

From digital knowledge into digital sovereignty, data protection in China as a model



Said Gherbi*

Research team of Public policy, Faculty of Political Sciences
and International Relations, University of Algiers3

saidsaad854@gmail.com

Ismahan Tamghart

University of Algiers3

saidjismahan@gmail.com

Date of submission: 18/09/2024 Date of acceptance: 25/10/2024 Date of publication: 17/12/2024



Abstract:

The concept of sovereignty has evolved since its inception by the French thinker John Bodin, from geographical sovereignty, which was manifested after the Treaty of Westphalia in 1648 in demarcating the borders between European countries, to digital sovereignty, represented by the attempt of major countries to protect their data from hacking and their cyber security from threat, especially all their commercial movement The economic and even military sectors are now controlled by computers, chips, and websites that are threatened by piracy.

China is one of the world's leading countries in protecting its digital data, achieving great numbers in the path of digital sovereignty.

Key words: Digital literacy, digital sovereignty, data protection, China, cyber security.

Introduction

The standards of international competition between major countries change in every period. In the early eras, the conflict of kingdoms and empires was over the expansion of agricultural lands and areas of military influence, then some wealth such as coal, oil, gas and minerals such as gold and uranium were transferred to the discovery of the Internet, which is considered an important event in the international arena, and in this way The criteria for this competition changed

* Corresponding Author

according to this great discovery. In addition to the possession of natural resources, which remained a basic criterion such as oil, gas and precious metals, digital knowledge products entered to intensify the struggle over technological, economic and military leadership.

This discovery in the late twentieth century led to a massive technological revolution, which resulted in the entering of digitization in all-important fields, such as saving data in computers and processing it automatically, which forced all countries to enter the world of digital transformation, thus transforming knowledge from the traditional concept to the modern concept, which is called knowledge.

Digital technology is considered the most important result of the technological revolution. Thus, knowledge was preserved and classified in a way that makes the reader and researcher not find it difficult to search for any topic that concerns him using modern technology. Thus, knowledge became available in electronic chips and computers whose memory accommodates what libraries were unable to carry previously.

However, the issue of digitization has posed a real threat to countries that are trying to protect their geographical sovereignty, so their interest has shifted to protecting their digital sovereignty by waging wars of a different ways, such as piracy, cybercrimes, and protecting cyber security, unlike traditional wars over land and wealth. This is a natural outcome of putting all the state's secrets and data in the Cyberspace is difficult to protect and monitor, especially in developing countries that import their technological means from outside.

From the above, the problem of the study can be formulated as follows:

- How does digital knowledge pose the problem of digital sovereignty? How does the Chinese model express this problem?

For research in this topic, we use two main approaches:

- The descriptive approach: to extract the specifications of the phenomenon under study and we used it in searching for the specifications of digital knowledge and digital sovereignty, as well as digital transformation in China.
- The historical approach: it uses to explain the development of digital knowledge and digital sovereignty on the one hand, and to know the great digital transformation that China has witnessed in this field.
- Case study approach: This study includes tracking the Chinese case in protecting its digital data.

In order to explain the study in detail, we asked the following sub-questions:

- What is the concept of digital knowledge, and what are its most important applications?

- What is digital sovereignty, and how can it be achieved?

What are the most important aspects of the Chinese experience in protecting its data and achieving its digital sovereignty?

Based on the previous questions of the study, the following hypotheses were formulated:

Controlling digital knowledge affects positively on the state's digital sovereignty.

China is considered one of the first countries in the world to achieve digital sovereignty through the special programs it follows.

- The digital field enters the ranking of countries in terms of power and control, along with the economic and military fields.

The objectives of the research are:

- Knowing the effects of digital knowledge on digital sovereignty.

- Discussing the most important structures and programs for achieving digital sovereignty.

- Projecting on the pioneering Chinese experience in the field of data protection and cyber security, and coming up with useful recommendations.

The first season: digital knowledge and digital sovereignty, a conceptual study

In this season we deal with the conceptual part of the topic, in which we will study the definition and development of digital knowledge as an essential part of understanding the subject of technological development leading to the second part of it, which is digital sovereignty and its emergence and the most important points in it, especially those related to data protection and cyber-security and the concepts according to them.

First: Digital Knowledge and Digital Transformation

Knowledge is one of the most essential aspects of the technological revolution that the world knew at the end of the twentieth century, with which the transition to other concepts related to information and communication technologies to reach to the digital sovereignty over the electronic facilities and programs of countries.

This topic discusses the concept of term digital knowledge and the most important concepts associated with it, which is digital transformation, to know about its definition and determinants as an important point to the topic of data protection.

1. The concept of digital knowledge

The massive spread of the Internet has led to the emergence of the concept of e-commerce, which it has facilitated the transactions of businesspersons in addition to constricting of time, effort and cost. E-commerce is not limited to this only, but has opened its scope to companies, institutions, individuals and governments, and from here signalize the digitization and the interest in it has increased even more, and it has become a significant matter in the overall prevailing economic processes in recent times¹.

According to a report by the National Telecommunications and Information Administration (NTIA), the number of users of digital technology in America doubled in 2015, reaching 75% compared to the year 2000, when the percentage reached 44%.²

On the other aspect, the important point in modern growth theory is that the generated knowledge from digital transformation leads growth, because ideas can be renewed, reused, and combined without restriction, and that increasing returns drive economic growth. This theory also helps to understand the continuous and renewed transformation of the economy. Resource-based to a knowledge-based economy.³

Although the main entrance to digital knowledge was the economy since it began in the field of electronic commerce, it extended to include all other fields of life. Technology and its digital developments intervened in the political, social, cultural, military, and environmental fields, the most important reasons are:

- Digitization allows a kind of speed in processing and classifying data.
- It created a kind of competition between all aspects of life, and which one serves the other to achieve development and well-being in all countries of the world.
- The increase in the quantity of informations, data and informations in all sectors, with the large increase in humanity, makes benefiting from digitization necessary for this.

2. Digital transformation, the concept and determinants of success:

A - The concept of digital transformation: It means the change associated with the application of digital technology in all different social aspects.⁴

It also means redesigning business in order to benefit to the maximum possible extent from the digital reality, and one of its meanings is that it is the process of applying digital technologies to renew the way business is done and to create and present new value.⁵

From all of these definitions, it can be said that digital transformation is the use of digital knowledge in order to improve the quality of business, projects, and services, through good management of technological and digital mechanisms.

B- Determinants of digital transformation success:

The digital transformation process takes a long period, so it is usually implemented in several stages by developing a future vision for digital transformation based on encouraging innovation and employing digital and technological capabilities. Among the most important determinants of the success of digital transformation as I mentioned are the following:⁶

1- Improving the state's readiness and developing the necessary technological infrastructure by directing and allocating local investments and attracting foreign money in the field of information and communications technology sector.

2- Expanding use of the Internet by delivering services to all regions inside the country, ensuring continuous maintenance and development of networks, in addition to reducing the cost of communication so that it becomes available to everyone.

3- Put a set of policies according to which the general national framework for the digital transformation process is drawn, and clarify the vision and principles on which these policies are depended on it, the goals to be achieved and the returns from them, and the entities responsible for implementing and monitoring them.

4- Institutions adopt their own digital transformation vision and strategy that relates to the government's strategic vision and it must include all public and private institutions within the country.

5- Interesting to applying the open data model, which helps in participation and cooperation between the government, citizens, and other concerned parties.

6- An inventory of services that can be developed and transformed into digital services, while working to implement the digital identity system by developing a plan to collect accurate data on citizens.

7- Developing legislative and regulatory frameworks commensurate with the nature of the digital economy.

8- Spreading awareness of the importance of the digital transformation process and its development benefits through awareness-raising operations in the written, visual and audio media.

9- Encouraging citizens, civil society organizations, and the private sector to submit ideas and proposals to the government through available technological platforms, which helps citizens in decision-making.

10- Eradicate financial and digital illiteracy while working to spread financial inclusion within the country and build consumer confidence in digital financial services, and to meet the needs of users.

Second: The concept of digital sovereignty and its dimensions

In this second point we deal with the concept of digital sovereignty and its main fields that countries rely on to achieve this, which has become a new standard by which large countries are measured, especially with regard to protecting their data and cyber security.

1. The concept of digital sovereignty

Because the Internet transcends the sovereignty of traditional states, the term digital sovereignty emerged, which means that electronic communications networks transcend national borders.⁷

The Internet and digital technology were initially closely linked to state security. Researches and discoveries in this field were affiliated with the state and supervised by intelligence and security services. With the end of the Cold War, the way was opened for engineers and private companies to work in this field, and what accompanied this was the conviction of the political and economic elites in many countries of the world could rely on digital technology to find solutions too many economic and social problems.

It should be noted here that since the end of the Cold War, American hegemony over the Internet has been embodied, along with the adoption by societies of a free view of the Internet, by embodying the standards of American liberal democracy, including freedom of expression, access to information, and market capitalism, thus consecrating the absolute hegemony of the United States over all digital information in all countries of the world. This has led to the emergence a new approach based on digital sovereignty, and call for equal participation in the international governance of cyberspace, while calling for countries not to engage in the pursuit of cyber hegemony, which means not interfering cyber in the internal affairs of other countries and harming their internal security.⁸

Therefore, digital sovereignty means the state's control over the digital space and various internet data within its geographical borders with programs and physical structures protect it from hacking, piracy and electronic attacks.

In contrast, sovereignty its violation by others means hacking its digital data and publishing its secrets and various data with the aim of harming it or controlling its citizens or blackmailing its officials.

Dimensions of Digital Sovereignty².

The dimensions of digital sovereignty extend to all vital fields of the state and society, such as the military, political, social and humanitarian fields. All of these areas together aim to achieve a digital system with strong sovereignty that achieves immunity against cyber threats. These dimensions can be explained as follows

:A. Military Dimension

This important dimension appears in maintaining the ability of various military units to communicate via wireless military networks, which allows for the exchange and flow of information and orders, which is the idea for which internal networks were created and developed into what is now known as the Internet. However, it also represents a point of weakness, especially if it is not well secured from hacking. This may lead to the destruction of military databases, or the severing of communication between the command and the various units, in addition to the possibility of controlling some weapons and getting them out of control (drones, guided missiles, satellites). The Stuxnet virus is considered the beginning of the use of cyber power to destroy the physical structure (it is a virus that attacked Iranian centrifuge computers)

:B. The economic dimension

There is no doubt, now that the Internet has entered all commercial and financial transactions related to banks and banking, and the matter is increasingly widespread regarding money transfer operations between countries, continents and regions within the same country. In addition to this, the control of the World Wide Web over many factories, airports and important economic facilities, so any breach of these sensitive economic systems costs countries, companies and institutions huge sums to compensate for their losses. Hence the necessity of achieving digital sovereignty through the economic dimension and protecting it from cyber threats

: C. The political dimension

Cyberspace has become a fertile ground for electoral propaganda campaigns and an arena for diplomatic battles between countries, especially after every electronic breach between one country and another. The Russian cyber intervention in the US presidential elections is considered the most important manifestation of the breach of digital sovereignty and the resulting trial of US President Donald Trump, the stages of which are still ongoing to this day

Therefore, all the dimensions mentioned above in which the digital sovereignty of countries and organizations appears have a direct impact on the political dimension because it is the most important in the strength of countries and the increase of their influence

D: The social dimension:

The world's Internet users exceed 4 billion people, 2.6 billion of whom use social media sites. The world has become as if it is in one room, to the point that it does not take seconds for the news to reach every part of the world. However, it poses a direct threat to the ethics, customs and religions of societies, which have become unsacred as they were before. Therefore, achieving digital sovereignty from this aspect requires an important regulatory authority to protect the data of individuals and public and private institutions.⁹

Third: The problems of digital sovereignty posed by digitization

In this point, we will try to talk about the depth of the relationship between digitization and digital sovereignty. Digitization is considered an important field for the vital fields that countries depend on, such as the economy, politics, and armament. On the other hand, it is a threat to digital sovereignty, especially for developing and weak countries. This is evident in the following two points

The Internet and the attack on digital sovereignty:1.

The information revolution or what is called the technological boom, constituted a qualitative leap. The world has become a small village. Through new communication networks, media, and satellites, it has led to the dominance of industrialized and powerful countries over information sources and their industry, which has led to their control over developing countries, led by the United States of America, according to their interests and strategic goals

Thus, these companies were able to penetrate the national sovereignty of countries by imposing their modern and high-level technologies and electronic marketing, and have become an influential player in international economic relations

Thus, the concept of information security came in several definitions, the most important of which are: "The science that studies theories and strategies for providing protection for information from the risks that threaten it and from the activities that attack it." From a technical standpoint, it can be defined as "the means, tools and procedures that must be provided to ensure the protection of information from internal and external risks." Therefore, developing countries and nation states are trying to put an end to foreign control over modern means of communication such as the Internet and to rely on themselves in the methods of developing software and machines aimed at developing society.¹⁰

It is clear from the above that the direct relationship between digitization and its access to all countries, given that it is necessary for the activity of economic, social and political life, makes it vulnerable to exploitation by large companies, especially those that manufacture software and modern social networking sites, whose owners have become at the top of the list of the richest people in the world.

2. Modern technologies and interference in the sovereignty of countries:

Michel Alliot-Marie describes the Internet as a place for all freedoms, and unfortunately also for deviation and crime on the path to growth.¹¹

This is an accurate expression of the Internet, which has become available to all peoples of the earth, man expresses his innermost feelings and learns about everything around him, but at the same time it has become a carrier of many factors that destroy human and moral values, and with it, threatening countries has become easy, because all their data and databases have become available and digital after they were traditional and secret.

If the sovereignty of the state is applied to a specific people, within specific borders and under a single political system, economic vision and military doctrine, the Internet creates a virtual group within social networks that have no national affiliation.¹²

This threat requires the nation-state in the Westphalia sense to return to its former glory in protecting its geographical and digital sovereignty, and to return to spreading the national spirit by invoking national symbols and preserving customs, traditions and religious rituals using information and communication technologies, which must be controlled by states away from global companies that negatively influence peoples' beliefs and religions.

The second topic: Chinese Digital Data, Between Protection and Sovereignty

This topic studies the case of digital transformation in China, which is in big competition with leading countries in this field regarding digital sovereignty, whether in terms of the modern technologies accompanying this transformation or the huge budgets allocated for this purpose every year.

The study will discuss the potential of digital transformation in China on the one aspect, then mention the most important points of digital sovereignty, methods of data protection and obstacles facing this transformation on the other aspect, and we will touch on the problem of the study in clarifying how digitization served digital sovereignty in China.

First: Digital transformation in China

There is no doubt that the process of digital transformation in any country is a very complex and difficult matter, due to its great importance in maintaining the work of vital areas in the country at full capacity, and preventing the citizen from feeling a decline or stopping serving his vital interests. China is one of the leading countries in this field and the first to it with a strong and clear strategy, which we can explain as follows:

1. Chinese cyber security technologies:

There are three technologies that have the greatest contribution to China's ability to shape the Chinese cyberspace in the present and future: semiconductors, quantity computing and artificial intelligence.

A. Semiconductors: In the past, China tried and failed to build a national industry of semiconductors, and these pieces are integrated circuits or "microchips" that we find in every technological device. In 2016, China imported about \$228 billion worth of these parts-more than it spent on oil imports-and imports account for 90 percent of Chinese consumption.

In 2015, China issued guidelines aimed at getting Chinese companies to produce 70 percent of the microchips used by Chinese industries by 2025.

Since then, Chinese authorities have provided support to domestic and foreign companies that move their operations to China, and encouraged domestic consumers to buy exclusively from Chinese suppliers. The government has pledged \$150 billion over the next 10 years to ensure its ability to design and manufacture advanced microprocessors. It has also acquired foreign technologies. According to the Rhodium Group, a

research firm, Chinese companies made 27 bids for U.S. semiconductor companies between 2013 and 2016, for a total of \$37 billion.

B. Quantity computing: which uses the laws of quantity mechanics, i.e. the ability of a quantity bit or "cubit" to perform a number of calculations at the same time, to solve specific and complex problems that classical computers cannot solve.

Developments in this field may allow the Chinese intelligence service to create large, encrypted communication stations that can penetrate known encryptions. Known quantum computers can also bring significant economic benefits through remanufacturing, data analysis, and drug development processes.

In 2016, China launched the world's first satellite that can communicate via channels secured by quantum encryption, and built the world's longest quantum communications cable, which connects Beijing and Shanghai.

C. Artificial intelligence: In addition to its investments in semiconductor research and quantum computing, China's ambitious plans in the field of artificial intelligence are what greatly worries Western countries.

At the AI conference in America, former Google CEO Eric Schmidt said of the Chinese: "By 2020 they will have caught up, by 2025 they will have overtaken us, and by 2030 they will have dominated the AI industry."

Automated Drones: China wants to become a "global AI innovation hub" by 2030. The plan also includes guidelines for central ministries and regional governments on how to invest in advancing progress through specific areas of research and development

China has chosen Baidu, Tencent, Ali-baba and iFLYTEK as its national champions in AI, identifying these networks with the goal of developing systems that can guide self-driving cars, diagnose diseases, act as intelligent voice guides and manage smart cities, urban spaces that use a wide array of sensors to harvest data on how people live

According to some of the country's leaders, China's current position in the current global division of labor looks like a trap, with foreign companies reaping profits from intellectual property while Chinese companies benefit from the thin margins they get from manufacturing and assembling physical products

China had been absent from the depth of discussions surrounding 3G and 4G mobile network technologies, but that changed in 2016, when

Huawei sent twice as many representatives as any other company to the Vienna global meeting that defined the advantages of the upcoming 5G mobile network.¹³

From the above, it can be said that the digital transformation in China has witnessed a major qualitative leap in terms of digital technology programs and the major companies accompanying them, which gives it priority to excel in the main areas that digital transformation has a positive impact on, such as the military, economic, .political, and social fields

China's digital data protection strategy2.

For the past fifty years, the United States has been the one driving the growth of the Internet, and from its beginnings as a limited program for the Pentagon to its arrival as a global platform connecting more than half the world's population and tens of billions of devices, the Internet has .been known as an American project

Today, the United States has ceded cyberspace leadership to China, the Chinese President Xi Jinping announced on his plans to transform China into a cyber-superpower.

China allows more of its citizens to connect to the Internet than any other country in the world, but Chinese President Xi Jinping has much .bigger plans

Through domestic regulations, technological innovation, and foreign policy, it appears to be aiming to build a strong cyber defense system, assert its voice in governing the Internet, and nurture more world-class .companies and global leadership in advanced technologies

In 2012, Chinese President Xi Jinping explained the major role the Internet played in his vision for China. Cyber policy was divided among a number of government departments, until Xi announced that he would head what he called a central leadership group for Internet and information security, and that he would lead cyber policy. He established a new agency called the Cyberspace Administration of China, which he tasked with controlling Internet content, overseeing cyber security, and .developing the digital economy

Cyber power is the knot that links four of China's national priorities :together

The first is the Chinese leadership's desire to ensure a harmonious Internet, which means a spider web that guides public opinion, .accompanies economic growth, and supports good governance

The second is China's attempt to reduce its dependence on external suppliers in the field of digital and communications equipment , and hopes to reach world leadership in the field of advanced technologies .such as artificial intelligence, quantum computing, and robotics

The third is the Chinese policymakers, like other world leaders, are concerned that cyber-attacks on government and private networks could disrupt critical services, hurt economic growth, and cause physical destruction. This belief was reinforced in 2013, when Edward Snowden, a former National Security Agency contractor, revealed that U.S. intelligence agencies had violated the privacy of millions of people's data in their possession and transferred to companies in the United States. - Finally, China has advanced the concept of "cyber sovereignty" as an organizing principle for governing the Internet, in direct and clear opposition to U.S. support for an open global Internet. This is what President Xi expressed about cyber sovereignty, which is "the right of every country to choose its own path to cyber development, its method of cyber regulation and the regulation of public policies for the Internet, and to participate in global governance of cyberspace on an equal footing with other countries."¹⁴

Hence, the Chinese digital strategy in protecting its data is characterized by clarity and uniqueness from the United States of America and the Western countries behind it in that it is an internal cyber policy controlled by one party, in addition to its tendency towards self-manufacture of digital equipment internally, which makes it far from penetration and threat by global companies and institutions that control the digital policies of the rest of the world. However, this does not prevent China from being constantly cautious of cyber-attacks launched by individuals, institutions or countries as a tax it always pays in return .for this clear superiority

Second: Principles and threats of international cooperation in digital sovereignty

Despite the enormous potential that China possesses in the digital field, it realizes that we are in a volatile and converging world, volatile in the common interests between countries and poles, and technologically converging with the emergence of social media that influence peoples negatively and positively. Therefore, it proposed, by virtue of its strength, principles for cooperation in this field to protect it, and all

countries of the world are exposed to successive cyber threats, which we will mention in the following two points

The Chinese view of the principles of international cooperation in 1. cyber issues

In the Budapest Conference on Cyber Issues in 2012, China proposed five principles for international cooperation in cyberspace, the first of which was sovereignty, which - according to it - is the right of every country to formulate its policies and laws in light of its history, traditions, culture, language and customs

By linking this definition of sovereignty to cyberspace and the Internet, it went on to say that: "Since the Internet falls under the authority of the state's sovereignty, everyone within the territory of that state is obligated to comply with its laws and regulations." As the Chinese President said in the Yuzhen Declaration at the first World Internet Conference in 2014: "We must respect the rights of each country to develop, use and manage the Internet, and refrain from exploiting technological resources and power to violate the digital sovereignty of other countries."¹⁵

Therefore, we find that China has come a long way in establishing its digital sovereignty. In 2017, it issued a special law on cyber security "in order to control and regulate cyberspace to achieve the advantage of protecting society and the state." From this, the concept of cyber security refers to the measures and means taken to keep electronic information safe from damage and theft. Cyber security also tends to protect everything from personal information to complex government systems.¹⁶ This tightening of concepts and definitions by China is undoubtedly not pleasing to many countries that want to dominate cyberspace, leaving the field open for them to intervene in order to obtain the data of others to keep them under control. This is the essence of the dispute between Western imperialism, which seizes wealth and data, and China and its allies in the East, who prefer economic and trade relations. With developing countries instead of dominating them

Threats to international cooperation on the path to digital sovereignty 2.

At the first meeting of the Central Committee of the Central Leadership of the cyber security and Information Group, the Chinese President delivered an important speech in which he stressed that "network and information security are two major strategic issues related to national security and national development, as well as the work and life of the broad masses of the people."¹⁷

This important speech from a person who is considered the head of state in the countries most concerned with the issue of cyber security, gives clear indications that this issue has become very important, especially after he put it before national development, and it is a clear indication that it affects China's strong security

The United States of America began ten years ago to accuse China of launching cyber espionage attacks, most of which were carried out using low-level phishing emails against it to steal intellectual property. The history of cyber threats between China and the United States can be mentioned as follows

Writer Nicole Billroth states in a report published by the New York-Times that the indictment of the administration of US President Joe Biden regarding cyber-attacks, along with interviews with a number of current and former US officials, shows that China has reorganized its hacking operations recently

According to the report, China is now carrying out stealthy and decentralized digital attacks that are difficult to track and prove their source on American interests and companies in all countries of the world

-In the 2009 National Intelligence Estimate, China and Russia topped the list of America's online adversaries, and espionage campaigns disappeared and advanced technologies were used. These techniques include exploiting unknown security vulnerabilities in widely used programs such as Microsoft's "Microsoft Exchange" email service and "Pulse VPN" security devices, which are difficult to defend and allow Chinese hackers to operate undetected for a long time

-The 2009 National Intelligence Estimate, a document representing the consensus of all 16 U.S. intelligence agencies, ranked China and Russia as America's top cyber adversaries, but China was considered the most pressing threat because of the scale of its theft of trade secrets.

-China's hacking prominence first came to prominence in 2010 with attacks on Google and security firm RSA, and again in 2013 with the New York Times hack

In 2015, U.S. officials threatened Chinese President Xi Jinping with sanctions on his first visit to the country after a massive breach that specifically targeted the U.S. Office of Personnel Management. In that attack, Chinese hackers stole sensitive personal information, including more than 20 million fingerprints of Americans with security clearances

-By early 2018, U.S. intelligence officials noticed a shift: China's People's Liberation Army hackers had resigned and been replaced by

agents working for the Ministry of State Security, which handles security, secret police, and secret intelligence

-In 2021, the United States accused China's Ministry of State Security in a detailed indictment of being behind a massive attack on Microsoft Exchange email systems

-China announced a new policy requiring Chinese security researchers to notify the relevant authorities within 48 hours if they find security vulnerabilities, such as the "zero days" that the state relied on to hack Microsoft systems.¹⁸

Conclusion

Digital knowledge has contributed to a qualitative and new shift in all fields of human life, and the digital transformation that the world has witnessed is considered one of the most important features of modern history. One of the most important manifestations of digital transformation in international relations is the protection of digital sovereignty, which we have shown through the study to be closely linked and have a direct relationship with the extent of control over digitization in any country

China is one of the leading countries in the field of controlling digital technologies, and differs from Western countries in trying to shut down the Internet within its territory in an attempt to avoid hacking and electronic piracy. This procedure has political justifications due to China's reliance on one-party rule and fear of foreign interference in its internal affairs and fierce competition with the United States of America economically and militarily

: From the above, the following conclusions can be drawn

-Greater control over various digital technologies has become necessary to protect the country's digital sovereignty

-China has passed the most important stage in digital transformation, which is possessing all the technological components for that, but protecting its digital sovereignty still requires more, as this matter has great complexities and interferences of many actors in it.

As for the important recommendation that we present in this study, it is that Algeria, as a country with its pivotal role in North Africa and the Arab world, can assume a more important position and achieve greater development by carefully controlling digital knowledge and achieving digital sovereignty to protect its data and achieve political and social stability

References

- ¹Chang, B: In the service of self-determination: Teacher education, service learning, and community reorganizing, Theory into Practice, 2015, 19
- ²Barefoot et al: Defining and Measuring the Digital Economy, Bureau of Economic Analysis, Washington, 2018, p3
- ³حماد، صلاح: المعرفة والاستثمار في بنية المعلومات، ورقة عمل، المؤتمر العربي الاول، القاهرة، مصر، 2005
- ⁴<https://ar.wikipedia.org>
- ⁵<http://www.automationanywhere.com>
- ⁶جميل، أمل صبري محمد محمد: محددات نجاح التحول إلى الاقتصاد الرقمي في الدول النامية -دراسة حالة مصر-، رسالة ماجستير غير منشورة، معهد البحوث والدراسات العربية، جامعة الدول العربية، القاهرة، 2020
- ⁷Karim Benyekhlef : L'Internet, un reflet de concurrence des Souverainetés, Revue Lex Electronica, Volume 8n°1 / Automne ,2002
- ⁸Dennis Broeders 'Bibi van den Berg: Governing Cyber Space: Behavior, Power and Diplomacy, Universiteit Leiden, The Netherlands, 2020, p 109
- ⁹عادل عبد الصادق: القوة الإلكترونية، اسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، مؤسسة الأهرام، مصر، العدد 188، 2012، ص32
- ¹⁰حسين زكريا: الأمن القومي، مفاهيم ومصطلحات، 2004، 2024/04/13
<http://www.islamonline.net/arabic/mafaheem/index.shtml>
- ¹¹Philippe Wolf, Lue Vallée : Cyber-conflits, quelques clés de compréhension, INHES, 7872011, p
- ¹²Michèle Alliot, Marie : Allocution aux actes du colloque du 17 Juin 2009, Intitulé, Souveraineté numérique, Assemblée nationale, Dossier, Fondation Prométhéums, France, Juin 2009, p 06
- ¹³<https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web>
- عصام 23:01، 2024/03/24 ترجمة: فرح
- ¹⁴المرجع نفسه.
- ¹⁵Broeders, Berg, p113
- ¹⁶European Commission: Eu Policy on Cyber Defence, Joint Communication to the European Parliament and the Council, 2022, pp. 1-2
- ¹⁷شي جين بينغ: بناء بلدي من قوة الإنترنت إلى قوة الإنترنت، 2014/02/27، 2024/04/06
<http://www.xinhuanet.com/politics>
- ¹⁸<https://www.aljazeera.net/tech/2021/7/27/>