POLITICON : Jurnal Ilmu Politik Vol.3 No.2 ; Hal 161- 184
Website : http://journal.uinsgd.ac.id/index.php/politicon
ISSN : 2685-6670 (Online)

Implikasi Ruang Siber Terhadap Geopolitik Negara

The Implication of Cyberspace Towards State Geopolitics

Iqbal Ramadhan
International Relations Department Universitas Pertamina, Gedung Griya Legita Lt.3
Kompleks Universitas Pertamina Jakarta
*Corresponding Author Email: iqbal.ramadhan@universitaspertamina.ac.id

Received: May 25, 2021; In Revised:Juny 27, 2021; Accepted: August 2, 2021

ABSTRAK

Perkembangan teknologi yang masif telah memengaruhi banyak dinamika perubahan sosial, politik dan ekonomi negara. Sebagai salah satu studi yang mengkaji interaksi antara dinamika politik dan geografi, studi geopolitik terkena implikasi dari perkembangan teknologi tersebut. Pada awal perkembangannya, studi geopolitik membahas tentang strategi dan kebijakan negara dalam memenangi pengaruh di wilayah tertentu. Geopolitik membahas tentang batas wilayah sebuah negara secara spesifik. Seiring berkembangnya teknologi, kemunculan ruang siber memberikan implikasi terhadap perkembangan geopolitik sebuah negara. Persaingan geopolitik tidak hanya terjadi di ranah fisik, tetapi juga ruang siber. Melalui artikel ini, penulis bermaksud untuk menganalisis pergeseran paradigma geopolitik yang bersifat fisik ke ruang siber. Melalui konsep geopolitik dan ruang siber, penulis menganalisis bagaimana eksistensi ruang siber dapat memberikan dampak politik khususnya rivalitas geopolitik antar negara. Pada artikel ilmiah ini, penulis menggunakan metode kualitatif khususnya teknik penulisan studi kasus untuk mengkaji fenomena ruang siber dan studi geopolitik. Berdasarkan hasil analisis dalam artikel ini, penulis berargumen bahwa geopolitik di ruang siber bersifat tanpa batas. Negara perlu menjadikan ruang siber sebagai domain politik mereka untuk menghindari konflik siber. Rivalitas geopolitik antar negara di ruang siber dapat berimplikasi terhadap dunia nyata. Salah satunya adalah penggunaan teknologi untuk dijadikan sebagai alat penekan kebijakan geopolitik negara lain. Karena keberadaan ruang siber yang tanpa batas tersebut, negara perlu menyusun tata kelola agar potensi konflik siber tidak berimplikasi terhadap geopolitik negara secara fisik. Penulis mengambil simpulan bahwa ruang siber perlu dipertimbangkan menjadi salah satu wilayah geopolitik sebuah negara, mengingat hampir seluruh dinamika kehidupan bernegara telah terintegrasi secara teknologi informasi.

Kata Kunci: Geopolitik, ruang siber, negara, konflik siber, tata kelola

ABSTRACT

Massive technological advancements have influenced many dynamics of the nation's social, political and economic changes. Geopolitical studies, as one of the

POLITICON : Jurnal Ilmu Politik Vol.3 No.2 ; Hal 161- 184
Website : http://journal.uinsgd.ac.id/index.php/politicon
ISSN : 2685-6670 (Online)

studies that investigate the interaction between political dynamics and geography, are exposed to the implications of these technological developments. At the outset of its development, geopolitical studies discussed the state's strategies and policies for gaining influence in specific areas. Geopolitics is the study of a country's boundaries. The emergence of cyberspace, along with the advancement of technology, has implications for a country's geopolitical development. Geopolitical competition takes place not only in the physical realm, but also in cyberspace. The purpose of this article is to examine the shift in the geopolitical paradigm from physical to cyberspace. The authors examine how the existence of cyberspace can have a political impact, particularly geopolitical rivalries between countries, using geopolitics and cyberspace concepts. This scientific article investigates cyberspace phenomena and geopolitical studies using qualitative methods, particularly case study writing techniques. The author contends that geopolitics in cyberspace has no borders, based on the findings of this article's analysis. To avoid cyber conflicts, states must make cyberspace their political domain. Geopolitical rivalries between states in cyberspace can have real-world consequences. One of them is the use of technology to suppress other states' geopolitical policies. Because cyberspace is infinite, the state must develop governance so that the potential for cyber conflicts does not have physical consequences for the country's geopolitics. Given that almost all dynamics of state life have been integrated into information technology, the author concludes that cyberspace should be considered one of a state's geopolitical areas.

Keywords: *Geopolitics, cyberspace, state, cyber conflict, governance.*

INTRODUCTION

Today's rapidly evolving technology has an impact on society's social, political, and economic system. Almost every aspect of human life is linked in the fast current of the Internet. Technology has evolved into the foundation of human social life. The advancement of technology has an impact on the advancement of science. It is impossible to deny that geopolitical issues, as one of the studies in International Relations, are also dragged into the flow of technological changes. Geopolitics was born out of a discussion about the connection and relationship between humans and the geography of the area (O Tuathail, 1996). As human culture evolves, geography becomes an important indicator of a society's ability to develop its strength capabilities (O Tuathail, 1996). Halford J. Mackinder, a pioneer in geopolitical studies, elaborated on geographical position with the possibility of developing a state's strength (McKinder, 1998). This can be seen in McKinder's development of the

Heartland theory, which asserts that a state that can control the world's island (Eurasia region) can control the entire world (McKinder, 1998). This theory, however, was rejected because it was too Western-oriented and imperialist (Power, 2010). Furthermore, classical geopolitical theory emphasizes ethnocentrism, masculinity, and the marginalization of third-world countries (Power, 2010).

Geopolitical studies become an insight or orientation for the state to carry out its foreign policy at the implementation level. Geopolitical studies became an indicator of the world's division of the West Block and the Ussr during the Cold War (Dodds, 2007). Winston Churchill emphasized in a speech at the end of the 1940s that the territory included in the Eastern Bloc was part of the "Iron Curtain" (Dodds, 2007). At the time, geopolitics was synonymous with superpowers controlling the world's territories in order to gain political and military advantages (Dodds, 2007). Furthermore, geopolitics is always associated with how geographical elements directly impact a state's political life (Flint, 2016). Geopolitical researchers can interpret how economic, political, and social interactions influence policy orientation by understanding the concept of geography (Flint, 2016). In geopolitical studies, for example, the location concept is defined as the characteristics of a place that correlate with the local concept (locale). Local is defined as a sociopolitical institution of society in a specific geographical area (Flint, 2016). A maritime society's social system and form of government, for example, will differ from an agrarian society's because their lifestyle is influenced by the geographical conditions in which they live (Flint, 2016). Geopolitics is more than just how a state controls a region (Power, 2010). Furthermore, geopolitics discusses the political benefits of developing inter-state cooperation among regions (Power, 2010). Geopolitics also investigates the population and flow of human movement, as well as the implications for the areas in which they live (Merchant, 2015).

The discussion of geopolitical issues has now shifted from a physical area to cyberspace. Sheldon (2014) described shifting geopolitical issues as a

result of the nation-prioritization state's of cyberspace as a part of its territory. Sheldon, on the other hand, stated that, aside from the invisible virtual world, conflicts in the virtual realm have consequences in the physical realm (Sheldon, 2014). Geopolitical issues must now be interpreted not only physically, but also digitally. Geopolitics no longer discusses the relationship between regions, politics, and economic instruments in developing regional investment (Ramadhan, 2018). Nonetheless, dominance and control of natural resources to achieve a country's geopolitical interests remains one of the issues addressed in this study (Ramadhan & Pratiwi 2020; Do et al 2018). Geopolitical contestation and competition to become a hegemon in an area, on the other hand, continue to play an important role in geopolitical studies (Ramadhan & Iskandar, 2020).

Apart from that, cyberspace has now become one of the most important domains in terms of geopolitics. According to the report compiled by Kausch (2017), cyber conflicts have implications for a state's geopolitical stability. In her case study, Kausch stated that geopolitical stability is dependent not only on physical relations between countries, but also on cyber relations (Kausch, 2017). He cited the Stuxnet attack on Iran's nuclear reactor enrichment by hackers allegedly from Israel as an example of how the two nations' relations were further complicated (Kausch, 2017). Finally, geopolitical stability became unstable, and tensions between state actors in the Middle East region are rising (Kausch, 2017). According to the report compiled by Public Private (2019), the geopolitical volatility of an area in the cyber realm can cause disruption. According to Public Private (2019), two actors, emerging actors and opportunistic actors, can pose a threat to geopolitical stability in the cyber realm. Emerging actors are state actors, terrorist groups, and criminal organizations capable of organizing and carrying out cyber attacks in a structured and organized manner (Public Private, 2019). Meanwhile, opportunistic actors have been linked to low-level criminal activity, with the primary goal of their activities being only short-term (Public Private, 2019).

However, the two actors mentioned above have the potential to destabilize geopolitical stability. The goal of writing this article is to explain how cyberspace affects the geopolitics of a state. Technology has now manifested itself as a tool for increasing the capability of state power. Furthermore, technological capabilities can be used as a bargaining tool by one country against another (Dunn-Cavelty & Egloff, 2019).

There are numerous definitions for geopolitical terminology. Colin Flint defines geopolitics as a study that connects a region's characteristics with its political dynamics (Flint, 2016). According to Flint, a geopolitical entity such as a state requires the ability to defend inhabited areas or expand areas beyond its borders (Flint, 2016). According to Dodds, this implementation was seen during the Cold War, namely the balance of power between two major powers fighting for dominance of global regions (Dodds, 2007). Saul B. Cohen, in contrast to Flint's assumptions, defined geopolitics as a constitutional science concerned with the management of territories through political doctrine (Cohen, 2015). According to Cohen, geopolitics is nothing more than a competition among countries to gain influence in a region by taking human geography and applied political science into account (Cohen, 2015). Cohen defined geopolitics as the interaction of the political process with the geographic order (Cohen, 2015). Cohen's geopolitical definition refers to many classical geopolitical ideas, including those of Haushoffer, Mackinder, Spykman, and Mahan (Cohen, 2015). Geopolitics cannot be separated from the role of the state in achieving power to become a hegemon in a region at the level of political implementation (Wu, 2018). In his research, Zhengyu Wu explained that in the context of classical geopolitics, the state would compete by balancing power. The state seeks to dominate and exert influence on land, sea, air, and other strategic areas such as the "Heartland" through the balance of power (Wu, 2018).

Following the end of the Cold War, international relations experts began to question the definition of geopolitics. Specifically, the geopolitical

definition, which firmly envisions imperialism and extols white supremacy (O Tuathail, 1996). In his book "Critical Geopolitics," O Tuathail questions the definition of geopolitics that emphasizes the aspect of "hard power" (O Tuathail, 1996). This critical geopolitics also emphasizes the importance of defining geopolitical terminology with non-political elements such as identity, race, gender, and even religion (Jones & Sage, 2010). Jennifer Hyndman, a critical geopolitical figure, has stated that the current definition of geopolitics is synonymous with war and violence (Jones & Sage, 2010). Conflicts resulting from a country's geopolitical expansion, he claims, frequently impact the suffering of noncombatants such as women and children (Jones & Sage, 2010). Geopolitical scholars such as Deborah Cowen and Neil Smith have even proposed a solution by deconstructing a geopolitical definition riddled with colonialism nuances (Cowen & Smith, 2009). They coin a new term, social geopolitics, to describe the study of the interaction between humans and geography, including political aspects as well as social and economic interactions (Cowen & Smith, 2009). Cowen and Smith even rejected a geopolitical definition of US influence that ridiculed other geopolitical actors (Cowen & Smith, 2009). They do, however, accept the concepts of space, power, and security (Cowen & Smith, 2009). They want the concept to be free of elements of regional colonialism (Cowen & Smith, 2009).

The author also discusses the concept of cyberspace in order to explain how countries interact geopolitically in cyberspace. Geopolitics is concerned with the interaction of how state agents control the land area, both physically and visibly (McKinder, 1998). Land and geopolitical space also cover the country's political ties to the sea and air space (Sobaruddin et al., 2017; Henry, 2014). Cyberspace is a network of digital activity that connects physical space and cyberspace (Riordan, 2019). Cyberspace, in Riordan's opinion, correlates with a country's geopolitical policies. All human activities, referred to as "human domains," are found in cyberspace (Riordan, 2019). This domain connects human activities to cyberspace technology and is in touch with a

country's geopolitical interests (Riordan, 2019). In their book "Mapping Cyberspace," Martin Dodge and Rob Kitchen define cyberspace as the geography of an information society (Dodge & Kitchin, 2001). This reason is inextricably linked to the diverse content of cyberspace. Every minute, millions of digital activities take place in cyberspace (Dodge & Kitchin, 2001). Cyberspace frequently intersects with a country's geopolitical interests. Cyberspace is devoid of territorial boundaries. However, cyberspace causes a change known as "global culture" (Dodge & Kitchin, 2001). The exchange of political, economic, and cultural information compels the government to map the scope of its interests in cyberspace (Dodge & Kitchin, 2001). Another way to define cyberspace is as a global domain with networks connecting hardware, software, and data packages (Tsagourias, 2015). Cyberspace must technically have three layers: software (computers, cable circuits, IT infrastructure), software (operating programs), and data packages (Tsagourias, 2015). When interpreted as sovereign territory, cyberspace describes how the state can control and exercise its authority in the same way that physical space is used to legitimize its policies (Tsagourias, 2015). The author will examine how geopolitics and cyberspace concepts relate to one another, as well as the implications for existing state relations.

State interactions in cyberspace have indirect physical geopolitical implications. Furthermore, cyber is one of the geoeconomics instruments that the state can use to achieve its geopolitical objectives (Blackwill & Harris, 2017). This article will examine the implications of cyberspace for a state's and its region's geopolitical stability. The state's geopolitical problem is that cyberspace is a region without borders (Sheldon, 2014). As a result, a country's geopolitical stability in the cyber realm must consider what kind of governance can maintain its security interests in a world without borders. The existence of cyber territory cannot be avoided by the state. As a result, countries must pay as much attention to these domains as they do to physical areas.

POLITICON : Jurnal Ilmu Politik Vol.3 No.2 ; Hal 161- 184
Website : http://journal.uinsgd.ac.id/index.php/politicon
ISSN : 2685-6670 (Online)

RESEARCH METHOD

The author of this scientific article employs qualitative methods as a method of analysis. Qualitative methods are used to analyze a phenomenon or scientific topic through the use of narrative or language as a means of scientific thought (Hammarberg et al., 2016). Language is commonly used as an analytical tool in qualitative scientific articles (Hammarberg et al., 2016). To investigate geopolitical issues, the author employs a literature review approach. A literature review is a method for answering research questions by combining findings and empirical studies from previous studies (Snyder, 2019). A scientific article writer can draw conclusions based on scientific references by conducting a literature review (Snyder, 2019). The authors used a semi-systematic review approach in particular (Snyder, 2019). Because it employs narration as an analysis tool, this type is closely related to qualitative methodology (Snyder, 2019). Furthermore, the type of "semi-systematic review" is appropriate for use in scientific articles that seek to identify research themes, answer problem formulations through the lens of specific scientific concepts and theories, and identify the components of a theory (Snyder, 2019). In this scientific article, the author also employs a case study writing technique. Case studies can be interpreted as issues of politics, security, or economics involving interactions between state and non-state actors (Roselle & Spray, 2012). Creswell explained in the case study writing technique that secondary data must be obtained from credible sources (Creswell, 2014). Creswell suggests obtaining scientific articles from reputable sources such as PubMed, Scopus, or Dimensions (Creswell, 2014). Furthermore, the authors include the element of "reflectivity," which is the analysis results in the form of the author's point of view on a case based on references or scientific data (Creswell, 2014).

RESULT AND DISCUSSION

Previous research is compiled by the author in order to explain research gaps that can be further researched and developed. To compile this

POLITICON : Jurnal Ilmu Politik Vol.3 No.2 ; Hal 161- 184
Website : http://journal.uinsgd.ac.id/index.php/politicon
ISSN : 2685-6670 (Online)

previous research, the authors conducted a bibliographic search using Dimensions and Crossref databases. According to Creswell (2014), a researcher can conduct scientific research using a credible database such as Pubmed, Scopus, Dimensions, or Crossref. The author also employs the VosViewer application to map out and identify research gaps that can be filled. The authors obtained geopolitical research written between 2012 and 2021 from Dimensions' database. The authors downloaded 2,500 bibliographic documents after conducting their research. The author then employs VosViewer to determine the bibliographic document threshold. As a result, 237 bibliographical documents are used to explain geopolitical issues. The following figure 1 depicts the mapping of previous research:

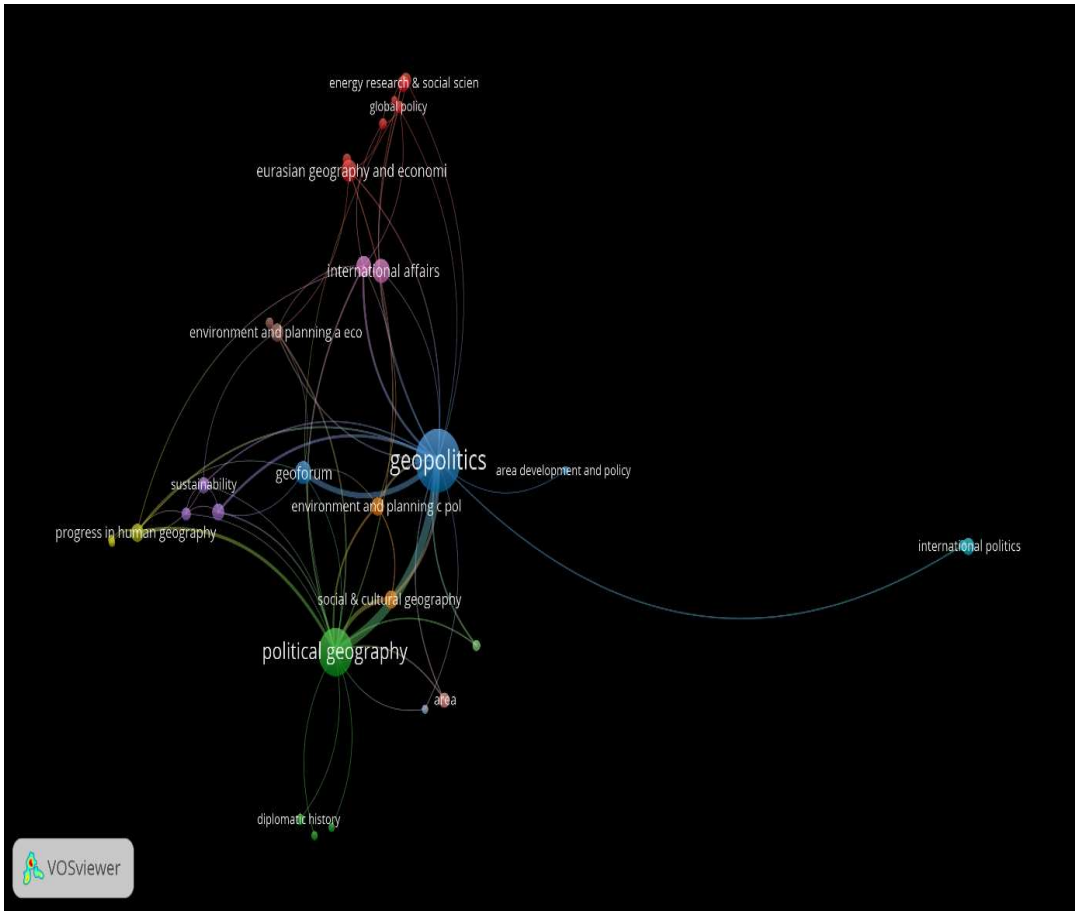

Figure 1. Mapping of Geopolitics' Previous Study

Source: (VosViewer, 2021)

POLITICON : Jurnal Ilmu Politik Vol.3 No.2 ; Hal 161- 184
Website : http://journal.uinsgd.ac.id/index.php/politicon
ISSN : 2685-6670 (Online)

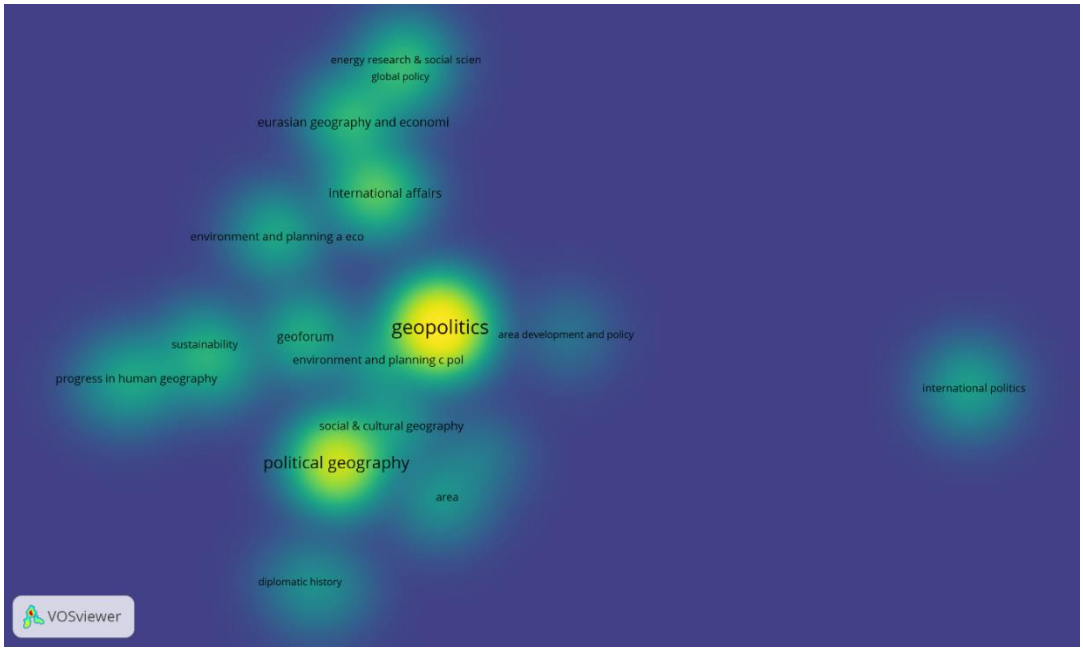

Figure 2. Research Density of Geopolitics' Previous Study

Source: (VosViewer, 2021)

Previous research on geopolitics has a lot to do with other issues or topics, as shown in Figure 1. A good example is the bibliography of geopolitics research, which contains a lot of information about geopolitics and sustainability (sustainability). There is also research that examines the relationship between international politics and geopolitics. Furthermore, some studies address geopolitical issues in regions such as Eurasia and Asia. In contrast, the author includes a mapping of the density level of geopolitical research in Figure 2. A light color in the image indicates that the topic has been discussed frequently. Geopolitical studies and political geography are the most frequently discussed topics in scientific journals from 2012 to 2021, according to the graph above. Another example is geopolitical issues intertwined with international issues, both of which are frequently discussed in scientific journals. Geopolitics and cyberspace, based on the two images above, have not been discussed or are not yet being discussed in scientific writing. As a result, the author will investigate the relationship between geopolitical issues and cyberspace in this paper.

The author will compare three studies that specifically discuss

geopolitical studies with cyberspace in the previous study. Researchers apply the basic assumptions of previous research analysis by focusing on the research background, issues or problems discussed, and differences between the research and the author's research (Creswell, 2014). The first study discussed was Ron Deibert's "The Geopolitics of Cyberspace After Snowden". Deibert explained in this study that the geopolitical constellation in cyberspace changed dramatically after the Snowden incident (Deibert, 2015). Deibert's research explains how the US government's role in implementing PRISM policies can disrupt the geopolitical stability of countries in other regions (Deibert, 2015). The study goes over the PRISM policy, which is the activity of spying on and infiltrating the entire global internet network for the benefit of the United States of America (Deibert, 2015). As a result of the Snowden incident, European Union member countries issued separate policies to protect their geopolitical interests from spying for the US government (Deibert, 2015). This previous research differs from the author's scientific article in that it does not address the PRISM policy or the Snowden incident specifically.

"The Geopolitics of Cyberspace: A Diplomatic Perspective" is the title of the second study mentioned in this article. This study examines case studies of the United States, Russia, and China in implementing their geopolitical policies in cyberspace (Riordan, 2019). Riordan explained the United States' position as an essential hegemon in technology during the analysis stage (Riordan, 2019). Given the United States' current status as the world's sole authority, their policies are also visible in cyberspace. Their activities can be traced back to the United States government's efforts to monitor internet activity around the world via their agency, the NSA or National Security Agency (Riordan, 2019). This activity appeared to emphasize the importance of the United States' geopolitical presence, both physically and virtually (Riordan, 2019). The United States' geopolitical influence can be seen physically in all regions of the world. This is what the United States wishes to achieve: their influence

must be felt even in a space without boundaries (Riordan, 2019). In terms of Russia's geopolitical implementation, they tried to maintain its influence in former Soviet Union states (Riordan, 2019). Russia, for example, has carried out numerous cyberattacks on critical infrastructure in Ukraine, Georgia, and Estonia (Riordan, 2019). Russia launched the cyberattack as a form of protest after its bilateral relations with the former Soviet Union failed to reach an agreement. The cyberattack emphasized Russia's overwhelming superiority and became a symbol of superiority over the former Soviet Union (Riordan, 2019). Meanwhile, from a geopolitical standpoint, China is attempting to be independent and free of Western influence (Riordan, 2019). Implementing the "Great Firewall of China", for example, emphasizes that China seeks to protect its cyber interests independently from any actor (Riordan, 2019). This policy represents a step toward China's technological independence from Western countries (Riordan, 2019). The difference in this research is that it will not focus on a single state actor, but will instead discuss the implications of the geopolitical shift from the physical to the virtual realm, as well as the potential for conflict and governance in the cyber domain.

The previous research to which the author refers is John B. Sheldon's Geopolitics and "Cyber Power: Why Geography Still Matters". Sheldon explains how cyber conflict affects the state's physical geopolitical interests in this study (Sheldon, 2014). Sheldon explained in one of his analyses that a state affected by cyber attacks has an impact on the areas under its influence (Sheldon, 2014). The cyber attack on Iran's nuclear reactor in Natanz, for example, is a form of disruption from Iran's political opponents in order to prevent Iran from becoming a hegemon in the Middle East (Sheldon, 2014). Another case in point is China's use of cyber spying to steal technology from developed countries such as Europe and the United States (Sheldon, 2014). China is attempting to develop domestic technology while also breaking away from Western influence through these spying activities (Sheldon, 2014). With this technological independence, China seeks to emphasize that it is a key

player in the global geopolitical landscape, both physically and virtually (Sheldon, 2014). Sheldon also discussed the possibility of cyber conflict and its impact on the integration of smart city technology developed by many countries (Sheldon, 2014). This study is similar in its explanation of the paradigm shift from physical geopolitics to cyberspace and future potential conflicts. The author's scientific articles, on the other hand, will explain how important governance is in preventing geopolitical disruption in a country or region.

At this point, the author will discuss about the relationship between geopolitics and cyberspace. The fact that cyberspace is a part of a country's domain must be explained first. According to Blackwill and Harris, information technology has integrated countries' entire social, political, and economic lives (Blackwill & Harris, 2017). They explained how the state could use technology to advance its geopolitical interests (Blackwill & Harris, 2017). For example, Blackwill and Harris argue that a well-planned cyber-attack on state infrastructure jeopardizes the state's and the region's stability (Blackwill & Harris, 2017). In his report, "Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East," Kausch emphasized the importance of protecting cyberspace in order to avoid geopolitical conflicts in the Middle East region (Kausch, 2017). According to Kausch's writing, the geopolitical instability in the Middle East is linked to both physical and cyberspace conflicts.

The rivalry between Iran, Saudi Arabia, and Israel exemplifies geopolitical competition in both the physical and cyber spheres (Kausch, 2017). The cyberattack that brought Iran's nuclear reactor in Natanz to a halt is empirical proof of Israel's reluctance to regard Iran as a significant geopolitical power in the Middle East (Sheldon, 2014). Stuxnet, a sophisticated computer virus, was responsible for the nuclear reactor's paralysis (Ramadhan, 2017). Iran responded to the cyberattack by crippling Saudi Aramco's technological infrastructure (Sheldon, 2014). Iran has rivalries with Israel and Saudi Arabia in the Middle East's geopolitical landscape. Meanwhile,

Iran's foreign policy is frequently at odds with that of the US and its allies. Not only that, but Iran and Saudi Arabia are competing to become the sole hegemon in the Middle East's geopolitical contestation. Both are the most powerful countries in the Middle East, competing for influence through political, military, and economic means (Ramadhan & Iskandar, 2020).

The eternal and massive nature of cyberspace's territory is the main issue. State conflicts in cyberspace, on the other hand, have implications for geopolitical stability in the physical sphere. What makes something like that possible? Apart from the examples given above, geopolitics is primarily a philosophy and a state perspective (Kelly, 2006). According to O' Tuathail, geopolitics is a philosophy that is sometimes used to legitimize expansionist states (Kelly, 2006). Geography or territory is not limited to objects visible to the naked eye. More specifically, O'Tuathail emphasized that geography for an expansionist country is a medium used to expand communication or facilitate war logistics (Kelly, 2006). According to O'Tuathail's viewpoint, there is the possibility of conflict and geopolitical competition in both the physical sphere and cyberspace. Cyberspace, due to its borderless nature, blurs the physical boundaries typically seen within a country's borders (Mueller, 2019). The lack of physical boundaries complicates the possibility of a state's geopolitical conflict. The existence of sovereignty enables a state to manage its territory autonomously. This, however, does not apply in cyberspace. Contradictory to the Westphalia Agreement in 1648, the state no longer recognizes territorial boundaries (Mueller, 2019). When a country must engage in cyberspace conflict to achieve its geopolitical interests, the peaceful resolution that must be achieved becomes even more difficult. Users can access the internet anonymously in cyberspace (Ramadhan, 2019). This anonymous function eventually leads to asymmetrical conflicts.

One thing to keep in mind is that the geopolitical structure is divided into three parts. According to Cohen's book, the main pillars that support geopolitical stability are "geostrategic realm," "geopolitical region," and

"national states" (Cohen, 2015). Cohen believes that the state is critical to maintaining geopolitical stability, both regionally and globally. In the context of geopolitics and cyberspace, the state requires special consideration in managing its life dimensions responsibly in the face of various threats that have the potential to disrupt geopolitical stability. It is important to note that threats in cyberspace are classified as either structured or unstructured (Dunn-Cavelty, 2010). Structured threats have long-term, predictable consequences that can destabilize geopolitical stability. Structured cyber attacks are typically planned by established professionals and organizations such as states, criminal organizations, or terrorist organizations (Dunn-Cavelty, 2010). Meanwhile, unstructured attacks are sporadic and have a short duration. This attack is distinguished by its use of illegal intrusion to alter the appearance of internet sites (Dunn-Cavelty, 2010). Regardless, the state must safeguard itself against geopolitical disruption in cyberspace. Some experts even propose that cyberspace be localized (Cornish, 2015). Westphalianization is primarily concerned with promoting the establishment of state boundaries in cyberspace. Cyberspace is now recognized as a shared space that cannot be contained within geopolitical boundaries (Cornish, 2015). However, in order to avoid various types of geopolitical disruption, several countries have begun to include cyberspace as part of their jurisdiction (Shen, 2016).

The state must unquestionably be prepared to deal with any type of cyberspace disruption. Countries interact in cyberspace in the same way they interact in the physical realm, namely through conflict and cooperation. Countries can employ the "self-help" strategy pioneered by the school of realism (Ramadhan, 2019). In this context, countries can improve their technological capabilities to protect themselves from cyber attacks of other countries. As a result, countries must develop human resource capabilities and technological innovation in order to compete in cyberspace (Ramadhan, 2019). Deterrence strategies can be used by countries with advanced

technology to prevent threats from other countries (Kassab, 2014). During the Cold War, deterrence strategies in geopolitical studies were common. NATO's and the Warsaw Pact's division of European political geography is tangible evidence of the superpower establishment's contests (Cohen, 2015). Kassab explained that the Cold War-style deterrence pattern could be used in the cyber realm to win the cyber and geopolitical space competition. Deterrence strategies can be put into action by developing practical technology. The goal is the same as in the physical domain, which is to deter their political adversaries (Kassab, 2014). This "self-help" pattern is heavily influenced by the state. As a result, the state's efforts to win geopolitical contestation in cyberspace are primarily focused on maximizing military, economic, and technological strength (Isnarti, 2016).

The Chinese government's commitment to making its country technologically independent and free of other countries is a clear example of this "self-help" implementation (Riordan, 2019). The Chinese government fully recognizes the significance of internet sovereignty in defending their cyberspace territory (Zeng et al., 2017). Cyber espionage, cybercrime, and cyber warfare are all terrifying threats to China's national interests. The reason for this is inextricably linked to the Snowden incident, which involved spying on all of the world's traffic. To ensure that China's geopolitical interests are not jeopardized, Xi Jinping's government is daring to implement modernisation in cyberspace (Zeng et al., 2017). The Chinese government encourages the country to be self-sufficient in the field of technology through the policy of "The Great Firewall of China." They recognize that technology can be used as a political tool to thwart a country's policies (Riordan, 2019).

Geopolitical stability is not solely dependent on a country's individual capabilities. From the standpoint of liberalism, the conflictual pattern promoted by the realism school is not entirely correct. This school emphasizes cooperative patterns in mitigating and resolving problems encountered together (Navari, 2013). According to Buzan and Weaver, the geopolitical

stability of a region can be seen in the pattern of "amity" and "enmity" among the region's countries (Buzan & Weaver, 2003). If countries' interaction patterns are hostile, the geopolitical situation in the region is likely to be conflictual (Buzan & Weaver, 2003). Conversely, if the interaction pattern is friendly, the cooperative relationship is more dominant (Buzan & Weaver, 2003). Furthermore, Navari explained that the state's problems are often the same. However, not every country is capable of problem solving. Sometimes, cooperative interactions between countries can help to solve these problems (Navari, 2013). As a result, liberalism believes that the state's geopolitical and cyberspace problems can only be solved through cooperation.

An empirical example is ASEAN-initiated cybersecurity cooperation in Southeast Asia, which aims to maintain geopolitical and geoeconomic stability (Ramadhan, 2020). The most difficult challenge in maintaining their geopolitical and geoeconomic stability is developing cybersecurity norms and rules that can be applied to each member country (Ramadhan, 2020). Southeast Asia has undeniably been transformed into an economically and politically integrated region. To maintain this stability, ASEAN is committed to ensuring the security of their cyberspace, which has implications for Southeast Asia's geopolitical situation (Ramadhan, 2017). In addition, ASEAN faces challenges in protecting its critical infrastructure from cyber attacks and transnational crimes perpetrated by terrorist groups and international criminal organizations (Heinl, 2014; Sieber & Neubert, 2017). Meanwhile, in the Eurasia region, countries like Russia, China, and Central Asian countries work together to maintain geopolitical stability in cyberspace. The region's countries create a code of conduct known as the "International Code of Conduct for Information Security" (Assaf et al., 2020). The coalition was formed because Russia, China, and Central Asian countries have geopolitical and geoeconomic interests, particularly in gas exploration. The country is a member of the "Shanghai Cooperation Organization," also known as the SCO (Ramadhan & Pratiwi, 2020).

Regardless of state policies implementing conflict or competition strategies, cyberspace governance is still required. A country's geopolitical position is fragmented in cyberspace (Fernández, 2020). Efforts to incorporate cyberspace into the geopolitical domain are ongoing. However, cyberspace is a highly connected public space. As a result, the lines of state authority in cyberspace are becoming increasingly blurred (Tsagourias, 2015). An important step in analyzing a country's geopolitical policies in cyberspace is the domestication, localization, or westphalianization of state authority in cyberspace; the Turkish government did the same as the Chinese government, which domesticated cyberspace. The Turkish government is developing a cyberspace security policy model through the Ministry of Transport and Infrastructure in order to protect their critical infrastructure (Eldem, 2020). Aside from the public domain of cyberspace, the state has the authority to protect its geopolitical interests in cyberspace (Khanna, 2018). When state security in cyberspace is jeopardized, they have the authority to defend their interests. As a result, the state must have a standard cyberspace security regulation in place so that the disruption does not interfere with geopolitical stability (Khanna, 2018). The majority of state positions are currently classified as "high-technology states" (Spiegel, 2000). It means that the majority of countries have evolved to combine the Westphalia-style state model with technological sophistication (Spiegel, 2000). In this stage, technology is the backbone of government operations (Spiegel, 2000). Countries must assert their authority in cyberspace and improve their technological capabilities as a matter of course. After all, technology can be used as a political tool to suppress geopolitical positions as well as a medium for balancing the power of the state (Dunn-Cavelty & Wenger, 2020).

When individual countries have decided on cyberspace governance, they must promote it at the inter-state level. In geopolitics, the existence of cyberspace governance is a process that brings all stakeholders together to form a mechanism for formulating policies related to specific issues (Glen,

2014). Given the highly heterogeneous nature of cyberspace, such governance must be cross-sectoral. Carol M. Glen stated that these governance principles must be structured based on the interests of the state, international organizations, businesses, and civil society (Glen, 2014). However, it appears that the conflict over the boundaries of state politics in cyberspace is a new issue. Particularly encouraging humanists who want cyberspace to be designated as a "common heritage" area. The area must be free of sovereignty claims, and any geopolitical influence and activities conducted there must be based on peace and prosperity for humanity (Klinger, 2020). Nevertheless, cyberspace governance to maintain the country's, region's, and global geopolitical integrity cannot be ruled out. However, cyberspace governance, such as that provided by the UNGGE (United Nations Group of Governmental Experts), is required to ensure that states do not recklessly misuse technology (Corn & Taylor, 2017). According to the UNGGE declaration, cyber governance must strike a balance between state sovereignty and international law (Corn & Taylor, 2017). In addition to UNGGE, countries can adopt the Tallinn Manual's behavior rules for state activities in cyberspace. The criteria for violating state sovereignty in cyberspace, according to these guidelines, are illegal infiltration or intrusion of information technology systems and violations of the country's territorial integrity (Schmitt & Vihul, n.d.). As a result, the state must have an intrusion detection system developed independently or through international cooperation (Ramadhan, 2019). Although the Tallin Manual and the UNGGE are not perfect governance measures for addressing geopolitical friction in cyberspace, the state should use them as a guideline. This action is required to ensure that cyberattacks that disrupt geopolitical stability, such as the Russian cyberattack on Estonia and the intrusion of North Korean hackers into the United States, do not occur again (Ramadhan, 2017).

CONCLUSION

Based on the simple analysis presented above, the authors conclude

that geopolitical conflict in cyberspace has real-world consequences. The Russian cyberattack on Estonia appeared to highlight the country's reluctance to relinquish its influence on former Soviet Union territory. Furthermore, the rivalry between Iran, Saudi Arabia, and Israel persists not only in physical space but also in cyberspace. They all want to be the winners of the Middle East's geopolitical competition. The intangible boundaries of cyberspace are difficult to define. It has an impact on overlapping country interactions and has geopolitical implications. The state requires governance to ensure that geopolitical friction in cyberspace does not become a long-term issue. Indeed, the state is finding it difficult to define authority in cyberspace, as evidenced by the emergence of several parties seeking to remain neutral in cyberspace. However, governance is still required in order to reduce the country's geopolitical competition in cyberspace and prevent it from spilling over into the real world.

BIBLIOGRAPHY

Assaf, A., Moshkinov, D., & Group, "International Law in The Digital Age" Research and Study. (2020). Contesting sovereignty in cyberspace. *International Cybersecurity Law Review*, *1*, 115–124. https://doi.org/Sovereignty · Cyberspace · Territory · Cyber-attack · Function theory

Blackwill, R. D., & Harris, J. M. (2017). *War by Other Means: Geoeconomics and Statecraft*. USA: Council on Foreign Relations.

Buzan, B., & Weaver, O. (2003). *Regions and Powers*. New York: Cambridge.

Cohen, S. B. (2015). *Geopolitics: The Geography of International Relations*. United Kingdom: Rowman & Littlefield.

Corn, G., & Taylor, R. (2017). Concluding Observations on Soverignty in Cyberspace. *AJIL Unbound*, *111*, 282–283. https://doi.org/doi:10.1017/aju.2017.77

Cornish, P. (2015). Governing cyberspace through constructive ambiguity. *Survival*, *57*(3), 153–176. https://doi.org/10.1080/00396338.2015.1046230

Cowen, D., & Smith, N. (2009). After geopolitics? From the geopolitical social

to geoeconomics. *Antipode*, *41*(1), 22–48. https://doi.org/10.1111/j.1467-8330.2008.00654.x

Creswell, J. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th Eds)*. London: SAGE.

Deibert, R. (2015). The geopolitics of cyberspace after snowden. *Current History*, *114*(768), 9–15. https://doi.org/10.1525/curh.2015.114.768.9

Do, Q., Shapiro, J. N., Elvidge, C. D., Abdel-jelil, M., Daniel, P., Baugh, K., Hansen-lewis, J., Zhizhin, M., & Bazilian, M. D. (2018). HHS Public Access. *Energy Res Soc Sci*, *44*, 411–418. https://doi.org/10.1016/j.erss.2018.03.013.Terrorism

Dodds, K. (2007). *Geopolitics: A Very Short Introduction*. New York: Oxford Press.

Dodge, M., & Kitchin, R. (2001). *Mapping Cyberspace*. New York: Routledge.

Dunn-Cavelty, M. (2010). Cyber Threats. In M. Dunn-Cavelty & V. Mauer (Eds.), *The Routledge Handbook of Security Studies*. New York: Routledge.

Dunn-Cavelty, M., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of The State. *St. Antony's International Review*, *15*(1), 37–57.

Dunn-Cavelty, M., & Wenger, A. (2020). Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, *41*(1), 5–32.

Eldem, T. (2020). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration*, *43*(5), 452–465. https://doi.org/10.1080/01900692.2019.1680689

Fernández, D. P. (2020). Will the Internet fragment? Sovereignty, globalization and cyberspace. *Revista Espanola de Ciencia Politica*, *2020*(53), 195–200. https://doi.org/10.1080/08109028.2018.1505877

Flint, C. (2016). Introduction to Geopolitics. In *Introduction to Geopolitics*. USA: Routledge.

Glen, C. M. (2014). Internet Governance: Territorializing Cyberspace? *Politics & Politiy*, *42*(5), 635–637. https://doi.org/10.1111/polp.12093

Hammarberg, K., Kirkman, M., & De Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, *31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Heinl, C. H. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *Asia Policy*, *18*(1), 131–159. https://doi.org/10.1353/asp.2014.0026

Henry, M. (2014). Australasian Airspace: Meteorology, and the Practical Geopolitics of Australasian Airspace, 1935-1940. In J. Beattie, E. O'Gorman, & M. Henry (Eds.), *Climate, Science, and Colonization: Histories from Australia and New Zealand* (pp. 234–249). USA: Palgrave Macmillan.

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *Andalas Journal of International Studies (AJIS)*, *5*(2), 151. https://doi.org/10.25077/ajis.5.2.151-165.2016

Jones, L., & Sage, D. (2010). New directions in critical geopolitics: An introduction. *GeoJournal*, *75*(4), 315–325. https://doi.org/10.1007/s10708-008-9255-4

Kassab, H. S. (2014). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In J.-F. Kremer & B. Muller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 59–76). Bonn: Springer.

Kausch, K. (2017). *Cheap Havoc: How Cyber-Geopolitics Will Destabilize The Middle East*.

Kelly, P. (2006). A Critique of Critical Geopolitics. *Geopolitics*, *11*(1), 24–53. https://doi.org/10.1080/14650040500524053

Khanna, P. (2018). State sovereignty and self-defence in cyberspace. *BRICS Law Journal*, *5*(4), 139–154. https://doi.org/10.21684/2412-2343-2018-5-4-139-154

Klinger, J. M. (2020). Critical Geopolitics of Outer Space. *Geopolitics*, *26*(3), 661–665. https://doi.org/10.1080/14650045.2020.1803285

McKinder, H. J. (1998). The Geographical Pivot of History. In G. O. Tuathail, S. Dalby, & P. Routledge (Eds.), *The Geopolitics Reader* (pp. 27–31). London: Rouledge.

Merchant, E. K. (2015). Book Review: Global population: History, geopolitics, and life on earth. *Global Public Health*, *10*(1), 129–131.

https://doi.org/https://doi.org/10.1080/17441692.2014.976241

Mueller, M. L. (2019). Against Sovereignty in Cyberspace. *International Studies Review*, *0*, 1–23. https://doi.org/10.1093/isr/viz044

Navari, C. (2013). Liberalism. In P. Williams (Ed.), *Security Studies: An Introduction* (2nd ed., pp. 32–47). New York: Routledge.

O Tuathail, G. (1996). *Critical Geopolitics*. London: Routledge.

Power, M. (2010). Geopolitics and "development": An introduction. *Geopolitics*, *15*(3), 433–440. https://doi.org/10.1080/14650040903500999

Public Private. (2019). *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*.

Ramadhan, I. (2017). Peran Institusi Internasional dalam Penanggulangan Ancaman Cyber. *Populis*, *2*(4), 495–508.

Ramadhan, I. (2018). China's Belt Road Initiative: Dalam Pandangan Teori Geopolitik Klasik. *Intermestic: Journal of International Studies*, *2*(2), 139. https://doi.org/10.24198/intermestic.v2n2.3

Ramadhan, I. (2019). STRATEGI KEAMANAN CYBER SECURITY DI KAWASAN ASIA TENGGARA: SELF-HELP ATAU MULTILATERALISM? *Jurnal Asia Pacific Studies*, *3*(1). https://doi.org/dx.doi.org/10.33541/japs.v3i1.1081

Ramadhan, I. (2020). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). *Journal of Social and Political Sciences*, *3*(4). https://doi.org/10.31014/aior.1991.03.04.230

Ramadhan, I., & Iskandar, J. A. (2020). Upaya Perimbangan Kekuatan Iran-Arab Saudi melalui Perang Suriah untuk Memenangi Kontestasi Geopolitik di Timur Tengah. *Insignia: Journal of International Relations*, *7*(2), 105. https://doi.org/10.20884/1.ins.2020.7.2.2391

Ramadhan, I., & Pratiwi, M. (2020). Perluasan Kerja Sama Shanghai Cooperation Organization (SCO) Dalam Pandangan Teori Geopolitik McKinder. *Frequency of International Relations*, *2*(1), 142–163.

Riordan, S. (2019). The Geopolitics of Cyberspace: a Diplomatic Perspective. *Brill Research Perspectives in Diplomacy and Foreign Policy*, *3*(3), 1–84. https://doi.org/10.1163/24056006-12340011

Roselle, L., & Spray, S. (2012). *Research and Writings in International Relations*. Boston: Pearson Longman.

Schmitt, M. N., & Vihul, L. (n.d.). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, *111*, 213–218. https://doi.org/doi:10.1017/aju.2017.55

Sheldon, J. B. (2014). Geopolitics and Cyber Power: Why Geography Still Matters. *American Foreign Policy Interests*, *36*(5), 286–293. https://doi.org/10.1080/10803920.2014.969174

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

Sieber, U., & Neubert, C.-W. (2017). Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty. In M. Planck (Ed.), *Max Planck Yearbook of United Nations Law Online* (pp. 239–321). Netherland: Brill-Nijhoff.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(August), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sobaruddin, D. P., Armawi, A., & Martono, E. (2017). Model Traffic Separation Scheme (TSS) Di Alur Laut Kepulauan Indonesia (AlKI) I Di Selat Sunda Dalam Mewujudkan Ketahanan Wilayah. *Jurnal Ketahanan Nasional*, *23*(1), 104. https://doi.org/10.22146/jkn.22070

Spiegel, S. L. (2000). Traditional space vs. cyberspace: The changing role of geography in current international politics. *Geopolitics*, *5*(3), 114–125. https://doi.org/10.1080/14650040008407694

Tsagourias, N. (2015). The Legal Status of Cyberspace. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 13–49). Cheltenham: Edward Elgar Publishing.

Wu, Z. (2018). Classical geopolitics, realism and the balance of power theory. *Journal of Strategic Studies*, *41*(6), 786–823. https://doi.org/10.1080/01402390.2017.1379398

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics & Politiy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202