Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July, 2021:7248 – 7256

Research Article

An approach to the concept of territorial sovereignty in cyberspace

Naser Garousi[1]

1. Faculty member of Payame Noor University, Alborz, Iran. Nasergarousi@gmail.com

Abstract

With the expansion of cyberspace and its influence in various areas of human social life and the transboundary effects that this technological field has left, the eyes and attention of researchers, government agencies, governments, non-governmental organizations and actors, citizens. It focuses on this space and its functions. Due to the effects that cyberspace has had in various fields, which has sometimes been in line with the national interests of countries and sometimes in conflict with their interests, there have been several discussions on the governance of cyberspace. Because countries seek to gain the power to decide and exercise power in cyberspace, just like in real space, without other actors being able to stand in their way. This has led to a variety of debates on how to govern and exercise territorial sovereignty in cyberspace, and different approaches have been proposed in this regard. Given the importance of this issue, this article will try to examine and analyze the concept of territorial sovereignty in cyberspace. In this process, an attempt will be made to examine the main approaches to governance in cyberspace and to point out the consequences and effects of each of them, and finally to answer the question that in the process of territorial governance in cyberspace should be expected What happened?

Keywords: Cyberspace, Territorial Sovereignty, Global Governance.

1. Introduction

Cyberspace is a global digital network whose influence can be seen in an important part of the modern life of human society. The importance of space has increased so much in recent years that researchers, citizens, entrepreneurs and governments have considered it as a vital infrastructure to support contemporary societies, as it helps diverse activities. Such as communication, financial and commercial transactions, banking, education, etc., and it is no longer possible to imagine a world in which the structures of government and territorial governance exist without the use of cyberspace. However, the influence and function of cyberspace in recent years has been so widespread that it has affected important areas such as politics, economics, culture and social sphere in different countries. In other words, cyberspace can be considered as a suitable path for the process of humanization through which, with the expansion of global interaction and communication, concepts such as the global village and the global battlefield are embodied. In the first sense, cyberspace is seen as an extraterrestrial space in which there are more free opportunities and wider socio-political mobility for citizen participation. In the second sense, however, cyberspace is seen as an expanded part of the real world space in which we face a lack of sovereignty, thus posing numerous security challenges to countries. (McEvoy Manjikian, 2010).

Due to the multidimensional, asymmetric, and multifunctional features of cyberspace, the territorial challenges posed by cyberspace have always been defined in terms of concepts such as security, borders, human rights, privacy, and state territorial sovereignty. Is (Slack, 2016: 69). What makes these concepts important for governments in terms of international law goes back to the issue of technological features and the political and social impact of cyberspace, which has led to a significant role for government in cyberspace. Considered. In addition, cyberspace creates new issues that are geographically important for the sovereignty of countries; First, cyberspace has infiltrated the jurisdiction of countries, second, cyberspace has greatly facilitated political activism in various countries, and finally, this technological infrastructure has made users of space Virtual or actors who work in this field hide their identities from the eyes of governments (Choucri, 2012: 4). Perhaps one of the most important cyberspace responses in this area can be seen in the formation of various protest movements that have taken place in the Middle East over the past decade, and in some cases have led to the overthrow of governments or the transformation of some countries. Political events took place in the governing structures of a number of Middle Eastern countries (Rashidi etal, 2016). This shows that the rapid developments that are taking place in the field of virtual communications have affected the interests of both governments and non-governmental actors in cyberspace. Advances in information technology, such as the Internet of Things (Weber 2013), big data and reference databases (Cukier and Mayer-Schoenberger 2013) and the Dark Web (Chertoff and Simon 2015) To reduce the ability of governments and international institutions to exercise governance and management in cyberspace. Given that cyberspace is an integral part of the communication infrastructure in terms of governance and is an important part of the functions and activities of the private sector and its affiliated citizens, the issue of cyber governance is a vital issue for Countries have become. Because the issue of cyberspace fluidity has led governments, international organizations, private companies, and civil society to struggle to regulate a wide range of activities in cyberspace. It should be placed under the umbrella of the law in order to prevent the activities of illegal organizations and criminals who are trying to exploit the capabilities of cyberspace for their own benefit. However, many experts in the field believe that any attempt to curb cyberspace could come at the cost of technical constraints, reduce development rates in different countries, and lower civil liberties in all human societies. At the same time, given that a large part of the facilities provided to citizens in cyberspace are owned by non-governmental organizations and companies, they have found the opportunity to increasingly influence the scope. Increase civil society itself while at the same time questioning the centralization of sovereignty in the hands of national governments. This issue has led the purpose of this article to examine the complexities of governance in cyberspace. In order to examine this issue and provide a proper view of it, in the first step, an attempt will be made to introduce the challenges that cyberspace has faced in the face of the territorial sovereignty of the nation-state. In the following, we will evaluate the extent to which we can witness a change in the territorial sovereignty of countries and a move towards global sovereignty in cyberspace, given the increasing role of cyberspace. Finally, using these analyzes and research findings, we will try to provide a comprehensive view of the issue of governance in cyberspace and present it to the audience of this work.

2. Theoretical foundations of research

Previously, several researchers with different research backgrounds and disciplines have tried to explain different aspects of cyberspace policy. However, some international law experts believe that in these studies, any researcher who has ignored the complexity of cyber governance has ultimately failed to successfully analyze the issue of cyber governance. Because national sovereignty has always been considered as one of the basic foundations of the international system, and even the activity and existential

nature of an institution such as the United Nations has been based on the basic principle of equality in sovereignty. The issue of sovereignty is not only the basis of the legal authority of states to exercise power within their geographical borders and distinguish them from other countries, but it is also an essential principle for membership in the world system (Liaropoulos, 2013: 21-22). Given the nature and function of cyberspace, the question that arises here is how a country in a borderless space based on Internet domains can exercise its authority, sovereignty and territorial integrity. Implemented the stage? To understand this issue and provide a proper answer to it, we first need to distinguish between the physical and non-physical dimensions of cyberspace. Mohammad Reza Hafeznia (2012: 32) believes that cyberspace is a virtual nature based on the Internet and data exchange, which requires a set of physical communication infrastructures for its existence and function. In other words, cyberspace is not functional without the existence of communication infrastructure. Stephen Gorrelli takes a similar approach to cyberspace and believes that there are significant differences between the domains of cyberspace (media medium) and "cyberspace". In this way, virtual activities are possible through virtual domains and ports that exist in cyberspace (Gourley, 2014: 278). The Internet domain is an artificial and man-made tool that is functionally geographically dependent on a land. These communication infrastructures are based on the permission and supervision of governments because they are created in real space, and therefore they cannot be safe from the territorial sovereignty of countries. Governments, because they have control of their country's Internet gateways, have the opportunity to exercise their sovereignty through the monitoring of Internet gateways. According to Gorley, territorial foundations allow countries to control the virtual activities that take place within their borders, which enables them to have jurisdiction over international law. Extend yourself to those virtual activities that are taking place within their territory. Of course, these cases depend on the fact that these activities are carried out using the communication infrastructure within a country and, of course, by users or people who are active within the country. This causes the spread of this issue to cyberspace itself, which has a global nature, and becomes a problem, and due to the fluid nature of cyberspace, governments exercise their hard power by using cyberspace beyond its borders. Exercise geography and use it to represent their power (Rashidi et al, 2014). Because there is no consensus in this regard that the content within cyberspace should be controlled and monitored based on the national sovereignty of countries. This is because different countries, based on national interests and conflicting legal definitions of cyberspace, use different approaches to legal issues that are effective or influenced by cyberspace, and thus each of these approaches can be due to Conflict with the interpretation of other countries or the threat to their national interests by other governments to face serious opposition (Gourley, 2014: 279-280).

The exercise of national sovereignty in cyberspace raises two issues. First, the attempt to exercise dominance in cyberspace conflicts with the idea that cyberspace is a global arena, and second, the attempt by countries to exercise dominance over cyberspace can be broken down. Lead (Cornish, 2015: 157). It should be noted here that cyberspace as a global arena is functionally different from sea, land and air, which are bounded by geographical boundaries. Because cyberspace as a man-made arena lacks physical space and thus no boundaries can be set for it. At the same time, contrary to popular belief, cyberspace cannot legally meet the criteria that make an area global in nature, and thus cannot enjoy the same practical freedom of action in the oceans. And the atmosphere of the earth (Betz and Stevens, 2011: 107).

Another point is the contradiction in cyberspace; Although cyberspace seems to be a boundless global space, its function and existence depend on infrastructures that facilitate the transfer of data and information. These infrastructures, which are owned by private companies in most countries of the world, are geographically within the territorial boundaries of different governments. In other words, although

cyberspace can be functionally considered a global entity, its functional dependence on the infrastructures that are within the territorial sovereignty of different countries makes the application of a global concept to cyberspace. Face serious doubts (Cornish, 2015: 158). This has led James Lewis to introduce cyberspace as a common domain with multiple owners (2010: 16). At the same time, Paul Cornish sees cyberspace as a shared virtual space that is neither privately owned, nor sovereign, nor can it be considered a universally owned concept. Which is already legally intended for the law of seas and space (2015: 159).

There is no doubt that different countries are trying to overcome the paradox of borders in cyberspace and thus be able to develop virtual borders in order to expand the scope of their territorial sovereignty into cyberspace (Demchak and Dombrowski, 2011). Therefore, one should always keep in mind the danger that this space may collapse due to the efforts of different countries to exercise dominance in cyberspace (Cornish, 2015: 159). Cyberspace fragmentation can lead to other side issues that can be technically, legally and politically controversial. Technically, cyberspace is unlikely to be completely dismantled by countries' efforts. Because the institutions that work for interaction and communication in cyberspace are always trying to ensure that the performance of cyberspace is always related to the international and global infrastructure. Although technology is always evolving faster than legal frameworks, countries are always striving to maintain their Westphalian foundations, and this has led to ideas around the world about data governance, space. Provide a national cloud and local storage space for data. The third point, which is no less important than the previous ones, is that the efforts of countries to exercise sovereignty in cyberspace and even the low probability of their success in creating a national cyberspace can have different political consequences and even contradict the structures. Sovereignty of countries. This can add to the legal complexities of relations between countries and create challenges that can be very complex and confusing in terms of international law (Fehlinger 2014).

3. Research methodology

In this research, an attempt will be made to provide a comprehensive overview of the nature of cyberspace and the perspectives that exist in the field of virtual governance, using an analytical and descriptive approach. Utilizing this method will allow the researcher to study and analyze the issue of governance in cyberspace and the approaches that exist in this field, and by analyzing their strengths and weaknesses, a tangible picture of the prevailing attitudes of governance. Provide a land in cyberspace for the audience.

4. Research Findings

The concept of sovereignty refers to the set of governmental institutions and regulatory-legal structures that regulate the collective activities of a society. Sovereignty creates a system of governance in which the boundaries between the private and public sectors are blurred. At the same time, it should be borne in mind that from a legal point of view, the concept of governance has a broader meaning than the concept of the state. The first concept (Ie, governance) can exist in the absence of a centrally destined institution, while the second concept can only exist within a country when a broad set of institutions has been created that allows the government They are allowed to expand their authority throughout the country (Rosenau, 1992). At the same time, the concept of governance within the framework of legal processes and literature governing international relations can become much more complex (Finkelstein, 1995: 336). Because the violation of the functions of the institutions affiliated to different governments with each other, the performance of international institutions, etc. cause the complexity of this concept to be added.

The concept of global governance does not mean the creation of a world government, but rather collective cooperation between countries, international institutions and non-governmental actors to overcome problems of a cross-border nature (Partick, 2014: 59). The term was first coined in the post-World War II years in response to problems such as climate change, globalization, and sustainable development that managed beyond the capabilities of a single country. A coherent and comprehensive structure of global governance has not yet been presented, but we are witnessing complexities in the relationship between actors in this area. If the level of international cooperation increases satisfactorily, this system of cooperation and participatory management can lead to the development of international norms in various fields and even in some cases lead to the conclusion of agreements in which countries witness cooperation. Be international institutions, NGOs, private sector actors and civic groups (Weiss and Wilkinson 2014: 208). One of these areas is cyberspace, where the need for international mechanisms is felt more than ever.

Some researchers believe that in any discussion in the field of international law, special attention should be paid to a few points (Weiss & Wilkinson 2014). First, the world is experiencing a shift from national to transnational regulation. Second, global politics encompasses more than intergovernmental politics, in other words, the powers of governments are far less than the consequences they are experiencing in areas such as cyberspace. Although the position of governments has not been destroyed by the world government, they are experiencing a situation in which they are witnessing the improvement and promotion of the position of non-governmental actors. Finally, supranational authority can only be lawful if the representatives of the institutions and groups whose interests are thus affected rely on decision-making processes that include specific rational standards, transparency and credibility. To be. Agree (Nye and Donahue, 2010: 12). In the field of cyberspace governance, there are several issues that require special attention for proper understanding because it raises fundamental questions in this area. Is there a need to govern cyberspace? Who can rule it? How not to dominate cyberspace? To what extent can cyberspace regulations be increased? Where is the place of power in cyber governance? How should this power be distributed among actors active in cyberspace? How to deal with important issues such as transparency, credibility and representation in cyber governance? It is not easy to provide clear answers to these questions, however, there are views in this area that have led to serious issues in the field of cyberspace governance. These issues include issues such as distribution of governance, multiple governance and participatory governance (West, 2014: 4). At the beginning of the emergence of cyberspace, this field was always defined as a wide field in which the scope of governance is limited and it is necessary for information to circulate freely and without any control (Deibert and Deibert and Crete-Nishihata, 2012: 341-42). Known as cyber utopians, they referred to cyberspace as a borderless space, and promised an era in which borders would lose their importance. In this man-made environment, concepts such as land and governance seemed irrelevant (McEvoy Manjikian, 2010). The scope of these utopians' optimism about cyberspace was so wide that in 1996, John Perry Barlow, one of the pioneers of thought in cyberspace, issued a declaration of independence for cyberspace, claiming that cyberspace had a place for There are no boundaries (Barlow, 1996).

In the 1990s, the number of Internet users did not reach several million, but today it is estimated that at least 60% of the world's population has access to it (Shen, 2016: 84). Today, the Internet has become an integral part of the modern world, and this issue has made the issue of territorial sovereignty one of the current topics of discussion in the field of cyberspace. This debate is one of the serious issues that is being seriously pursued by the followers of multilateralism. From the perspective of multilateralism, cyberspace is viewed in the context of a Hobbesian perspective. Cyberspace is a reflection of traditional power structures and reflects the mysteries of security and power competition between governmental and non-

governmental actors (McEvoy Manjikian, 2010: 386) and shows that the feeling of threat and fear (Ahmadipour and Rashidi, 2018) There are functional implications of cyberspace. Because the function of cyberspace may cause the interests of these countries to be threatened by other governmental and non-governmental actors in global geopolitical competitions (Ahmadipour and Rashidi, 2020). Proponents of her case have been working to make the actual transcript of this statement available online. The model of multilateralism in cyberspace is followed by governments such as Russia, China, India, Iran and Saudi Arabia. In general, this model is most popular among developing countries. These countries emphasize that the exercise of sovereignty in cyberspace can help them in creating ideas, and managing issues such as political and social uprisings and cultural change. Cyberspace, and especially the development of social media, has demonstrated its function and power during the formation and spread of protest movements in the Middle East (Rashidi et al, 2016).

In other words, these countries seek to differentiate cyberspace as well as real space by exercising territorial sovereignty (Rashidi; AhmadiPour; Alemi; and Bayat, 2021). In general, in the multilateral approach to cyberspace, theorists are more than trying to emphasize that in the global governance of cyberspace, the Westphalian perception of territorial sovereignty must always be respected. In this legal-geographical perception, each country has the absolute right of territorial sovereignty over its territory and internal affairs, and no country has the right to interfere in the internal affairs of other countries (Jayawardane, Larik and Jackson, 2015: 6).

Another dominant approach in the attitude towards cyber governance is known as the multilateral partnership model. The model of multilateral participation is in stark contrast to the multilateral approach in cyberspace, as it involves the participation of both governmental and non-governmental actors in the governance of cyberspace. The rationale for this approach is based on the principle that given the increasing participation of citizens, NGOs and technology companies in cyberspace, it cannot be accepted that governance and regulation are left to governments alone. Followers of this approach believe that the norms of cyberspace can be accepted by Internet users only if they also participate in the process of designing a way to govern cyberspace. Thus, this approach strengthens the legal foundations and powers of non-governmental institutions and actors, in other words, challenges the authority of countries in governing cyberspace. In addition, UN General Assembly Resolution 239/57, adopted in 2002, emphasized that governments, corporations, other organizations and cyberspace users are involved in development processes. Ownership, production, management, service delivery and operation of information systems and networks must be involved in this process. The resolution also emphasizes that participants must take responsibility for the security of these information technologies in proportion to their role (Kremer and Müller, 2014: 15).

In this way of governing in cyberspace, due to the fact that more non-governmental organizations are involved in decision-making processes in cyberspace, it is possible to prevent the monopoly of governments in cyberspace and thus Provide grounds to limit the power of governments to limit and exercise opinions. However, this approach, in turn, can lead to problems. On the one hand, some critics believe that in this structure due to the great diversity of government actors, some of whom may have fierce competition with each other or try to organize the situation in their favor for specific purposes. The conditions for management become more complex, and this can make the process of global governance of cyberspace more challenging. On the other hand, given the growing power of large companies operating in cyberspace, it is likely that by excelling in this field, they will shape the situation in a way that is not in the best interests of the world and the people of the world, but to be within the framework of the partial interests of these

economic institutions (McEvoy Manjikian, 2010). This could ultimately completely destroy national sovereignty in cyberspace and lead to an issue that would limit the national interests of some countries. This has led some countries, especially those in developing countries, to show serious opposition and try to share part of their territorial authority in the geographical area. Extend real and national borders to cyberspace.

5. Conclusion

As mentioned in the previous lines, with the development of cyberspace and the increasing tendency of the world's citizens to use cyberspace, this environment has become a challenging issue for different countries of the world. On the one hand, countries, due to the opportunities that cyberspace has presented to people and countries around the world, intend to increase their capabilities by increasing the opportunities provided in cyberspace for processes. Take advantage of various developments in their country and thus increase the pace of economic growth, increase welfare and improve their position at the national and global levels. On the other hand, due to concerns in the various financial, economic, political, social, cultural, and security spheres, these same countries seek to extend part of their sovereignty from the territorial sphere to cyberspace in order to in this way, they can achieve their national goals that they seek to achieve in cyberspace. These conflicts have led to various issues in the field of cyberspace governance, which has led to the emergence of different approaches in the field of territorial sovereignty over cyberspace. Currently, several different approaches to cyber governance have been proposed. Among these, two approaches have become more important than the others and have brought more complex issues. The first approach is based on multilateralism in cyberspace, in which we see the success of the Hobbesian approach. In cyberspace multilateralism, a number of countries seek to base their analysis on the Westphalian nature of world politics, extending the issue of territorial boundaries and the need to exercise territorial sovereignty and national authority from the real environment to cyberspace. So that countries can exercise their powers authoritatively in cyberspace without any other country being able to disrupt or disturb them. Countries such as China, Saudi Arabia, Iran and Russia are supporters of this approach. This approach has faced various oppositions from international institutions, social activists, political activists and other countries because it increases the power of oversight and control of governments in cyberspace. The second approach is participatory multilateralism in cyberspace, which places a strong emphasis on the distribution of power and authority between governmental and non-governmental actors. Proponents of this approach, who are relatively in the majority compared to the first approach, believe that cyberspace is largely based on the activities of various governmental and non-governmental organizations, private companies, citizens and ordinary users, and so on. The reason for the process of governance is that all actors need to be involved in the process of governing cyberspace at the same time. In a way, this approach can be considered as a kind of global governance in the field of cyberspace, which causes the level of authority and power of governments in this field to be significantly reduced compared to real space. This approach, with all its strengths, has faced various objections and criticisms. This is because, in the first instance, it will reduce the scope of governments' authority to govern cyberspace, and on the other hand, it may lead to the dominance of technology companies operating in cyberspace.

However, the findings of this study indicate that not only the issue of governance and territorial sovereignty in cyberspace remains unresolved, but also the type of response of countries to this issue indicates that it will be unlikely in the future. That there should be a global consensus on how to govern cyberspace. Even if most countries can agree to establish a legal system for global governance of cyberspace, a number of countries may seek to use their limited authority to exercise national authority within their territorial

boundaries. Establish territorial sovereignty over cyberspace that will, more than anything else, restrict international communication for those countries and their citizens. However, given the benefits that the global nature of cyberspace has created, it is still unlikely that countries will move toward cyberspace fragmentation due to national considerations.

References

1. Ahmadipour, Zahra and Rashidi, Younes. (2018). Geopolitical analysis: Representation of fear spaces in cinema. Geopolitical Quarterly. Fourteenth year. Second Issue. Summer.
2. Ahmadipour, Zahra and Rashidi, Younes. (2020). Geographical illustration and geopolitical representation. Tehran: University of Tehran.
3. Barlow, John P. (1996). A declaration of the independence of cyberspace', viewed 15 August 2021. <https://www.eff.org/cyberspace-independence>.
4. Betz, Davis and Stevens, Tim. (2011). Cyberspace and the state: toward a strategy for cyber-power. Adelphi Paper 424, IISS. Abingdon, Oxfordshire, UK: Routlegde.
5. Chertoff, Michael and Simon, Thomas. (2015). The impact of the Dark Web on Internet governance and cyber security', The Centre for International Governance, Global Commission on Internet Governance: Paper Series No. 6, viewed 15 August 2016, <https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf>.
6. Choucri, Nate. (2012). Cyberpolitics in international relations. Cambridge, MA: The MIT Press Cukier, Kent and Mayer-Schoenberger, Victor. (2013). The rise of Big Data. Foreign Affairs, vol. 92, no.3. Pp. 27-40.
7. Cornish, Petr. (2015). Governing cyberspace through constructive ambiguity. Survival, vol. 57, no.3. Pp. 153-76.
8. Deibert, Raymond and Crete-Nishihata, Matthew. (2012). Global governance and the spread of cyberspace controls. Global Governance, vol. 18, no. 3. Pp. 339-61.
9. Deibert, Raymond. (2013). Bounding cyber power: escalation and restrain in global cyberspace. The Centre for International Governance Innovation, Internet Governance Papers: Paper No. 6, viewed 15 August 2021, <https://www.cigionline.org/sites/default/files/no6_2.pdf>.
10. Demchak, Chandler and Dombrowski, Powel. (2011). Rise of a cybered Westphalian Age. Strategic Studies. Quarterly, vol. 5, no. 1. Pp. 32-61.
11. Fehlinger, Peter. (2014). Cyberspace fragmentation: an Internet governance debate beyond infrastructure', Internet Policy Review, 17 April, viewed 15 August 2021. <http://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debatebeyond-infrastructure/266>.
12. Finkelstein, Larry. (1995). What is global governance?', Global Governance, vol. 1, no. 1. Pp. 367-72.
13. Gourley, Samuel K (2014). Cyber sovereignty', Conflict and cooperation in cyberspace, eds. Peter Yannakogeorgos and Antony Lowther. New York: Taylor & Francis.
14. Hafizunia, Mohammad Reza (2011). The political geography of cyberspace. Tehran: Samat Publications
15. Jayawardane, Sydney, Larik, Jack and Jackson, Edward. (2015). Cyber governance: challenges, solutions and lessons for effective global governance', Policy Brief 17, The Hague Institute for Global Justice. viewed 15 August 2021. <http://www.thehagueinstituteforglobaljustice.org/wpcontent/uploads/2015/1
16. Kremer, Jeff F. and Müller, Bernard. (2014). Cyberspace and international relations: theory, prospects and challenges. Heidelberg: Springer.

17. Lewis, James A. (2010). Cyber security: next steps to protect critical infrastructure. testimony to the U.S. Senate Committee on Commerce, Science and Transportation, 23 February, viewed 15 August 2016, <https://www.gpo.gov/fdsys/pkg/CHRG-111shrg57888/pdf/CHRG 111shrg57888.pdf>.
18. Liaropoulos, Alex. (2013). Exercising state sovereignty in cyberspace: an international cyber-order under construction? Journal of Information Warfare. vol. 12, no. 2. Pp. 19-26.
19. McEvoy Manjikian, Mark. (2010). From global village to virtual battlespace: the colonizing of the Internet and the extension of realpolitik. International Studies Quarterly. vol. 54, no. 2. Pp. 381- 401.
20. Nye, Joseph S & Donahue, James. (2010). Governance in a globalizing world. Washington, D.C.: Brookings Institution Press.
21. Patrick, Simon. (2014). The unruled world: the case for good enough global governance. Foreign Affairs, vol. 93, no. 1. Pp. 58-73.
22. 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.
23. 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.
24. 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.
25. Rosenau, James. (1995). Governance in the twenty-first century', Global Governance, vol. 1, no. 1. Pp 13-43.
26. Shen, Yang. (2016). Cyber sovereignty and the governance of global cyberspace. Chinese Political Science Review. vol. 1, no. 1. Pp. 81-93.
27. Slack, Christopher. (2016). Wired yet disconnected: the governance of international cyber relations. Global Policy, vol. 7, no. 1. Pp. 69-78.
28. Weiss, Tom and Wilkinson, Ritter. (2014). Rethinking global governance? Complexity, authority, power, change. International Studies Quarterly. vol. 58, no. 1. Pp. 207-15.
29. West, Sebastian. (2014). Globalizing Internet governance: negotiating cyberspace agreements in the post Snowden Era. Conference Paper, TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy, viewed 15 August 2021, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418762##>.