Nat. Volatiles & Essent. Oils, 2021; 8(4): 15278-15286

NVEO
Natural Volatiles &
Essential Oils

Challenges Of Cyberspace For Territorial Sovereignty

Naser Garousi[1]

Faculty member of Payame Noor University, Alborz, Iran.

Abstract

Cyberspace can be considered as one of the symbols of the contemporary world today. The development of communication technologies and the development of people's level of access to communication infrastructures and tools have made the Internet an important and inseparable part of the social, economic, cultural and political activities of citizens. In this process, due to the access provided in cyberspace, a diverse range of governmental and non-governmental actors and various economic institutions are trying to take advantage of the opportunities that are presented to them in cyberspace. Take steps to achieve their sectoral and organizational goals. What adds to the importance of this field more than anything else is the information that is constantly flowing in this space. This has led to competition between countries, different companies and different institutions for the ownership and use of this information, and this in turn has raised concerns among governments. Has made them intend to extend their territorial sovereignty from geography to cyberspace, not only to monitor and control the activities of citizens and non-governmental organizations, but also to use it to their advantage. But these efforts have created new challenges and added to the scope of concerns about cyberspace governance and governance. This article will try to examine the issue of governance and governance in cyberspace and raise the point that with the expansion of cyberspace, what are the challenges facing the exercise of governance in cyberspace and what are its consequences?

Keywords: cyberspace, territorial sovereignty, governance, supervision, competition

Introduction

In the last decade, with the expansion of cyberspace and the growing tendency of the world's citizens to use cyberspace, social media and international interaction, there is a feeling among different countries that the global flow of information, which includes personal information and data. Economic, political, financial, commercial and sometimes security is rapidly circulating in space and it is possible that this information will be exploited by other actors active in cyberspace. In other words, the feeling of threat in the field of geopolitical rivalries (Ahmadipour and Rashidi2017) has spread from real space to cyberspace. The range of concerns of different countries in this field has increased with the increase of

cyberspace functions for global competition and its influential role in national power (Rashidi et al, 2014) of countries and has caused this area to become one of the focal points of countries (Rashidi, 2012).

In 2015, the Russian Duma passed a law requiring Internet service providers to make arrangements to protect citizens' information and prevent global surveillance by the US National Security Agency. External servers, but also stored in Russian databases. This meant that the Russian Internal Security Service was legally allowed to access this information. That same year, the European Court of Human Rights ruled that the Safe Door Agreement would remain in force until the United States transferred the databases of European citizens to the union. Both Russia and the European Union had concerns about access to citizens' information, and each, of course, with different goals and different vocabulary, tried to provide appropriate legal reasons for it so that they could have their own information. And prevent the United States of America from accessing information in cyberspace that relates to the activities and citizens of Russia and the European Union. In other words, through these measures, Russia and the European Union sought to extend their sovereignty over information, such as territorial sovereignty over domestic actions and assets, and to address their concerns about international security.

The growing importance of sovereignty for countries in cyberspace can be compared to the era in the nineteenth century with the expansion of global communications and transportation, a pervasive economic competition to dominate global transportation routes, important ports and bases for sending and consuming goods. Formed (Buzan and Lawson, 2015). Today, the efforts of countries to dominate the global flow of information can be compared to the competition of world powers in the nineteenth century for supremacy over shipping routes. In addition, the history of cyber-governance debates can be traced back to liberal traditions in international relations, which emphasize that there is a meaningful relationship between economic interdependence and expansion. There is peace based on common interests. First, based on this view, it can be said that the freedom of cyberspace is an important feature that should not be protected against traditional logic in the field of power policies (Bendiek, 2014: 62). However, the relationship between commercial interests and the reduction of the likelihood of war is very different from the liberal approach it emphasizes. This largely depends on what countries expect in terms of future trade and investment environment in terms of access to raw materials and markets (Copeland, 2014: 145).

Creating cyberspace has become more of an environment for competitors to compete (Lindsay, 2015: 12) than an environment for interaction. The importance of this issue has expanded to the point that it has created a cyber security conundrum in the field of international security (Buchanan, 2015). Second, the representations of the nature of relationships in cyberspace have given credence to security measures and processes because they have raised the threats and harms that exist in this area to the level of national security. Therefore, it must be said that there is a logical relationship between claiming territorial rights and the authority of cyberspace on the one hand, and striving for superiority over other actors, on the other. Transnational spaces, however, challenge this particular dimension of governance that focuses on regulating and controlling both transnational currents and stakeholder actors (Krasner, 2019 and Stevens and Betz, 2011). In other words, as in other transnational spaces, the issue of sovereignty is more dependent on the issue of control than sovereignty, while at home countries

continue to emphasize their territorial rights in cyberspace (Kindleberger, 1973: 145). In other words, this extraterrestrial realm has an underdeveloped regime of rules that relies on partnership between countries or a hegemonic power that seeks to assert its will (Gilpin, 1981: 202).

Some researchers believe that this situation has led to the United States and its allies finding the upper hand in cyberspace and putting other countries at the bottom. For this reason, it is necessary to create a set of international mechanisms in the field of governance and its application in cyberspace, which is trusted by all national actors. The dominance that the United States has gained through cyber and non-state actors in cyberspace has made many countries concerned about their territorial sovereignty in cyberspace. Many countries are trying to respond to US atrocities in cyberspace in order to defend or regain territorial sovereignty in cyberspace. This has led any country that sees itself in danger of American hegemonic supremacy in cyberspace to consider a set of measures that, more than anything else, fit their national perceptions of the concept of sovereignty in the digital age. But all these countries and national actors have one thing in common. The point is that by gaining American supremacy in cyberspace, this country can become a hegemonic and central actor in cyberspace in this field, which has the ability to outperform other actors and participants in cyberspace. The title revolves around the exercise of power. For this reason, some researchers believe that a series of efforts are taking place in cyberspace in which different national actors are trying to create a kind of balance of power in cyberspace. To reduce the level of American supremacy in this area (Krasner, 2019).

In this article, we try to analyze this issue to examine the challenges that exist in the field of territorial sovereignty in cyberspace and have caused the reaction of national actors and governments. Has been in this area and where this route will probably lead.

2. Theoretical foundations of research

Governance in cyberspace refers to the involvement of a wide range of actors, including government actors and governments, private companies, civil society organizations, citizens, and international organizations. In collaboration with each other, these institutions define and develop norms that should be used and respected by users and users in cyberspace. Therefore, it should be said that in cyberspace, the issue of governance should be compared to a kind of participatory governance in which all actors should actively play appropriate roles without this role creation preventing other actors from achieving their rights.

Countries have always tried to exercise their territorial sovereignty in various ways and tools. While a number of countries are constantly trying to establish themselves as independent of the current Internet network, which is largely dominated and influenced by the United States, other actors are seeking to become more widespread. Gain control and control over their physical, communication and social infrastructure in the field of cyberspace. Although both approaches take different paths in gaining dominance in cyberspace, they ultimately share a common denominator, which is the acquisition of legal authority to exercise power in cyberspace in a way that provides to represent the interests of the country that is taking this path. In this process, each country may have its own reasons for exercising sovereignty in cyberspace and try to take control of cyberspace within their own territory based on national interests or the interests of the ruling class (Rashidi et al, 2016: 100), in global geopolitical

competitions in the world of information and media to achieve superiority or competitiveness (Ahmadipour and Rashidi, 2021) or by exercising control over modern information and media to provide conditions that give them Help them to differentiate between us and others in order to preserve their values (Rashidi et al, 2021: 97).

As Kresner has already pointed out, sovereignty is a concept that is largely dependent on the social and political structures that have developed within the framework of complex historical processes (Krasner, 2019). Part of the problem of governance in cyberspace in the international fluid environment, which has led governments to pay attention to it, stems from the fact that the current world has become a dangerous society in which countries They need to act in order to secure their geopolitical interests in a way that reduces the amount of threats and dangers that exist in front of them and provide a suitable environment for their security (Ahmadipour and Rashidi, 2017: 23). Therefore, it should be said that not only the issue of sovereignty is something that makes a country feel more secure and secure than Iran, but also provides the ground for gaining independence from the external environment to create conditions for to enforce the law and regulations in the form of which the government is considered to serve the interests of the country. This has led to the diverse functions of cyberspace in many countries to provide a situation in which they can monitor their internal affairs or issues related to these countries in the field of information and cyberspace, power Have intervention and control. However, in the field of cyberspace governance, there are two major and different variables that have caused each country to pursue different policies in this area. The first variable relates to how countries perceive that they need to increase their control over Internet domains and cyberspace. The second variable includes the context in which countries assess that they are exposed to potential threats or dangers in cyberspace. Of course, it goes without saying that both of these variables are interrelated and this relationship can affect the attitude of countries to the issue of security and governance in cyberspace.

However, it should be borne in mind that each of these variables can act independently or cause different results in understanding the concept of sovereignty in cyberspace of a country. In other words, these two variables, if they play a role separately, will have very different results than when they play a role simultaneously. It goes without saying that the end product of the functioning of these variables and the type of attitude and perception of governments in the fluid environment of international politics and law can add to the complexity of the issue and create conditions that its perception and management require extensive efforts. It is (Agnew, 2009: 178). In addition, the issue of exercising sovereignty over cyberspace raises the question of how and in what form countries want to exercise their sovereignty in cyberspace. It seems that it is legally, technically and politically very difficult for countries to implement exactly the same model of territorial sovereignty over their geographical space, where borders, territory, jurisdiction and population are clear, in the field of cyberspace. Because no trace of the border can be found in cyberspace, a definite range cannot be identified, and cyberspace users can not freely operate in different domains and on various Internet domains. Therefore, it must be said that issues that depend on the current, fluid, global and pervasive nature of cyberspace make it impossible for countries to exercise full sovereignty in this area.

As the efforts of countries such as Russia and China have shown that the impact and success of these efforts is cross-sectional or limited to a limited area or parts of cyberspace. Thus, in the real world,

attempts to control cyberspace have failed. In this regard, geographers who have conducted research in the field of territorial sovereignty believe that the idea that the Westphalian territories are dominated only by governments has remained only on a theoretical level. Because even in the real world geographical environment, countries have never been able to fully exercise their sovereignty over the land, and this failure to exercise full sovereignty over space in the field of cyberspace is much greater and wider (Agnew, 2009: 183).

In this regard, it should be remembered that cyberspace is a combination of both infrastructure and content. Therefore, it should be said that the Internet is a fluid environment that, while dependent on the physical infrastructure that is within the territorial sovereignty of countries, has the flexibility and large-scale change (Castells, 2011: 780) that at the same time, it represents the bright and dark points of the connectivity of the current world to the world of information (Betz, 2015). This means that in this space there are various opportunities and threats facing governments, countries, government actors, non-governmental actors, public institutions, private companies, civil society organizations and citizens, and any Which of these actors can take advantage of the capabilities that are available to actors in cyberspace in a different way.

Research Methods

In this research, an attempt will be made to investigate the issue of territorial sovereignty in cyberspace using a qualitative-descriptive analysis approach. In this regard, it will try to provide theoretical foundations for research by using research that has already been done by other researchers. In the following, an attempt will be made to examine the challenges facing the sovereignty of countries in the field of cyberspace with the help of the theoretical foundations of research that has been formulated in the field of governance and space.

Research Findings

The issue of cyber governance covers a wide range of political, cultural, economic and security issues. One of the issues that has caused controversy in the field of virtual governance is the issue of political economy of information and technology, in which there are differences between different countries. This is because some countries, especially the European Commission and France, believe that the world's largest technology companies, most of which are American, evade their social responsibility in the field of taxation and are always trying to use The fluid nature of cyberspace, which allows companies to operate in areas of their choice, is tax-exempt. One of the differences between these countries can be seen in the tension between European companies and the United States. Large companies such as Google and Facebook focus on paying taxes by focusing on countries such as the Republic of Ireland and Luxembourg, which offer easier tax conditions than other EU member states. Billions of dollars in tax evasion (Copeland, 2014).

This shows that there are serious differences even among important allies such as the United States and the European Union. On the one hand, the United States is trying to protect the interests of its large technology companies, which have led the country in the field of cyberspace, and on the other hand, the European Union, led by France and Germany. They are to prevent the United States from becoming a superpower in this area, given the long-term horizon. For this reason, the European Union seeks to

simultaneously emphasize the common European values of the activities of the world's largest technology companies in the Union under the umbrella of its rules and legal opinions, and on the other hand at the request of the United States. And for American companies to move major servers to EU territory, make sure that US intelligence agencies do not have access to information from European citizens, institutions and companies beyond the agreement between the EU and the US. One of the legal arguments put forward by France relates to a law passed in France in 1978 that called on the government to prevent the transfer of domestic information abroad. In other words, countries such as France, given the importance of cyberspace and powerful companies such as Facebook, Google and Microsoft, seek to use their domestic laws to make arrangements as the elected government of their people. To control the information that pertains to the citizens, institutions, and private companies of this country. This could have two major strategic and legal implications for US-European relations: on the one hand, it would prevent US intelligence from gaining ground in this area, and on the other hand, it would provide the basis for European countries prevent the increase of their power over national governments by monitoring the activities of large technology companies (Nakashima, 2015).

Although EU law, which places a strong emphasis on protecting citizens' privacy, can serve as a major obstacle to international cooperation, especially between the United States and Europe, the fact is that these countries have a diverse range of common interests that encourage them to not only work together, but also to encourage or encourage companies operating in cyberspace. To provide information that is of great importance to governments in enforcing the law. An important case in point is the efforts of European and Irish police to apprehend a drug trafficker. An Irish court needed the police to have access to the information held by Microsoft in order to prosecute and convict the offender. Microsoft, which has one of its largest European offices in the Republic of Ireland, has been working together with the European Union and the United States to provide information about the Irish criminal to regulators, police and The Irish judiciary. This indicates that although countries in some areas have serious differences in cyber governance and access to information in this area, in many cases for activities such as the fight against organized crime. Terrorism, extremism, racism, etc. need to work together. In other words, the issue of cyber governance can be much more complex legally and technically than it is now. Because in various cases when it comes to the issue of collective security and safety of communities, both countries and private companies need to exchange information with each other to prevent the spread of criminal activities that can ¬ Can have destructive results (Farrell and Newman, 2016: 142).

Therefore, it must be said that the issue of governance in cyberspace is very complex from a political and legal point of view. Information, security and cybersecurity experts advising the EU are aware of another risk. According to these researchers, most of the innovations and innovations that occur in the field of information and cyberspace are either made by American companies and citizens or are in the realm of their economic or intellectual property. This has de facto given the United States economic, technological, and political supremacy in cyberspace, giving it a significant advantage over other actors. In this process, although the efforts of different countries to exercise sovereignty over cyberspace can bring them a level of authority and even pose challenges to US hegemony in cyberspace, in practice the fragmentation of cyberspace It can lead to America's absolute superiority in this area. Because, as

mentioned, much of cyberspace infrastructure, technology, information, and innovation is owned by American companies and institutions, and efforts to dismantle cyberspace will ultimately provide an opportunity for the United States to in this area, it achieves broad legal powers through which it can exercise broad territorial sovereignty and authority in the field of cyberspace (Krasner, 2019).

This can not only create various problems for citizens, civil society organizations and smaller companies if they occur, but also has the potential to increase tensions between citizens and governments. However, two points should not be overlooked: first, any change in the conditions of cyberspace depends on the cooperation of large technology companies, which, given their financial and economic benefits in the global flow of information, are very unlikely to These private actors are expected to succumb to the conditions in which cyberspace was fragmented; Second, the issue of the fragmentation of cyberspace and its transformation into permissible sovereign domains will ultimately be affected by the national interests of countries. Given that in the long run countries do not have any suitable alternative to the current fluid structure of cyberspace, it still seems unlikely that this global consensus on cyberspace fragmentation will be possible. In this process, some may believe that the current state of cyberspace is more influenced by the public will and the role of the United States as a hegemonic power (Posen, 2003: 39). But it should be noted that hegemony is not guaranteed. Because hegemony is something that is more than political capabilities, it is related to the issue of creating broad social relations, in the framework of which a power can gain a position of superiority over other actors in terms of value and cause a consensus. To serve the interests of that country. In other words, the regulatory power of the United States in cyberspace depends on the extent to which it will try to conduct its actions in the international arena within a legal framework that is credible. The majority of actors are governmental, non-governmental, and citizen (Lebow and Reich, 2014: 41).

The issue of governance in cyberspace has created numerous geopolitical rivalries between governmental and non-governmental actors, and each of the actors is trying to achieve superiority by using different tools. Most of these competitions are either between countries or between large technology companies. Governments may sometimes seek to assist private actors in the competition process by exercising their legal powers and powers acquired through sovereignty over the land. In this process, we see that the powerful countries of the world, especially China and the United States, are trying to use the technological facilities at their disposal to confront each other more than anything in the fields of artificial intelligence and hard balance in cyberspace. These countries are trying to concentrate an important part of the technological infrastructure in their country, develop technical knowledge in the field of artificial intelligence and offer their products to different countries of the world, not only to be technically superior to other competitors, but also to Increase the representation of their hard power in world politics (Rashidi et al, 2014) and thus gain hegemonic status in the information space by gaining global prestige. On the other hand, the extensive competition between large global companies such as Google, Facebook, Microsoft, Huawei, ZTE, Samsung, Apple, etc. in the field of hardware, communication infrastructure, and there is excellence in the management of Internet platforms. Take steps in the interests of some companies or to counter their influence. An example of this can be seen in the Chinese government's influence to limit American social media activity, which is aimed at preventing American influence. Of course, the scope of these rivalries is not limited to the

rivalries between China and the United States, or the efforts of Russia and the European Union to gain power. Other countries, such as Saudi Arabia, Iran, Russia, India and Israel, have also entered the competition and are trying to pursue their own interests. In other words, the issue of governance in cyberspace has become so complex and fluid that we are witnessing pervasive geopolitical rivalries between different countries and actors, each of which seeks to take advantage of this emerging space to expand its interests.

Conclusion

The findings of this study indicate that the expansion of space, as much as it has created numerous opportunities for different actors, has also provided grounds for some actors, especially governments, to discuss the consequences of expansion. Cyberspace and the exploitation of this space by other countries or actors for their own interests. This is more than anything else a reflection of the geopolitical and economic rivalries that have not only spread under the influence of cyberspace, but have made it a focal point for competition for supremacy. The importance of cyberspace is more than anything else because of the fluidity of the information flowing in it, and this has led to different actors simultaneously seeing it as an opportunity and a threat to their interests. This issue has caused some countries to try to extend their sovereignty from the real space to the virtual arena with legal and political arguments, and to try to control and monitor this space to a part of the interests and goals that are They intend to achieve. These countries are justifiably trying to conclude, based on political, security, and legal reasons, that a lack of cyberspace oversight could do harm to these countries and set the stage for cultural and political threats. Provide economic and security. Issues such as the fight against organized crime, terrorism, cultural change and the protection of national, traditional and religious values can be considered among these reasons. This has led some researchers to warn that the space may be fragmented as a result of countries trying to exercise territorial sovereignty over cyberspace. However, the fluid nature of cyberspace, which has made it extraterrestrial in nature, has minimized the likelihood of this happening. But it is still possible that different countries will try to exercise some of their dominance over the Internet by using the tools at their disposal to monitor and manage communications infrastructure. This can ultimately limit government actors and cause various economic losses. As a result, countries are increasingly trying to assert their sovereignty through technology development and global influence.

Resources

Agnew, John. (2009).Globalization & Sovereignty, New York, NY: Rowman& Littlefield.

Ahmadipour, Zahra and Rashidi, Younes. (2017). Geopolitical analysis: Representation of fear spaces in cinema. Geopolitical Quarterly. Fourteenth year. Second Issue. Summer, pp. 21-55.

Ahmadipour, Zahra and Rashidi, Younes. (2020). Geographical illustration and geopolitical representation. Tehran: University of Tehran.

Bendiek, Antony. (2014).Beyond US Hegemony: The Future of a Liberal Order of the Internet. in Liberal Order in a Post-Western World, C. Kupchan Ed. Washington, DC: Transatlantic Academy. Pp.57–69

Betz, David. (2015). Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power.London: Hurst & Co.

Buchanan, Benjamin. (2015). The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, London: Hurst & Co., Forth.

Buzan, Bary and Lawson, Geogrge. (2015). The Global Transformation: History, Modernity and the Making of International Relations. Cambridge: Cambridge University Press.

Castells, Manuel. (2011).A Network Theory of Power. International. Journal. of Communications. Vol. 5. Pp 773–787.

Copeland, David.C. (2014). Economic Interdependence and War, Princeton, NJ: Princeton.

Farrell, Harold and Newman, Ayra. (2016). The Transatlantic Data War. Europe Fights Back Against the NSA", Foreign Affairs, vol.95, n°1. Jan.-Feb. 2016, p. 214–134.

Gilpin, Robin. (1981). War and Change in World Politics, Cambridge: Cambridge University Press.

Kindleberger, Chris. (1973). The World in Depression 1929-1939, Berkeley, CA: University of California Press.

Krasner, Simon. (2019). Sovereignty: Organised Hypocrisy, Princeton, NJ: Princeton.

Lebow, Raymond and Reich, Simon. (2014). Good Bye Hegemony! Power and Influence in the International System, Princeton, NJ: Princeton. Pp.35–49.

Lindsay, John. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. International Security. Vol.39. No 3. Winter 2014-2015. Pp.7–47.

Nakashima, Edward. (2015).Top E.U. Court Strikes Down Major Data-Sharing Pact Between U.S. and Europe", The Washington Post, Oct. 6, 2015. [Online]. Available: https://www.washingtonpost.com/world/national-security/eucourt-strikes-down-safe-harbor-data-transfer-deal-over-privacyconcerns/2015/10/06/2da2d9f6-6c2a-11e5 b31cd80d62b53e28_story.html

Posen, Bernard. (2003). Command of the Commons: The Military Foundation of US Hegemony. International Security. Vol.28. No 1. Summer 2003. Pp.5–46.

Rashidi, Yunes (Younes) et al. (2014). The Mediating Role of Cinema in Representation of Hard Power Case Study: The movie "Zero Dark Thirty". Research on Humanities and Social Sciences. Vol.4. No.12. Pp 128- 135.

Rashidi, Yunes (Yuones) et al. (2016). The impact of cyber space on Egypt's revolution. International Journal of Humanities. Volume 23. Issue 1. Pp 99-119.

Rashidi, Yunes; AhmadiPour, Zahra; Alemi, Akbar; and Bayat, Moloud. (2021). The Role of Geographical Imagination and Geopolitical Representation in Dividing Space/Place into "our" and "their". Geopolitics Quarterly. Volume 16. No 4. Winter 2021. Pp 79-100.

Stevens Tim and Betz, David. (2011). Cyberspace and the State: Toward a Strategy for Cyber-Power. Adelphi Series. vol.51. no 424. Pp.6–158, Nov. 2011.