REALISM AND CYBERSECURITY: A COMPARATIVE APPROACH

Murat POYRAZ*

Abstract

This article aims to analyze the relationship between cybersecurity and realism, which is one of the founding debates in IR discipline. In addition to this, it also examines the security perspective of realism and cybersecurity. The security perspective of realism is that there must be no threat to values gained. In terms of the realist approach, the state is the only actor whose security can be threatened and who can threat security and can provide a secure environment. The birth of cyberspace has brought with a lot of positive and negative facts that directly relate to states. Initially, state that is accustomed to physical threat did not show any interest in threats that comes from the cyber area. However, it has been changed by practical events. Attacks that can take place within seconds have altered the security perception of the states.

Key words: Realism, Cybersecurity, Cyberspace, Nation-state, International Relations Theories.

REALİSM VE SİBER GÜVENLİK: KARŞILAŞTIRMALI BİR YAKLAŞIM

Özet

Bu makale siber güvenlik ve Uluslararası İlişkiler disiplinindeki kurucu tartışmalardan birisi olan realizm arasındaki ilişkiyi incelemeyi amaçlamaktadır. Ayrıyeten, bu çalışma realizmin güvenlik perspektifi ile siber güvenlik anlayışını da incelemektedir. Realizmin güvenlik perspektifi kazanılan değerlere karşı bir tehdidin olmaması şeklindedir. Realist anlayış da devlet, güvenliği tehdit eden, tehdit edilen ve güvenliği sağlayacak tek aktör konumundadır. Siber uzayın doğuşu devletlere yönelik olarak olumlu ve olumsuz birtakım olguları da beraberinde getirmiştir. Fiziksel tehdide alışkın devlet, siber alandan gelecek tehditleri önceleri çok umursamasa da pratikte yaşanan gelişmeler ile birlikte bunun böyle olmayacağı anlaşılmıştır. Saniyeler içerisinde gerçekleşen saldırıların varlığı, devletlerin güvenlik algılarını değiştirmiştir.

Anahtar kelimeler: Realizm, Siber Güvenlik, Siber Uzay, Ulus-devlet, Uluslararası İlişkiler Teorileri.

* Research Assistant, Department of International Relations, Recep Tayyip Erdoğan University, Rize-Turkey. The author can be reached via e-mail: murat.poyraz@erdogan.edu.tr.

Login: Realism Build by Power, Security, and Interest and Cyberspace

It is a well-known fact that the First World War has great importance in the emergence of International Relations[4] (hereafter IR) (Little, 1999, p. 292). In this regard, it may be claimed that IR is a result of the war (Dunn, 1948, p. 145). Accordingly, with the impact of the war, basic subjects of IR were such as peace, security, war, international organizations, and so on (Özlük, 2014, p. 106). After the First World War, by taking into account the question of the war is inevitable, which has been an underlying problem in IR discipline (Carr, 2015, p. 8), it can be said that IR is a result of the search for pursuing security. It was only after the First World War when IR began to crawl; realism[5] is one of the sides known as the first great debate (Çalış & Özlük, 2007, p. 225).

As Gilpin indicated (2011, p. 300), according to realism, it is generally claimed that the state is seen as a primary actor and a fundamental unit of analysis. Other actors such as international organizations or non-governmental organizations are not included in the analysis made due to state which has sovereignty by itself (Sümer, 2014, p. 79). From this point of view, individuals, multinational corporations, terrorist organizations, mafia groups, and states are the main actors in the cyber area rather than the notion based on a single actor in realism. Since it may be said that not only states but also other actors are effective in the cyber area (Korhan, 2017, p. 78-84).

In realism, one of the most important characters of the state as a primary actor of international relations is rational (Kolasi, 2013, p. 157). In the context of human nature, actually by being homologizing, rational states pursue their interest and avoids things deemed as bad in international relations. Actors positioned in the cyber area also can act rationally, with exceptions.[6] According to this point, for instance, assuming the war between Russia and Georgia in 2008 (Güntay, 2016, p. 112), Russia was conducting a war against Georgia. It was a conscious movement for Russia to consider all possibilities as to winning the war at a

[4] In this paper, the term *International Relations* refers to a discipline when its first letters are capitalized and refers to just a relationship when its first letters are lowercase.

[5] In some researches, realism might refer to classical realism or political realism. In this study, the term realism covers these terms.

[6] Occasionally, an individual may try to carry out a cyberattack on account of the fact that he or she wants to prove itself in the area.

minimum cost. From the perspective of realism, Russia must wield possible opportunities in order to win a war. In this context, cyberattacks from Russia to Georgia's service server are a conscious movement.

As Yalvaç pointed out, the states acting separately from social relations (2014, p. 22) have a recognized identity (Christian, 1992, p. 14) on account of its rational nature and politics, as a specific area isolated from all areas. States are the delegate of national interest with its recognized identity. Thus, it may not be claimed that cyber actors act separately from social relations in the cyber area in which there is no one actor. Additionally, it may not be asserted that the cyber area is an autonomous area from all areas, as the political and economic processes may affect the cyber area. Besides, the state may represent its national interest in the cyber area, but also state may represent its national interest by getting in contact with the other actors.

Another feature of states is the black-box (İlimvemedeniyet, 2016). That is to say, political regime, constitution, national norms, and political parties in a country make no sense. It is worthy of note that a foreign policy of states stems from black-box are essential. The component forming content of the black box is not essential in international relations in which there is no higher authority designating everything. As the main viewpoint of states towards other states is the security (Mowle, 2003, p. 561). In this regard, it is challenging to implement the concept of the black box upon other actors in the cyber domain. Since, if we take into consideration the black box concept through global companies which are one of the actors in the cyber area, the decision in some international companies are taken through more than one process. The impact of every process eventually may affect the decisions taken.

Realists have deemed the international system as the absence of the upper hand, which would intervene to issues between state and solve conflicts between state or ensure the security of states, as in the case of domestic policy. This circumstance is termed as anarchy (Aydın, 2004, p. 37). Similarly, actors in the cyber field act in the absence of higher authority; thus, cyberspace is anarchic as well (Turan, 2014, p. 727). The state may govern actors situated in internal structure through its sovereignty or some instruments such as army and police (Soresen, 2005, p. 81-82). However, states in anarchic cyberspace cannot govern individuals or other actors in the cyberspace. Furthermore, none of the actors in the cyberspace be

decisive in the relationship between cyber actors since states as a higher authority in domestic policy have no power of control in anarchic cyberspace.

It is usually accepted that a state acting in an anarchic environment may desire to continue its existence and to guard its power owing to its avails that people of the state benefit from (Balcı, 2014, p. 123). In the same manner, no actors, especially individuals, in the cyberspace desire to be limited due to the power they have, while some arrangements are introduced in cyberspace. In a sense, there is no subsidiarity for the actors in cyberspace as well.

Realists may assert that the ultimate and the most crucial task for states are pursuing power (Arı, 2010, p. 160) by considering the power in its historical background (Gismondi, 2004, p. 460). It is the state as the main actor that may attain power (Sandıklı, 2012, p. 6). States and individuals are getting into power struggle due to some features of human nature, such as the pursuit of self-desire, self-interest, selfishness. Thus, actors in cyberspace acting in a set of objectives, economic gain, information stole, or demonstrating themselves (Folker, 2002, p. 72). In this setting, one of the goals is to increase their power in the cyber area. That is to say, the struggle for power is valid in the cyberspace.

As Balcı says (2014), by taking into account the starting point of anarchic international relations, realism is an approach that tries to grasp how states acting basically on behalf of their interest in the anarchic international system in which there is no regulator (p. 119). Hence realists argue that human being has an unbearable desire for power and interest with an analogy from the notion of human nature (Folker, 2002, p. 78). From this point of view, the state can pursue its interest (Eralp, 2004, p. 73), which is deemed as a universal principle (Shimko, 1992, p. 281-283). Although the interest is not precisely identified (Çalış, 2008, p. 10), actors in cyberspace also acting on their interest, for instance, the conflict between Syria and Israel can exemplify this argument. Israel was sensing the first-rank security threat from Syria in 2007. From the realist view, Israel's interest was to eliminate the existing security threat at that time. In this respect, by showing itself as a friend in the Syrian air defense system with the trojan horse, Israel bombed nuclear facility made by in cooperation between North Korea and Syria.

Hans J. Morgenthau (1954, p. 14) brings forward the six basic principles of realism in his work written in 1954. Accordingly, he put it ‘‘political realism refuses to identify the moral

aspirations of a particular nation with the moral laws that govern the universe.'' In this context, he put forward that moral norms and factors cannot be applied to politics and interstate relations. Thus, it may not be anticipated that these factors could impact on international relations (Deşilmek, 2015). As what the most significant is the state's power, interest, and security. For cyberspace, that moral laws or norms are not being taken into consideration cannot be deemed as a general principle. It may be, however, valid for black hat hackers (Karakullukçu, 2017) or for those who act in a way seen as a bad intention.

As can be practiced in security studies, four questions can be raised here to understand the parties' perspectives towards security. Who is the actor whose security is threatened? What is the threat that endangers the actor? How can we secure the actor whose security is threatened? Who are the actors that can ensure safety? (Kardaş, 2014, p. 337). With these questions, I try to analyze different and similar aspects of the parties while evaluating the relationship between realism and cybersecurity.

Realist Security Perspective and Cyber Security

The security perspective of realism is state-centric due to the state as the primary actor. At this point, security is considered as ''the absence of threats to acquired values'' (Wolfers, 1952, p. 485). The security of the individual is only made dependent on the security of the state (Sandıklı, 2012, p. 5). While the security perception in realism is only as to the state, it is claimed that the security perception in the cyber area is associated with the user (a person), the state, the international company, the network, the computer, and so on (Bıçakçı, 2013, p. 4-8).

In this concept, according to realism, the only actor that could threaten the state acting in the anarchic international system is another state. In realism, it is the other state that puts the state into a security crisis. In other words, the state is the only actor that both have security problems and threatens security in general since the primary actor in international relations is the state. From this perspective, the situation is not the same as cyberspace. With the increase in the number of actors in the cyber area, the actors who have security problems increased. The perception of threat may be directed towards not only actors but sometimes physical infrastructure in cyberspace (Choucri, 2012).

Morgenthau (Morgenthau, 1954), sets forth the six fundamental principles of realism, claims that ‘‘politics, like society in general, is governed by objective laws that have their roots in human nature.’’ (p. 4). On the other hand, Hobbes (Hobbes, 2007) feel that wars and conflicts are inevitable and natural with his analogy to human nature. Conflicts in cyberspace can be seen as natural and inevitable as well since war and conflict are natural and inevitable at the level of states, individuals, and other actors confronting threat in cyberspace (Akyeşilmen, 2013, p. 18-19). Accordingly, there could be security problems for actors in cyberspace.

As wars and conflicts are natural, idealistic arguments such as justice, law, international organizations, and trade cannot be effective in preventing related issues (Balcı, 2014, p. 120). Conflict may also occur in cyberspace, but the current level of conflict can be reduced or controlled by laws that will be established and by an international organization that regulates relations between the actors in this area.

Eralp (2004, p. 71-72) thinks that human nature is inherently selfish and self-seeker while examining human nature. In addition to this point, individuals who have the said characteristics also can act under the desire to dominate (Kolasi, 2013, p. 157). This notion is the answer to why the wars emerged in realism (Donnelly, 2004: 9). To put it more clearly, the wars break out on account of some features in human nature. Therefore, states have security problems and struggle for power or interest. In this respect, it can be said that the conflicts in the cyber field might reflect some of the characteristics of human nature. At this point, one of the actors in cyberspace, namely the black-hat hackers, stands out. Russian hacker Vladimir Leonidovich Levin stole a total of 107 million dollars from organizations such as Saint Petersburg and Citibank with the help of a laptop in 1994 (Karakullukçu, 2017). Such events taking place in the cyber field illustrate human nature that might be consistent with realists’ arguments.

In addition to the argument pointed out above, it can be predicted that the rational actor, the state, can act in a particular manner in its foreign policy (Balcı, 2014, p. 125) İf the state has a security problem, the fact that there are ways or means which help it to solve is undeniable. The security problem can be resolved by opting for an alliance option (balancing) or war option. Such arguments show that realism is a-historic theory as well. In other words, one of the most critical features of realism is that the arguments concerned are universal. Even

though the realism can be seen as a theory isolating itself from the impacts of history, this is not the case in cyberspace. Actors who are in the cyber area may pursue a range of strategies while trying to ensure their security. For an individual, taking educational courses and wielding safety programs on the Internet may be sufficient for the security. For a state, due to its sovereignty, it may need different and practical tools such as comprehensive security software for its institutions or establishing an organization to prevent cyber-attacks. In this respect, as cyberspace is an area that brings all people together, the concept of universal arguments is also valid for cyberspace (Tarhan, 2017, p.119).

The most crucial factor that can help the state to ensure its security, increase its power, and pursue its interest is military power. From this point of view, it is necessary to be in constant preparation to support military power (Donnelly, 2004ü p. 12-15). In this respect, issues such as military power and security are included in the high policy that is effective in the conduct of international relations (Hobden, 1999, p. 260). Although the cyber area is essential for military power due to its unique nature, it is information that matters rather than military power (Tarhan, 2017, p. 119).

The balance of power that is thought to exist first in the Tukidides period and then the 17th century is believed to be functional in ensuring the security of the states, even though wars are inevitable (Varlık and Demir, 2013, p. 72). States in foreign policy can enter into an alliance relationship either to turn the tables on their interests or to balance the powerful actor in the existing system. The main motivation of states to enter an alliance is first to ensure their security expectations, then to create a balance of power. At this point, according to a classification made, internal balancing is termed as choosing to increase internal capacity and external balancing is termed as an attempt to stop the powerful actor by getting together in an alliance system (Özlük, 2017, p. 234-236). States can seek internal balancing in their domestic policy by establishing cyber defense centers, providing cybersecurity training, cooperating and coordinating between public and private sectors; or they can both cooperate and reduce security problems by choosing external balancing towards the issues that they can face in the cyber field by setting some regimes or procedures among them.

When one of the states located in the system increases its power and passes the other states, the balance of power will start to be functional. In such a case, the rising power can want to dominate the other states by showing expansionist tendencies in international politics. In this

case, if the growing force is not be balanced, wars will arise (Arı, 2010, p. 22). The actor, who increases his power with knowledge in cyberspace, may not attempt to direct wars but may want to test his strength. Hackers who increase their knowledge and develop their skills may turn to targets (such as banks, company accounts) in a way where they could achieve higher profits

Realists believe that the structure of international relations is characterized by the self-help principle based on the anarchic condition; thus, anarchic nature of the international system leaves states alone in the matter of security (Balcı, 2014, p. 126). Given the fact that the cyber area is anarchic, self-help is relatively valid in cyberspace. An attack made in the cyber area may give rise to security problems. On account of the attack taking place within seconds, the actor that is exposed to the attack must respond to the security problem in question at first by itself. If the issue cannot be eliminated, the problem may bring about a severe security crisis. In this regard, to illustrate this, Estonia firstly tried to set against the attacks of Russia, and when the situation started to worse, Estonia calls for assistance from NATO[7] and the EU[8] (BBC, 2007).

Since the state is located in an anarchic environment, it cannot rely on other states to ensure its security. In this environment, states can intervene in other states to reinforce their security, and engage in some attempts to weaken them. States that want to ensure their security and increase their power may prevent each other's goals (Deşilmek, 2015). Although this is not valid for every actor in the cyber area, some actors act upon this direction from time to time. That BND[9] monitored all electronic correspondence of the Ministry of Industry and Trade of Afghanistan and cyber spying activities made by North Korea against South Korea may set an example (Ünver & Canbay, 2010, p. 99).

A Shift in Security

In realism, war is a tool to ensure states' security and balance of power. From this point of view, if we take into account the state's battle with another state, it is not difficult to determine the direction of the attack. For instance, suppose that there is a war between state X and state Y in the early 1990s. These two states are adjacent to each other. At this point,

[7] North Atlantic Treaty Organization

[8] European Union

[9] German intelligence service (Bundesnachrichtendienst)

according to realism, the security aspect of this war might be guessed with its exceptions. In this situation, the state knows its enemy or enemies. However, this is not the case in cyberspace. First of all, it is complicated to identify the other actor attacking you. Because the cyber field does not allow it. Unidentified actors can show themselves anywhere in the world and carry out a cyberattack (Öğün & Kaya, 2013, p. 167). In this case, it will create uncertainty for actors who may be exposed to a cyberattack. In such a case, cybersecurity measures taken must take into consideration this circumstance.

In the second place, the weapons that the state will use in the war are apparent, which is in tune with realism. In other words, there are land, naval, and air weapons that the state can use. The state can respond to the current attack with physical weapons. Nevertheless, the primary thing that stands out in cyberspace is information. We can use such physical tools in cyberspace. However, if the cyber dimension of security comes into question, we may have to take into account cyber tools in cyberspace (Daban, 2016, p. 96). In this respect, the cyber threat comes into prominence instead of physical danger. Again, in this direction, our understanding of security has also changed. Instead of material security, cybersecurity comes to the fore for the state's security as well.[10]

In the related war, war weapons that state X will use against state Y have a burden for citizens of state X and state X's economy. The precautions taken in both war and peacetime are economically expensive. As for the cyber area, the tools we use in cyberspace are cheaper than the devices in the physical world. A computer or telephone is enough equipment to carry out an attack. With these tools, attacks such as DDoS (Distributed Denial of Service), phishing, and spam can be made.

Moreover, people who will take part in this war are certain, usually soldiers. These soldiers' training, tools, war experience are essential for the war. Soldiers are expected to have

[10] Yet there is an extraordinary situation in the cyber domain. That is to say, with a cyber-attack against the critical infrastructure of states, it can make life difficult, even if it does not kill people. In this context, life in Estonia became difficult for almost one month, owing to cyber-attacks aiming at the critical infrastructure of Estonia in 2007 (Gücüyener, 2015, p. 18). Besides, it may be asserted that cyber-attacks carried out by Russia against Estonia have caused the introduction of the phenomenon of cybersecurity to the security agenda of the state (Korns & Kasternburg, 2009, p. 60-70). Therefore, non-physical attacks in the cyber area may have a great impact on the physical life of people.

information on the physical world. This circumstance could be the same in the cyber field in terms of some points. In order to cope with the recent security problems in cyberspace, cyber armies have been established, and cyber soldiers have been trained. The most important thing expected from the cyber soldiers is to have knowledge and skill regarding the virtual world.

According to realist understanding, the said war will be carried out by organized groups against each other. This approach is similar to cyberspace. That is to say, an individual as a user in cyberspace can carry out cyberattacks to particular targets such as international organizations or a state through zombie computers in an organized manner. In this respect, the cyber area contains a feature that strengthens every individual as well. The main target in this organized war is the state and, in particular, the soldiers and even the people. It is possible that people fighting against another organized group can die in this war. However, there has been no known human death in cyber-related conflicts or attacks so far.

Conclusion: A Realistic Cybersecurity?

The relationship between realism and cybersecurity was analyzed above. At this point, realism and cybersecurity have similar approaches in rational state understanding, in representing the national interest, in the anarchic situation, in opposing the transfer of power, in the power struggle, in interest-oriented steps, in the delineation of human nature, in expansionist tendency, in intervention to internal affairs and self-help.

Just as there are similar points, there are different points in the relationship concerned. In this respect, realism and cybersecurity have different approaches in the number of primary actors, in the number of actor that is independent from autonomous and social relations, in domestic and foreign policy distinction, in high and low policy distinction, in the decisiveness of moral principles, in the security perception, in the proliferation of actors that can threat, in the military power, and the continuous insecurity environment.

In realism, the actor, whose security is threatened, is the state. It is the state that threatens the actor whose security is threatened. The actor who can ensure the elimination of the security problem is again the state. The state can eliminate the security problems with two options, the balance of power or war.

In terms of cyberspace, the actor, whose security is threatened, is not only the state. There are many actors, such as individuals or international companies, whose security can be threatened. Because of the reasons showed above, cybersecurity has changed the understanding of the threat and the states' perspective on security.

Bibliography

Akyeşilmen, N. (2013). Çatışma Yönetimi: Kavramsal ve Kuramsal Bir Analiz. N. Akyeşilmen (eds), in Barışı Konuşmak: Teori ve Pratikte Çatışma Yönetimi. Ankara: ODTÜ Yayıncılık.

Arı, T. (2010). Uluslararası İlişkiler Teorileri, Çatışma, Hegemonya, İşbirliği. Bursa: MKM Yayıncılık.

Aydın, M. (2004). "Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği", Uluslararası İlişkiler, Vol. 1, Issue. 1.

Balcı, A. (2014). Realizm. Ş. Kardaş & A. Balcı (eds), in Uluslararası İlişkilere Giriş. İstanbul: Küre Yayınları.

BBC. (2007). http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml [Accessed on: 11. 11. 2019].

Bıçakçı, S. (2013). 21. Yüzyılda Siber Güvenlik. İstanbul: Bilgi Üniversitesi Yayınları.

Carr, E. (2015). Yirmi Yıl Krizi 1919 - 1939. İstanbul: Yirmi Yıl Krizi 1919 - 1939.

Choucri, N. (2012). Cyberpolitics in International Relations. London: MIT Press.

Christian, R.-S. (1992). "Realist and Resistance Utopias: Community, Security, and Political Action in the New Europe", Millennium, Vol. 21, Issue 1.

Çalış, Ş. (2008). Türkiye-Avrupa Birliği İlişkileri: Kimlik Arayışı, Politik Aktörler ve Değişim. Ankara: Nobel Yayınları.

Çalış, Ş. & Özlük , E. (2007). Uluslararası İlişkiler Tarihinin Yapısökümü: İdealizm - Realizm Tartışması. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Issue. 18

Daban, C. (2016). "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", Cyberpolitik Journal, Vol. 1, Issue. 1.

Demir, M. (2012). http://www.muratcandemir.com/nesnelerin-interneti-nedir-iot.html [Accessed on: 21. 11. 2019]

Deşilmek, E. (2015, Ocak). https://www.academia.edu/28198267/REAL%C4%B0ZM%C4%B0N_G%C3%9CVENL%C4%B0K_ANLAYI%C5%9EI_VE_SO%C4%9EUK_SAVA%C5%9E_SONRASI_BALKANLARIN_G%C3%9CVENL%C4%B0%C4%9E%C4%B0[Accessed on: 19. 10. 2019].

Donnelly, J. (2004). Realism and International Relations. Cambridge: Cambridge University.

Dunn, F. (1948). "The Scope of International Affairs", World Politics, Vol. 1, Issue. 1.

Eralp, A. (2004). Uluslararası İlişkiler Disiplininin Oluşumu: İdealizm-Realizm Tartışması. in Devlet Sistem ve Kimlik, Uluslararası İlişkilerde Temel Yaklaşımlar. İstanbul: İletişim Yayınları.

Folker, J. (2002). "Realism and the Constructivist Challenge: Rejecting, Reconstructing, or Rereading", International Studies Review, Vol. 4, Issue. 1.

Gilpin, R. (2011). "The Richness of the Tradition of Political Realism", International Organization, Vol. 38, Issue. 2.

Gismondi, M. (2004). "Tragedy Realism and Postmodernity: Kulturpessimismus in the Theories of Max Weber, E. H. Carr, Hans J. Morgenthau, and Henry Kissinger", Diplomacy and Statecraft, Vol. 15, Issue. 3.

Gücüyener, A. (2015). Kritik Enerji Altyapılarına Yönelik Gerçekleşmiş Siber Saldırılara İlişkin Bir Değerlendirme. in Kritik Enerji Altyapı Güvenliği. Gießen: Hazar Strateji Enstitüsü.

Güntay, V. (2016). "Ulusal Güvenlik Çerçevesinde Siber Güvenlik Yaklaşımı Oluşturma Sorunu", Cyberpolitik Journal, Vol. 1, Issue. 1.

Hobbes, T. (2007). Leviathan. (S. Lim, Çev.) İstanbul: Yapı Kredi Yayınları.

Hobden, S. (1999). "Theorising the International System: Perspectives from Historical Sociology", Review of International Studies, Vol. 25, Issue. 2.

İlimvemedeniyet. (2016). https://www.ilimvemedeniyet.com/the-black-box-in-realist-approach.html [Accessed on: 12.10. 2019].

Karakullukçu, E. (2017). https://www.webtekno.com/dunyanin-en-populer-10-siyah-sapkali-hacker-i-l737.html#image10 [Accessed on: 13. 09. 2019].

Kardaş, T. (2014). Güvenlik. Ş. Kardaş, & A. Balcı (eds), in Uluslararası İlişkilere Giriş (s. 337-351). İstanbul: Küre Yayınları.

Kolasi, K. (2013). "Soğuk Savaşın Barışçıl Olarak Sona Ermesi ve Uluslararası İlişkiler Teorileri", Ankara Üniversitesi Siyasal Bilgiler Fakültesi.

Korhan, S. (2017). "Siber Uzayda Aktör-Güç İlişkisi", Cyberpolitik Journal, Vol . 2, Issue. 4.

Korns, S., & Kasternburg, J. (2009). "Georgia‘s Cyber Left Hook", Parameters.

Kurnaz, İ. (2016). "Siber Güvenlik ve İlintili Kavramsal Çerçeve", Cyberpolitik Journal, Vol. 1, Issue. 1.

Little, R. (1999). "Historiography and International Relations", Review of International Studies, Vol. 25, Issue. 2.

Mansfield, E., & Synder, J. (1995). "Democratization and the Danger of War", International Security, Vol. 20, Issue. 1.

Morgenthau, H. (1954). Politics Among Nations: The Struggle for Power and Peace. New York: McGraw-Hill Education.

Mowle, T. (2003). "Worldviews in Foreign Policy: Realism, Liberalism and External Conflict", Political Psychology.

Öğün, M., & Kaya, A. (2013). "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri, Issue. 20.

Özlük, E. (2014). Uluslararası İlişkiler Disiplinin Doğuşu, Kimliği ve Sorunları. Ş. Kardaş, & A. Balcı (eds), in Uluslararası İlişkilere Giriş. İstanbuk: Küre Yayınları.

Özlük, E. (2017). "Dengeleme mi Peşine Takılmak mı?: Dış Politika Stratejilerini Yeniden Düşünmek", Akademik Bakış, Vol. 10, Issue. 20.

Sandıklı, A. (2012). Güvenlik Yaklaşımlarında Değişim ve Dönüşüm. A. Sandıklı (eds), in Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri. İstanbul: Bilgesam Yayınları.

Senarclens, P. (1991). "The 'Realist' Paradigm and International Conflicts", International Security, Vol. 42, Issue. 127.

Shimko, K. (1992). Realism, Neorealism, and American Liberalism. The Review of Politics, Vol. 54, Issue. 2.

Soresen, G. (2005). State Transformation and New Security Dilemmas. E. Aydınlı, & J. Rosenau (eds), Globalization, Security, and the Nation-State: Paradigms in Transition. Albany: State University of New York Press.

Sümer, V. (2014). Egemenlik. A. Özcan, & Y. Çınar (eds), in Uluslararası İlişkilerin Temel Kavramları. İstanbul: Hükümdar Yayınları.

Tarhan, K. (2017). "Siber Uzayda Realist Teorinin Değerlendirilmesi", Cyperpolitik Journal, Vol. 2, Issue 3.

Turan, Y. (2014). Siber Savaşlar. A. Balcı, & Ş. Kardaş (eds), in Uluslararası İlişkilere Giriş. İstanbul: Küre Yayınları.

Ünver, M., & Canbay, C. (2010). "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", Elektrik Mühendiliği Dergisi.

Varlık, A., & Demir, S. (2013). Uluslararası İlişkilerde Realist ve Liberalist Kurumların Güç Kavramına Yaklaşımı. H. Çomak, & C. Sancaktar (eds), in Uluslararası İlişkilerde Teorik Yaklaşımlar. İstanbul: Beta Yayınları.

Wolfers, A. (1952). "National Security as an Ambiguous Symbol", Political Science Quarterly, Vol. 67, Issue. 4.

Wordpress. (2013, Eylül 26). https://ohitsmerivera.wordpress.com/tag/20-and-robert-lyttle/ [Accessed on: 15. 10. 2019].

Yalvaç, F. (2014). Devlet. A. Eralp, E. Keyman, O. Tanrısever, & F. Yalvaç (eds), in Devlet ve Ötesi. İstanbul: İletişim Yayınları.