CYBER CHALLENGE: DIMINISHING POWER OF THE STATE IN INTERNATIONAL RELATIONS

İdris Demir[♣]

Abstract

Cyberspace is a new domain for the actors of international relations to interact and formulate new types of engagements and relationships. International relations theories and practices should reconsider and review the basic approaches and concepts of the discipline in accordance with the developments and applications in the cyberspace. International relations practices and theories have influenced deeply from the interactions in cyberspace. It is evident that cyber developments will continue to affect international relations both as a discipline of study and as the type of engagement among states and non-state actors. States are, traditionally, the central to and most influential actors in international relations. However, some of the activities in cyberspace that states have limited or no control have challenged the roles of the state. Possible cyber-attacks to the citizens, military communications, and critical infrastructures pose threat to national security. The use of cyberspace for terrorist activities is another threat to national security that states have to deal with. These challenges pose threats to the strength of states in international relations.

Key Words: state, sovereignty, anarchy, international relations, cyberspace.

SİBER MEYDAN OKUMA: ULUSLARARASI İLİŞKİLERDE DEVLETIN AZALAN GÜCÜ

Özet

Siber uzay uluslararası ilişkiler aktörlerinin etkileşime geçme ve yeni ilişki ve ortaklık türleri formüle etmelerinin yeni zeminini oluşturmaktadır. Uluslararası ilişkiler teorileri ve uygulamaları disiplinin temel yaklaşımlarını ve kavramlarını siber uzaydaki gelişmeler ve uygulamalar ile uyumlu olarak tekrar düşünmeli ve gözden geçirmelidir. Uluslararası ilişkiler uygulamaları ve teorileri siber uzaydaki etkileşimlerden derinden etkilenmiştir. Siber gelişmelerin uluslararası ilişkileri hem bir disiplin olarak hem de devletler ve devlet dışı

♣ Assoc. Prof. Dr., @ İstanbul Medeniyet University, Faculty of Political Sciences, Department of International Relations. Can be accessed via idris_demir@yahoo.com

aktörler arasında bir ilişki biçimi olarak etkilemeye devam edeceği açıktır. Devletler geleneksel olarak uluslararası ilişkilerin merkezindedir ve en etkili aktörleridir. Ancak, siber uzayda devletlerin kontrolünde olmayan ya da devletlerin kontrolünün sınırlı olduğu bazı aktiviteler devletlerin gücüne karşı meydan okumaktadır. Vatandaşlara, askeri haberleşmeye ve kritik altyapılara karşı yöneltilmesi muhtemel siber saldırılar ulusal güvenliğe tehdit oluşturmaktadır. Siber uzayın terör eylemleri için kullanılması devletlerin ilgilenmeleri gereken bir başka ulusal güvenlik meselesidir. Bu meydan okumalar uluslararası ilişkilerde devletin gücünün azalmasına zemin hazırlamaktadır.

Anahtar Kelimeler: devlet, egemenlik, anarşi, uluslararası ilişkiler, siber uzay

Introduction

International relations theories and practices used to take into consideration of the interactions of various actors such as state or non-state actors, in these domains: land, sea, air and the airspace. There is a new domain of interaction: the cyberspace. International relations epistemology, ontology, concepts and assumptions should reformulate, redefine and/or reconsider themselves in order to tackle and/or keep up with the developments in the cyber domain. This paper is about the challenge of cyber interactions and developments to the notion of state in international relations. In this respect, this study argues that the authority and centrality of states as dominant and major players of international relations have been challenged by rapid technological advances and widespread usage of virtual domain of the cyberspace(Avella Huerfano,2018:16).

States continue to be the prominent and central actors of international relations in physical domains. Though states are, still, the central players and authorities of international relations, cyberspace has prepared a ground where non-state actors of various kinds such as individuals, private companies, non-governmental organizations(NGOs) and international organizations are expanding their influence and involve heavily in politics, security and trade affairs worldwide. The role and effect of states started to erode in the early stages of globalization even before the 21st century.

In clarifying its proposition under discussion, this paper is divided into three parts. First part introduces cyberspace as a new sphere of interaction for actors of international politics. The

differences in actual, real world or kinetic domain and the unique features of cyber domain are presented. Second part deals with the nation states. States are the core features of international relations. It is regarded to be the single actor in the realist paradigm of international relations. Yet, how states are being affected from the novelties of the cyberspace will be analyzed in the second part. Last part deals with cybersecurity. Possible cyber threats to citizens, military and critical infrastructures are discussed in this part. Last part also deals with global cyber terrorism which requires international cooperation and collaboration for an effective response.

Cyberspace as a Novel Domain of Interaction

Cyberspace is a novel/ new arena of interaction. Cyberspace is a venue which provides ground for various actors to engage and formulate activities that are conducted over the electronic fields stemming from technological advancements and innovations. Spatial domains of cyberspace go beyond, transcend territorial borders and economic, social and cultural boundaries with almost none or limited control.

This novel domain of interaction, cyberspace, used to be considered a matter of low politics by the states and in international relations studies. However, it is no longer a matter of low politics; it is a matter of high politics. The challenge that states has to face that the interactions of various types of actors in the cyberspace has created are concerned with the national security, underlying values and principles, core institutions and decision mechanisms of nation states. Currently, cybersecurity related issues are among the highest realm of high politics. Cyberspace has the potential to pose a threat to national security of a nation state and disturb the existing, functional international order (Choucri, 2012: 3).

It should also be indicated that it is inevitable to obstruct the flourishing use of cyberspace and the internet. Cyberspace welcomes new modes and voices in communication, interaction and networking through the internet. Knowledge and information can easily be stored and distributed worldwide among libraries and users of various kinds. Political discourse, norms, goals and modes of behavior can be presented to different users in the global scale. There are shared and common problems of the whole humanity such as air pollution, environmental protection and human rights concerns. Cyberspace provides a ground to publicize common demands and formulate collective responses (Choucri, 2012: 23).

The usage of cyberspace has spread immensely in a –relatively- short span of time. One should recall that the first email in the world was sent in 1971. In 2018, more than 250 billion emails are sent daily. More than half of the population of the world (more than 4 billion people) have access to and use internet. The first web page was created in 1991. Currently there are more than 1,9 billion internet sites in the world. More than 6,26 billion searches are made from the internet daily. Almost 2,240 million people use Facebook actively. Twitter users have acceded 335 million people. There are more than 250 million Skype calls daily. Daily usage of internet exceeds 5 billion GBs (Akyeşilmen, 2018: 62).

It is important to quote the definition of cyberspace. In 2008 Pentagon termed cyberspace as "the global domain within the information environment consisting of the independent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" (Singer and Friedman, 2014: 13).

There are thirteen root servers around the world. These root servers provide domain names for internet addresses. Ten of these root servers are located in the United States of America; remaining three are located in the United Kingdom, Sweden and Japan. There are 191 co-root servers that are located in various parts of the globe.[2] The reason why the root servers and co- root servers are not located in a single place results from the concerns about the physical security of internet. By this way, internet would be able to continue to operate in case of a physical assault or natural disaster to any of these facilities (Akyeşilmen, 2018: 30).

Cyberspace has a multi centered structure. This feature of internet system forms the base for the notion and nature of anarchy concerning its governance. These servers are managed and inspected by civil society institutions such as Internet Engineering Task Force (IETF) and The Internet Corporation for Assigned Names and Numbers (ICANN). Operational management of these servers in global internet governance causes a ground for a great conflict among prominent international actors. It is going to be wise to argue that this particular issue is going to continue to be a major problem in international relations agenda in the foreseeable future (Akyeşilmen, 2018: 30).

[2] There are three co- root servers in Turkey; two of them are in İstanbul and the other one is in Ankara.

The unanswered question on who runs internet is gaining more importance day by day. In 1997 manager of Google Eric Schmidt at a conference of programmers in San Francisco has indicated that "The internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." (Singer and Friedman, 2014: 26). In the meantime, it should be indicated that major actors, dominant players in the cyberspace are private companies, ie non-state actors. States, as sovereign entities, major actors in international relations are regarded to be late comers as influential contributors in the virtual domain of the cyberspace.

Cyberspace has an anarchic nature. It eliminated borders and distances. It has strengthened non-state actors. It has increased the influence of various non-state actors in the field of international relations. International relations theories, processes and actors have been influenced deeply in both epistemological and ontological aspects (Choucri, 2013: 4). The notion of state has been influenced and effected deeply and heavily from the novelties supplied through the active and effective usage of the cyberspace.

It has been indicated that advancements and developments in cyberspace and cyber communication have considerable reflections on the study of international relations. Decision making calculations, information sharing procedures and diplomatic processes are under heavy influence. There are new interest groups in international politics (Wescott, 2008: 2). These groups are active and have contributed to the decision making processes ie: government officials have to take the role and the influence of these new actors into account in formulating and shaping their policies. State is no longer the sole actor in distribution and control of information. Either fake or accurate information can easily and cheaply be distributed both domestically and internationally with a limited and sometimes no control of the state. Diplomatic services can be maintained faster with the help of advancements in cyber domain.

States in Cyberspace

States are polities that are defined in terms of territoriality, sovereignty, centrality and nationality (Yurdusev, 2012: 64). States are political entities that have geographical boundaries (borders) and are governed by their own central authorities. States are taken as the most important, primary actor in international relations. Defending the physical security of

their population and ensuring the economic prosperity of their citizens are two of the most central responsibilities of states. States provide focus for loyalty and identity and claim sovereignty (Viotti and Kauppi, 2013: 6). States claim and represent authority over their population within their territories and are autonomous in the international arena.

One should keep in mind that there are two main modes of interactions concerning organizational behaviors ie. hierarchy and anarchy. If the relations and interactions among the participants/actors involve clear and strict lines of obedience and authority, this type of relationship is considered to be hierarchical. Relations among actors/units are classified to be anarchical if there exist no such lines of defined and structured obedience and authority.

States are sovereign entities. Sovereignty is a claim of political authority to formulate policies and conclude actions within territorial borders. Single authority is the state (Viotti and Kauppi, 2016: 446). There is not an higher authority over states. There is not an authority that dictates or shapes the behaviors of states in a hierarchical structure. Therefore, international relations are regarded/described to be anarchic concerning the mode of interaction among units. An overcharging authority or government that rules, regulates and enforces law on all states is absent, does not exist in international relations. It is going to be wise to argue that his notion of anarchy is more visible and effective in cyberspace (Akyeşilmen, 2016:45; Wu,2013: 6).

States have territorial boundaries. States are the rule makers and sole authorities within their borders. This is an empirical reality. However, this central notion of sovereignty has started to be treated as, just, a definitional factor rather than a jurisdictional component concerning interactions in cyberspace. The regulatory authority of states in physical, political, social and economic aspects face new types of interactions that are brought by the cyberspace.

Cyberspace has the potential to diminish state sovereignty. It weakens the link between geographic location and the control of governments (each nation states) on the control of online activities and behaviors. States cannot control or direct the effects of online behaviors and activities on their citizens. There can also be a mismatch between the rules that are applicable to the global phenomena and the approaches of each sovereign unit (Johnson and Post, 1997: 6).

In addition to the alterations or the new outlook it brings to the concept of sovereignty, cyberspace has already effected and/or would affect some other aspects of international relations studies where states are in the center(Korhan,2017:79-81). Contrary to the traditional international relations thinking, cyberspace is not state centered. Its denominator-centered structure include individuals, private companies, NGOs,states and international institutions. International boundaries are more permeable. The notion of territoriality has gained a new dimension. There are no state borders in cyberspace. Thus, borders are no barriers for cyber-attacks anymore. Cyber-attacks are asymmetric in their nature. Therefore, cyber conflicts and cyber wars need to accommodate novel types and ways of security and defense. Cyber governance is another major issue of concern that states has to face as a challenge to their authorities (Akyeşilmen, 2018: 180-181).

The power and authority of states in cyberspace is diminishing step by step in the light of rapid developments and advancements that are brought by cyberspace only some of which have been mentioned in this particular article. What states can/should do as sovereign entities and major actors of todays' international relations in order to continue to remain at the center of international relations studies in the future, too is the content and subject of a future study.

Cybersecurity and the States

In traditional sense, the notion of security is attached to military security. Security of the borders of the state against the enemy states and the capability of the military to defend these borders are regarded to be external security of the state. Internal security and stability of the state, on the other hand, is achieved by the strength of domestic institutions and their capabilities in enforcing law and order. This is attached to the notion of sovereignty of the states. Environmental security is another dimension of security. The ability and capability of the states in meeting the demands of their citizens are important components of environmental security.

Cybersecurity is a new phenomenon. The ability of states to protect their institutions against possible 'threats, espionage, sabotage, crime and fraud, identity theft and other destructive e-interactions and e-transactions' (Choucri, 2012: 39) has become fundamental in national security studies. Cyberspace, in fact, creates security questions and problems from the individual level to global level of analysis in international relations. States are responsible for

the wellbeing of their citizens in all aspects of security. In this regard, states are vulnerable to attacks in the cyberspace.

Activities in the cyberspace in interactions of various kinds are expanding at all levels of analysis in international relations from the individual to systemic and, even, the global level. Nowadays, cybersecurity has become a vital component of global security. It has a multi centered and multi pillared structure. It has turned out to be an anarchy which can neither be controlled nor regulated and inspected in the international and global levels of analysis.

Cyberspace has become an important issue of security, military and strategy for state authorities. It is one of the vital components of national security concerns. In todays' world, states find it hard to tackle with the problems coming from the cyberspace. The challenges range from individual level such as unauthorized accesses targeting the intellectual properties of the citizens to destabilizing the economic, strategic and military facilities of state infrastructures.

Violation of the right to privacy cases increase tremendously as a cyber-threat to citizens of each sovereign state. There may be some gaps in domestic legislations of the states. Therefore crime and punishment balance may –sometimes- not be distributed equally. This is considers to be threat to the basic principles of statehood concerning domestic aspects.

It should also be indicated that the use of cyberspace for military purposes poses other challenges for states to prepare solid grounds for integrity, prosperity and stability. It is regarded to be a powerful requisite for national security. Cyber-attacks on networks can obstruct the communication systems of the military (Choucri, 2012: 149). It can paralyze the army. This would, with no doubt, cause a serious threat to national security. Cyber-attacks toward Estonia in 2007 and Georgia in 2008 are clear examples of the importance and vitality of cybersecurity for states in terms of military and national security.

Cyber-attacks to critical infrastructures are another major issue of concern that states have to tackle with. Possible external or internal threats towards energy, transportation and/or banking infrastructures would have negative reflections upon citizens in various aspects. This would cause social unrest at the same time. One should remember that states are in defensive position in the cyberspace and sometimes are unable or incapable to defend the critical

infrastructures because of the unique aspects of the cyber domain to its own. This is regarded to be another issue undermining the strength of states.

Terrorists of any kind can use the cyber domain to express and distribute their political messages and counter arguments in violent ways. This is a problem almost all nation states face. In order to safeguard the state, authorities and rule makers cooperate with other states. International collaboration and cooperation is important for an effective functioning of a safe and secure cyberspace in the global level. This can help prevent terrorist activities conducted in the cyberspace. However, the anarchic nature of the cyberspace prevents such kind of an joint action. The multiplicity of actors -from private sector companies to various nation states; from individuals to different interest groups; from international organizations to civil society institutions- bring different definitions and perceptions of interests and priorities into agenda. This results in a difficulty in formalizing, concluding and implementing cooperative action. Cooperate activities against global terrorism is no exception.

Conclusion

The discipline of international relations has emerged in the early twentieth century (Devetak,2012: 1). International relations theories and practices are trying hard to be able to keep up with and tackle with the developments, advances and challenges illustrated with the increasing usage of the cyberspace (Choucri and Clark, 2012: 2). Cyberspace has strengthened and has increased the role and influence of non-state actors in international relations. Individuals, especially, have expanded their capacities and capabilities as –more-influential actors in international relations.

The anarchic structure of the global internet has reflected itself as a kind of anonymity in cyberspace. This places different burdens of security and freedom approaches over the shoulders of the states. Cyberspace has given an opportunity and ground for both individuals and various types of groups (non-state actors) to be able to bypass the rules and regulations that are placed by the power and the authority of the state. Although there are efforts and studies of states to control and regulate activities in the cyberspace, different types of users and actors from individuals to interest groups and other states have been able to break the chains of control and regulation efforts embodied by nation states as a part of their sovereign activities.

Sovereign states are the main actors in the international system. International organizations, non-governmental organizations, interest groups are also actors in kinetic, actual international relations with different capacities of influence. However, cyberspace has created and strengthened new actors, networks and interests in the virtual domain that started to find place in international relations studies. Moreover, it should be indicated that cyber studies will continue to increase its influence on international studies and would most likely dominate all aspects of global affairs.

This newly structured global affairs would most likely face state power and influence of which has diminished in confrontation with other actors. The ability and capability of state in establishing cybersecurity both for its citizens in the individual level and protecting the survival of the nation as a unit in international system show some signs of weaknesses.

Access to internet has tremendously increased. It affects all aspects of economic, political and technological lives of all levels of analysis of international relations from individuals to global systemic level. Internet is not controlled or regulated by a single institution and/or authority. This results in anarchy. Non state actors –especially private sector actors- are very active in the cyberspace and cyber conflicts(Oruç, 2017:49-51).

Contrary to the kinetic domain of international relations where state sits in the center of international relations, as sovereign, has the capacity and the capability of rule and regulation in both domestic and international dimensions, cyber domain has challenged the paramount role of states. There are no doubts and question marks about the –diminishing- role, authority, capacity and capabilities of states. States lack the capacity to control, regulate and provide security of this virtual domain alone. States have to accommodate and cooperate with non-state actors for a safe and secure cyberspace. States are no longer regarded to be the actors of the first and the last resort in international relations.

Bibliography

Akyeşilmen, Nezir. (2016). Cybersecurity And Human Rights: Need For A Paradigm Shift.? *Cyberpolitik Journal*, Volume1, Number 1&2 Winter 2016, pp.38- 61.

Akyeşilmen, Nezir. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Güvenlik ve Siber Politika*, Ankara, Orion Kitabevi.

Avella Huerfano, Luis Caros.(2018). The Implications Of The Lack Of A Cyber-Conflict Definition. *Cyberpolitik Journal*, Volume 3, Number 5, Summer 2018, pp.10-22.

Choucri, Nazli and Clark, David. (2012). Integrating Cyberspace and International Relations: The Co-Evolution Dilemma, *Massachusetts Institute of Technology Harvard University Working Paper, ECIR Workshop on Who Controls Cyberspace*? November 6-7, 2012.

Choucri, Nazli. (2013). Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences. *World Social Science Forum*, Montreal, Canada, 2013. https://ecir.mit.edu/sites/default/files/documents/%5BChoucri%5D202013%20Co-Evolution%20of%20Cybersoace%20and%20International%20Relations.pdf. (Accessed: 12/12/2018).

Choucri, Nazli. (2016). *Cyberpolitics in International Relations, Cambridge*. The MIT Press.

Devetak, Richard. (2012). An Introduction to International Relations: The Origins and Changing Agendas of a Discipline. in Devetak, Richard., Burke, Anthony. and George, Jim, (edts.) *An Introduction to International Relations*: Second Edition, Cambridge: Cambridge University Press.

Johnson, David. and Post, David. (1997). The Rise of Law on the Global Network. Kahin, Brian. and Nesson, Charles(eds.). *Borders in Cyberspace: Information Policy and the Global Information Structure*. Cambridge: MIT Press.

Korhan, Sevda.(2017). Siber Uzayda Aktör-Güç İlişkisi. *Cyberpolitik Journal*, Volume2, Number 4, Winter 2017, pp.75-103.

Oruç, Hüseyin.(2017). Cyberconflict: An Efffect of Globalization on Conflict Ecosystem. *Cyberpolitik Journal*, Volume2, Number 4, Winter 2017,pp.44-56.

Singer, P. W. and Friedman, Allan. (2014). *Cybersecurity and Cyberwar*, Oxford: Oxford University Press.

Viotti, Paul. and Kauppi, Mark. (2013). *International Relations World Politics*. USA, Pearson.

Viotti, Paul. and Kauppi, Mark. (2016). Translation Editor Aksoy, Metin. *Uluslararası İlişkiler Teorisi*. Ankara: Nobel Akademik Yayıncılık.

Wescott, N. (2008). Digital Diplomacy: The Impact of the Internet on International Relations. Oxford Internet Institute. *Research Report* No: 16.

Wu, Timothy. (2013). .Cyberspace Sovereignty?- The Internet and the International System. *Harvard Journal of Technology*. Vol no.3, Issue no.1.

Yurdusev, Nuri., (2012). Ulus-Devlet: İnsanlığın En Tehlikeli İcadı, Arı, Tayyar(ed.). *Uluslararası İlişkilerde Postmodern Analizler-1*. Bursa: MKM Yayıncılık, pp: 59-75.