GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2024, War and International System Special Issue, 131-149
DOI: 10.17752/guvenlikstrtj.1486265

Research Article

Is a Theory of Cyberspace Dominance Possible? An Assessment from the Perspective of China's Cyber Sovereignty Approach

Bir Siber Uzay Hâkimiyet Teorisi Mümkün mü? Çin'in Siber Egemenlik Yaklaşımı Perspektifinden Bir Değerlendirme

Aybala LALE KAHRAMAN*

*Asst. Prof. Dr., Bursa Technical University, Faculty of Humanities and Social Sciences, Department of International Relations, Bursa, Türkiye
e-mail: aybala.lale@btu.edu.tr
ORCID: 0000-0003-3289-5403

Geliş Tarihi / Submitted:
18.05.2024

Kabul Tarihi / Accepted:
31.07.2024

Abstract

In today's rapidly digitalizing world, cybersecurity requires the protection of information and communication technologies as well as the infrastructure of countries. In this framework, some countries consider cyber sovereignty to be connected with cybersecurity as an approach that discloses the control and authority of states over their digital infrastructures. This study analyzes the cybersecurity policies and understanding of cyber sovereignty in China. In doing so, the possibility of theorizing dominance in cyberspace is discussed. In this context, the main purpose of this study is to examine the theoretical dimensions of cybersecurity and cyber sovereignty concepts and to analyze China's cybersecurity policies and cyber sovereignty approach. Cyberspace represents a new field of dominance in international relations. Rather than providing a definitive answer to whether cyber sovereignty is possible under international law, the focus should be on how cyber sovereignty can play a role in international power struggles and shape cybersecurity policies. In this context, the study's methodology consists of a brief introduction to cybersecurity, followed by an analysis of the research question of whether cyberspace dominance is possible and the concept of cyber sovereignty. Within the scope of the theoretical framework, a literature review of the relevant concepts was conducted, and China's cybersecurity policies and cyber sovereignty approach were analyzed as a case study. The documents, sources, and data discussed throughout the study demonstrate China's understanding of cyber sovereignty and how it is shaped on international platforms. The study concludes that if China sees cyberspace sovereignty as the key to becoming a global power in the international system, it must integrate all factors, including military, political, and economic factors, besides cybersecurity.

Keywords: Cyberspace, Cybersecurity, Cyber Sovereignty, Cyberspace Dominance Theory, Chinese Cyber Sovereignty

Öz

Günümüzün hızla dijitalleşen dünyasında siber güvenlik, ülkelerin altyapılarının yanı sıra bilgi ve iletişim teknolojilerinin de korunmasını gerektirmektedir. Bu çerçevede siber egemenlik, devletlerin dijital altyapıları üzerindeki kontrol ve otoritesini ortaya koyan bir yaklaşım olarak bazı ülkeler tarafından siber güvenlik ile ilişkilendirilmektedir. Bu çalışma, Çin'deki siber güvenlik politikalarını ve siber egemenlik anlayışını derinlemesine analiz etmektedir. Bunu yaparken, siber uzayda hakimiyeti teorileştirme olasılığı tartışılmaktadır. Bu kapsamda çalışmanın temel amacı, siber güvenlik ve siber egemenlik kavramlarının teorik boyutlarının incelenmesi ve Çin'in siber güvenlik politikaları ve siber egemenlik yaklaşımının analiz edilmesidir. Siber uzayın uluslararası ilişkilerde yeni bir hâkimiyet alanını temsil ettiği düşünülmektedir. Siber egemenliğin uluslararası hukuk kapsamında mümkün olup olmadığına dair kesin bir cevap vermek yerine, siber egemenliğin uluslararası güç mücadelelerinde nasıl bir rol oynayabileceğine ve siber güvenlik politikalarını nasıl şekillendirebileceğine odaklanılmalıdır. Bu bağlamda çalışmanın metodolojisi, siber güvenliğe kısa bir girişin ardından siber uzay hâkimiyetinin mümkün olup olmadığı araştırma sorusunun ve siber egemenlik kavramının analizinden oluşmaktadır. Teorik çerçeve kapsamında ilgili kavramlara ilişkin literatür taraması yapılmış, Çin'in siber güvenlik politikaları ve siber egemenlik yaklaşımı vaka çalışması olarak analiz edilmiştir. Çalışma boyunca ele alınan belge, kaynak ve veriler, Çin'in siber egemenlik anlayışını ve bu anlayışın uluslararası platformlarda nasıl şekillendiğini göstermektedir. Çin, siber egemenliği uluslararası sistemde küresel bir güç olmanın anahtarı olarak görüyorsa, siber güvenliğin yanı sıra asker, siyasi, ekonomik faktörler dâhil olmak üzere tüm faktörleri entegre etmelidir.

Anahtar Kelimeler: Siber Uzay, Siber Güvenlik, Siber Egemenlik, Siber Uzay Hâkimiyet Teorisi, Çin Siber Egemenliği

Introduction

Recently, geopolitical theories have concentrated on possibly including cyberspace as a fifth security domain in addition to land, air, sea, and space. The rise of cyberspace as a force field with penetrating qualities poses practical challenges for the discipline of International Relations.[1] The need to develop cybersecurity technologies becomes more prominent as new information threats emerge. Developing cybersecurity technologies that can resist cyber-attacks is vital, especially at the national level.[2] In this respect, cybersecurity enables the emergence of technological innovations and initiatives crucial for state security, such as information and patent generation.[3]

Cyberspace is a complex and dynamic field that has increasingly gained importance. Via the development of information and communication technologies, this field has become a fundamental element in inter-state relations and international security. Shaping relations between states in the context of cyberspace brings concepts such as cybersecurity, cyber warfare, cyber-attack, and cyber sovereignty into discussion. Because all cyber-related issues have risen to a level that might bring states into conflict, the use of cyberspace by states and other actors for aggressive purposes escalates conflicts and destabilizes societies. This situation threatens international peace and security. The catastrophic scenarios such as "digital Pearl Harbors" have not yet materialized; however, the uncontrolled spread of many attacks across the globe demonstrates the potential destructive threat and systemic risks of conflicts in cyberspace.[4] This situation makes cybersecurity a new security parameter. The concept of sovereignty in cyberspace stands out as a central issue for the management and control of this field. Nonetheless, the rapid expansion and complexity of this digital environment pose new problems and challenges in international relations, with the states unable to reach a consensus regarding cyberspace sovereignty and dominance.

In international relations, the power struggle is also impacted by developing technologies and spills over to cyberspace in its changing and renewed form. The 21st century's main agenda, the global power struggle between the United States (US) and China, continues in cyberspace. There is a consensus that the US and China are competing to turn the global cyber order in their favor.[5] In addition to owning critical components of cyber resources such as infrastructures, networks, and servers, the US has positioned itself as the leading cyber power shaping the multi-stakeholders in the Internet governance regime.[6] Issues of sovereignty and security in cyberspace divide the world into two poles, just like the ideological struggle in the 20th century. On the one hand, there are liberal ideas defending the principle of freedom in cyberspace; on the other hand, there are views defending the

[1] Breno Pauli Medeiros and Luiz Rogério Franco Goldoni, "The Fundamental Conceptual Trinity of Cyberspace", *Contexto Internacional*, 42:1, 2020, p. 45.

[2] Yuliia Kyrdoda, Giacomo Marzi et.al., "Cybersecurity Technology: An Analysis of the Topic from 2011 to 2021", Daim, Tuğrul U. Daim & Marina Dabić (eds.), *Cybersecurity, Applied Innovation and Technology Management*, Springer, Cham, 2023, p. 36.

[3] Mürsel Doğrul, Haydar Yalçın and Tugrul U. Daim, "Cybersecurity Technology: A Landscape Analysis", Tuğrul U. Daim & Marina Dabić (eds.), *Cybersecurity, Applied Innovation and Technology Management*, Springer, Cham, 2023.

[4] Frédérick Douzet and Aude Gery, "Cyberspace is Used, First and Foremost, to Wage Wars: Proliferation, Security and Stability in Cyberspace", *Journal of Cyber Policy*, 6:1, 2021, p. 97.

[5] Chien-Huei Wu, "Sovereignty Fever: The Territorial Turn of Global Cyber Order*", Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht/Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht*, 81:3, 2021, p. 654.

[6] John Kerry, Secretary of State, "An Open and Secure Internet: We Must Have Both", VOAnews, 2015, https://www.voanews.com/a/text-of-john-kerrys-remarks-in-seoul-on-open-and-secure-internet/2776139.html, accessed 13.07.2024.

sovereignty of states in cyberspace. In this context, China's proposed concept of Internet sovereignty is of interest not only to authoritarian regimes but also to liberal democracies.[7] This makes Internet sovereignty worthy of discussion.

China has strengthened its presence in cyberspace via various documents and actions as a rising power. It has recently gained power in cyberspace and become a crucial international player. Hence, China's cybersecurity policies and claims of dominance in cyberspace are of great importance in terms of international relations and the development of global cybersecurity. In 2010, when China published its first White Paper on the Internet, it characterized the topics of usage, management, and construction of the Internet as an issue that concerns national economic prosperity and development, state security and social harmony, state sovereignty and dignity, and the basic interests of the people.[8] While China defends the idea that the Internet is within the jurisdiction of the Chinese government, these ideas of China are in sharp contrast with the paradigm of the international cyber order. In this context, this study intends to investigate China's cybersecurity policies and the idea of cyber sovereignty to question if it is possible to construct a theory of cyberspace sovereignty and its potential global implications. The problem of the study is to comprehend the applicability of the concept of sovereignty in cyberspace and its role in the international system. In this context, it is imperative to reveal how traditional understandings of sovereignty have changed in cyberspace and how China has adopted this new understanding of sovereignty.

1. Theoretical Framework

1.1. The Concept of Cybersecurity

The word "cyber" was first referred to in 1982 in the science fiction novel "Neuromancer" by William Gibson.[9] The author narrates the story of a hacker infiltrating a computer system called the Matrix.[10] By fictionalizing the digital age very early, the author has helped to shape cyberspace in the minds. The International Organization for Standardization (ISO) defines the word cyber as *"the complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"*.[11] Cyber, a concept related to computers and computer networks, constitutes cyberspace, which has come into existence as the "fifth area of struggle" in International Relations literature. Singer and Friedman describe cyberspace as *"the realm of computer networks (and the users behind them) in which information is stored, shared, and transmitted online"*.[12] It is necessary to pay special attention to the expression "the realm of users" in this definition. Apart from all kinds of virtual and physical elements (code, programs, fiber optic cables, hardware, etc.) making up the content of cyberspace, the most crucial factor that creates cyberspace is the human being. Technological opportunities developing with human intelligence cannot be thought of independently of humans. For this reason, a complex and multi-dimensional system dominates the background of cyberspace.

Cyberspace has become a battlefield where all kinds of conflicts might occur, and cyber-crimes are committed. The control of information and telecommunications infrastructure, and the ability to respond to cyber-attacks and ensure cybersecurity have

[7] Chien-Huei Wu, "Sovereignty Fever: The Territorial Turn of Global Cyber Order", p. 657.

[8] Information Office of the State Council of the People's Republic of China, "The Internet in China", June 8, 2010, Beijing, http://www.china.org.cn/government/whitepaper/node_7093508.htm, accessed 20.01.2024.

[9] Etymonline, "Cyber-", https://www.etymonline.com/word/cyber-, accessed 25.01.2024.

[10] P. W. Singer and Allan Friedman, *Siber Güvenlik ve Siber Savaş*, Buzdağı Yayıncılık, Ankara, 2018.

[11] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn, 2012, p. 8.

[12] Singer and Friedman, *Cyber Security and Cyber Warfare*, p. 29.

become important elements of power among actors. In this framework, the importance of the concept of cybersecurity has increased continuously. Cybersecurity revolves around technical or social fields and problems such as computer science, economics, engineering, information systems, criminology, management, psychology, sociology, and international relations, and, thus, it needs to be interpreted via various disciplines.[13] Merriam-Webster Dictionary defines cybersecurity as *"measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"*.[14] The definition of cybersecurity by the International Telecommunication Union (2008) is as follows:

> *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attention and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."*[15]

Thus, there is no agreed definition of cybersecurity. Nevertheless, there are some perspectives in the literature that are defined by the dominant powers of cyberspace. For instance, the US government report titled "2024 Report on The Cybersecurity Posture of The United States", has brought the term "cybersecurity posture" into the agenda. This concept means "*the ability to identify, protect against, detect, respond to, and recover from an intrusion in an information system, the compromise of which could constitute a cyber-attack or a cyber campaign of significant consequence*".[16] According to the United Nations (UN), cybersecurity means; "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets*".[17] Even though there are different interpretations, the goals of cybersecurity are certain. The three objectives defined as "CIA Triad" are confidentiality, integrity, and availability. Confidentiality refers to the storage of data. It includes the protection of secrets and personal data, as well as technical tools such as encryption and access control. Integrity implies that the system and the data within it cannot be changed unless there is authorization. Availability is the ability to use the system as expected.[18] Measures to improve the confidentiality or integrity of information might sometimes negatively influence accessibility. When accessibility is improved, confidentiality and integrity might be compromised.[19]

[13] V. Kavitha and S. Pretha, "Cyber Security Issues and Challenges-A Review", *IJCSMC*, 8:11, 2019, p. 1.

[14] Merriam-Webster, "Cybersecurity," n.d., https://www.merriam-webster.com/dictionary/cybersecurity, accessed 21.05.2024.

[15] International Telecommunications Union (2008), "ITU-T X.1205: series X: Data Networks, Open System Communications and Security: Telecommunications Security: Overview of Cybersecurity", https://www.itu.int/rec/t-rec-x.1205-200804-i, accessed 20.05.2024.

[16] The White House, 2024 Report on The Cybersecurity Posture of The United States, 20,https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf, accessed 14.07.2024.

[17] United Nations, *Cybersecurity in the United Nations System Organizations Report of the Joint Inspection Unit*, JIU/REP/2021/3, 2021, p. 7.

[18] Singer and Friedman, *Cyber Security and Cyber Warfare,* p. 57.

[19] Hakan Hekim and Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, 4:2, 2013, p. 137.

Like the actors of international relations, cyberspace actors are composed of states and non-state actors. Nonetheless, actors' motivations in cyberspace may differ, and many actors remain undetected because of their ability to remain anonymous and conceal their identities.[20] This issue makes it challenging to ensure cybersecurity. According to realists, states are the primary actors in international relations, but in cyberspace, the phenomenon of "state sovereignty" is impossible. Instead, non-traditional actors such as multi-national corporations, hackers, or intergovernmental organizations play a crucial role in cybersecurity problems. Thus, the environment dominating cyberspace is complex and uncertain.

Cybersecurity, defined as "*the security of the environment formed by physical and non-physical components and characterized by the use of computers and other networked devices"*, ensures security in a certain capacity.[21] This is because the widespread increase in communication technologies has brought the production of digital data, and the security of data not only of companies, institutions, or political structures but also of individuals has gained importance. Furthermore, the most fundamental element that makes cybersecurity a conceptual approach is the possibility that attacks or moves in the cyber domain can also impact the physical domain. Therefore, cybersecurity terminology also encompasses national security concepts.[22]

Today, as technology improves, there is an increase in the types of cyber threats encountered, although a decrease is expected. The definition and content of cyber-attack types (such as malware, spyware, viruses, worms, phishing attacks, DDoS and APT attacks, botnets, and artificial intelligence attacks) are beyond the scope of the study.[23] Nevertheless, cyber-attacks, which might disrupt and impact computer systems, networks, and all hardware, have become an asymmetric element in the inter-state struggle, especially in cyberspace. After all, cyber-attacks cost little and are relatively easy to carry out. However, it is necessary to distinguish cyber-attacks from traditional attacks. Instead of using kinetic power (bomb, fist, etc.), digital tools are implemented. The attack is targeted at information, not directly causing physical damage to its target.[24] The shift of power away from the sphere of influence of governments is one of the significant power shifts of the 21st century.[25] Great powers are unlikely to dominate cyberspace like they have dominated other areas of struggle (land, air, sea, and space). States with more significant resources also have more cyber vulnerabilities.[26] Hence, the power difference between states that have a great power status in the international system and states that are developing or underdeveloped might show the opposite direction in cyberspace.

1.2. Theorizing Experiment on Cyberspace Sovereignty

Chinese President Xi Jinping's use of the phrase "respect for cyber sovereignty"[27] at the World Internet Conference in 2014 coincides with a similar period in which the principle of

[20] Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict", *The Johns Hopkins University Applied Physics Laboratory*, 14:7, 2015, p. 15.

[21] Jamie Collier, "Cyber Security Assemblies: A Framework for Understanding the Dynamic and Contested Nature of Security Provision", *Politics and Governance*, 6:2, 2018, p. 14.

[22] Salih Bıçakcı, "Siber Güvenlik ve Savunma", *Güvenlik Yazıları Serisi*, 42, 2019, p. 1.

[23] For access to detailed and technical information about the types of cyber-attacks; Şeref Sağıroğlu and Mustafa Alkan, *Siber Güvenlik ve Savunma*, Grafiker Yayınları, Ankara, 2018.

[24] Singer and Friedman, *Cyber Security and Cyber Warfare*, p. 101.

[25] Joseph S. Nye, *The Future of Power*, Public Affairs Press, New York, 2010.

[26] Joseph S. Nye, "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, 5:4, 2011, p. 20.

[27] Binxing Fang, *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*, Science Press & Springer, Singapore, 2018, p. v.

"cyber sovereignty" gained importance in global governance. Though the concept of cyber sovereignty may seem vague as a concept expressing the power and independence of states in cyberspace, the fact that the concept of sovereignty is clearly defined makes it possible for the concept of cyber sovereignty to gain meaning.[28] The understanding that states have sovereignty over their own territory and internal affairs has brought the principle of equality to the forefront and raised the issue of "sovereign equality of states". On the one hand, cyber sovereignty,[29] as a concept regarding the determination of ownership of rights over networks and space in which networks are involved, is independent of a territory. Thus, while the transboundary nature of cyberspace challenges the concept of sovereignty, the question of how sovereignty is possible in cyberspace remains uncertain. Researchers who claim that cyberspace is a field that is not subject to sovereignty highlight that cyberspace should have its own legal regulations instead of sovereignty. The absence of borders in cyberspace deprives the sovereign state of the ability to exercise power over a defined population and territory. Accordingly, cyberspace needs to develop its own regulatory system.[30] The affirmation by the UN General Assembly in 2015 that states must respect international law and the principles of sovereignty in the use of information and communication technologies, including cyberspace,[31] has made cyberspace visible as a new type and sphere of sovereignty.

Xinhuanet interprets cyber sovereignty as follows: *"internally, cyber sovereignty refers to independent development, supervision, and management of a state's own Internet affairs; and externally, cyber sovereignty refers to preventing a state's Internet from external invasion and attack."*[32] Fang, on the other hand, defines sovereignty in cyberspace as follows:

> *"Cyberspace sovereignty is a natural extension of state sovereignty in the cyberspace hosted by the ICT infrastructure located in the territory of a state; Thus, a state has jurisdiction (right to interface in data operation) over ICT activities (in respect of cyber roles and operations) present in cyberspace, ICT systems per se (in respect of facilities), and data carried by the ICT systems (virtual assets)."*[33]

Franzese suggests that state sovereignty might be possible in cyberspace owing to the physical infrastructures necessary for cyberspace and that this sovereignty should be considered an extension of the principle of territorial sovereignty.[34] Jensen also argues that cyberspace sovereignty is achievable when nations acknowledge each other's sovereignty and the right to advance their cyber capabilities independently.[35] On the one hand, the contradiction between the concept of cyber sovereignty and the spirit of the Internet stems from the fact that the Internet comprises unlimited interactions and connections.[36] Thus, it is difficult for countries to establish their own cyberspace. Winston Churchill's remark on the

[28] Marie and Patrice Robin, "Cyber Sovereignty", ETH Zürich, 2018, https://www.researchcollection.ethz.ch/bitstream/handle/20.500.11850/314398/Cyber-Reports-2018-01.pdf?sequence=1&isAllowed=y, accessed 17.05.2024.

[29] Fang, *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace,* p. 77.

[30] John P. Barlow, "A Declaration of the Independence of Cyberspace", Davos, 1996, https://www.eff.org/cyberspace-independence, 16.05.2024; Lawrence Lessig, *Code: Version 2.0*, Basic Books, New York, 2006.

[31] United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, No. 15-12404, United Nations, July 2015.

[32] Xinhuanet, "What Is 'Cyber Sovereignty'?", 2014, http://news.xinhuanet.com/politics/2014-07/10/c_126736910.htm, accessed 23.02.2024.

[33] Fang, *Cyberspace Reflections on Building a Community of Common Future in Cyberspace,* p. 83.

[34] Patrick W. Franzese, "Sovereignty in Cyberspace: Can it Exist?", *Air Force Law Review*, 64, pp. 1-42.

[35] Eric Talbot Jensen, "Cyber Sovereignty: The Way Ahead", *Tex. Int. Law J.,* 50, 2015.

[36] Hao Yeli, "A Three-Perspective Theory of Cyber Sovereignty*", PRISM*, 7:2, 2017, p. 109.

Iron Curtain may come to mind if an analogy explains this situation. The term "iron curtain" refers to the non-physical borders that divided Europe at the end of World War II, and it has evolved into a process in which some countries want to create digital iron curtains to protect their sovereignty and control public opinion.[37]

Considering the connotations of the concept of sovereignty, the fact that the Internet occupies a vast global area makes it difficult to apply the concept to cyberspace because it is an area that no one owns or controls. This issue is guided by thoughts about where the space dominated by states in cyberspace begins and ends. Heinegg claims that "*the integration of physical components of cyber infrastructure located on a state's territory into the global domain of cyberspace is not a waiver of territorial sovereignty*".[38] With such an approach, states have all kinds of rights over the cyber infrastructure in their areas of sovereignty. On the other hand, how actors define cyberspace boundaries is also linked to the type of cyber threats directed against the relevant country.

Another problem lies in the contradiction between the concept of cyber sovereignty and human rights. The notion of the Internet facilitating freedom of expression and the possibility of cyber sovereignty restricting the free flow of information does not match.[39] State sovereignty in cyberspace, which is envisioned as a space of freedom, has been brought to the forefront by cyber-attacks that are thought/alleged to be state-sponsored. The 2007 Estonia cyber-attack, the 2008 Georgia cyber-attack, and the 2010 Stuxnet attack on Iran paved the way for the emergence of cybersecurity as an essential security issue.[40] It is evident that this situation leads states to establish sovereignty and dominance in cyberspace.

Even though there is no comprehensive and binding legal text containing cyberspace, efforts in this direction might shed light on the issue. The Tallinn Manual is one of the documents including an assessment of cyber-attacks under the principle of non-use of force. The sentence *"a State must not conduct cyber operations that violate the sovereignty of another State"*[41] in Rule 4 of the said document assesses cyber operations in the context of sovereignty. The interpretation of this rule revolves around two bases when assessing the compatibility of cyber actions with international law: The extent to which the territorial integrity of the target state has been violated and whether this violation inherently involves interference or usurpation of governmental functions. Rule 4, which also expresses that states have internal and external sovereignty, legitimizes sovereignty in cyberspace by considering cyber operations preventing/ignoring another state from exercising its sovereign rights as a violation of such sovereignty.[42] Still, this rule does not disclose which cyber operations make the violation of sovereignty possible.

Moreover, the provisions of the Tallinn Manual on the relationship between cyber operations and sovereignty are in line with the 1970 "Declaration on Principles of International Law Friendly Relations and Cooperation among States" and the 1975 "Conference on Security and Co-operation in Europe Final Act" in terms of sovereignty principles. Nonetheless, the

[37] Eldar Haber and Lev Topor, "Sovereignty, Cyberspace, and the Emergence of Internet Bubbles", *Journal of Advanced Military Studies*, 14:1, 2023, pp. 144-145.

[38] Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, 89:123, 2013, p. 126.

[39] Hao, Ibid, p.110.

[40] Tuba Eldem, "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik", *Istanbul Hukuk Mecmuası,* 79:1, 2021, p. 350.

[41] Michael N. Schmitt, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, Cambridge University Press, New York, 2017, p. 17.

[42] Ibid, p. 17.

said document does not outline a clear framework for applying sovereignty principles in the cyber context.[43] The document also focuses on *jus ad bellum* principles and requires a more comprehensive view of cyber sovereignty.

According to a 2011 document published by the US government titled "International Strategy For Cyberspace: Prosperity, Security, and Openness in a Networked World", the following activities violate territorial sovereignty: "exploitation of networks, attacks on networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties, and privacy".[44] In this context, it is evident that the US has developed a governmental perspective preferring to use force against cyber actions, if necessary, and now considers cyberspace within the scope of the principle of sovereignty. The Chinese government also emphasizes that no violation of sovereignty in cyberspace will be tolerated. According to China, states should exercise jurisdiction over ICT infrastructure, resources, and data in their territory and have the right to protect themselves against attacks. Stating that the use of technology is possible, especially in the context of "interference in internal affairs", China has repeatedly underlined that states should participate in Internet governance equally.[45]

Following all these discussions, the perspective of this study will be to seek an answer to the question: "Is a theory of cyberspace dominance possible?". The insufficiency of international law in explaining cyberspace and cyber action fields and its inability to produce binding texts suggests whether discussing sovereignty in cyberspace from the perspective of geopolitical theories is possible. Though the concept of geopolitics refers to the visible and known areas such as land, sea, air, and space, it is possible that cyberspace-related approaches may emerge as a fifth area of dominance within the context of their potential to affect the tangible space. As a field outside geopolitics but with the potential to have geopolitical effects, cyberspace exists as a field where sovereignty and dominance are suggested. In an era in which scientific and technological developments have been shaping International Relations and all other disciplines, it may be necessary to open the phrase "whoever dominates cyberspace dominates the world" for discussion. However, the relationship of cyberspace, which is a virtual space, with global domination is a complex and multi-dimensional one. The dependence of technologies worldwide on digital infrastructures seems to disclose the superiority of those who rule cyberspace. States seeking to counter this phenomenon have been developing approaches that consider cyberspace dominance in terms of global dominance. Nonetheless, the understanding of power in cyberspace is distinct from the classical understanding of power, and countries with asymmetric power also stand out. In this context, a perspective on the control and dominance of cyberspace is planned, with the example of China in the conclusion section of the study.

[43] Dmitry V. Krasikov and Nadezhda N. Lipkina, "Sovereignty in Cyberspace: A Scholarly and Practical Discussion", *Advances in Social Science, Education and Humanities Research*, 498, 2020, pp. 157-158.

[44] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, 2011.

[45] Ministry of Foreign Affairs of the People's Republic of China, "China's Positions on International Rules-making in Cyberspace", 2021, https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html, accessed 01.10.2024.

2. China’s Cybersecurity Policies

About one-fifth of the 5.4 billion Internet users worldwide live in China. China’s Internet users increased by 24.8 million[46] and reached 1.05 billion in December 2023.[47] Nonetheless, an evaluation of the period from the country’s foundation in 1949 to its period of reform and opening to the outside world points out that the only goal was to maintain sovereignty and preserve the regime. At this point, it is observed that China has achieved a significant position in information technologies.

From the early stages of China’s digitalization, the government has taken on a regulatory role for online platforms. As early as 1994, before China was fully connected to the Internet, the State Council issued regulations on information system security, designating the Ministry of Post and Communications (MPS) to handle the matter. MPS published special regulations on Internet security in 1997, banning hacking, data corruption, and spread of malware.[48] The Chinese government recognizes the opportunities for economic growth, prosperity, and investment that the Internet brings but controls it in anticipation of political crises. Therefore, the content of all information sources is highly censored by the Government.[49]

As of the late 1990s, China has pursued a policy of “informatization” [*xinxihua*信息化], which covers using digital technology in all major areas of economic and social life and government operations.[50] Until 2014, China’s main body responsible for cybersecurity policy was the CCP State Informatization Leading Group (SILG), established in 2001 to guide national information technology development.[51] Thus, by moving digital policy to the highest priority level, the “cyber power strategy” (*wangluo qiang- guo zhanlue* 网络强国战略) has been encouraged to be created.[52] In 2003, China published a national strategy document on cybersecurity called Document 27. Initially classified, Document 27 envisaged an active defense, addressing issues such as protecting critical infrastructures, strong encryption, better coordination, and financing.[53]

China’s White Paper titled “Jointly Build a Community with a Shared Future in Cyberspace” sets out the country’s vision for global Internet development and management. The document underlines that the Internet has transformed the world into an interconnected structure and states that China supports a people-oriented approach and inclusive global governance. The White Paper also mentions China’s efforts for international cooperation to enhance Internet access for developing countries and fight against poverty, as well as international cooperation to create a safer cyberspace. The document calls for joint efforts to build a just and stable digital world.[54]

[46] Lai Lin Thomala, “Number of Internet users in China 2013-2023”, 2024, https://www.statista.com/statistics/265140/number-of-internet-users-in-china/, accessed 15.09.2024.

[47] Simon Kemp, “Digital 2023: China”, 2023, https://datareportal.com/reports/digital-2023-china, accessed 20.09.2024.

[48] State Council, “Provisional Management Regulations for the International Connection of Computer Information Networks of the People’s Republic of China”, Feb 1, 1996, https://chinacopyrightandmedia.wordpress.com/1996/02/01/provisional-management-regulations-for-the-international-connection-of-computer-information-networks-of-the-peoples-republic-of-china/, accessed 12.10.2024.

[49] Anne S. Y. Cheung, “The Business of Governance: China’s Legislation on Content Regulation in Cyberspace”, *International Law and Politics*, 38:1, 2006, p. 2-3.

[50] Weizhi Qu, *China’s Path to Information,* Cengage Learning Asia, Singapore, 2010.

[51] Jon R. Lindsay, “The Impact of China on Cybersecurity”, *International Security*, 39:3, 2014/15, p. 17.

[52] Rogier Creemers, “Cybersecurity Law and Regulation in China: Securing the Smart State”, *China Law and Society Review*, 6, 2021, p. 112.

[53] Mikk Raud, “China and Cyber: Attitudes, Strategies, Organizations”, NATO CCD COE, Tallinn, 2016, p. 11.

[54] Information Office of the State Council of the People’s Republic of China, June 8, 2010.

As of 2011, online security concerns have become more urgent, primarily through the proliferation of mobile devices and the emergence of the online platform and social media industry.[55] In 2014, in a tense environment created by the Edward Snowden incident, the Cybersecurity and Informatization Leading Group (CILG) was established, chaired by Xi Jinping. CILG contributes to Xi's effort to contain the Party discipline and respond to foreign cyber threats.[56] In the 2016 Outline of National Information Development Strategy, the Chinese authorities emphasized the importance of establishing a powerful cyber-nation, stating that there is a pressing need for it and that there should be no delay in addressing it.[57] In the same year, Xi Jinping made a speech at the "National Work Conference on Cybersecurity and Informatization" and defined cybersecurity as a "holistic" concept organically integrated into broader national security concerns, as "dynamic" requiring flexibility in management, as "open" emphasizing the need for foreign interaction and exchange, as "relative" indicating the need for priority setting rather than comprehensive perfection, and as "shared" requiring cooperation with non-state actors.[58] President Xi Jinping also emphasized the critical and immediate need for Internet security and informatization, equating these dual objectives to the essential elements of a bird's wings or an engine's wheels. The Chinese president also stated that there is no national security without Internet safety and that there can be no modernization without information.[59]

Stating that cybersecurity is inseparable from national security,[60] Beijing continues to develop national/international cybersecurity strategies and cooperation. Nonetheless, the government's lack of transparency hinders the coordination of cyber policies. Drafted in 2015 and published in 2016, the "Cybersecurity Law of the People's Republic of China" is a binding text on cybersecurity policies. The holistic approach that Xi talks about is clearly seen in this document.

> *"Cyberspace security (hereafter named cybersecurity) concerns the common interest of humankind, concerns global peace and development, and concerns the national security of all countries. Safeguarding our country's cybersecurity is an important measure to move forward the strategic arrangement of comprehensively constructing a moderately prosperous society, comprehensively deepening reform, comprehensively governing the country according to the law, and comprehensively and strictly governing the Party in a coordinated manner and is an important guarantee to realize the Chinese Dream of the great rejuvenation of the Chinese nation."*[61]

Article I of this law mentions objectives such as ensuring cybersecurity, protecting cyberspace sovereignty, public interest, and national security, and protecting the legal rights and interests of citizens, legal entities, and other organizations.[62] Adopting the principle

[55] Creemers, "Cybersecurity Law and Regulation in China: Securing the Smart State", p. 116.

[56] Lindsay, "The Impact of China on Cybersecurity", p. 17.

[57] The Central Committee of the Communist Party, "The 13th Five Year Plan for Economic and Social Development of the People's Republic of China (2016-2020)", 2016.

[58] Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informatization", April 19, 2016, https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/, accessed 04.10.2024.

[59] Xinhua, "Xi Jinping Leads Internet Security Group," February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm, accessed 04.10.2024.

[60] Creemers, "Cybersecurity Law and Regulation in China: Securing the Smart State", p. 112.

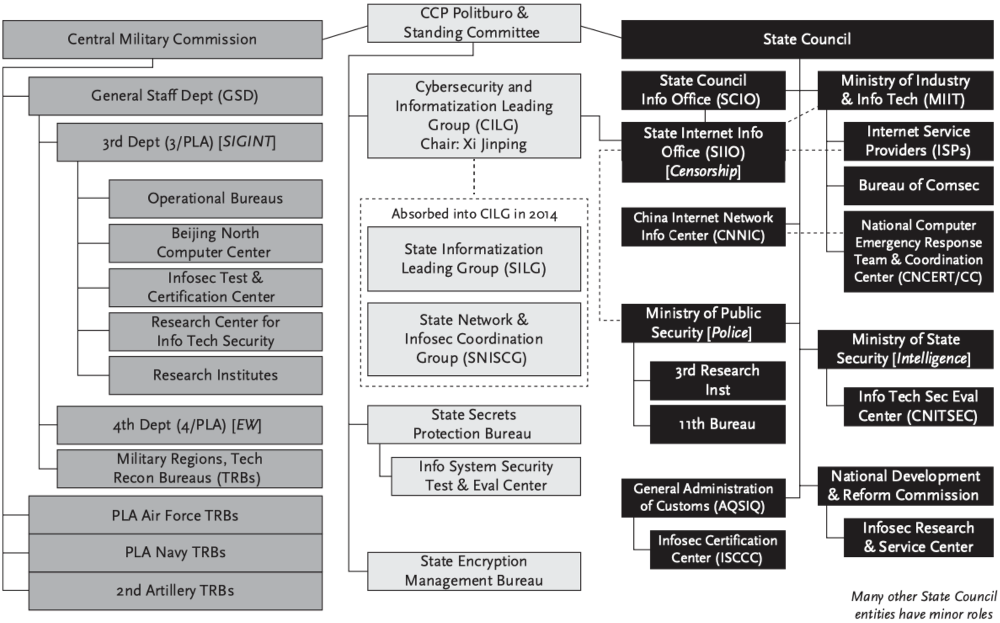
[61] Cyberspace Administration of China, "《国家网络空间安全战略》全文", 27 Dec 2016, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm, accessed 02.05.2024.

[62] The Standing Committee of the National People's Congress, "Cybersecurity Law of the People's Republic of China", July 11, 2016, http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode=, accessed 10.09.2024.

of national security of China's National Security Law, the Cybersecurity Law recognizes cyberspace sovereignty as the highest priority. Regulations achieve this goal by protecting the security of critical information infrastructure, network operations, and online information. In addition, the Chinese government cooperates with international efforts to aid the development of the Internet economy while safeguarding national cyberspace sovereignty. These legal objectives reflect a multi-dimensional cybersecurity perspective covering security and development interests.[63]

Though China has a centralized one-party government, in practice, it has a regionally and functionally fragmented structure. The Politburo, the highest-ranking organ of the Chinese Communist Party (CCP), is mainly headed by members of the Standing Committee and supported by "Small Groups of Pioneers" who work on an issue-by-issue basis to determine essential policies. The State Council manages the country's vast bureaucracy, implements policies, and regulates state-owned enterprises. On the one hand, the People's Liberation Army (PLA) depends on the party rather than the state and is a powerful political force in its own right. China's provincial governments enjoy considerable autonomy while competing with each other to win support and patronage from the CCP's top leaders. China's cybersecurity policy is shaped within this complex and non-transparent structure, and rapid technological developments in cyberspace progress much faster than policy coordination.[64] The following table shows China's national cybersecurity structure.

Table 1. China's National Cybersecurity System[65]


CCP Politburo & Standing Committee
Central Military Commission
State Council
General Staff Dept (GSD)
3rd Dept (3/PLA) [SIGINT]
Operational Bureaus
Beijing North Computer Center
Infosec Test & Certification Center
Research Center for Info Tech Security
Research Institutes
4th Dept (4/PLA) [EW]
Military Regions, Tech Recon Bureaus (TRBs)
PLA Air Force TRBs
PLA Navy TRBs
2nd Artillery TRBs
Cybersecurity and Informatization Leading Group (CILG) Chair: Xi Jinping
Absorbed into CILG in 2014
State Informatization Leading Group (SILG)
State Network & Infosec Coordination Group (SNISCG)
State Secrets Protection Bureau
Info System Security Test & Eval Center
State Encryption Management Bureau
State Council Info Office (SCIO)
State Internet Info Office (SIIO) [Censorship]
China Internet Network Info Center (CNNIC)
Ministry of Public Security [Police]
3rd Research Inst
11th Bureau
General Administration of Customs (AQSIQ)
Infosec Certification Center (ISCCC)
Ministry of Industry & Info Tech (MIIT)
Internet Service Providers (ISPs)
Bureau of Comsec
National Computer Emergency Response Team & Coordination Center (CNCERT/CC)
Ministry of State Security [Intelligence]
Info Tech Sec Eval Center (CNITSEC)
National Development & Reform Commission
Infosec Research & Service Center
Many other State Council entities have minor roles

[63] Aimin Qi, Guosong Shao et al., "Assessing China's Cybersecurity Law", *Computer Law & Security Review*, 34, 2018, p. 1344.

[64] Jon R. Lindsay, "Introduction: China and Cybersecurity: Controversy and Context", Jon R. Lindsay, Tai Ming Cheung & Derek S. Reveron (eds.), *China and Cybersecurity Espionage, Strategy and Politics in The Digital Domain*, Oxford University Press, Oxford, 2015, p. 7.

[65] Ibid., p. 9.

Many institutions affiliated with the State Council in China are responsible for implementing policies and regulating information technologies. The PLA possesses significant military and intelligence cyber capabilities, depends on the CCP, not the state, and has civilian regulatory responsibilities. Expenditures in China's information security industry have increased from $527 million in 2003 to $2.8 billion in 2011.[66] As of 2024, China, recently making science and technology a budget priority, aims to spend $51.5 billion in this field.[67] That is to say, information operations are one of the elements that the PLA considers vital for high-tech wars. In this context, the general strategic principle has been defined as "active defense".[68]

Protecting the Internet from harmful activities directed against national security or individual, social, or commercial interests is the primary goal for China. The privacy and security of citizens, the ability to compete fairly and efficiently in the economic order, and the preservation of social norms are essential goals of Chinese cybersecurity.[69] Actions designed to disrupt cyber-based infrastructure, disseminate information or images potentially damaging to society, governance, or the economy (such as pornography or misinformation), espionage, theft of private commercial data, as well as undermine the state's capacity to defend itself have led China to characterize cybersecurity as a national/international issue.[70] Accordingly, China continues to develop its own information technology (IT) industry and tries to remain isolated from international information technologies. China, maintaining a dominant position in the IT sector via its large state-owned enterprises, has been trying to protect the local market from external influences while developing its own standards in the field of software and hardware. For this reason, China's *sine qua non* of cybersecurity is to build an independent information technology.[71] On the one hand, the concept of information security in China attaches importance to Internet content beyond its technical security. However, the Western understanding of cybersecurity focuses more on technical threats. Because information security is a part of social stability in the country, China encourages efforts to strengthen censorship and surveillance infrastructure. Instead of defending against economic cybercrime and technical abuse by foreign intelligence services, China tends to mount a more consistent defense against perceived threats such as "terrorism, separatism, and extremism".[72]

3. China's Approach to Cyber Sovereignty and its International Implications

While China has an understanding of cyber sovereignty, which was initially developed by Western actors, it has continued tailoring it to its views on sovereignty and rejected US hegemony in the international system and other discourses on the global international environment. Therefore, China's understanding of cyber sovereignty is hybrid. Although the

[66] Lindsay, *The Impact of China on Cybersecurity*, p. 18.

[67] Dannie Peng, "China Makes Science and Tech a Budget Priority with 10% Jump in Spending During Two Sessions", March 6, 2024, https://www.scmp.com/news/china/science/article/3254290/china-makes-science-and-tech-budget-priority-10-jump-spending, accessed 03.08.2024.

[68] Lindsay, "The Impact of China on Cybersecurity", p. 31.

[69] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations", *China Leadership Monitor*, 42, 2013, p. 3.

[70] Zhong Sheng, "填补网络空间 '规则空白'", People's Daily, July 12, 2013, http://www.people.com.cn/24hour/n/2013/0709/c25408-22123842.html, accessed 09.10.2024.

[71] Hauke Johannes Gierow, "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses", *China Monitor*, 22, 2015.

[72] Lindsay, "Introduction: China and Cybersecurity: Controversy and Context", p. 11.

previous understanding influences the country, China has been shaped in accordance with its own internal discourses.[73]

Cyber sovereignty was included in a high-profile document for the first time in the 2010 White Paper, which is a summary of China's attitude towards the Internet.[74] Within the framework of the Shanghai Cooperation Organization and together with Russia, China has promoted reforms for Internet governance. In these reforms, the regulatory principle of "Internet sovereignty" is agreed on issues such as avoiding any unwanted interference in the information space of any state and regulating the Internet via an international forum such as the UN International Telecommunication Union. China and Russia proposed these two issues to the UN in September 2011 under the title of the "International Code of Conduct for Information Security".[75] This document is the first comprehensive and systematic proposal in this field and offers recommendations for creating international cyberspace rules.[76] The principles set out in this document are as follows: the non-use of information and communication technologies to apply hostile activities or acts of aggression and to threaten international peace and security, the affirmation by all States of their right and responsibility to defend their information spaces and network structures, critical information and network infrastructures against threats, disturbances, attacks, and sabotage under relevant laws and regulations, the establishment of multilateral, transparent, and democratic international governance of the Internet, the principle of respect for the rights and freedoms in the information and networking sphere to the extent that they comply with relevant national laws and regulations, the assistance to developing countries to improve their information and networking technologies, cooperating to combat network crime.[77]

At the Budapest Conference on Cyber Issues held in 2012, China suggested five principles to enhance international cooperation in cyberspace, reflecting "The Five Principles of Peaceful Coexistence". The first of these, sovereignty, has been defined as the right of each state to *"formulate its policies and laws in light of its history, traditions, culture, language, and customs*".[78] These principles show China's clear stance on global Internet governance. That is, sovereign nations should contribute equally to Internet governance by adhering to the principle of respect for the cyber sovereignty of other nations, the principle of cyber sovereign equality, the principle of non-interference in cyberspace, and the principle that all nations benefit each other in cyberspace.[79] Xi Jinping argues that this norm is derived from the sovereign equality principle covered in the UN Charter. Moreover, he defines the norm as not establishing hegemony but as providing non-interference and respect for each country's cyberspace management model and Internet policies.[80] All these discourses are related to the Chinese political discourses of the period, such as the Belt and Road Initiative, the Chinese Dream, and the Community of Common Destiny.

[73] Aleš Karmazin, "China's Promotion of Cyber Sovereignty Beyond the West", Šárka Kolmašová & Ricardo Reboredo (eds.), *Norm Diffusion Beyond the West Agents and Sources of Leverage*, Springer, Switzerland, 2023, pp. 61-62.

[74] Information Office of the State Council of the People's Republic of China, June 8, 2010.

[75] Lindsay, "The Impact of China on Cybersecurity", p. 38.

[76] People.cn, "填补网络空间 "规则空白"", July 9, 2013, http://www.people.com.cn/24hour/n/2013/0709/c25408-22123842.html, accessed 03.09.2024.

[77] Fang, *Sovereignty Reflections on Building a Community of Common Future in Cyberspace,* p. 187.

[78] Ministry of Foreign Affairs, "Statement at Budapest Conference on Cyber Issues", October 4, 2012, http://www.chinesemission-vienna.at/eng/zgbd / t977627.htm, accessed 10.08.2024.

[79] Fang, Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace, p. v.

[80] Xi Jinping, "在第二届世界互联网大会开幕式上的讲话", February 7, 2016, https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/, accessed 14.10.2024.

> *"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, including 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, connect, or support cyber activities that undermine other countries' national security."*[81]

In the above excerpt, which is a section from Xi Jinping's speech at the Second World Internet Conference in 2015, emphasis is put on the principle of sovereign equality, especially as a concept originating from the Westphalian system. Most importantly, this emphasis is made with an understanding that includes cyberspace, reminding the principles of peaceful coexistence with the term "cyber hegemony". Accordingly, applying the principle of cyber sovereignty to cyberspace shows that each country has the right to independently determine its own cyber development and regulation.

Lindsay claims that China's concept of cyber sovereignty has two main principles: First, it is to prevent the entry of unwanted influences into a country's "information space", thereby preventing citizens from being exposed to ideas and opinions that the regime depicts as harmful. Second, Internet management should be shifted to an international forum such as the UN.[82] China is heavily dependent on technology, just like other states. This situation makes the government concerned about the developments created by the Internet and the flow of information. China regards uncontrolled information as a threat to the regime. For this reason, while benefiting from the economic benefits of the Internet, it also maintains political control.[83] Thus, China's understanding of cyber sovereignty is basically defensive and reactive. The main goal is to maintain control over processes that may jeopardize the leadership position of the Chinese Communist Party. This understanding brings the stance of the party-state monopolizing the ability to regulate and dominate the online world and rejects all kinds of external interference.[84] The Chinese-type understanding of cyber sovereignty underlines cybersecurity by tightening control and management mechanisms over the Internet and content because the size of the country makes it difficult to control information.

International diplomacy and domestic developments have shaped China's active approach to cybersecurity and cyber sovereignty. Against the Western approach of "Internet freedom", China has opened the discussion of the unlimited authority of countries on the Internet. China especially considered the Tallinn Manual, mentioned in the first part of the study, a strengthening of Western control over the legal regulation of cyberspace.[85] Furthermore, in addition to the Shanghai Cooperation Organization, the BRICS countries (Brazil, Russia, India, China, and South Africa) have also been influential in negotiations related to cybersecurity. They have shaped the governance of the digital space based on respect for sovereignty and non-interference in their internal affairs. They also agree that international information security and digital sovereignty should be recognized as a new principle of international law and that the UN Member States support the Russian-proposed "UN Convention on International Information Security" and "Future UN Convention against

[81] Fang, *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace,* p. 173.

[82] Lindsay, "The Impact of China on Cybersecurity".

[83] Brigid Grauman, *Cyber-security: The Vexed Question of Global Rules*, Report by Security & Defense Agenda, 2012, p. 55.

[84] Creemers, "Cybersecurity Law and Regulation in China: Securing the Smart State", p. 129.

[85] Milton L. Mueller, "Against Sovereignty in Cyberspace"*, International Studies Review*, 22:4, 2020, pp. 779-801.

the Criminal Misuse of ICTs”. The essence of both documents is based on respect for the principle of state sovereignty in the digital environment. As a fundamental principle of international information security cooperation, it is particularly emphasized that each state has the right to determine norms and mechanisms to manage its information and cultural space under its national legislation.[86] From the perspective of the European Union (EU), international policies in cyberspace should be formulated through existing governance procedures, and a multi-stakeholder approach should be adopted. On the other hand, China argues that all governments should equally participate in international rulemaking in cyberspace rather than the status quo. According to China, this is the only way to protect the national interests and sovereignty of developing countries.[87]

So, how does China assess cyber sovereignty within the framework of international law? The document “China’s Views on the Application of the Principle of Sovereignty in Cyberspace”, published by the Chinese Ministry of Foreign Affairs, underlines that state sovereignty is legally binding under international law. This has been interpreted as follows: If a state encroaches on the inherent superiority and external independence of another state based on its national sovereignty, ICT infrastructure, organizations, activities, and data and information located on its territory, this constitutes an unjust act under international law. According to the document, *“relevant actions could include unauthorized infiltration of network systems in the territory or jurisdiction of another state, causing disruption or damage to the related infrastructure, or undermining a state’s exclusive sovereign rights in cyberspace. An ICT activity may simultaneously violate the principles of sovereignty, non-interference in internal affairs, and prohibition of the use of force”*.[88]

While China has made references to the concept of cyber sovereignty in all these assessments and platforms, the formalization and theorization of the concept have not yet been realized. As China’s primary goal is to balance the US hegemony in cyberspace, it is necessary to institutionalize cyber sovereignty.[89] Nonetheless, China’s definition and principles of cyber sovereignty stand out as a problem that mainly addresses anti-regime threats. The phenomenon of cyber sovereignty is at the heart of China’s cybersecurity policies. In this context, it is a mystery if China desires to seize the leadership of cyberspace with its contribution to the idea of cyber sovereignty. Perhaps China’s only goal is to ensure that it has great power and weight in cyberspace.

Conclusion

In the 21st century, countries are in a technological dilemma. The rise of information and communication technologies at an unpredictable pace makes it possible to access, use, change, or destroy them. At this point, cybersecurity has emerged as a crucial concept. On the other hand, cyber sovereignty refers to a state’s full authority and control within its own cyber infrastructure. The *sine qua non* factor for some states ensuring cybersecurity is the provision and maintenance of cyber sovereignty.

The documents, sources, and data discussed throughout the study point out China’s understanding of cyber sovereignty and how this understanding is shaped on international

[86] Alexander Ignatov, “BRICS Agenda for Digital Sovereignty”, February 14, 2024, https://moderndiplomacy.eu/2024/02/14/brics-agenda-for-digital-sovereignty /, accessed 20.08.2024.

[87] Cai Cuihong, “Global Cyber Governance: China’s Contribution and Approach”, *China Quarterly of International Strategic Studies*, 4:1, 2018, pp. 55-76.

[88] Ministry of Foreign Affairs of the People’s Republic of China, “China’s Views on the Application of the Principle of Sovereignty in Cyberspace”, p. 3.

[89] Karmazin, “China’s Promotion of Cyber Sovereignty Beyond the West”, p. 73.

platforms. China's approach also shows how cybersecurity has evolved in different ways and shaped the dynamics of the balance of power between states because its approach to cyber sovereignty is considered equal to cybersecurity and a part of national security. At the same time, China wants to have a say through its efforts to guide the global governance of cyberspace. Setting almost digital boundaries in this regard, China wants to achieve a strategic position in cyberspace competition within the framework of the principle of sovereign equality in cyberspace, based on the principles of the UN.

The fact that cyberspace cannot be regulated in an agreed manner within the framework of international law raises the question of the applicability of a theory of cyberspace dominance considering cyber sovereignty. Chinese and Russian recommendations on cyberspace governance in international platforms such as the UN demonstrate the need for institutionalization. The affirmation obtained from the UN General Assembly in 2015 on the subject of compliance with international law and sovereignty principles, including cyberspace, results from a parallel approach to the views of China and Russia.

This study does not seek an answer to whether cyber sovereignty is clearly possible. Instead, it focuses on how the concept of cyber sovereignty will play a role in the power struggle in the international system and how it will shape cybersecurity policies. Cyber sovereignty has the potential to transform the traditional understanding of sovereignty. Nevertheless, there are uncertainties regarding its effects and applicability in the international system. In this context, seeking control and dominance of cyberspace discloses a new geopolitical area of struggle in international relations. Instead of dominating cyberspace as a necessity of a system that has evolved to multi-dimensionality, standard international norms and policies should be shaped. The selection of China as a dominant example in the study points out that establishing dominance in cyberspace is a dynamic and multi-dimensional process.

More specifically, is a Chinese-led cyberspace dominance theory conceivable? While success in efforts to control cyberspace does not make it possible to achieve direct world domination, it can potentially increase China's influence in the international arena. China might develop more cybersecurity policies, conduct cyber investments, fight cyber threats, and encourage cyber diplomacy. Nonetheless, the unlikely prospect of cyberspace dominance must be integrated with military, political, economic, diplomatic, and other factors regarding the race for global leadership.

Conflict of Interest Statement:

The author declares that there is no conflict of interest.

References

Published Works

AIMIN Qia and GUOSONG Shao (2018). “Assessing China’s Cybersecurity Law”, *Computer Law & Security Review*, 34, 1342-1354.

BIÇAKCI Salih. (2019). “Siber Güvenlik ve Savunma”, *Güvenlik Yazıları Serisi*, 42, 1-8.

Central Committee of The Communist Party (2016). The 13th Five Year Plan for Economic and Social Development of the People’s Republic of China (2016–2020).

CHEUNG Anne S.Y. (2006). “The Business of Governance: China’s Legislation on Content Regulation in Cyberspace”, *International Law and Politics*, 38:1, 1-37.

COLLIER Jamie (2018). “Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision”, *Politics and Governance*, 6:2, 13-21.

CREEMERS Rogier (2021). “Cybersecurity Law and Regulation in China: Securing the Smart State”, *China Law and Society Review*, 6, 111-145.

CUIHONG Cai (2018). “Global Cyber Governance: China’s Contribution and Approach”, *China Quarterly of International Strategic Studies,* 4:1, 55-76.

DOĞRUL Mürsel YALÇIN Haydar and DAİM Tugrul U. (2023). “Cybersecurity Technology: A Landscape Analysis”, Tuğrul U. Daim & Marina Dabić (eds.), *Cybersecurity, Applied Innovation and Technology Management*, Springer, Cham.

DOUZET Frédérick and GERY Aude (2021). “Cyberspace Is Used, First and Foremost, to Wage Wars: Proliferation, Security and Stability in Cyberspace”, *Journal of Cyber Policy,* 6:1, 96-113.

ELDEM Tuba (2021). “Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik”, *İstanbul Hukuk Mecmuası*, 79:1, 347-378.

FANG Binxing (2018). *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*, Science Press & Springer, Singapore.

FRANZESE Patrick W. (2009). “Sovereignty in Cyberspace: Can It Exist?”, *Air Force Law Review*, 1-42.

GIEROW Hauke Johannes (2015). “Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses”, *China Monitor*, 22.

GRAUMAN Brigid (2012). “Cyber-Security: The vexed question of global rules, An independent report of cyber-preparedness around the World”, *Security & Defense Agenda (SDA)*.

GROHE Edwin (2015). “The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict”, *The John Hopkins University Applied Physics Laboratory*, 14:7, 1-25.

HABER Eldar and TOPOR Lev (2023). “Sovereignty, Cyberspace, and the Emergence of Internet Bubbles”, *Journal of Advanced Military Studies*, 14:1, 144-165.

HEKİM Hakan and BAŞIBÜYÜK Oğuzhan (2013). “Siber Suçlar ve Türkiye’nin Siber Güvenlik Politikaları”, *Uluslararası Güvenlik ve Terörizm Dergisi*, 4:2, 135-158.

JENSEN Eric Talbot (2015). “Cyber Sovereignty: The Way Ahead”, *Tex. Int. Law J.*, 276-304.

KARMAZIN Aleš (2023). “China’s Promotion of Cyber Sovereignty Beyond the West”, R. R. Šárka Kolmašová (eds.), *Norm Diffusion Beyond the West Agents and Sources of Leverage*, Springer, Switzerland, 61-78.

KAVITHA V. and PRETHA S. (2019). “Cyber Security Issues and Challenges-A Review”, *IJCSMC*, 8:11, 1-6.

KLIMBURG Alexander (2012). *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn.

KYRDODA Yuliia MARZİ Giacomo DABIC Marina and DAİM Tugrul U. (2023). “Cybersecurity Technology: An Analysis of the Topic from 2011 to 2021”, Daim, Tuğrul U. Daim & Marina Dabić (eds.), *Cybersecurity, Applied Innovation and Technology Management*, Springer, Cham.

LESSIG Lawrence (2006). *Code: Version 2.0*, Basic Books, New York.

LINDSAY Jon R. (2014/15). “The Impact of China on Cybersecurity”, *International Security*, 3:3, 7-47.

LINDSAY Jon R. (2015). “Introduction: China and Cybersecurity: Controversy and Context”, Jon R. Lindsay, Tai Ming Cheung & Derek S. Reveron (eds.), *China and Cybersecurity Espionage, Strategy and Politics in The Digital Domain*, Oxford University Press, Oxford, 1-26.

MEDEIROS Breno Pauli and GOLDONİ Luiz Rogério Franco (2020). “The Fundamental Conceptual Trinity of Cyberspace”, *Contexto Internacional,* 42:1, 31-54.

MUELLER Milton L. (2020). “Against Sovereignty in Cyberspace”, *International Studies Review*, 22:4, 779-801.

NYE Joseph S. (2010). *The Future of Power*, Public Affairs Press, New York.

NYE Joseph S. (2011). "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, 5:4,18-38.

RAUD Mikk (2016). China and Cyber: Attitudes, Strategies, Organizations, NATO CCD COE, Tallinn.

SAĞIROĞLU Şeref and ALKAN Mustafa (2018). *Siber Güvenlik ve Savunma*, Grafiker Yayınları, Ankara.

SCHMITT Michael N. (2017). *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, Cambridge University Press, New York.

SINGER P.W. and FRIEDMAN Allan. (2018). *Siber Güvenlik ve Siber Savaş* (trans. A. Atav), Buzdağı Yayınevi, Ankara.

SWAINE Michael D. (2013). Chinese Views on Cybersecurity in Foreign Relations, *China Leadership Monitor*.

The White House (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington.

United Nations General Assembly (July 2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations.

United Nations (2021). Cybersecurity in the United Nations system organizations Report of the Joint Inspection Unit, JIU/REP/2021/3.

VON HEINEGG and WOLFF Heintschel (2013). "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, 89:123, 123-156.

WU Chien-Huei (2021). "Sovereignty Fever: The Territorial Turn of Global Cyber Order", *Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht/Zeitschrift Für Ausländisches Öffentliches Recht Und Völkerrecht*, 81:3, 651-676.

QU Weizhi (2010). *China's Path to Informatization*, Cengage Learning Asia, Singapore.

YELI Hao (2017). "A Three-Perspective Theory of Cyber Sovereignty", *PRISM*, 7:2, 108-115.

Internet Sources

BAEZNER Marie and ROBIN Patrice (2018). "Cyberspace Sovereignty", https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/314613/20180907_MB_TA_Cybersovereignty_V2_rev.pdf?sequence=1&isAllowed=y, accessed 17.05.2024.

BARLOW John P. (1996). "A Declaration of the Independence of Cyberspace", https://www.eff.org/cyberspace-independence, accessed 16.05.2024.

Cyberspace Administration of China. "《国家网络空间安全战略》全文", 2016, December 27, https://www.cac.gov.cn/2016-12/27/c_1120195926.htm, accessed 02.05.2024.

Etymonline (n.d.). "Cyber-", https://www.etymonline.com/word/cyber-, accessed 25.01.2024.

IGNATOV Alexander. "BRICS Agenda for Digital Sovereignty", 2024, February 14, https://moderndiplomacy.eu/2024/02/14/brics-agenda-for-digital-sovereignty/, accessed 20.08.2024.

Information Office of the State Council of the People's Republic of China. "The Internet in China", 2010, June 8 , http://www.china.org.cn/government/whitepaper/node_7093508.htm, accessed 20.01.2024.

International Telecommunications Union (2008), "ITU-T X.1205: series X: Data Networks, Open System Communications and Security: Telecommunications Security: Overview of Cybersecurity", https://www.itu.int/rec/t-rec-x.1205-200804-i, accessed 20.05.2024.

JINPING Xi. "在第二届世界互联网大会开幕式上的讲话, 2016, February 7, https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/, accessed 14.10.2024.

JINPING Xi. "Speech at the Work Conference for Cybersecurity and Informatization", 2016, April 19, https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/, accessed 04.10.2024.

KEMP Simon (2023). "Digital 2023: China", https://datareportal.com/reports/digital-2023-china

KERRY John. Secretary of State, "An Open and Secure Internet: We Must Have Both", VOAnews, 2015, 18 May, https://www.voanews.com/a/text-of-john-kerrys-remarks-in-seoul-on-open-and-secure-internet/2776139.html, accessed 13.07.2024.

Merriam-Webster. (n.d.). "Cybersecurity", https://www.merriam-webster.com/dictionary/cybersecurity

Merriam-Webster. (n.d.). https://www.merriam-webster.com/dictionary/cybersecurity

Ministry of Foreign Affairs. "Statement at Budapest Conference on Cyber Issues", 2012, October 4, http://www.chinesemission-vienna.at/eng/zgbd/t977627.htm, accessed 22.01.2024.

Ministry of Foreign Affairs of the People's Republic of China. (n.d.). "China's Views on the Application of the Principle of Sovereignty in Cyberspace", https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

Ministry of Foreign Affairs of The People's Republic of China. (2021). "China's Positions on International Rules-making in Cyberspace", https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html, accessed 01.10.204.

PENG Dannie (2024). "China Makes Science and Tech a Budget Priority with 10% Jump in Spending During 'Two Sessions", https://www.scmp.com/news/china/science/article/3254290/china-makes-science-and-tech-budget-priority-10-jump-spending, accessed 03.08.2024.

PEOPLE.CN. "填补网络空间"规则空白", 2013, July 9, http://www.people.com.cn/24hour/n/2013/0709/c25408-22123842.html, accessed 03.09.2024.

SHENG Zhong (2013). "填补网络空间"规则空白", http://www.people.com.cn/24hour/n/2013/0709/c25408-22123842.html, accessed 09.10.2024.

Standing Committee of the National People's Congress. "Cybersecurity Law of the People's Republic of China", 2017, July 11, http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode=, accessed 10.09.2024.

STATE COUNCIL. "Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China", 1996, February 1, https://chinacopyrightandmedia.wordpress.com/1996/02/01/provisional-management-regulations-for-the-international-connection-of-computer-information-networks-of-the-peoples-republic-of-china/, accessed 12.10.2024.

The White House (2024). "2024 Report on The Cybersecurity Posture of The United States", https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf, accessed 14.07.2024.

THOMALA Lai Lin (2024). "Number of Internet Users in China from 2013 to 2023", https://www.statista.com/statistics/265140/number-of-internet-users-in-china/, accessed 15.09.2024.

XINHUA.NET. "Xi Jinping Leads Internet Security Group", 2014, February 27 , http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm, accessed 04.10.2024.

XINHUA.NET (2014). "What is Cyber Sovereignty?", http://news.xinhuanet.com/politics/2014-07/10/c_126736910.htm, accessed 23.02.2024.