Sovereignty in Cyberspace: EU and China Compared

Yik Chan Chin
Beijing Normal University, China
Yik-Chan.Chin@bnu.edu.cn

Ke Li
Xi'an Jiaotong-Liverpool University, China
892752689@qq.com

Chin, Yik Chan and Li, Ke (2021, December) Sovereignty in Cyberspace: EU and China Compared. *Paper presented at the 2021 Annual GigaNet Symposium (virtual),* 6 December, 14.00-18.30 CET

Abstract

The paper analyzes the similarities and differences between the EU's and China's policies on "sovereignty" in cyberspace. Facing some of the same challenges, the EU and China advocate various concepts of "sovereignty" in cyberspace, including "cyberspace sovereignty" and "data sovereignty". However, the differences in strategic positioning result in great differences in the specific sovereignty positions between the EU and China. The EU does not explicitly propose the concept of cyberspace sovereignty, but regards data sovereignty as its own sovereignty in cyberspace. China claims cyberspace sovereignty as its core sovereignty, and further endorses the position of data sovereignty. The EU's position on data sovereignty is not only to maintain its ability to act in facing the competitions from China and the U.S., but also to become a global standard setter and export its rules and standards internationally. China's positions on data sovereignty are: internally, defining the general rules of cross-border data flow and imposing data localization requirements for some specific industries, and externally, actively exercising extraterritorial legislative jurisdiction adhering to cyberspace sovereignty principle.

Introduction

The "sovereignty" in cyberspace is one of the most controversial issues in Internet governance. Just as the earliest theoretical concept of political sovereignty appeared in the context of political chaos caused by the Reformation[1] and the integration of small principalities into large territorial nation states[2], the connection between cyberspace and sovereignty must be evaluated in the context of contemporary geopolitical conflicts[3]. In modern times, the concept of cyberspace is often associated with the global commons. There is no generally accepted definition of "global commons" at present, but most definitions of "global commons" focus on natural resources that are not controlled by specific states. For example, Organization for Economic Cooperation and Development (OECD) defines "global commons" as "natural assets outside national jurisdiction such as the oceans, outer space and the Antarctic".[4] The academic circles and governments have different views on whether cyberspace belongs to the global commons. Some scholars believe that cyberspace should belong to the global commons. Their views can be divided into three categories: 1) only some aspects of cyberspace will or may constitute the global commons (Chander, 2003[5]; Kanuck, 2010[6]); 2) cyberspace itself belongs to the global commons (Bossomaier and Bradbury, 2014); and 3) cyberspace is not the traditional global commons in the strict sense, but a kind of "virtual commons" with the characteristics of global commons (Scott, 2013)[7]. Other scholars regard cyberspace as an artificial creation based on the structure of tangible materials (Franzese, 2009[8]; Lewis, 2010;[9] and Nye, 2011)[10]. It is worth noting that this dispute does not only exist in academic circles. Every state,

[1] DE CARVALHO, B. 2018. "The Emergence of Sovereignty in the Wake of the Reformations." International Studies Review 20, 502–6.

[2] GRIMM, DIETER. 2015. Sovereignty: The Origin and Future of a Political and Legal Concept. Translated by Belinda Cooper. New York: Columbia University Press.

3 Mueller, Milton L. "Against Sovereignty in Cyberspace." International Studies Review (2020)，vol. 22,779-801.

[4] https://stats.oecd.org/glossary/detail.asp?ID=1120

[5] Anupam Chander, The New, New Property, 81 TEX. L. REV. 715, 749-50 (2003).

[6] Kanuck, Sovereign Discourse on Cyber Conflict Under International Law, 88 TEX. L. REV. 1571, 1573-80 (2010)

[7] Scott J. Shackelford, "Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance," American University Law Review, Vol. 62, No. 5 (2013), p. 1322.

[8] Franzese, Patrick W. "Sovereignty in Cyberspace: Can It Exist?" The Air Force law review 64 (2009)

[9] Lewis, "Sovereignty and the Role of Government in Cyberspace," p. 56.

[10] Joseph S. Nye, The Future of Power (New York: Public Affairs, 2011), p. 143.

especially the EU and China, also have different positions on whether cyberspace belongs to the global commons. In 2010, Department of Defense of U.S. of American released *Quadrennial Defense Review Report*. The report not only clearly defines the "global commons" as "domains or areas that no one state controls but on which all rely", but also points out that it mainly includes "air, sea, space, and cyberspace domains".[11] Under the influence of the U.S., the EU also agrees with the view of cyberspace as a kind of global commons. However, to some extent, the EU also recognizes that national network sovereignty should play a role in cyberspace.[12] Compared with the EU, *Cyberspace Security Strategy (《国家网络空间安全战略》)* released by Cyberspace Administration of China on 27 December, 2016 presents "cyberspace has become a new field of human activities as important as land, sea, sky and outer space, national sovereignty has been extended to cyberspace, and cyberspace sovereignty has become an important part of national sovereignty".[13] This strategy reflects the Chinese government does not recognize the cyberspace as global commons but having sovereignty, and the setting of cyber rules needs to respect national sovereignty.[14] As Cai (2018) points out "cyberspace is neither part of the global commons, nor a completely domestic domain, but a mixed common pool of resources".[15] It regards cyberspace sovereignty as the core concept and the fundamental of global Internet governance, support the formulation of universally accepted cyberspace international rules and cyberspace international anti-terrorism conventions under the leadership of the United Nations[16]. The differences between China and the EU on whether cyberspace belongs to the global commons contributes to the dispute between the EU and China on the "sovereignty " in cyberspace. Besides, it is argued that the debates on "sovereignty" in cyberspace is not a pure theoretical debate, also reflects the power struggle of the world's major military

[11] Department of Defense of United States of American. (2010). Quadrennial Defense Review Report, pp. 8-9.

[12] 郭美蓉.网络空间治理中的国际法路径[J].信息安全与通信保密,2019(05):48-55.

[13] http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

[14] Lindsay J R, Cheung T M, Reveron D S., China and cybersecurity: Espionage, strategy, and politics in the digital domain [M]. London: Oxford University Press, 2015.

[15] Cuihong, Cai. "Global Cyber Governance: China's Contribution and Approach." China quarterly of international strategic studies 4.1 (2018): 55–76.

[16] Cornish, Paul. "Governing Cyberspace through Constructive Ambiguity." Survival (London) 57.3 (2015): 153–176.

powers in Internet governance (Mueller, 2019: 786). In the past, developed countries represented by the EU believe that "cyberspace is not and should not be subject to sovereign control"; They view that the concept of "cyberspace sovereignty" and "a community with a shared future in cyberspace" were proposed because China wants to control the flow of contents on the Internet and Internet may become a tool of oppressive regions.[17] Whilst the developing countries represented by China believe that "sovereigns should, singly or in combination, control cyber".[18]

Traditionally, the EU has largely followed the position and philosophy of the U.S. on the "sovereignty" issue in cyberspace and paid little attention to playing a leading role.[19] However, in recent years, because of the concerns about cyberspace security, the fear of the U.S. abusing its digital dominant position, and the vigilance of China as a rising economic and political competitor, the EU has reflected its position on cyber sovereignty. And the policy differences between the EU and China on the "sovereignty" in cyberspace mainly focus on the positions and claims on definitions and laws of cyberspace sovereignty and data sovereignty, as well as the different measures taken to support these positions and claims. This paper aims to explore the distinctions and commonalities between the EU and China's cyber sovereignty policies by comparing a series of laws, regulations and measures related to the "sovereignty" in cyberspace.

In this paper, we begin by briefly reviewing the historical development of the concept of "sovereignty", and exploring how to apply the traditional concept of sovereignty in the context of cyberspace. Secondly, we study the laws, regulations and specific measures of the EU and China on the two different concepts of "sovereignty" in cyberspace, including "cyberspace sovereignty" and "data sovereignty". Thirdly, we will discuss the distinctions and commonalities of these policies in detail. We finally conclude that even though the EU still generally agrees with the "multi-stakeholder

[17] "SECRETARY OF STATE GONZALO DE BENITO CLOSES THE SEMINAR 'CYBERSECURITY: GLOBAL RESPONSES TO A GLOBAL CHALLENGE.'" States News Service 2014.

[18] Eichenseir, Kristen E. "The Cyber-Law of Nations." The Georgetown law journal 103.2 (2015): 317–.

[19] Thomas Renard, EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain, European Politics and Society, 19:3, pp.321-337.

model" proposed by the U.S., the EU is trying to redefine the "sovereignty" in cyberspace.

Research Questions

Major Question

What are the similarities and differences between the EU's and China's policies on "sovereignty" in cyberspace?

Sub Questions

1. What are the policies of China and the EU on the "sovereignty" in cyberspace?
2. What are the similarities and differences between these policies?

Problematizing Sovereignty

The concept of traditional sovereignty can be traced back to *Westphalian Peace Treaty* of 1648. The sovereignty is described in the treaty that all countries have sovereignty over their own territory and internal affairs, and other countries should not interfere.[20] Sovereignty is generally defined as the highest power over a political entity (regime).[21] Philpott (2003) explained the four principles of sovereignty from the perspective of philosophy: 1) it is authoritative; 2) the authority "from some mutually acknowledged source of legitimacy", including natural law, a divine mandate, hereditary law, a constitution, even international law; 3) the authority is supreme; and 4) the authority is based on territory.[22] In international relations and international law, the traditional concept of sovereignty includes four principles: 1) every country has the right to monopolize the exercise of certain powers from the perspective of its territory and citizens (power monopoly); 2) among states the idea of equality of nations applies; 3) officials of a state enjoy consequential immunity for various purposes if living in another state; and 4) sovereignty means opposing any interference or interference in domestic affairs by foreign (or international) forces.

[20] Weber, Rolf H. "New Sovereignty Concepts in the Age of Internet?" Journal of Internet law 14.2 (2010): 12–.

[21] Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(2), 2305–2322. https://doi.org/10.1177/1461444819865984

[22] Philpott D (2003) Sovereignty. Stanford Encyclopedia of Philosophy Archive, 31 May. Available at: https://plato.stanford.edu/archives/sum2016/entries/sovereignty/

The scope of this traditional concept of sovereignty is limited by United Nations (UN) Charter, which takes the prohibition of force as the premise of the concept of sovereignty and excludes some substantive areas from the “reserved areas” (such as human rights).[23]

However, in the current situation of global interdependence, the concept of “sovereignty” is difficult to unify.[24] Due to the emergence of global telecommunications infrastructure and the Internet, the scope of sovereignty is limited.[25] Therefore, how to apply the traditional concept of sovereignty to the background of cyberspace is the focus of academic debate. The concept of “cyberspace sovereignty” often appears with the concept of “national sovereignty”. There are four different views on the relationship. The first view opposes “national sovereignty determines cyberspace sovereignty”. Milton Mueller (2020) argues against sovereignty in cyberspace since there are only two ways to achieve cyber sovereignty: isolating all digital connections with the outside world and becoming a digital island at the expense of global compatibility and information service trade; or competing for the sole sovereignty of global cyberspace with excluding other countries and nations.[26] The second view holds that the principle of national sovereignty can be “applied” to a country’s cyber activities. The Chatham House’s report on *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention* in 2019 points out that a country can exercise sovereignty over the cyberspace infrastructure within its territorial boundaries as well as over citizens within its territory and overseas citizens. Hence, the principles of sovereignty do apply to the cyberspace activities of a state, that is, a state has the ability to manage

[23] [2]Weber R H. NEW SOVERENTY CONCEPT IN THE AGE OF INTERNET? [J]. Journal of Internet Law, 2010: 12-20

[24] Bhandar B (2011) The conceit of sovereignty: toward post-colonial technique. In: Lessard B (ed) Stories Communities: Narratives of Contact and Arrival in Constituting Political Community. Vancouver, BC, Canada: University of British Columbia Press, pp. 66–88.

[25] Couture, S. & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? New media & society, 2019, Vol. 21(10) 2305– 2322.

[26] Mueller, M. (2020). Online Conference: Moving Forward: Fragmentation, Polarization and Hybridity in Cyberspace – the text of the keynote speech delivered by Milton Mueller at the 2020 conference of the Hague Program for Cyber Norms of Leiden University, https://www.internetgovernance.org/2020/11/13/hague-keynote-sovereignty-in-cyberspace/

these activities within its territorial boundaries and exercise independent state authority.[27]

The third view perceives that cyberspace sovereignty should be developed on the basis of the national sovereignty. In 2019 and 2020, the document *cyber sovereignty: theory and practice* (version 1.0 and 2.0) published by China's think tanks and scholars defines and interprets the definition, principles, and specific manifestations of cyber sovereignty as "the natural extension of national sovereignty in cyberspace. It is the supreme power and external independence that a country enjoys over its own cyber entities, behaviors, facilities, information, governance, etc. based on national sovereignty. The four basic rights of cyberspace sovereignty consist of the right to cyberspace independence, equality, self-defense and jurisdiction. The five basic principles of exercising cyber sovereignty are principle of equality, justice, cooperative, peace and rule of law." The 2019 version 1.0 document states that "advocating and practicing cyber sovereignty does not mean closing or splitting cyberspace, but to build a fair and reasonable international order in cyberspace and universally accepted international rules and national codes of conduct in cyberspace on the basis of national sovereignty." This is contrary to Mueller's view that neither of the two paths can achieve cyberspace sovereignty.[28]

The 2020 version 2.0 document provides a detailed and very broad interpretation of the specific manifestations of cyber sovereignty, corresponding obligations and international rules/standards. The cyberspace sovereignty is reflected through the three categories of national activities of "cyber facilities and operation, data and information, society and people". When a state enjoys cyber sovereignty, it should also bear corresponding obligations, including "non-aggression against other countries, non-interference in other countries' internal affairs, prudent prevention obligations and safeguard obligations". In addition, the version 2.0 also emphasizes the diversity in the practice of countries exercising sovereignty in cyberspace, which

[27] Harriet Moynihan (2019) The Application of International Law to State Cyberattacks Sovereignty and Non-intervention, London: Chatham House.

[28] 《网络主权：理论与实践》（1.0 版）(2019）

will exist for a long time. Furthermore, it suggests to balance the relationship between the sovereign rights and obligations of states and formulate generally accepted international rules and national codes of conduct in cyberspace under the framework of the United Nations.[29]

This position shares some similarities with the fourth view proposed by other western scholars to establish cyberspace sovereignty with “minimum cooperation”. For example, Tim Wu (1997) advocates the establishment of a "minimum sovereign cyberspace" on the basis of consensus around widely accepted Internet standards and norms. Rolf H. Weber believes that the principle that "the policy authority of Internet related public policy issues is the sovereign power of the state" published in the 2005 Tunis agenda of the United Nations is no longer in line with the needs of the global governance framework. The global public good and global public nature of the Internet and the global coverage of communication infrastructure make the regulatory framework must be transferred to the international level, Countries have "core sovereignty", but they need "cooperative sovereignty" to share national responsibilities at the international level.[30]

Methodology

The current comparative studies on “sovereignty” in cyberspace tend to regard cyberspace sovereignty as a part of national security strategy. For example, Zhang, Liu and Chhachhar (2020) discuss the development of the global Internet governance system by comparing the “multilateral and democratic intergovernmental cooperation” proposed by China under the core concept of cyber sovereignty with the “multi-stakeholder” governance concept proposed by the US.[31] Hu, Li and Yang (2019) analyze the similarities and differences between China and the EU’ positions of cyber sovereignty in the framework of cybersecurity.[32] Therefore, this paper considers “sovereignty” as an independent topic of research and conducts a systematic

[29] 《网络主权：理论与实践》（2.0 版）(2020）

[30] Rolf H. Weber (2010) NEW SOVEREIGNTY Concept IN THE AGE OF internet? Journal of Internet Law, pp. 12-20).

[31] Zhang C, Liu J, Chhachhar AR (2020) A comparative study of the global internet governance system between China and the United States. Indian Journal of Science and Technology 13(23): 2303-2310. https://doi.org/10.17485/IJST/v13i23.774

[32] 胡尼克,黎雷,杨乐.中国与欧盟的网络安全法律原则与体系比较[J].信息安全与通信保密,2019(09):58-69.

research of cyber sovereignty policies, including: 1) what are the similarities and differences between China and the EU in defining the various concepts related to the "sovereignty" in cyberspace? These concepts include cyberspace sovereignty and data sovereignty. 2) How do China and the EU preserve and develop the sovereignty in their relevant laws and regulations? and what are the similarities and differences? 3) What actions and measures have been taken by China and the EU to support their respective positions and claims related to the sovereignty? What are the similarities and differences?

The selection of representative policy documents related to cyber sovereignty from China and the EU is also significant. The types of documents used in this research can be divided into two categories: 1) China and the EU's laws and policies about "sovereignty" in cyberspace; 2) academic literature, research reports and news coverages related to the measures taken by China and the EU to achieve cyber sovereignty.

The EU and China's Policies of Cyberspace Sovereignty

The positions of developing countries represented by China and developed countries represented by the EU on cyberspace sovereignty seem incompatible, but in fact, there are still some similarities on basic principles. In 2013 and 2015, UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) agreed that the principles of *the United Nations (UN) Charter* were applicable to national actions in cyberspace. However, in 2017, UNGGE reached an impasse due to the lack of consensus. In 2018, the UN General Assembly established a new group of governmental experts to discuss these issues from 2019 to 2020, and established an Open-ended Working Group (OEWG) to discuss these issues. The OEWG re-emphasizes "International law, in particular the UN Charter, is applicable to the cyber-sphere and is essential for an open, secure, peaceful and accessible ICT environment."[33]

More recently, the drafted *United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes* explicitly endorsed the protection of state sovereignty in countering both online and offline criminal use of ICT. Its article 3 states that "the States parties shall carry out their obligations under this Convention in accordance with the principles of State sovereignty, the sovereign equality of States and non-intervention in the domestic affairs of other States. This Convention shall not authorize the competent authorities of a State party to exercise in the territory of another State the jurisdiction and functions that are reserved exclusively for the authorities of that other State under its domestic law, except as otherwise provided for in this Convention."[34]

The developed countries represented by the EU generally believe that international policies in cyberspace should be formulated using the existing governance framework and procedures, and the multi-stakeholder approach is the most appropriate (including government, commercial and non-governmental interests). However, the developing countries represented by China seek to advocate an international rule-based cyberspace order via intergovernmental agreement,[35] and the governments of all countries should participate equally in the formulation of common rules in cyberspace at the international level, so as to safeguard their own and developing countries' sovereignty and national interests[36]. In other words, the EU and other western governments promotes the inclusion of "network freedom" and multi-stakeholder model in international cyberspace norms; It is worth noting that the general consensus of the EU has gradually shifted from global Internet freedom to the end of a free

[33] United Nations Office for Disarmament Affairs (UNODA). FACT SHEET: DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY [EB/OL]. [2019-07]. https://www.un.org/disarmament/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

[34] United Nations (June 2021) United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. document A/75/L.87/Rev.1 https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

[35] Cornish, Paul. "Governing Cyberspace through Constructive Ambiguity." Survival (London) 57.3 (2015): 153–176.

[36] Cuihong, Cai. "Global Cyber Governance: China's Contribution and Approach." China quarterly of international strategic studies 4.1 (2018): 55–76.

international order in recent years. Based on the concerns about the disadvantage of EU Internet enterprises and the threat to citizens' privacy, the EU gradually began to recognize the importance in protecting its own cyberspace sovereignty.

China, is argued, adopts a multilateral pluralism model based on safeguarding cyberspace sovereignty and national security[37]. This model supports dominant role of government and the pragmatic participation of other actors in global cyber governance, when their participations is perceived as beneficial or at least not harmful to its national interest and not a challenge to the government's authority, in building an multi-tiered and multi-actor global cyberspace governance mechanism, and enhancing multilateralism, democracy and transparency in cyberspace in line with national realities. For instance the Chinese government's *International Strategy of Cooperation in Cyberspace* states that:

> International cyberspace governance should feature multiparty participation and all parties, including governments, international organizations, Internet companies, technology communities, nongovernmental institutions and individuals, should play their respective roles in building an all-dimensional and multi-tiered governance platform.[38]

Moreover, China has clearly expressed its support for governments of all countries to jointly participate in cyberspace governance equally, and advocates an incremental approach to reform the global governance system.

Nevertheless, the two draft resolutions adopted by the First Committee of the Seventy-fourth UN General Assembly in 2019 reflect the influence of geopolitics in realization of global cyberspace governance. The first draft *"Promoting responsible behavior of cyberspace states from the perspective of international security"* won the support of the United States and the European Union, while countries such as China and Russia opposed it. It emphasizes that "although countries have the primary responsibility for maintaining a safe and peaceful information and communication technology environment, a mechanism that decides the appropriate participation of

[37] Cuihong, Cai. "Global Cyber Governance: China's Contribution and Approach." China quarterly of international strategic studies 4.1 (2018): 55–76; International Strategy of Cooperation on Cyberspace

[38] International Strategy of Cooperation on Cyberspace

the private sector, academia, and civil society organizations will facilitate effective cooperation." It promotes the multi-stakeholder model and the implementation of "voluntary, non-binding norms, rules or principles of responsible conduct" to regulate country's use of information and communication technologies.

The second draft *"looking at the development of information and telecommunications from the perspective of international security"* has won the support of China and Russia and other countries while the United States and the European Union opposed it. It emphasized that "the United Nations can play a leading role in promoting dialogue among member states and reaching consensus on the safety and use of ICT", partly because these countries hope to strengthen their influence through the United Nations or other multilateral, country-based platforms and the directly enforceable obligations of UN resolutions. The second draft also hopes to adopt "binding international legal supervision" and "regulations, rules and principles for responsible national behavior" under the leadership of the United Nations to regulate national activities in the field of ICT, and establish regional trust and transparency measures to support capacity building and dissemination of best practices.

Thus, one of the differences between the EU and China's positions of cyberspace sovereignty is reflected in the preference for "multi-stakeholder model" and "multilateral pluralism model". EU countries generally support the "multi-stakeholder model" based on the non-governmental control on the position of cyberspace sovereignty. As early as the Tunis Agenda in 2002, Working Group on Internet Governance (WGIG) defines that Internet governance is formulated and applied by the government, the private sector and civil society by playing their respective roles. They adhere to unified principles, norms, rules, decision-making procedures and plans, and determine the evolution and use form of the Internet.[39] In 2012, *European Parliament Resolution on the Forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunications Union, and the Possible Expansion of the Scope of International Telecommunication Regulations*

[39] https://www.un.org/chinese/events/wsis/agenda.htm

clearly expressed that the European Union supports the continuation of the "present bottom-up, multi-stakeholder model" and "believes that internet governance and related regulatory issues should continue to be defined at a comprehensive and multi-stakeholder level".[40]

In comparison, China supports the "multilateral pluralism model" with cyberspace sovereignty as the core. *Global Initiative on Data Security (*《全球数据安全倡议》*)* issued by the Ministry of Foreign Affairs of the People's Republic of China in September 2020 calls for all countries to respect the sovereignty, jurisdiction and security management of data of other countries, and proposes to formulate the global data security rules through multilateralism.[41]

A very interesting phenomenon is that Chinese and Western scholars have very different interpretations on the multilateral pluralism model proposed by China. Chinese scholars believe that this model is only a variant of multi-stakeholder. For example, Cai (2018) believes that government-led multilateralism is also a form of multi-stakeholder model. China encourages "enhanced communication and cooperation among all stakeholders" to "contribute their share based on their capacity"[42]. Although the multi-stakeholder advocates no central authority as well as an inclusive and networked decision-making process, while China's multilateral pluralism model emphasizes the relatively dominant position of governments among various stakeholders, they both engage multiple actors in cyber governance. Moreover, Cai Cuihong argues that the multi-stakeholder and government-led multilateral pluralism models are not necessarily against but could work to complement each other, they have different advantages in dealing with different internet governance issues. China does not oppose, has no intention to export or ability to challenge the multistakeholder approach, but aiming to gain international

[40] European Parliament Resolution on the Forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunications Union, and the Possible Expansion of the Scope of International Telecommunication Regulations, EUR. PARL. Doc. P7_TA (2012)0451, 5 (2012) [hereinafter European Parliament Resolution], available at https://oeil.secure.europarl.europa.eu/oeil/popups/printficheglobal.pdf?id=614166&l=en

[41] Global Initiative on Data Security. 8 September 2020. Available at: http://www.xinhuanet.com/world/2020-09/08/c_1126466972.htm

[42] International Strategy of Cooperation on Cyberspace.

understanding and recognition of its own approach.[43] In contrast, western scholars believe that the model proposed by China is openly opposed to multi-stakeholder model (Tews, 2015) [44].

Besides governance models, in 2019 and 2020, some EU countries have begun to announce their positions on sovereignty. In 2019, the Estonian government issued a statement on various aspects of the application of international law in cyberspace. It believes the state needs to be responsible for its activities in cyberspace. Sovereignty includes not only rights but also obligations. The Netherland government indicates that the internal and external aspects of sovereignty are fully applicable to the cyber domain, and a country is not allowed to carry out cyber operations that infringe on the sovereignty of other countries. In September 2019, France explained in more detail its views on the application of international law to cyberspace, including any impact on French territory caused by cyber means may constitute an infringement of sovereignty.

At the same time, how international law and sovereignty rules are applied to the actual situation of cyberspace is still a subject of ongoing discussion. Not only is the law in this area unclear, but countries are often ambiguous when citing the law or how to interpret the law, and there are still many gray areas, including how to accurately apply international law in cyberspace. As Brian Egan, former legal counsel of the US State Department, said, countries need to clarify their positions on cyberspace sovereignty. The international community is currently "faced with a relative vacuum of open state practice." "Countries should publicly explain to the greatest extent their views on how existing international laws apply to states' behavior in cyberspace in international and domestic forums."[45]

[43] Cuihong, Cai. "Global Cyber Governance: China's Contribution and Approach." China quarterly of international strategic studies 4.1 (2018): 55–76. Online interview with Cuihong, Cai, 4 August 2021.

[44]Shaw Tews (2015) China challenges multi-stakeholder model of Internet governance. https://www.aei.org/technology-and-innovation/china-challenges-multi-stakeholder-model-internet-governance/

[45] Brian Egan, Remarks on International Law and Stability in Cyberspace at Berkeley Law 5 (Nov. 10, 2016), https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf

China's *State Security Law of the People's Republic of China (《中华人民共和国国家安全法》)* passed on July 1, 2015 defined the concept of "cyberspace sovereignty" for the first time.[46] The concept was elaborated by President Xi in December 2015:

> The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security[47].

Afterwards, cyber sovereignty was also highlighted in China's Cybersecurity Law, the National Cybersecurity Strategy, and the International Strategy of Cooperation in Cyberspace.

The EU has not directly endorses the concept of cyberspace sovereignty, but this does not mean that the EU refuses to claim sovereignty in cyberspace. *Digital Economy Report 2019* released by the UN shows that China and the United States account for 75% of global blockchain technology related patents, 50% of global Internet of things spending and more than 75% of the global public cloud computing market.[48] China and the U.S. have absolute advantages in global information technology and market. In some key areas, the EU lags behind the U.S. and China,[49] in responding, the EU needs to adhere to its sovereignty in cyberspace. As German Economy Minister Peter

[46] State Security Law of the People's Republic of China. 1 July 2015. Available to: http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm

[47] Xi Jinping's Remarks at the Opening Ceremony of the 2ndWorld Internet Conference, Wuzhen, China, December 16, 2015, http://www.fmprc.gov.cn/mfa eng/wjdt 665385/ zyjh 665391/t1327570.shtml

[48] Digital Economy Report 2019. https://unctad.org/system/files/official-document/der2019_en.pdf

[49] Andrés Ortega Klein (2020). The view from Spain: The EU's bid for digital sovereignty. In Carla Hobbs (ed.) EUROPE'S DIGITAL SOVEREIGNTY: FROM RULEMAKER TO SUPERPOWER IN THE AGE OF US-CHINA RIVALRY.

Altmaier mentioned that when companies and institutions have to store data on cloud platforms such as Amazon and Microsoft, Europe is losing part of its sovereignty.[50] In responding to this concern of erosion of its sovereignty (or cyberspace sovereign). the concepts of "strategic sovereignty", "technological sovereignty" and "digital sovereignty" appeared to promote Europe's leadership and strategic autonomy in cyberspace. And the most significant change in thinking about the sovereignty of cyberspace in the EU seems to be that the field of digital technology has become a key battlefield of geopolitical struggle. The questions of who owns the technologies of the future, who produces them, and who sets the standards and regulates their use have become central to geopolitical competition and the core motivation of the EU to propose the discourse and concept of digital and technological sovereignty, which also leads to the EU's new ideas on future technologies and standards, especially artificial intelligence (AI) and next-generation telecommunications.[51]

First, in 2019, the European Council on Foreign Relations proposes a new concept of "strategic sovereignty", and the promotion European digital sovereignty of this key part of this strategic sovereignty. The "strategic sovereignty" aims to guide the EU and its member states through this new era of geopolitical competition. It means that even if countries are still deeply interdependent, the EU and its member states need to reserve their ability to act in the world.

Secondly, in Europe, the impact of non-EU technology companies on the economy and society has attracted strong attention, which threatens EU citizens' control of their personal data, while also restricting the development of EU high-tech companies and the legal implementation capacity of national and EU rule-makers. In this context, digital sovereignty has become one of the important political priorities of the European Commission. It stresses that Europe must achieve "technological sovereignty" in key areas. In February 2020, the European Commission President Ursula von der Leyen (Ursula von der Leyen) took office and proposed "technological

[50] CDU (2019). Peter Altmaier: Technologische Souveränität der EU erhalten. 18 March 2019. Available at https://archiv.cdu.de/artikel/peter-altmaier-technologische-souveraenitaet-der-eu-erhalten

[51] Shapiro Jeremy. Introduction: Europe's digital sovereignty. In: Hobbs Carla (ed.) EUROPE S DIGITAL SOVEREIGNTY: FROM RULEMAKER TO SUPERPOWER IN THE AGE OF US-CHINA RIVALRY. European Council on Foreign Relations

sovereignty". Sovereignty issues include "data sovereignty", "digital sovereignty" and "technical sovereignty" have given unprecedented attention, and various strategies have been launched. In 2020, the European Parliament issued the report of *Digital sovereignty for Europe*, The term "digital sovereignty" in the report is defined as "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)". The aim of raising digital sovereignty is to protect rights and promote economic and social development.[52]

Due to the lack of technical strength as a digital player competing with China and the United States, the EU began to shape its digital ecosystem. As French President, Emmanuel Macron said in his speech on July 2, 2020, "European freedom of action requires economic and digital sovereignty. European interests, which Europeans alone should define, must be heard. It is Europe's job to define the framework for regulation that it imposes on itself, for it is a matter of protecting individual freedoms and economic data of our companies, which are at the core of our sovereignty, and of our concrete operational capacity to act autonomously."[53]As a result, today's EU has become the world's leading digital regulatory power, but whether its regulatory power can protect its vision of the Internet and digital technology is still a problem. Therefore, the emergence of the EU's concepts of "digital sovereignty" is the result of data security and geopolitical problems caused by digital economy and technology competition. For EU policymakers, the idea of digital sovereignty is part of a larger struggle they face. They need not only maintain their ability to act and protect their citizens in the era of intensified geopolitical competition, but also pursue greater independence, flexibility and economic benefits .[54]

The EU has taken some measures to implement the laws and regulations of digital sovereignty. Firstly, the EU has tried to narrow its technological gap with the U.S. and

[52] Matthias Bauer,Fredrik Erixon - Europe's Quest for Technology Sovereignty - Opportunities and Pitfalls

[53] Emmanuel Macron, French President, Speech, 7.2.2020. https://www.elysee.fr/en/emmanuel-macron/2020/02/07/speech-of-the-president-of-the-republic-on-the-defense-and-deterrence-strategy

[54] Shapiro Jeremy. Introduction: Europe's digital sovereignty. In: Hobbs Carla (ed.) EUROPE S DIGITAL SOVEREIGNTY: FROM RULEMAKER TO SUPERPOWER IN THE AGE OF US-CHINA RIVALRY. European Council on Foreign Relations

China by investing in research on key technologies and adopting high ethical standards in AI technology development. Secondly, the EU has established relevant institutions to ensure that EU countries comply with strict EU privacy standards in technology development and use, such as introducing Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) system. Thirdly, the Commission adopted a recommendation for a common EU approach to the security of 5G networks in March 2019 and published an EU toolbox on 5G cybersecurity in January 2020.[55]

In addition, the EU has also drawn up a series of measures to build digital sovereignty. In March 2021, the European Commission issued *2030 Digital Compass*, which provides the vision, objectives and ways to successfully realize the digital transformation of Europe by 2030. The compass proposes three specific paths for digital transformation. The first path is to formulate corresponding digital policy plans. The second path is to strengthen cooperation among EU member states. The third path is to strengthen international cooperation. The EU will formulate global and bilateral digital trade rules based on European values and export its rules and standards to the rest of the world.[56] This is called "normative power of Europe" or "Brussels effect".[57] The EU also proposed the establishment of a new EU-US trade and Technology Council, the development of compatibility standards and cooperation with multiple stakeholders, including government, civil society, the private sector, academia and other stakeholders.[58]

As early as March 2019, the European Commission elaborates the EU's attitude towards China and the relationship between the EU and China. The policy recognizes that "China is, simultaneously, a cooperation partner with whom the EU has closely aligned objectives, a negotiating partner with whom the EU needs to find a balance of

[55] European Parliament Research Service (EPRS). Digital sovereignty for Europe [S/OL]. [2020-07]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[56] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. 2030 Digital Compass: the European way for the Digital Decade. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF

[57] European Parliament and Council of the European Union. General Data Protection Regulation (GDPR) [S/OL]. (2016-04-14) [2018-03-25]. https://gdpr-info.eu/

[58] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. 2030 Digital Compass: the European way for the Digital Decade. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF

interests, an economic competitor in pursuit of technological leadership, and a systemic rival promoting alternative models of governance".[59] The EU does believe that China's rapid technological development and proposed governance model hinder it from becoming a technological power and "formulating the rules of the game" at the international level. However, the EU also hopes to continue to cooperate with China and does not want to be completely divorced from China's technological ecosystem or its economy.[60]

Overview of Data Sovereignty in Cyberspace

In addition to "cyberspace sovereignty", "data sovereignty" is another concept of "sovereignty issues" in cyberspace. The differences between the two concepts mainly lie in the different language and cultural backgrounds, and they also have different emphases. The concept of cyberspace sovereignty has strong political connotation, which is not only a sovereignty[61], but also the basis and framework of the other kinds of sovereignty. What cyberspace sovereignty and data sovereignty have in common is that they both reflect the state's management and control over information and related technologies and equipment. Nonetheless, data sovereignty belongs to special sovereignty, which emphasizes the absolute power of national independent jurisdiction and controlling the dissemination and circulation of national data, is a useful supplement to cyberspace sovereignty.[62] More importantly, the latest development of sovereignty in cyberspace is the competition in normative power, that is, the power of standard setting and rule-making at the regional and international levels.

The EU and China's Policies of Data Sovereignty

The concept of data sovereignty mainly emerged in the context of government cloud services, but there is no unified concept at present. Generally speaking, data

[59] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. EU-China – A strategic outlook. https://ec.europa.eu/info/sites/default/files/communication-eu-china-a-strategic-outlook.pdf

[60] Hobbs Carla (ed.) EUROPE'S DIGITAL SOVEREIGNTY: FROM RULEMAKER TO SUPERPOWER IN THE AGE OF US-CHINA RIVALRY. European Council on Foreign Relations, pp. 42.

[61] 孙伟,朱启超. 正确区分网络主权与数据主权[N]. 中国社会科学报,2016-07-05(005).

[62] 孙伟,朱启超. 正确区分网络主权与数据主权[N]. 中国社会科学报,2016-07-05(005).

sovereignty means that “data should be bound by the laws and governance structures of the countries it collects”[63] and that “the attempt by nation-states to subject data flows to national jurisdictions”[64].

Chinese scholar Bo He (2019) believes that the core of data sovereignty is the extension and expansion of traditional concept of national sovereignty in the cyberspace and data. The purpose is to ensure that the state has the highest power to manage and control its own data.[65] He (2019) divides data sovereignty into internal and external data sovereignty. The former refers to the power of a country to manage data related infrastructure, activities and personnel in its territory under the condition of the compliance of international law. It aims to fulfil its governance of the generation, collection, storage, transmission and processing of data. External data sovereignty refers to a country’s independence in performing data related activities in external relations, such as the independent right to participate in the formulation of international rules related to cyberspace data or join relevant international treaties and agreements.[66] Polatin-Reuben and Wright (2014) also divide “data sovereignty” into weak and strong sovereignty. The weak sovereignty refers to “private sector-led data protection initiatives with an emphasis on the digital-rights aspects of data sovereignty” and strong sovereignty refers to “a state-led approach with an emphasis on safeguarding national security”.[67]

In the EU context, the application of data sovereignty has undergone a process of transformation from individual to group, from private sector dominance to state dominance.

EU’s claim on sovereignty in cyberspace is reflected in its proposition on data sovereignty. The territorial scope of EU’s GDPR is based on three principles. They are nationality principle- controller or processors process data of national subject;

[63] 朱莉欣. 嬗变中的数据主权及法律支持[R].北京：第十一届信息安全法律大会：主权 治权 权利, 2020

[64] Polatin-Reuben, D., & Wright, J. (2014) An Internet with BRICS characteristics: data sovereignty and the Balkanisation of the Internet. Usenix. 7 July.

[65] 何波.数据主权的发展、挑战与应对[J].网络信息法学研究,2019(01):201-216+338.

[66] 何波.数据主权的发展、挑战与应对[J].网络信息法学研究,2019(01):201-216+338.

[67] Polatin-Reuben D and Wright J (2014) An Internet with BRICS characteristics: data sovereignty and the Balkanisation of the Internet. Usenix, 7 July. Available at: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf

territorial principle-the controller or processor has establishment in the land; and the protective principle-harmful activity targeting at the people in the land. The protective principle actually recognizes that a state can exercises extraterritorial jurisdiction over acts that do not occur within its territory. One the other hand, the purpose of *GDPR* is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[68] By protecting personal data rights, *GDPR* has actually embodied the EU's data sovereignty, in other words, *GDPR* is an instance of weak data sovereignty. The territorial scope of the GDPR is also a clear demonstration of the EU's territorial and national sovereignty.

Chapter 5 specifies three conditions that must be met when transmitting data to a third country or international organization for processing.[69] If data controller or processor wants to transmit data to a third country or international organization, their data protection must meet the EU standards or the standards recognized by the EU. This allows the EU have important legal power when negotiating data protection with third countries, international organizations or enterprises, and increase EU legal influence in the data market, in essence, it is the extraterritorial extension of EU data sovereignty.[70] The impact of such regulation goes far beyond the union borders to countries that are not specific or directly related to the personal data of EU citizens. The EU has successfully influenced privacy laws in other regions and restricted the transfer of personal data from member states to countries without adequate privacy protection.[71]

In addition, *A European strategy for data* is issued on February 19, 2020 and the *Proposal for a Regulation of the European Parliament and of the Council on European data governance, i.e. Data Governance Act* is also announced on November 25, 2020. Both aim to create a single data market to ensure Europe's global

[68] Art. 1 GDPR: Subject-matter and objectives. https://gdpr-info.eu/art-1-gdpr/

[69] Chapter 5: Transfers of personal data to third countries or international organisations. https://gdpr-info.eu/chapter-5/

[70] 翟志勇.数据主权的兴起及其双重属性[J].中国法律评论,2018(06):196-202.

[71] Ian Brown and Christopher T Marsden, Regulating Code: Good Governance and Better Regulation in the Information Age (The MIT Press, 2013) 59.

competitiveness, data sovereignty and common European data space. This is the embodiment of a strong data sovereignty model led by the super-state.

The strategy wants to ensure that European data is controlled (and monetized) by European companies in accordance with European rules, such as the introduction of financing for European clouds and data centers.[72] Firstly, the EU believes that Europe must evolve from a regulatory superpower to a technological superpower in order to truly safeguard its values and interests in the digital technology and protect Europeans from false information and cyber-attacks.[73] Secondly, in terms of data management and economic utilization of data, the vast majority of core data in Europe are owned by American companies. Europe intends to compete with other world powers of new data economy, especially China's national power and American commercial market power, and promote a new European data governance mode in line with EU values and principles.[74] As an important support of *A European strategy for data*, *Data Governance Act* put forward the establishment and development of common private and public data spaces in Europe in strategic areas (specifically health, environment, energy, agriculture, liquidity, finance, manufacturing, public management, etc.), and through the establishment of a public sector data reuse mechanism to ensure that data intermediaries, as organizers of data sharing or collection, take four measures to enable citizens and enterprises to provide data for social interests and promote the development of trusted data sharing system.[75] Nevertheless, it's worth noting that the EU has not clearly defined the concept of data sovereignty in these documents.

[72] European Commission. The European Data Strategy [S/OL]. [2020-02-19]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[73] Hobbs C. Project note: In search of Europe's digital sovereignty. In C. Hobbs (Ed.) Europe's digital sovereignty: From rule maker to superpower in the age of US-China rivalry (pp. 91-94). 2020. https://ecfr.eu/archive/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

[74] Klein A O. The view from Spain: The EU's bid for digital sovereignty. In C. Hobbs (Ed.) Europe's digital sovereignty: From rule maker to superpower in the age of US-China rivalry (pp. 32-35). 2020. https://ecfr.eu/archive/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

[75] European Commission. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) [S/OL]. [2020-11-25]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

In competing with western countries, China relatively lacks the core technology of independent innovation.[76] On August 31st, 2015, *Action Plan for Promoting the Development of Big Data (*《促进大数据发展行动纲要》*)* issued by the State Council made an official statement on data sovereignty for the first time, calling for "enhancing the ability to protect cyberspace data sovereignty".[77]

China's positions and claims on data sovereignty include four parts. The first is to advocate cyberspace sovereignty and data sovereignty, and issue *Global Initiative on Data Security (*《全球数据安全倡议》*)*. Although the initiative does not explicitly mention the concept of data sovereignty, it promotes the proposition of data sovereignty from the aspects of respecting each country's sovereignty, jurisdiction and data security right.[78] The second is to formulate *Cybersecurity Law of the People's Republic of China (*《中华人民共和国网络安全法》*)* and adopt data localization measures. *Cybersecurity Law of the People's Republic of China (*《中华人民共和国网络安全法》*)* regulates Internet data security. The law requires that critical information infrastructure operators that collect and generate personal information and important data shall store data collected and generated in the territory of China. If it is really necessary to provide overseas services due to business needs, a security assessment shall be conducted in accordance with measures promulgated by national cyberspace administration and state council.[79]

Thirdly, *Data Security Law of the People's Republic of China*（《中华人民共和国数据安全法》 launched on June 10, 2021 announces the jurisdiction model of "territorialism plus protectionism" to respond to the problems of extra-territorial juridical enforcement of other countries. The external goal of the legislation is to maintain China's data sovereignty. Article 2 stipulates that this law applies to data activities within the territory of China. And for organizations and individuals outside

[76] 何傲翾.数据全球化与数据主权的对抗态势和中国应对——基于数据安全视角的分析[J].北京航空航天大学学报(社会科学版),2021,34(03):18-26.

[77] Action Plan for Promoting the Development of Big Data. August 31 2015. http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm

[78] Global Initiative on Data Security. 8 September 2020. Available at: http://www.xinhuanet.com/world/2020-09/08/c_1126466972.htm

[79] Cybersecurity Law of the People's Republic of China. 7 November 2016. Available to:

http://www.npc.gov.cn/wxzl/gongbao/2017-02/20/content_2007531.htm

China carrying out data activities that harm the national security, public interests or the legitimate rights and interests of citizens or organizations of China, they shall be investigated for legal responsibility in accordance with the law.[80]

Fourthly, it aims to maintain the cross-border "legal, secure and free flow" of data. Article 11 of the data security law stipulates that the state actively carries out international exchanges and cooperation in data security governance, data development and utilization, participates in the formulation of international rules and standards related to data security, and promotes the safe and free flow of cross-border data transmission.

Like its European Counterpart, the Chinese government also emphases on the economic benefit of the data economy, developing data industry and economy as a way to protect data security. The *Data Security Law* requires the state implements a big data strategy, to support the construction of data infrastructure and innovative application of data. China has adopted a series of measures to implement the data sovereignty policy. Data security protection technology is widely used. Data security disciplines and research institutes, training and assessment programmes are set up to strengthen the construction of data security talent team. It also encourage the development of the data security industry demonstration zone.[81]

Conclusion

A tension between global cyberspace and territorial sovereignty is a major issue in Internet governance (Müller, 2020). After the Second World War, national sovereignty was partially moved to a higher global level such as the WTO. However, there is currently no multilateral binding legal instrument in cyberspace (except for the ITU ITR), and therefore, cooperative sovereignty at international level has not yet

[80] http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml

[81] 朱梅胤. 5 年政策梳理：数据安全的监管路径与体系建设. 零壹智库. https://www.01caijing.com/article/282282.htm

been achieved. The tension of geopolitics has also made it more and more difficult to establish a global framework for Internet government.

The EU and China have some common attitudes and propositions on the “sovereignty” in cyberspace. However, due to the different challenges and strategic directions, there are great differences in the specific sovereignty positions of the two countries. The reason of why the EU and China advocate various concepts of “sovereignty” in cyberspace, including “cyberspace sovereignty” and “data sovereignty” is that they are facing some common challenges. The first is the concern about cybersecurity. After the “Prism” in the U.S., cybersecurity issues such as stealing secrets and violating personal privacy have attracted great attention from other countries. The second is the lack of international rules for cross-border data flow, which makes the control of data outside the country very complex. The third is the technological hegemony of the U.S. is constantly encroaching on the living space of other countries. Therefore, the EU and China have shared certain similarities in some aspects. The premise of these similarities is that international law, especially the UN Charter, is applicable to activities in cyberspace. Under this premise, the EU and China believes that it is necessary for multi-actors to participate in Internet governance. Moreover, they have incorporated the data of virtual space into the jurisdiction of real territory at the legal level, and completed the construction of exclusive power based on their territorial scope and even beyond.

Even so, there are still some fundamental differences between the EU and China in the policy settings of cyberspace and data sovereignty. Primarily, there is a dispute between the EU and China on whether to adopt the multi-stakeholder model or the multilateral pluralism model in the position of cyber sovereignty. Secondly, the EU and China face diverse challenges in big data, resulting in some differences in the claims of sovereignty. In terms of data sovereignty, the EU’s position is based on a direct protection of public’s right and European economic interests, while China’s position is a mode based on protection of national security and economic development, and indirectly protecting personal information right.

It seems that the ideas of the EU and China on the concept of "sovereignty" in cyberspace are incompatible. However, the EU has incorporated the role of state as the core layer of the data control through various provisions of *GDPR*, *A European strategy for data* and *Data Governance Act*. Although the government does not directly participate in the control, it will indirectly and strictly restrict the flow of cross-border data according to certain standards.

Previously, the claims and practices of various countries on data sovereignty focused on cross-border data flow government, and showing three trends: 1) impose restrictions on the cross-border export of important data to maintain their own data security; 2) strengthen the control of personal data through legislation; and 3) extend extraterritorial jurisdiction over data.

However, the latest development of sovereignty in cyberspace is in the area of normative power, namely, the power of standard setting and rule-making at the regional and international levels. The EU aims to be a global standard setter and try to use its rule making ability to export its rules and standards to the rest of the world. This is called "normative power of Europe" or "Brussels effect" by commentators and scholars. Along the lines of the experience of the EU's GDPR, it will bring the introduction of extraterritorial rules to restrict those who want to interact with the European single market and its consumers, no matter where their corporate headquarters are. It is difficult to predict whether the EU strategy will succeed at the international level, because without a broad international alliance, the EU's efforts will be dwarfed by the huge investment and military efforts of the U.S. and China.[82]

The debate on the sovereignty of cyberspace is not only a dispute over national sovereignty, because national sovereignty is necessary but increasingly insufficient. It shall also be supplemented by supranational sovereignty to provide a broader coordination interest (such as standards and requirements) and an equal competition environment for all stakeholders, as well as to increase coordination opportunities. For example, data sovereignty is more feasible and effective at the EU level through

[82] Andrea Renda （2020） Artificial intelligence: Towards a pan-European strategy.

GDPR. The EU may move in the same direction in another key digital field such as the artificial intelligence sovereignty because it is believed that the best answer to defend multinational corporations' control of digital technology may be to establish supranational digital sovereignty at the supranational level. The question is how to expand the coverage of the sources of legitimacy of supranational sovereignty, and how countries can establish supranational sovereignty by pooling and transferring their national sovereignty.

On the other side, *the Global Initiative on Data Security (《全球数据安全倡议》)* issues by China's Ministry of Foreign Affairs calls on all countries to uphold the principle of maintaining balance between development and security, i.e. balancing the relationship between technological progress, economic development and the protection of national security and social and public interests. It calls on all countries to support and confirm their commitments through bilateral or regional agreements, and call on the international community to reach an international agreement on this issue on the basis of universal participation.[83]

Therefore, the data and digital strategies of the EU and China are also closely related to future partnerships and alliances at the international level. As far as the larger geopolitical pattern is concerned, the U.S. hopes that Europe will not regard the U.S. as equal partner in the triangular relationship with China, but develop a common transatlantic position to affect the norms defining the digital ecosystem and the possible direction of key players such as India.[84]On the other hand, the continuation of bipolar competition between China and the U.S. will undermine the cooperation between the two countries on science and technology issues. It is uncertain whether the EU can reach a compromise with the United States, and China's authoritarian model will pose some serious restrictions on the cooperation between the EU and

[83] 《全球数据安全倡议》

[84] Andrea Renda (2020) Artificial intelligence: Towards a pan-European strategy; and Carla Hobbs (2020) Project note: In search of Europe's digital sovereignty, in Carla Hobbs (ed.) Europe's digital sovereignty: From rule maker to superpower in the age of US-China rivalry

China.[85] Some scholars suggest that the EU can act as a mediator of the digital regulatory methods of the U.S. and China.[86]

[85] Jeremy Shapiro（2020）Introduction: Europe’s digital sovereignty. In Carla Hobbs (ed.) Europe’s digital sovereignty: From rulemaker to superpower in the age of US-China rivalry:6-13

[86] Andrew Puddephatt (2020) Governing the internet: The makings of an EU model