ISSN NO: 2770-0003
Date of Publication: 26-11-2022

Cybersovereignty: The Example of China

Inoyatova Oyshabonu Farrkhodovna
Aminova Asilabonu Alisher qizi
Students of Tashkent State University of Law
E-mails: oyshainovatova@gamil.com
a7amonova@gmail.com

Abstract: this article explores the concept of understanding of countries' sovereignty on the web space, based on the example of the People's Republic of China and influence of globalization process to comprehension of sovereignity. Territorial sovereignty can be easily recognised by territorial borders, however a country's cyber sovereignty involves a more complex approach to limiting it. In addition, there is currently no exact binding law regulating and defining the scope of cybersovereignty. From a historical perspective, China, as a developed country, was one of the first countries, which introduced the Internet into its states And therefore, s strict system of control and restriction of Internet use, called the Golden Shield, was introduced to regulate legal relations in the Internet sphere. This system imposes censorship, restrictions of anonymity, and practice of banning unnecessary web domains and VPN services. Whether such a system is effective in terms of reducing crime on the one hand or on the other hand making the political environment in the country more fragile. The purpose of this article is to reveal the essence of the concept of cyberspace, the extent to which it is developed, what restrictions states are entitled to impose on Internet space and to examine China's practices and their consequences.

Key words: cybersovereignty, sovereignty, cyberspace, Great Firewall, internet policy, VPN services, Golden Shield, anonymity in web space, digital economy, cybercrime, web security.

Introduction

From pre-historic times territorial self-determination and state border issues have been a motive for transnational conflicts leading to two world wars in the history of humanity. This intern pushed society to develop a commonly accepted set of norms for defining the territorial integrity of each country and led to the formation of a concept of sovereignty. First of all, to understand what sovereignty is in today's context, one should look at a set of definitions of the term given by scholars from various backgrounds and periods. It should be noted that the term sovereignty has always been defined differently. Scholars Bodin and Hobbes state that "sovereignty means authority over all matters; it was absolute, unconditional", while famous USSR scholars E. G. Ponomarev and G. A. Rudov argued that "sovereignty means a system of domestic and foreign political opportunities and development opportunities aimed both at ensuring one's own development and at identifying any pressure from outside". Burgess characterized sovereignty as the "Original, absolute, unlimited power over the individual subjects and overall associations of subjects". Meanwhile, Woodrow Wilson states that "Sovereignty is the daily operative power of framing and giving efficacy to the laws"[1]. Sovereignty has also found its reflection in numerous conventions. For instance, the UN Charter, the Montevideo Convention, The Hague Convention, and the UN Convention on the law of the sea. The UN Secretary-General defines it as "state sovereignty being redefined—not least by the forces of globalization and international cooperation."[2] It is evident that "sovereignty" is being interpreted from a different angle. Hence, in the light of territorial concerns "sovereignty is recognized when states recognize each other's territorial integrity, entering into treaties, independence of political and economical system within the country."

Meanwhile, due to rising globalization, sovereignty is not only embracing the territorial purpose of common law practice, but its application in cyberspace is creating a totally new set of issues. Now, in the modern world, the legitimacy of sovereignty is collapsing in the age of globalization. In the modern shape of socio-life, billions of people are having access to the internet and no matter in which territorial jurisdiction an individual can be, the network is ingressed in any part of the territory thus, putting cyberspace into the challenge under the core principles of sovereignty. Whether the "traditional" concept of sovereignty is applicable to cyberspace reality remains open. This article will try to look at modern trends and issues of sovereignty principles in cyberspace in a brief study case of China. Before we move further let's take a look at what does cyberspace mean?

Cyberspace - according to the U.S. Department of Defence, is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers”[3].

One can surely state that the internet has become “a fourth dimension” of our time in which we communicate, learn, do business, or get entertained. It is a specific place that reflects a vast part of our personal life. Multiple declarations by the UN, NATO, OSCE, the European Union, and individual States have confirmed that international law applies in cyberspace. Accordingly, one can expect that so do the principles of sovereignty. It is understood that sovereignty has both an internal and an external component. This is the internal superiority and external independence that the state enjoys on the basis of its national sovereignty over cyber infrastructure, organizations, behavior, and related data and information on its territory [4].

Cyberspace is so vast that it not only constitutes communication between individuals but also, constitutes the economic value of the country. In 2011 the Internet accounted for, on average, 3.4 percent of GDP across the large economies that make up 70 percent of global GDP [5]. Further, it alleged further increase in the world economy in the digital network. By 2020, Australia’s digital economy will be worth as much as $139 billion, or 7.3 percent of GDP [6].

Unlike territorial sovereignty which has abundant jurisdictions on control, cyberspace lacks digital jurisdiction. Modern world law is failing to catch up with the present and let alone the future. It is estimated that by 2040 at least half a billion people's metaverse will be important and yet, there is not any strict law regulation in cyberspace not mentioning the metaverse. However, there is another debate arising that while some concepts of sovereignty would require changes in law, other aspects of virtual space —and, now, metaverse governance—do not. Current law may be sufficient to create the rights envisioned by metaverse users. For instance, in lieu of a legal framework for virtual worlds, Wu says, attorneys turned to contracts to create rights within virtual worlds. His view is that metaverse governance will be a mixture of new laws, potentially narrow statutory or regulatory enactments, and long-established laws and doctrines.

The applicability of sovereignty matters becomes important in the context of the new cyberspace reality.

Now sovereignty is not interpreted in modern days as it used to be. New definitions and new concepts of sovereignty have been added. And the most spreading became “the Internet”. No one could have thought that sovereignty could get extended to cyberspace. In order to apply sovereignty to cyberspace it is important to establish digital boundaries which consequently thereafter create challenges. But, let's take a look at what sovereignty in cyberspace is and what kind of essence it has.

If cyberspace is an artificial space built on the foundation of information technology then it breaks the traditional geographical limits and has a strong impact on the exercise of sovereignty based primarily on territorial jurisdiction and supported by personal jurisdiction meaning independence of state apart from other countries focusing on the information and content provided by the internet. The reason why it is important to implicate cyber-sovereignty lies within the control of the flow of information, and censorship, and to prevent anti-political turnouts. Although there is no proper regulation or law which exactly sets whether sovereignty applies to cyberspace:

While there was formerly some dispute about whether the existing rules of international law were applicable to cyberspace at all, states agreed at the UN GGE in 2013 and 2015 that international law, including the principles of sovereignty and non-intervention, does apply to states’ activities in cyberspace, as it does in the non-cyber context:

> *State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory* [7].

Meanwhile, neither state has a properly drawn line over territorial cyberspace except for China. In this context, China sets a different approach toward cyberspace. China has clearly illustrated its position on what sovereignty in cyberspace means:

‘In June 2015, China passed the National Security Law with the stated purpose of safeguarding China’s security, but it included sweeping provisions addressing economic and industrial policy. China also drafted laws relating to counterterrorism and cybersecurity in 2015 which, if finalized in their current form, would also impose far-reaching and onerous trade restrictions on imported ICT products and services in China (Aaronson 2016). These all projects started after the Great Firewall when in 1998 it was introduced and in 2015 the government toughened it up.

China's top priority was ensuring sovereignty in cyberspace and creating a legal basement for national security. In the discussion of new norms, or codes of conduct in the governance of global cyberspace China prefers more on the ‘‘multilateral model'' to the ‘‘multi-stake-holder model'' during the negation on how to govern the key information infrastructure that supports global cyberspace represented by the Root DNS Sever, the root file and the root file system.

In the realm of Internet governance, we use the term multistakeholder often and with great pride. The term multistakeholder defines the heart of the Internet ecosystem. It reflects the commitment to an open dialog between governments, private sector organizations, civil society, and the technical community to shape the growth of the Internet and the policies that support and protect it. Sadly, it was noted by one commenter that this term is used only in the past tense in the current draft.

In other places, the term multilateral is used. In governmental terms, multilateral is used to describe discussions or agreements between multiple governments. It does not provide for the inclusion of other communities that have been part of the multistakeholder process. Where multilateral is used instead of multistakeholder, it has raised concerns with many participants who believe that the statements should include a wider number of players [8].

Beijing doesn't trust the multi-stake-holder approach which is especially favored by the States since China is concerned that the US will abuse its advantages in the ICT field to expand the sovereignty of the state into the global space while at the same time the model has become a kind of an excuse to avoid other states like China protecting their interests in cyberspace. The idea of "building a cyberspace community of shared destiny," introduced in 2015 by President Xi at the Second Wuzhen Summit, entails establishing a multilateral governing structure and turning the internet into development opportunities commonly shared by people across nations. It is a vision for reshaping transnational structures of communicative relations, opportunities, resources, and protocols. Claiming that China has become a "big internet nation" in the world—thanks to the efforts of all stakeholders and to the integration of advanced technologies and ideas from around the world, commentaries contrast the ideal of shared development with the reality of domination and monopoly and oblige internet superpowers, especially the US, to fulfill the promise of global justice [9].

Challenge the links between territorial sovereignty and cyberspace sovereignty.

Cyberspace is described as a "world without borders" meaning that sovereign territory does not apply to physical borders. Territorial sovereignty is based on the principle of geographical borders rather than transcending borders where limits are often unseen and vague. The digital world transforms the understanding of traditional borders and compared to establishing territory in cyberspace is much more complex. In reality, state borders in cyberspace are more complex, more fluid, and perpetually reconfigured. They also may create nonadjacent spaces that can, in certain ways, overlap. States come across difficulties in exercising their national law, defense prerogatives, and national security. In "A Declaration of the Independence of Cyberspace," published in 1996 by the late John Perry Barlow, co-founder of the Electronic Frontier Foundation; "the statement defines cyberspace as a territory that does not fall under the sovereignty of states, thus establishing a new boundary between the geographic territory of states and cyberspace" [10].

Even though some states manage to clearly define the concept of cyberspace and establish database borders within their geographical territory. China, for the past decade, has been constantly working on establishing physical borders and in the end having one of the strongest systems that filter the data inflow in its cyberspace. China actively censors various Internet resources, thus restricting access to some of the most popular Internet sites such as Google, Facebook, YouTube, and Wikipedia. According to experts, the Chinese firewall blocks about 311 thousand sites, including the unintentional blocking of about 41 thousand of them [11].

As described by Xi Jinping at the 2015 World Internet Conference in Wuzhen, "cyber sovereignty means respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet and equal participation in international cyberspace governance'' [12]. He argues that states should refrain from engaging in cyber hegemony, interfering in other countries' internal affairs, and engaging in, tolerating, or supporting online activities harming the national security of other countries. From it two key principles of China's cyber sovereignty concept arise: 1. Unwanted influence in a country's 'information space' should be banned. In effect, this would allow countries to prevent their citizens from being exposed to ideas and opinions deemed harmful by the regime.

2. Shifting the governance of the Internet from current bodies which include academics and companies, to an international forum such as the UN. This move would also entail a transfer of power from companies and individuals to states alone [13].

Marked by mattering the way territorial sovereignty is respected by other countries, cyberspace shall equally get the same favor. As China's Ambassador Liu Xiaoming noted "each country has "the right to participate in international cyberspace governance on an equal footing" and "each country can develop their own model of cyber regulation and internet-related policies" [14]

By establishing its own network model, all the data information that circulates in the territory is processed through governmental censorship. No other country than China has developed such a powerful program as Great Firewall which plays the role of Golden Shield without missing extraneous information and processing them.

History of creation of Golden Shield and the way it runs.

Historically, China was among first countries, which have introduced the Internet to its state. At first, it was used intimately amongst scientists and politicians. However, later it became publicly available, which obviously caused some challenges, which were needed to be regulated by law. From 1994 onwards, the Internet became widespread in society, with the first Internet cafés opening in Shanghai. According to Tai Zixue, Internet security specialist and author of "Internet in China: Cyberspace and Society", the first acts of legal regulation of the Internet occurred in 1994 [15]. Another legal act was signed in 1996 by Premier Li Peng of the Chinese State Council. This act stipulates that *"only the state has the right to plan, national standardization, development and control of all areas related to the Internet"*.

In 1998, a political event occurred which, marked the beginning of China's Internet policy. Since during this period, opposition forces - the Democratic Party of China, appeared in the country, which obviously were soon arrested by the authorities. We assume that the emergence of opposition forces is closely linked to freedom of speech and the spread of the Internet. The same view is held by Jack Goldsmith and Tim Wu, authors of book "Who Controls the Internet? Illusions of a Borderless World". In their book they note the following: "it was the emergence of the Democratic Party that signaled to the Chinese leadership that forces beyond the control of party elites may be emerging in the country" [16]. Since that year the government started developing data-analyzing project "Golden Shield".

In 2000, two important pieces of legislation came into force: "the Regulation of Telecommunications" and "Measures for the Management of Internet Information Services". These prohibit the dissemination of opposition materials that are harmful to the state and destabilizing to society, as well as fake information, information propagating drugs, alcohol, gambling, and pornographic materials and stipulated responsibility for violations of these rules. It was only in 2001 that the Golden Shield project was approved by the Chinese State Council and included in the country's list of important projects. The same year the project was publicly demonstrated in Trade Show in Beijing. Officially in November 2003 the launch of the project took place.

At first, the project worked with IP addresses and domains: it blocked undesirable resources and blacklisted them. Thus, access to sites was blocked and people simply could not find it or access it. A research study conducted in 2020 found that Golden Shield blocks about 311,000 domains every day. Of these,270,000 are blocked intentionally and 41,000 are banned accidentally [17]. From there, the fight against undesirable content at the Internet was already underway. The program had included keywords to which it reacted by blocking content with such forbidden words. The next step was to fight against VPN services: the program learned to detect when users were using such programs to get around blocking and now the program can still discard banned sites, even if the users use a VPN. The operation of non-registered VPN services has been banned since 2017, and a total prohibition of using it came into force in 2018. For example, a resident of China was sentenced to 5.5 years in prison for illegally setting up a VPN network and selling access to it. The sentence was handed down by a court in the Guangxi Zhuang Autonomous Region. Local Prosecutor's Office managed to prove that Wu Xiangyang set up a virtual private network in 2013, which allowed him to evade China's existing internet censorship [18].

Stage four, the comprehensive stage, is now being implemented. Today, internet users in China cannot download several apps such as Twitter, YouTube, Instagram, Facebook, Google and VPN services. These apps are being replaced by their Chinese counterparts - WeChat, Weibo, etc. Some news agencies such as The New York Times, The Independent, Bloomberg and the BBC are also subject to a ban as well. This also affects freedom of expression in the mass media, according to reports last year there have been the biggest number of journalists arrested by the Chinese government than in any other country [19].

In addition to this, anonymity on the Internet space has recently been banned. Users must verify themselves with their ID, so that no message or post on the internet can be without its author. By this way, the Chinese authorities collect information about the opinions and political stances of their citizens. Even any actions of citizens can be monitored by the government. In 2005, China began developing a nationwide surveillance system. Its official name is Skynet. The anonymity of citizens is eliminated by the widespread use of biometric recognition technology – video cameras, estimated to number around two hundred million.

Conclusion

Currently, the concept of cyber sovereignty is blurred, but one thing is clear: states have the right to implement such policies as they see appropriate, and therefore China's cybersovereignty is undoubtedly legitimate. However, it raises the question of what effect its policies will have on the country itself. The Golden Shield project has enabled China to maintain its cyber sovereignty and has become an effective mechanism for tackling cybercrime, as well as terrorism. The system against anonymity also has a positive effect, as the introduction of facial recognition helps to identify wanted criminals. China's cyber policy has allowed the country's political situation to stabilize and has led to national security. But at the same time, the question arises: isn't the blocking of certain content a caprice of the ruling elite? After all, sooner or later, without ensuring competitiveness in the political arena, a political and social crisis could erupt in the country.

References:

1. Political Theory, R.C Agarwal, S.Chand & Company LTD, 2004, p. 576
2. United Nations, Secretary-General, Kofi Annan, 1999
3. Department of Defense Dictionary of Military and Associated Terms, 2010
4. Sovereignty in Cyberspace: Theory and Practice (Version 2.0), Jointly Launched by Wuhan University China Institute of Contemporary International Relations Shanghai Academy of Social Sciences, p. 14
5. The great transformer: The impact of the Internet on economic growth and prosperity, McKinsey Global Institute, James Manyika and Charles Roxburgh October 2011, p. 10
6. 2017 Foreign Policy White Paper, Australian Government, p. 85
7. UNIDIR (United Nations Institute for Disarmament Research), Palais des Nations, CH 1211 Geneva 10 Switzerland p. 2
8. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/
9. Lu Wei, Director of the Cyberspace Administration of China
10. A Declaration of the Independence of Cyberspace, Davos, Switzerland, February 8, 1996
11. https://www.tadviser.ru/index.php/Статья:Цензура_(контроль)_в_интернете._Опыт_Китая
12. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-28: Defense Support of Civil Authorities, 31 July, 2013, pp. 1-4.
13. Lindsay, Jon R. 2015. 'The Impact of China on Cybersecurity, Fiction and Friction', http://belfercenter.ksg.harvard.edu/files/ IS3903_pp007-047.pdf Accessed 13.01.2017
14. Charles Doyle, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Criminal Laws, Congressional Research Service, October 15, 2014
15. The Internet in China: Cyberspace and Civil Society, by Zixue Tai. New York: Routledge, 2006, 365 pages.
16. Goldsmith, Jack and Wu, Tim, "Who Controls the Internet?: Illusions of a Borderless World" (2006). Faculty Books. 175.

ISSN NO: 2770-0003
Date of Publication: 26-11-2022

17. How Great is the Great Firewall? Measuring China's DNS Censorship Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, Michalis Polychronakis
18. Рустамбеков И., Гулямов С. Международное частное право в киберпространстве (коллизионное кибер право) //Гулямов Саид Саидахрарович. – 2020. – №. 1.
19. Inamdjanova, E. (2021). INVESTMENT AND INVESTMENT ACTIVITY IN THE DIGITAL ECONOMY. Збірник наукових праць SCIENTIA.
20. Imamalieva , D. . (2022). Recent Challenges of Big Data Application in Healthcare System. International Conference on Multidimensional Research and Innovative Technological Analyses, 121–124. Retrieved from http://conferenceseries.info/index.php/ICMRITA/article/view/198
21. https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn
22. https://www.voanews.com/a/report-number-of-jailed-journalists-worldwide-hits-all-time-high/6346645.html