and Future War (1994), he proposed the power transition, new types of warfare and political processes under the tide of information. To inspire researchers. British academics' book: "Big Data: A Revolution That Will

Transform How We Live, Work, and Think"(Viktor Mayer-Schönberger and Kenneth Cukier 2014), is regarded as the pioneering work of foreign big data system research. The book prospectively points out that the information storm brought by big data is changing our life, work and thinking, and big data has opened the second major transformation of The Times. The book makes clear that the biggest shift in the era of big data is to abandon the desire for causation and focus instead on correlation. This means knowing the "what", not the "why". This has overturned thousands of years of human thinking conventions, and posed new challenges to the way humans perceive and communicate with the world. Slouka, an American scholar, pointed out that "the politics of virtual reality 1 refers to the influence that technologies will bring to politics that may permanently blur the line between real and unreal," adding that "the digital revolution, at its deep core, is related to power." (Slouka. 1999) Negroponte lists "decentralization" as the first of the four qualities of digital existence, arguing that the traditional idea of centralization will become obsolete as the Internet grows. (CAI Yali. 1997) According to Walter Reston, the Internet has broken the monopoly of information and the consensus of opinion. The openness and discreteness of data determine that the communication is completely free, and the data information on the network "can spread to every corner of the world without any obstacle with the help of electronic network like a microorganism". (Lian Jiajian. 2015) Some scholars assert that data crimes seriously endanger national security.(Yu Zhigang, & Li Yuangrain. 2014) More importantly, the boom in the era of big data has weakened the government's control. According to American scholar De Tuzos, the data information market worries governments from two aspects: on the one hand, its influence is omnipresent and tends to ignore national boundaries; Another aspect is secrecy, which the new encryption regime can give to criminals and anyone deemed an "enemy of the state". So far, it has been possible for a state to track people's behavior, especially criminal sabotage, in the data space, but it has undoubtedly increased the cost and difficulty of government. (De Tuzos, & Zhou Changzhong. 1998). Anthony Orom believes that the disorder and irrationality of online public participation in the era of big data will harm the democratic principle of majority consent, so that it is difficult to find effective means to coordinate the overall interests of the society, which may lead to increasingly serious anarchy or even the collapse of the country.(Walter B.Wriston 1997).

3. How Does Big Data Affect National Security?

3.1. Big Data Has Changed the Global Strategic Landscape Subversively

Big data is changing the overall national strength of countries, reshaping the international strategic landscape in the future, and posing new challenges to national sovereignty and security.

(1) Big data is becoming a new driving force for economic and social development.

With the application, development and popularization of new network technologies such as the Internet of Things, cloud computing and mobile Internet, the process of social informatization has entered the data era, and the generation and flow of massive data has become normal. In the next 20 years, five billion people around the world will be connected to the Internet. "Everyone will have a terminal, access to the Internet everywhere and be connected all the time", which will make the global data volume grow exponentially. It is estimated that by 2025, global data usage will reach about 163ZB (1ZB=1 billion TB), which will cover all fields of economic and social development and become a new important driving force. (https://www.sohu.com/a/139853369 _380891)

(2) Big data redefines the space for great power gaming.

In the era of big data, countries around the world are rapidly increasing their dependence on data, and the focus of national competition has shifted from fighting for capital, land, population and resources to fighting for big data. In the future, national competitiveness will be partly reflected in the scale, activity, interpretation and application of data owned by a country. Digital sovereignty will become another space for great powers to play games after border defense, coastal defense and air defense.

Big data makes the distinction between data-strong countries and data-weak countries no longer depend on economic size and strength, but on a country's big data capability. For example, a country like Singapore can also rely on its abundant funds and talents to win against major competitive powers through big data, Such as neighboring Malaysia, Indonesia, etc., to enhance international competitiveness.

(3) Big data will change the architecture and model of national governance.

Big data is not only a technological revolution, an economic change, but also a change in national governance. Big data era, rely on the practice of government management and protection of data would make the government in the face of large-scale and complex data overwhelmed, overwhelmed, and big data can through to the massive amounts of data, dynamic, high growth, diversification, diversification of high-speed processing, rapid access to valuable information, improve the ability of public decision-making.

In addition, the proposal of data sovereignty also changes the roles of the government, enterprises and individuals, and makes the national governance structure gradually realize the transformation from the country's dominant governance structure to multiple co-governance, from closed governance structure to open governance, from the government allocation of resources to the market allocation of resources. Big data as infrastructure and big data as fundamental institutions exist at the same time.

(4) "Big data security" has been equated with national security.

In the era of big data, data security threats may occur at any time. All kinds of national information infrastructure and is bearing the important institutions of huge data information, such as controlled by information network system of oil and gas pipelines, water, electricity, transportation, banking, financial, commercial and military, etc., are likely to be the attack target, big data security has risen to become crucial part of national security.

3.2. Big Data Increases National Security Risks

From the large-scale leak of network data, to the mobile phone is monitored by APP (mobile application software); From the user is the portrait of "ripe", to the state classified information is accurate analysis. Big data has long been closely linked with people and national security. Data has become the fourth largest resource after energy, resources and

information, and the fourth space after territory, territorial sea and airspace.

(1) Data is the strategic intelligence of a country, and the party with the advantage of data can carry out "dimensionality reduction" strikes. By retrieving user information on social software, individuals can be quickly depicted and positioned accurately. Analysis of a country's economic data can bring down its financial system in an instant; By processing road information, missiles can be guided to strike key facilities accurately. An analysis of a nation's genetic and health data could easily wage a one-sided biological war. In the digital economy, whoever controls the data will control the whole world. The side with the advantage of data can see all the opponent's cards, and can launch a "dimensionality reduction" war at any time.

(2) Data from all over the world is flowing to the US, and "data dependency" seriously erodes national sovereignty. According to Synergy Research, the world's 20 leading cloud and Internet services companies operated 597 supersized data centers as of 2020, with the U.S. accounting for 40% more than any other country. China was second but accounted for only 10%. (https://www.chinairn.com/report/20220120/102946738.html). Storing your data on another country's servers or in the cloud leaves your fate in someone else's hands.

(3) The attacks of hacker organizations are becoming more and more powerful, and the country's key data is almost unguarded. Unlike other tangible assets, data assets are mostly stored on the servers of Internet companies, despite the national security implications. This is essentially different from the traditional "heavy guard" in the field of national security, and also leaves huge room for hacking. In early May 2021, a ransomware attack on the U.S. Company Colonial Pipeline shutdown a pipeline for several days, causing a fuel supply crisis in several states and regions. The attack, which has reached the national attack level, can not only take control of users' computers, but also steal data from servers. If these attacks were carried out by groups with a state-backed background, the consequences would be dire. And it's not out of the question. Around 2010, the Stuxnet worm was used by the United States to attack Iran's nuclear facilities, disabling Centrifuges and posing a serious national security threat to Iran. (http://world.people.com.cn/n/2015/0531/c1002 - 27080992.html)

4. Case Study of Big Data Affecting National Security

The influence of big data on national security involves many aspects of national security, such as obvious science and technology security and information security, while the influence on national security, political security, ideological security and social public security is often ignored by us. The following focuses on the negative impact of big data on national security by studying some cases affecting national security in recent years.

4.1. Threats to National Information Security Cases

4.1.1. The Prism Scandal

In June 2013, former CIA contractor Edward Snowden revealed to the Guardian and The Washington Post that the NATIONAL Security Agency (NSA) had been conducting a top-secret electronic surveillance program code-named PRISM since 2007. Under the plan, the NSA demanded that U.S. telecom giant Verizon (VZ) turn over the call records of millions of its customers every day. The NSA and FBI have access to the servers of nine Internet giants, including Microsoft, Google, Yahoo, Apple, Facebook, YouTube, Skype and Palalk.AOL, to track users' emails, chats, videos, audio, files and photos in real time. For a long time, the US government has been conducting round-the-clock surveillance of many countries through prism, and has obtained a large amount of intelligence information through the mining and analysis of the data obtained from the surveillance system. (Tang Ronghao. 2013). Undoubtedly, the national security of other countries has been seriously threatened in this program, while the United States continues to maintain its hegemony in the international community, especially in the field of network, with the help of big data.

4.1.2. Case Analysis

The exposure of the prism program shocked the world and made us reconsider information security in the era of big data. In fact, for a long time, many countries have, all in the name of maintaining national security and terrorism to arrange the related intelligence agencies, with a number of monitoring scheme, "prism" plan has attracted the attention of all over the world, because people suddenly realized that the monitoring plan has been pervasive go deep into the people working in every corner of life. In this era of data flooding, no information is secure through this prism.

Big data brings great threats to information security. Once information security is lost, it will bring immeasurable harm to national security. One of the reasons for this is that people nowadays rely too much on data. The rapid popularization and development of big data has led to the dependence of the whole country and society on data information. At present, the data information has already penetrated into a country's political, economic, military, culture and other aspects, can be said to all areas of work and operation of each part is inseparable from the support of data information, it seems that every aspect of a country, an area of operation process can also pass data to analyze reduction." Prism collects and analyzes these everyday data to gain a wealth of intelligence information. Second, the particularity and concealment of data information generation, storage and transmission increase the risk of information leakage. Especially for the developed countries with the early start of big data research and monopoly of technology, it is easy to use the advantages of technology to realize the intrusion of other countries' data systems and data information theft, while for the countries with technological disadvantages, they often do not know the data information is stolen. Thirdly, the amount of data information is large and the transmission is convenient. To take a very simple example, transferring and stealing documents of the same amount of information, in the era of paper documents required a truck to travel for a long time, in the era of big data only requires a USB or a few seconds of network transmission.

4.2. Threats to National Political Security Cases

4.2.1. The Jasmine Revolution

On Dec. 17, 2010, Mohammed Bouwajji, a 26-year-old street vendor, set himself on fire in the North African country of Tunis to protest his harsh treatment by the police. The incident sparked massive street demonstrations and pro-democracy movements across Tunisia that eventually led to

the fall of Ben Ali's regime. (https://en.wikipedia.org/wiki/Tunisian_Revolution). The main causes of the revolution were inflation, political corruption, lack of free speech and poor living conditions, but the Internet and big data also played a big role. Wikileaks obtained a trove of US government diplomatic cables that cited reports by the US ambassador to Tunisia revealing corruption in the Ben Ali family. These data are rapidly disseminated around the world through online media. The Revelations of corruption thoroughly inflamed popular anger against Ben Ali's regime and helped fuel the Jasmine Revolution. According to Foreign Policy magazine, the wikileaks cables may have been the catalyst for the world's first "Wiki revolution" in Tunisia. (https://foreignpolicy.com /2011/01/15/the-first-twitter-revolution-2/) The Tunisian economy grew rapidly until 2011, which was called the "Tunisian miracle". According to the 2009-2010 Annual report of the World Economic Competitiveness Forum, Tunisia ranked first in Africa and 40 of 133 countries in the world in terms of economic competitiveness, coping with the financial crisis, promoting communication and information technology and improving the quality of life. Tunisia is a model for developing countries in terms of clean government and people's livelihood. However, since the "Jasmine Revolution" in 2010, Tunisia's inflation rate, government debt ratio and currency devaluation have "snowballed", forming a vicious circle, leading to the intensification of social unrest in Tunisia. Tunisians said: "We have won our freedom, but we are still looking for work and dignity."

4.2.2. Case Analysis

The important role played by Internet whistle-blowing in the "Jasmine Revolution" makes us see the influence of the coming of the era of big data on political security, especially regime security. For one thing, in order to maintain political security, the government often releases information beneficial to the government selectively by controlling public opinion and media, so as to establish a good government image among the public and maintain its political rule. Before the era of big data, people had relatively few ways to obtain information -- at the same time, the government could better control the media through corresponding technology and management means. The advent of the era of big data has broken the government's monopoly on public opinion and media. Due to the immediacy of data information generation and the diversity of information release channels, the government's ability to control public opinion is reduced, and the public can learn political information more timely and widely. Some information that is not conducive to the image of the government is also rapidly spread, thus giving the government a heavy blow. Second, Western countries use big data as a tool to interfere in other countries' internal affairs. They use various advanced data communication terminals and means to interfere in other countries' democratic, human rights, ethnic and religious affairs, stir up hot issues, incite public sentiment, and create political crises, thus shaking the ruling foundation of other countries. The third reason is that the development of big data enables the public to have more right to speak, thus the power is transferred from the government to the public, and the public authority of the government is greatly weakened, which is very dangerous for developing countries with imperfect democratic systems. When the old authority is weakened and the new authority has not been established, it is easy to cause political disorder, thus endangering political security.

4.3. Threats to Social Stability and Public Security Cases

4.3.1. Violence and Terrorism in Xinjiang

On July 5, 2009, a serious crime of beating, smashing, looting and arson took place in Urumqi, Xinjiang. The criminals rampaged on People's Square, Jiefang Road, Big Bazaar, New South China Road and Outer Ring Road, resulting in 156 deaths and 1,080 injuries. A number of vehicles were burned and many shops were smashed and burned. (https://en. wikipedia.org/wiki/July_2009_%C3%9Cr%C3%BCmqi_riots)

On October 28, 2013, Usman Aishan, his wife, mother and three other people drove a jeep into Chang 'an Avenue. They drove fast along the road and deliberately rammed tourists. Finally, they crashed into the guardrail of Jinshui Bridge, ignited gasoline inside the vehicle and set it on fire. Five people were killed and 40 injured. Three people in the car, including Usman Esan, died on the spot. (https://en.wikipedia.org/wiki/2013_Tiananmen_Square_attack)

On March 1, 2014, Xinjiang separatist forces led by Kuerban created a violent terrorist incident at Kunming Railway Station. Five thugs armed with knives started from the waiting area of the railway station, through the square in front of the station, the second ticket area, ticket hall, small items storage and other places, wantonly cut and killed innocent people, and beat out violent terrorist flags, resulting in 31 deaths,141 injured, 40 of them seriously. (https://en.wikipedia.org/wiki/2014_Kunming_attack)

4.3.2. Case Analysis

The development of big data makes the Internet and new media play an increasingly important role in violent terrorist incidents and large-scale mass incidents, challenging public security and social stability. First of all, the arrival of the era of big data has greatly stimulated the enthusiasm of the public to participate in politics. Due to the diverse cultural levels and life experiences of the public, they have different views on the same event, resulting in many irrational attitudes and opinions. Due to the fast transmission speed and wide diffusion of data information, once social public crisis and violent terrorist events occur, these irrational participation is easy to accelerate the deterioration of the situation, making the event into an uncontrollable situation, seriously affecting social stability and public security. Second, big data facilitates terrorist activities. More and more terrorist organizations abroad through the network remote control command personnel in violent attacks, post training video and scenes of the hostages, promote religious extremism, and even the implementation of network attack, bow | social panic. Again, the virtualization of the data network brings a sense of security to the criminals. Hiding behind the data, it is easier for them to escape the law and the crackdown, allowing them to indulge their behavior with impunity.

5. Big Data Strategies for National Security Around the World

5.1. USA

At present, countries around the world are using big data to improve their national governance and strategic capabilities and seize the commanding heights of international competition in the new era. It has become a global consensus to elevate big data as a national strategy to ensure national

security.

The US government was the first to make a strategic response to the technological revolution of big data, using big data to improve national governance and national competitive advantage. So far, the US government has carried out three rounds of policy actions on big data. The first round was in March 2012, when the White House released the Big Data Research and Development Plan and established the Senior Steering Group on Big Data. The plan has two objectives: first, to transform traditional national governance methods and systems with big data technology, and second, to form new types and sectors of economic growth. (Lang Yangqin, & Kong Lihua. 2012)

The positive use of big data in the field of national strategic focus on breakthrough, including innovation of science and technology, education system, environmental protection, engineering technology, homeland security, biological medicine, and concrete plan involves the national science foundation, national institutes of health, the defense department, the department of energy, the defense advanced research, geological survey and other six federal departments and agencies. (Lang Yangqin, & Kong Lihua. 2012). And set up new big data courses in Stanford, Berkeley and other universities to reserve "data scientists" for the era of big data.

The second round was in November 2013, when the White House launched the "Data to Knowledge to Action" plan, which further detailed the path of using big Data to transform national governance, promote cutting-edge innovation and boost economic growth. (http://www.chinanews.com.cn /cj/2015/06-08/7328863.shtml). This is an important step in the TRANSFORMATION of the US towards digital governance, digital economy, digital city and digital national defense. The DEFENSE Advanced Projects Agency (DARPA), the National Institutes of Health (NIH), the National Science Foundation (NSF), and the Department of Energy are launching their own big data innovation initiatives.

The third round was in May 2014, when the OFFICE of the President of the United States submitted the policy report big Data: Seizing Opportunities and Maintaining Value, emphasizing the close cooperation between the government and the private sector to maximize the use of big data to promote growth and interests and reduce risks. Along with these strategic plans, the U.S. government has launched the Open Data Initiative, releasing government data in 50 categories, including health, energy, climate, education, economy, public safety and global development, to facilitate the development and innovation of the business sector.(CAI Jingxuan, & Huang Ruhua. 2017)

In 2021, the US Congress will introduce a series of bills aimed at ensuring America's scientific and technological advantages, such as the American Innovation and Competition Act, which will invest hundreds of billions of dollars to develop 5G, artificial intelligence and other new technologies. (Sun haolin, & Cheng Ruyan. (2021)). These technologies are based on data and algorithms, which are actually "fed" by data. In addition, the US has strengthened its control over US-listed companies through the Foreign Company Accountability Act and obtained a large amount of data from Chinese companies in the name of censorship. In the face of the grim situation, China has also stepped up its defense, passing legislation to close data loopholes and strictly censoring Internet companies listed in the United States. A battle is under way over data.(Ma gengxin, Zheng Yinglong, & Cheng Le. 2020)

5.2. Europe

The European Union is pushing forward the Strategic Plan for Data Value Chains, which aims to transform traditional governance models with big data in an attempt to significantly reduce costs in the public sector and boost economic growth and job creation. In September 2012, the EU further published the strategic plan "Unlocking the Potential of Cloud Computing Services in Europe" and submitted the proposal "Cloud Computing Development Strategy and three Key Actions" to the European Council and the European Parliament. (Zhang Zhiqin. 2013)The strategy aims to build the EU into a leading economy in cloud computing services over a two-year period, creating a foundation for the EU's "cloud take-off" from 2014 to 2020, and allowing the big data technology revolution to permeate all sectors of the economy and society.By 2020, big data technology will create A GDP of 957 billion euros for the EU and increase the number of jobs by 3.8 million.

The UK has also made great plans to transform the national governance system by taking advantage of the big data revolution. In 2013, the British government issued the Strategic Plan for the Development of UK Data Capability, aiming to use data to generate business value and boost economic growth. It promised to open core databases in transport, weather and healthcare by 2015 and establish the world's first "Open Data Institute". (Great Britain. Department for Business, Innovation and Skills (BIS). 2013). According to the study, the UK government could save about 33 billion pounds a year in administrative costs through the efficient use of big data technology, equivalent to about 500 pounds a year for every person in the COUNTRY.

5.3. Asia

Japan is actively planning to use big data to transform its national governance system and hedge against economic downside risks. In June 2013, the Abe Cabinet officially announced a new IT strategy, "Declaration of Building a Cutting-edge IT Nation", which aims to build Japan into a society with "the world's highest level of extensive use of information technology". (http://pythontip.applinzi.com/bigdata/post/388). All government information systems will be cloud-based in 2020, reducing operating costs by 30 percent. Japan sees emerging industrial clusters derived from big data and cloud computing as an important way to boost economic growth and optimize national governance.

In 2011, the Korea Institute for Science and Technology Policy officially proposed "Big data Center strategy" and "Building Intel comprehensive database." At the same time, the Ministry of Social affairs in South Korea is making plans to cope with the era of big data. In 2012, the National Science and Technology Commission of South Korea released an important strategic plan on the future development environment of big data. In 2013, under the guidance of president Park Geun-hye's new national development strategy of "creative economy", the Ministry of Science, Ict and Future Planning of South Korea proposed a national big data development plan of "fostering 1,000 enterprises related to big data and cloud computing system" and a number of big data development strategies such as the Fifth National Informatization Basic Plan (2013-2017).(Luo Zichao, & Lv Zhijian. 2014)

5.4. Other Organization

Some international organizations also pay close attention to the development of big data. The United Nations has launched its Global Pulse project, which uses "big data" to accurately predict unemployment rates, spending cuts and disease outbreaks in certain regions to promote Global economic development and public service management. The G8 released the G8 Charter on Open Data, which calls for accelerating data openness and use to build a safer world.

In general, foreign governments' big data policies and measures reflect the following obvious characteristics: First, they issue strategic plans for overall layout. In order to seize the opportunity of big data and enhance the international leading position of the country in the field of big data, the leading countries of big data will promote the development of big data as a national strategy to support, so as to play a positive role of big data in guaranteeing national security. Second, we should focus on the establishment of supporting policies, including talent training, industrial support, financial guarantee, data opening and sharing, so as to build a good ecological environment for the development of big data in China, take the lead in big data competition, and protect national security.

6. China's Strategy: Facing the Challenge of Big Data to National Security

On June 10, 2021, the Standing Committee of the 13th National People's Congress passed the Data Security Law, elevating data security to the height of national security. It clearly stipulates that "the state establishes a data security review system to conduct a national security review of data processing activities that affect or may affect national security. The safety review decision made in accordance with the law shall be final. "

On July 2, Didi was investigated for "preventing national data security risks" and the APP was removed from the market.

On July 10, the Cyberspace Administration of China (CAC) issued a notice soliciting public opinions on a draft revision of the Measures for Cyber Security Review, stipulating that "operators with personal information of more than one million users who want to go public abroad must apply to the Cyberspace Review Office for cyber security review." (http://www.gov.cn/xinwen/2021-06/11/content_5616919.htm)

Landmark events have always been watershed events. These incidents show that the era of savage growth of Internet companies has passed, and the era of data compliance has arrived, which is elevated to the height of national security strategy. Therefore, in the view of national security, China's big data development should get rid of foreign technology dependence, guard against foreign capital control, and guard against ideological paralysis on big data security.

6.1. To Ensure National Security, We Must Get Rid of Big Data Technology Dependence

In the final analysis, big data is supported by Internet technology, and technological control plays a crucial role in the development of big data. Although China's big data construction and development trend is good, it is needless to say that compared with western developed countries, China's Internet technology level, especially the security and prevention and control level of big data platforms, will have an obvious disadvantage in a long period of time. This technical "asymmetry" affects China's big data security to a great extent. The country's critical information infrastructure is faced with great risks and hidden dangers, and the network security prevention and control capacity is weak, which makes it difficult to effectively respond to state-level and organized high-intensity cyber attacks. This is a challenge for countries around the world, and we are certainly no exception.(Li Daisu, & Liu Qiqiang. (2017)). Big data platforms carry massive data resources, including a large number of sensitive resources, which will inevitably become an important target of all kinds of hostile forces including hackers to carry out network attacks on China.

With the development of the Internet into the era of big data, the proportion of information data theft in China's network security incidents is obviously on the rise. There are several reasons for this phenomenon: Firstly, China's network infrastructure, PC terminal, mobile terminal and operating system are all developed and introduced from abroad, and there is a lack of independent "controlling, licensing and technology controlling" manufacturers in China, which makes it difficult to control the Internet in China at the infrastructure level. Second, for big data platform of hardware and software system in our country has yet to realize the independent research and development, many relations to the strategic industry of the national economy of big data server, database is occupied by a handful of countries such as America enterprises, these enterprises long-term market monopoly, as it gave data theft is a difficult to close the back door; Thirdly, according to the statistics of China's Internet security enterprises, software products produced by Microsoft, Google, Apple, Adobe and other major Internet enterprises in the world all have dozens or even hundreds of security loopholes, which seriously threaten the security of big data platform.

Core Internet technologies are our biggest 'lifeline', and being controlled by others is our biggest hidden danger. (Li Daisu, & Liu Qiqiang. (2017)). To deal with this challenge, it is fundamental to adhere to independent innovation and vigorously build an innovative country, the key is to establish and improve the national Internet technology security review mechanism, and the guarantee is to promote the legalization of big data security.

In terms of independent innovation, on the one hand, we should increase the research on big data security and strive to keep pace with the development of the world's Internet advanced countries; On the other hand, it is necessary to speed up the development of a batch of national enterprises in big data application and big data security research that "hold, control brand and control technology", so as to realize the localization of relevant equipment and software as soon as possible.

In the establishment and improvement of the national Internet technology security review mechanism, to give full play to the party since the 18th National Congress of China to set up an independent network information department system advantage, will ensure network security as the network information work of the top priority to grasp. First, sensitive and important big data services and applications should be included in the scope of national cybersecurity review to ensure the security of these big data platforms is absolutely reliable. Second, relevant rules and regulations should be established to reasonably restrict the use of

software and mobile applications involving big data uploading by employees in sensitive and important departments; Third, we should monitor all kinds of cloud storage services in a timely manner to guard against cloud leaks in light of the new situation of Internet applications shifting from local storage to cloud storage. For big data services provided by Western companies in China, cyber security checks should be more stringent and data, especially sensitive data, should be strictly prevented from flowing out of the country.

6.2. National Ownership of Big Data Will Be Further Highlighted

Another major challenge facing China's big data security is that most of the existing big data enterprises are foreign-owned or have foreign-funded background, and national enterprises, especially state-owned enterprises, are scarce. State-owned capital not only does not occupy the dominant position in this field, but also lacks the necessary control. The danger of this situation is that foreign companies can easily acquire sensitive data concerning national security and citizens' privacy by analyzing existing data in China. It is worth noting that it is usually easier for foreign high-tech enterprise managers to enter the government and military through the unique "revolving door" system of capitalist countries than private enterprise personnel in other industries, which casts a shadow on China's big data security. Internet companies are in charge of a lot of data related to national interests and security, and they need to ensure the security of such data. Enterprises should attach importance to data security. "If companies have problems with data protection and security, it will have a negative impact on their reputation." At the same time, the national cyberspace administration should strengthen and improve the guidance and management of non-public big data enterprises, requiring them to ensure the security of big data on the one hand, and enhance the social responsibility of enterprises on the other hand, and take the initiative to provide data support for relevant national economic decisions.

From the perspective of ensuring big data security, the NATIONAL Security Commission of the CPC Central Committee should incorporate the review of national big data industrial policies into its responsibilities. The government should properly discriminate between big data enterprises of different ownership when formulating this policy, and ensure that the control of big data is firmly in its own hands.

For state-owned big data enterprises, the experience of "Guiyang model" and "Shanghai model" has their own merits, which can be used for reference by provinces (cities) and autonomous regions. In the shareholding structure of Guiyang Big Data Exchange, the first big data trading platform in The country, Guizhou Sunshine Equity Exchange (on behalf of the State-owned Assets Supervision and Administration Commission of Guizhou Province) invested 51% and gained absolute control of the company. Shanghai is an area where traditional state-owned capital is developed. The "Shanghai model" of big data trading platforms is reflected in the strong alliance between local state-owned enterprises Shanghai Credit Investment And Shanghai Sheneng And state-owned enterprises China Telecom and China Unicom in the telecommunications industry to absolutely control the Shanghai Big data Trading center. The advantages of these two modes are as follows: First, the absolute holding of state-owned capital reflects the government's control over local big data security; Second, to leave certain equity space for other ownership economies, in line with the spirit of the central government to actively promote mixed ownership reform.

The situation of non-public big data enterprises is more complicated than that of non-public enterprises in other industries. Generally speaking, the shareholding structure of non-public enterprises is relatively simple, and private enterprises in most industries do not need the complicated shareholding structure such as VIE and foreign capital holding positions. However, Baidu, Alibaba and Tencent, the "big three" Chinese Internet companies with massive data resources and strong technological advantages, are all companies with complex equity structures, which brings great difficulty to the national big data security supervision. The first way to solve this problem is to strengthen cooperation between government and enterprises. Taking Taobao as an example, some scholars pointed out that TCPI, which is based on Taobao's big data, is "more sensitive and more advanced" than the official consumer price index (CPI) released by the National Bureau of Statistics. Therefore, the government can take the data of private enterprises as an important reference when making macroeconomic policies in the future. Second, we will implement a "negative list" management system for big data through legislative and administrative means. Not only the national level such as economy, finance, defense, industrial security sensitive big data should not be privately operated enterprises, especially large data with a foreign background of big enterprise master data, the big data about citizen health class, unfavorable also into the other hand, beware of some information power and genetic research power to master these data, There is no smoke to our country but it is very harmful gene war.

Those stored in the enterprise servers, the cloud, big data can't be the "private capital" of the enterprise, it is impossible to remain at the basic of the "open" or "folk" scattered state, its acquisition, processing, use, classification, trading, protection must be standardized and legalized track, was relatively vague data ownership will tilt to the national interests and public interests.

Cross-border flow of big data will become the focus of compliance management in the future

The cross-border flow of big data directly affects the nerve of national security, and is the most sensitive and complex part of data security. At present, the EU has built up a high wall on cross-border data flows through the General Data Protection Regulation, and also set aside four channels: "Adequate protection resolution", "standard contractual provisions", "binding enterprise rules" and "specific circumstances". (Wang Haochen. 2018). With the "Cloud Act" as the backbone, the United States has established a cross-border data flow rule system with "more in and less out". At the same time, the United States, Mexico and Canada Agreement has established a regional data free flow system. China has always adhered to the rigid principles of "local storage" and "security assessment" in data flow across borders to coordinate security and development. It can be said that in front of the huge dividend of the data economy, all countries have not blocked the road. "Security and control" is the common goal of all countries, but the scale of grasp is different.

(1) Establish the balance concept of big data flow

Although the cross-border flow of big data may bring about potential national security risks, countries still hope to realize the free flow of data to the greatest extent on the premise that

the risks can be controlled because the data flow can bring huge economic benefits. For example, the United States adheres to the idea of strengthening international cooperation to promote the free flow of data in the regulation of cross-border data flow, and includes provisions on cross-border data flow in bilateral or multilateral agreements, which has become the main path for the United States to implement the above ideas. There are legitimate reasons for globalization to allow data to cross borders, and an outright ban on cross-border data transfer is neither practical nor operational. China should emphasize the establishment of clear regulations based on rational grading of data to improve the business environment.

(2) Improve the big data legal system to ensure that there are laws for data flow

Through the investigation of information data protection legislation in other countries, it can be found that the legislative track of each country basically follows the basic path of protection of basic law rights → protection of civil law framework → protection of special law → protection of specific rights in different fields.

From the current legislative status of Our country, the Constitution does not stipulate the right of individual information and data; In "civil code" for personal privacy, personal information, state institutions and medical institutions of the confidentiality obligations have been reflected, the network safety "data exit safety management requirements, the personal information protection act and the data security law has also been included in the main work of the standing committee of the National People's Congress next arrangement. Generally speaking, China has realized the importance of information data protection and carried out a series of legislative activities, but the coverage of relevant laws and regulations is not enough, the provision of provisions is not operational, the connection between laws is not close, China's legislation system for information data protection is still incomplete. For example, there is no clear constitutional basis for the rights of personal information data in China. In terms of special laws, regulations on personal information data are still in principle, and specific regulations on collection, transmission, storage, use, deletion, destruction, sharing and cross-border are insufficient.

Specifically, in terms of cross-border flow of big data (mainly refers to cross-border outflow), first of all, the collection, transmission and storage of big data should be regulated from the source, the legality of cross-border outflow data should be ensured, and the rights and responsibilities of data controllers and data subjects should be clarified. Secondly, we should do a good job in the classification of big data, clarify the classification elements of big data, grade discrimination; Third, different circulation approvals should be set up for cross-border outflow of different levels of big data to clarify which data can be exported. How do I leave the country? If there is a safety assessment involved, who will assess it? What are the evaluation criteria? A sound supervision and protection mechanism should be established for big data involving national security and public rights and interests. Finally, the cross-border outflow operation of big data should be standardized to solve the problem of "who applies? Who's approval? Who supervises? Who will be punished?" To ensure that data is operable and regulated across borders.

(3) Identify departments in charge of big data and implement big data management subjects

In practice, all countries have set up independent departments to be responsible for the implementation of information data, with independent authority of management, supervision and punishment, or special information data protection agencies by the supervision departments in various segments. From a worldwide perspective, there are two modes of setting up information data protection supervision departments at present:

The first is the unified supervision model represented by the European Union, that is, to establish a special supervision department for information data protection to implement centralized supervision over all information data protection. The European Union, for example, has created the European Data Protection Board as an independent regulator. In Hong Kong, the Office of the Privacy Commissioner for Personal Data (PCPD) has been set up to oversee the implementation of the Personal Data (Privacy) Ordinance.

The second is the separate supervision mode represented by the United States, that is, no special supervision department of information and data protection is set up, but each functional department supervises according to their respective authority. For example, in the financial field of the United States, the Consumer Financial Protection Bureau (CFPB) is responsible for the supervision of GLBA, FACTA, CFPA, etc., and the Federal Trade Commission and the Federal Bank also participate in the supervision when it comes to corresponding fields.

But at present, there is a tendency of compatibility and inclusiveness between the two supervision modes. A recent proposal in the United States suggests the enactment of the Data Protection Act and the establishment of a special Federal Data Protection Agency (DPA) as an independent enforcement agency responsible for protecting personal privacy and limiting "the collection, disclosure, In addition to setting up the UK Information Commissioner to conduct unified supervision on information and data protection, the UK Financial Services Authority is also responsible for joint supervision in the financial field.

Therefore, it is urgent for China to define special administrative subjects of data protection supervision from the legal level and exercise the overall management responsibility for data protection and circulation. While in the financial field, should be defined in the law by the existing financial supervision and regulation department, to perform for the financial sector big data protection and circulation special management responsibility, the main reason is that financial regulators to the financial business, and data of cross-border scenarios as well as the more familiar, thus more conducive to ensure the effective implementation of the relevant laws and regulations as well as the system.

(4). Establish standards and a white list system for countries receiving cross-border data to improve cross-border efficiency of big data

China and the United States are the two largest countries in the world in terms of digital industry scale, and China's digital industry scale in e-commerce and fin-tech segments is the largest in the world. Cross-border big data will be an important way for China to become the world's data center, so it cannot meet the requirements of timeliness to evaluate all cross-border big data one by one. , cross-border recipient countries usually adopt data "white list" mode, namely after data flow of exporter assessment, confirm specific countries and regions to provide the protection level of "full", in its list of "white list" to "white list" of countries and regions as the

data in the receiving country, and transfer of sensitivity of big data, can flow freely, In order to meet the data cross-border efficiency requirements. In addition, the United States has established data flow certification through bilateral and multilateral agreements to ensure the timeliness of data crossing borders. However, if the data receiving country is not included in China's "white list" or has not reached data flow certification with China through agreement, the cross-border big data of the country or region shall comply with relevant provisions of laws and regulations and be subject to certain approval. Sensitive big data, or those that may affect China's national security or public interests, should undergo a full security assessment.

(5) Grasp the cross-border jurisdiction of big data and safeguard national data sovereignty

In the process of cross-border data transfer, it is inevitable that there will be cases of breach of contract and infringement, and the possibility of serious threats to China's national security and public interests. The United States has traditionally extended its international enforcement powers through "long-arm jurisdiction", and the European Union has included "long-arm jurisdiction" provisions on data (Article 3 of the GDPR, "geographical scope"). Therefore, from the perspective of safeguarding China's data and protecting the legitimate rights and interests of Chinese enterprises and individuals, China should adhere to the grasp of judicial jurisdiction. We can learn from the legislation of the new Securities Law to add the "long-arm jurisdiction" clause for cross-border data.

7. Conclusion

In the era of big data, the definition of security is constantly evolving and deepening. Big data security has become a core element of national security. The traditional thinking and model of national security governance are relatively less adaptable in the era of big data, and big data is promoting new changes in national security governance. In the process of reform, all countries hope to seize the opportunity and use big data as a means and tool to build a more secure international and domestic environment. However, there is a long way to go for national security governance in the era of big data, and it requires patience and wisdom to enhance awareness of big data and build capacity.

Today, human society is moving irreversibly towards an informativeness and digitized big data society. As a new focus of the game between great powers, big data is the strategic commanding point of a new round of national scientific and technological competition. A country's data sovereignty in cyberspace has become an important part of safeguarding national security. Standing at the new starting point of the new era of big data, it is of great strategic significance to think and seek new methods of national security in the future.

References

[1] Seagate Technology and IDC draw data together in the future idc released "Data Age 2025" to indicate the trend of data development,2025 global data will climb to 163ZB. Digital Photography (6), 1.

[2] viktor mayer-schonberger, KennethCukier, viktor mayer-schonberger, KennethCukier, mayer-schonberger, & cukier, et al. (2013). Big Data Era: Great Changes in life, work and thinking. Zhejiang People's Publishing House.

[3] Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, S. (2015). Application of big data for national security: a practitioner's guide to emerging technologies. Butterworth-Heinemann.

[4] Leffler, M. P. (1990). National security. The Journal of American History, 77(1), 143-152.

[5] EB/OL].[2021-06-13].http://www.gov.cn/xinwen/2021-06/11/con-tent_5616919.htm.

[6] Slouka. (1999). The Great Conflict. Jiangxi Education Press.

[7] CAI Yali. (1997). Digital Whirlwind from the other side of the Ocean -- Negroponte and Digital Survival. Electronic Outlook and Decision (02), 51-52.

[8] Lian Jiajian. (2015). Analysis of computer network information security problems and prevention. Information Systems Engineering (10), 1.

[9] He zhilin. (2019). Research on computer information security and protection based on big data. Communications World, 26(1), 2.

[10] Yu Zhigang, & Li Yuangrain. (2014). Thoughts on data crime sanctions in the era of big data. Social Sciences in China (10), 21.

[11] De Tuzos, & Zhou Changzhong. (1998). Future society. Shanghai Translation Publishing House.

[12] Tang Zhefeng. (2015). Negative Impact of Network participation on democratization. Journal of Shanghai University of Political Science and Law: Essays on Rule of Law, 30(2), 7.

[13] Wriston, W. B. (1997). Bits, bytes, and diplomacy. Foreign Aff., 76, 172.

[14] https://en.wikipedia.org/wiki/Big_data

[15] http://intl.ce.cn/specials/zxgjzh/201408/27/t20140827_3436534.shtml

[16] https://www.chinairn.com/report/20220120/102946738.html

[17] http://world.people.com.cn/n/2015/0531/c1002-27080992.html

[18] Tang Ronghao. (2013). The Intelligence Supervision mechanism of the United States from the Prism Gate Incident. Journal of Intelligence (09), 6-10.

[19] https://en.wikipedia.org/wiki/Tunisian_Revolution

[20] https://foreignpolicy.com/2011/01/15/the-first-twitter-revolution-2/

[21] https://en.wikipedia.org/wiki/July_2009_%C3%9Cr%C3%BCmqi_riots

[22] https://en.wikipedia.org/wiki/2013_Tiananmen_Square_attack

[23] https://en.wikipedia.org/wiki/2014_Kunming_attack

[24] Yang Jing, Kang Qi, & Li Zhe. (2021). Analysis and enlightenment of the Federal Data Strategy and 2020 Action Plan of the United States. (2020-9), 150-156.

[25] Lang Yangqin, & Kong Lihua. (2012). "Big Data Research and Development Plan" released in the United States. Journal of Information Science and Technology, 3(2), 5.

[26] http://www.chinanews.com.cn/cj/2015/06-08/7328863.shtml

[27] CAI Jingxuan, & Huang Ruhua. (2017). The policy and regulation guarantee of us government data opening and its enlightenment to China. Books and information.

[28] Sun haolin, & Cheng Ruyan. (2021). The American Innovation and Competition Act for Fiscal Year 2021 will significantly increase R&D investment in the United States. Science and Technology China (10), 4.

[29] Ma gengxin, Zheng Yinglong, & Cheng Le. (2020). The American "Security View" of the Foreign Corporation Accountability Act and China's countermeasures. Business Economics and Management (9), 10.

[30] Zhang Zhiqin. (2013). Cloud Computing Strategy and Action measures of The European Union: Fully Releasing the potential of Cloud computing services in Europe. Global outlook on science and technology economy.

[31] Great Britain. Department for Business, Innovation and Skills (BIS). (2013). Seizing the data opportunity: a strategy for UK data capability.

[32] http://pythontip.applinzi.com/bigdata/post/388

[33] Luo Zichao, & Lv Zhijian. (2014). Development and application analysis of Big data in South Korea. Global S&T Economic Outlook, 29(3), 5.

[34] Li Daisu, & Liu Qiqiang. (2017). "Xi" Language: Talk about Internet Core Technology. Guangdong Science and Technology, 26(004), 51-51.

[35] Wang Haochen. (2018). The influence and enlightenment of the European Union's General Data Protection Regulation on the development of artificial intelligence. China Economic and Trade Guide (17), 3.