

T.C.
SELÇUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER BİLİM DALI

SİBER GÜVENLİĞE REALİST BİR BAKIŞ

OZAN SABRİ TUNCER

YÜKSEK LİSANS TEZİ

DANIŞMAN

DOÇ. DR. ÖNDER AYTAÇ AFŞAR

KONYA 2023

SİBER GÜVENLİĞE REALİST BİR BAKIŞ

ÖZET

21. yy'da küreselleşmenin bir sonucu olan siber uzay gün geçtikçe hayatımızdaki etkisini arttırmaktadır. Siber uzayın uluslararası ilişkileri derinden etkilediği bir çağda geleneksel realist teorinin siber uluslararası ilişkileri açıklayıp açıklamadığı tartışılmaktadır. Devlet merkezli realist teorinin siber alanı açıklamada birtakım eksiklikleri vardır. Siber alanın doğası ile sıkı bir uyum sağlayan realist teori ilkeleri güç, güvenlik ve Hobbesçu anarşi gibi yüksek politika alanlarında güçlü bir etkileşim sağladığı tespit edilmiştir. Buna karşın realist teorinin devlet merkezli eleştirel yaklaşımları siber alanda da geçerliliğini korumaktadır. Realizm siber alanı daha iyi okuyabilmesi için geleneksel anlayışın ötesine geçen bir yaklaşım geliştirmek durumundadır. Çalışmada dünya genelinde yaşanan siber saldırıların sonuçları analiz edildiğinde realist teori siber uzayı açıklama noktasında eksik kalan yönlerine karşın büyük oranda başarı sağlamaktadır. Bunun temelinde ise realist teorinin hâkim algısı anarşi ilkesinin siber uzayın doğasında bulunan algı düzeyi olduğu söylenebilir. Soğuk Savaş dönemi güç ilişkisi ve nükleer silah algısı gelecekte yerini siber silah konseptine bırakacağı öngörülmektedir. Bu sebeple güç algısı kavramını açıklamada yine realist teori sistemdeki hakimiyetini sağlayacağı düşünülmektedir.

Anahtar Kelimeler: Realist Teori, Güç, Güvenlik, Siber Politika, Siber Savaş, Siber Güvenlik.

A REALISTIC LOOK AT CYBERSECURITY

SUMMARY

In the 21st century, cyberspace, which is a result of globalization, is increasing its impact on our lives day by day. In an era when cyberspace deeply affects international relations, it is debated whether the traditional realist theory can explain cyber international relations. State-centered realist theory has some shortcomings in explaining cyberspace. The principles of realist theory, which are closely aligned with the nature of cyberspace, have been found to interact strongly in high policy areas such as power, security and Hobbesian anarchy. However, the state-centered critical approaches of realist theory remain valid in cyberspace. Realism needs to develop an approach that goes beyond the traditional understanding in order to better read cyberspace. When the results of cyber-attacks around the world are analyzed in the study, realist theory succeeds to a great extent despite its shortcomings in explaining cyberspace. On the basis of this, it can be said that the principle of anarchy, the dominant perception of realist theory, is the level of perception inherent in cyberspace. It is predicted that the Cold War-era perception of power relations and nuclear weapons will be replaced by the concept of cyber weapons in the future. For this reason, it is thought that the realist theory will again ensure its dominance in the system in explaining the concept of power perception.

Keywords: Realist Theory, Power, Security, Cyber Policy, Cyber Warfare, Cyber Security.

TEŞEKKÜR

Siber güvenlik alanında çalışmanın zorluğu ve karmaşıklığına rağmen çalışmamda bana sürekli destek olan, çok geniş bir alana sahip literatürden iyi bir analiz yapabilmemde önemli katkılar sağlayan, birlikte çalışmaktan onur duyduğum, tecrübelerinden yararlanırken göstermiş olduğu hoşgörü ve sabrından dolayı değerli danışmanım Doç. Dr. Önder Aytaç Afşar'a, ayrıca siber alanı tanımamda ve sevmemde bana yardımcı olan ve gerektiği yerde desteklerini esirgemeyen değerli hocam Prof. Dr. Nezir Akyeşilmen'e ve ayrıca bu çalışma sürecinde bana moral veren ve desteklerini her zaman hissettiğim değerli aile bireylerime teşekkürlerimi sunuyorum.

İÇİNDEKİLER

ÖZET	i
SUMMARY	ii
TEŞEKKÜR	iii
KISALTMALAR	vi
GİRİŞ	1

BİRİNCİ BÖLÜM

ULUSLARARASI İLİŞKİLER DİSİPLİNİ ÇERÇEVESİNDE REALİST TEORİ

1.1 Teorik ve Kavramsal Çerçeve	8
1.2 Realist Teori	9

İKİNCİ BÖLÜM

ULUSLARARASI İLİŞKİLERDE SİBER POLİTİKA

2.1 İnternetin Gelişimi	40
2.2 Siber Uzak	42
2.3 Siber Savaş	51
2.3.1 Stratejik Siber Savaş	53
2.3.2 Hibrit Siber Savaş	53
2.3.3 Operasyonel Siber Savaş	55
2.4 Siber Saldırıları	57
2.4.1 1999 Kosova Krizi	59
2.4.2 2007 Estonya Siber Saldırısı	60
2.4.3 2008 Gürcistan Siber Saldırısı	61
2.4.4 Litvanya Siber Saldırısı	62
2.4.5 Kırgızistan Siber Saldırısı	63
2.4.6 2010 Stuxnet Saldırısı	63
2.4.7 Türkiye’de Yaşanan Siber Saldırı Vakaları	65
2.5. Siber Casusluk	66
2.6. Siber Güvenlik	69
2.7 Siber Caydırıcılık	74

ÜÇÜNCÜ BÖLÜM

RELİST TEORİ AÇISINDAN SİBER POLİTİKA

3.1 Siber Uluslararası Sistem	79
3.2 Siber Alan ile Birlikte Değişen Uluslararası Güvenlik	83
3.3 Siber Alan ve Realist Teorideki Tanımlar	87
3.4 Siber Alanda Uluslararası Güvenliğin Kısıtlılıkları	89
SONUÇ	93
KAYNAKÇA.....	102



KISALTMALAR

AB: Avrupa Birlięi

ABD: Amerika Birleşik Devletleri

BM: Birleşmiş Milletler

NATO: Kuzey Atlantik Ticaret

RF: Rusya Federasyonu

BTK: Bilgi Teknolojileri ve İletişim Kurumu

TİB: Telekomünikasyon İletişim Başkanlığı

TSK: Türk Silahlı Kuvvetleri

AFAD: Afet ve Acil Durum Yönetimi Başkanlığı

MİT: Millî İstihbarat Teşkilâtı

ITU: Uluslararası Telekomünikasyon Birliği

ICANN: İnternet Tahsisli Sayılar ve İsimler Kurumu

IETF: İnternet Mühendisliği Görev Grubu

SCADA: Gözetleyici Kontrol ve Veri Toplama Sistemi

ATM: Otomatik Vezne Makinası

DDOS: Dağıtık Hizmet Reddi Saldırıları

USOM: Ulusal Siber Olaylara Müdahale Merkezi

GİRİŞ

Siber uzay, günümüzde uluslararası ilişkiler açısından büyük önem taşıyan bir konudur. Teknolojik ilerlemelerin hızla gelişmesiyle birlikte, siber alan artık devletler, şirketler ve bireyler için stratejik bir alan haline gelmiştir. Bu bağlamda siber güvenliğin sağlanması, bir ülkenin ulusal güvenliğinin temel bir unsuru haline gelmiştir. Günümüzde devletler bu alanda birçok taktik ve stratejiler geliştirmektedirler. Türkiye'nin bu alana özel kullandığı bir kavram olan Siber Vatan kavramı ön plana çıkmaktadır.

İnternetin sınır aşan doğası, ülkeler arasındaki siber uzayı birbirine bağlamıştır. Sınır kavramının ortadan kalkmasıyla siber güvenlik tehditleri de artmış ve çeşitlenmiştir. Bu çerçevede siber saldırılar bir ülkenin ekonomik, diplomatik, askeri ve demokratik süreçlerini etkileyebilecek düzeye ulaşmıştır. Siber güvenlik günümüzde devletler arası ilişkilerin temel bir unsuru haline gelmiştir.

Uluslararası ilişkiler kuramlarından biri olan realist teori yüzyıllar öncesine uzanan kökleri ile günümüzün modern gelişimini açıklamaya çalışması ve realizmin uluslararası politikada değişimi dışlayan söylemi, bilimsellik görüntüsü altında savunduğunu varsayımların tekrar doğru olduğunu kanıtlamaktadır. Siber alanın önemini devlet merkezli bir bakış açısıyla ön plana çıkaran siber alan klasik anlamdaki savunma ve caydırıcılık temelli iddiasını bu alanda da sürdürmektedir. Teknolojik açıdan güçlü olan devletler siber alanda caydırıcı bir statü elde etmeyi başarmışlardır. Bu da realizmin güç kavramına yüklediği anlamı ve önemi 21. yy'da da kanıtlar niteliktedir.

Küreselleşme sürecinin hızlı bir şekilde ilerleme sağladığı bir çağda değişen güvenlik algıları ve güvenlik araçları doğrultusunda bilimsel alanda da dönüşüme uğrayan bu alanda yeniden çalışmalar yapılması doğrultusunda hareket eden bu çalışma da başta modern anlamda devletlerin, kurumların, toplum ve bireylerin de siber alanda ortaya çıkan değişim ve derinleşmeler kapsamında yeni bir bakış açısı kazandırmayı amaçlamaktadır. Zaman ve mekân kavramının ortadan kalktığı bu alanda değişim ve gelişim zorunlu olmuştur. Birey, toplum, kurum ve devlet temelli

bu çalışma realist teori ve neo-realist teori temelli siber uzay açıklanmaya çalışılmış ve böylece realist teorinin siber alanı açıklamadaki yetkinlikleri ve kısıtlılıkları açıklanmıştır.

Küreselleşmenin bir çıktısı olan siber uzayı realist teori açıklayabiliyor mu? Realist teori literatürdeki hakimiyetini siber alana rağmen devam ettirebilecek mi? Realist teorinin siber uzayı açıklarken eksikleri nelerdir? Uluslararası İlişkiler Disiplinindeki değişimleri analiz edebilmek adına Siber alanın realist teorideki karşılığını açıklamak? Bu çalışma genelinde bunun gibi ana sorular çerçevesinde tezin amacı açıklanmaya çalışılacaktır. Bu çalışmada ana konumuz yaklaşık bir asırdır uluslararası ilişkiler alanında hâkim teori olan realizmin, siber alanın getirdiği yenilikleri açıklamadaki yetkinliğini yanıtlamayı amaçlamaktadır. Ayrıca çalışmada realist teorinin siber uzay söylemlerini ve bu alana yönelik açıklamalarını anlamlandırılması amaçlanmıştır.

Teoriler sosyal bilimlerde ve doğa bilimlerinde olaylarla ilgili doğrudan açıklama ve tahmin etme imkânı sağlarlar. Bu sebeple teoriye gereksinim vardır. Teoriler basite indirgeme ve anlamlandırmada kolaylık sağlarlar. Genel olarak teorilerden beklenen de tam olarak budur (Arı, 2018a). Gelecek ile ilgili öngöründe bulunması (tahmin) ve günün şartlarını açıklamasıdır. Bu kapsamda teoriye gereksinim vardır. Uluslararası İlişkiler disiplininde her bir bilim insanı teoriye ihtiyaç duymaktadır. Bu çalışmada olaylar arasındaki ilişkiyi açıklamak için realist teorinin reel dünyayı açıklamasının daha sağlam ve tutarlı öngörülerde bulunduğu için analize dahil edilmiştir.

Çalışmada ele alınan realist teori ve siber alan konusu yaşanan olaylar araştırılarak ve literatür taraması yapılarak çalışmamızda siber alan realist teori ışığı altında açıklanmaya çalışılmıştır. Realist teori köklerini M.Ö. 500'li yıllardan gelişim göstererek oluşan bir teoridir. Var olan olayları ve olguları gerçekçi bir bakış açısıyla ele alan ve perspektifin temelinde ise insanoğlunun doğasında olan kötü düşünce algısından hareket eden bir yaklaşımdır. Günümüzde de geçerliliğini koruyan realist teori, siber alanın yenilikleri karşısında temel ilkeleri ile yaşanan gelişmeleri açıklamadaki yetkinliği önem arz etmektedir.

Realist teori evrensel bir niteliğe sahip olduğunu savunurken, bu düşünce siber alanın sınırları ortadan kaldırması ile dünyanın küresel bir köy haline geldiğini savunanlar için geçerli bir düşüncedir.

Günümüzde milyarlarca insanın kullandığı internette her geçen gün farklı güvenlik zaafiyetleri ile karşılaşmaktayız. Güvenlik algısı realist teoride yüksek öneme sahip bir konudur. Siber alanda var olan güvenlik algısı ise birey, toplum, devletler ve kurumlar için yüksek öneme sahiptir.

Siber alanın gelişim göstermesi sadece güvenlik değil aynı zamanda diplomasi, ekonomi ve egemenlik alanında da devletleri etkilemekte ve değişime zorlamaktadır. Tüm bu gelişmeler dikkate alındığında realist teorinin hâkim olan disiplini açıklamadaki yetkinliği tezimiz için önem arz etmektedir.

Son yıllarda siber uzay hakkında çok fazla mürekkep harcanmıştır. İçinde yaşadığımız yüzyıl bizlere savaşlar, çatışmalar ve şiddetli politik gerilimlere tanık olmamızı sağladı bu sebeple içinde bulunduğumuz konjonktür ise realist perspektifin daha da ön plana çıkmasını sağlamıştır.

Siber uzay ve teknolojik gelişmelerin doğrudan uluslararası ilişkiler disiplinini ve başta insan olmak üzere birçok faktörü derinden etkilemesiyle birlikte disiplinde egemen konumda olan realist teorinin analiz birimini değiştirmesi sebebiyle bu alan çalışma konusu haline gelmiştir. Modern devletin 1648 sonrası süreçte etkili olan egemen ilkelerinin siber uzay ile değişmesi çalışmamız için temel teşkil etmektedir. Siber uzayla beraber devletler de egemenliklerini korumak için geleneksel bilindik yöntemlerin dışında siber alanın doğasına uygun hareket ederek birtakım tedbirler almışlardır. Devletler sadece askeri anlamda güvenlik önlemleri ile yetinmeyip aynı zamanda kritik alt yapılar, e- devlet, ekonomi (kripto para ve bankacılık, korsan saldırılar) ve eğitim sistemi gibi alanlar da önlemler almışlardır.

Uluslararası ilişkilerin temel aktörleri olan devletleri etkileyen değişime ve gelişime zorlayan yeni bir alan olarak siber uzay karşımıza çıkmaktadır. Siber uzayın hızla değişerek son derece akıcı olduğu teknolojik yeniliklerle birlikte bazı durumlarda

devletlerin politikalarına ve ikili ilişkilerine müdahalesine giderek daha fazla etki ettiği ve mevcut siyasal sistemi (egemenlik algısı) kökünden etkilediği için bu alanda daha fazla çalışmalar yapılmaya başlanmıştır. Gerçekçiliğin temel bir varsayımı, devletlerin uluslararası politikadaki en güçlü ve en önemli aktörler olduğudur. Bu noktada ortaya çıkan siber tehditler, günümüzde hükümetler için kritik altyapılara yönelik saldırılara karşı uyarıda bulunurken en önemli ulusal güvenlik endişesi olarak algılanmaktadır.

Başta realist teori olmak üzere teoriler varoluşun tarihselliğine karşı büyük bir duyarlılığa sahiptir. Dünyanın bir sistem içinde değişim halinde olduğu paradoksu da teorileri derinden etkilemektedir. Realist teori ve diğer teorilerde de olmak üzere değişimin olması ve buna olan ilgi beraberinde korkutucu teorik ve felsefi sorunları getirmektedir (Walker, 1987). Burada temel olarak ortaya çıkan sorunlar ve felsefi meseleler aslında teorinin epistemolojiden yoksun ve daha çok ontolojik bir çerçevede ortaya çıkmasıdır.

Bu çalışmanın amacı siber alanda yaşanan değişimleri açıklamayı amaçlayan temel teorilerde gerçekleşen değişimlerle birlikte realist teorideki algının ve değişimlerin siber alanı açıklamadaki yetkinliği ve kısıtlılıklarını gözönünde bulundurmasıdır. Bu konunun epistemolojik olarak önemi ise siber alanın literatürde sadece realist teori üzerinden açıklanmasına ek olarak realist teorinin bir alt çıktısı olan neo-realist teorinin ilkeleri ile de uyum sağlayan siber alanın daha kapsamlı bir şekilde ele alınması olacaktır. Ayrıca realist teorinin siber alanı açıklamada eksik kaldığı noktalar üzerinde detaylı analiz yapılacaktır. Çalışmanın bu yönüyle literatüre katkı sağlaması amaçlanmaktadır.

Bu çalışmada realist teorinin güç ve güvenlik ilişkisine ek olarak ekonomi, egemenlik ve diplomasi alanında ortaya çıkan yenilikler de analize dahil edilmiştir. Literatürde siber alan genellikle güç ve güvenlik ilişkisine odaklı bir çalışma olarak ele alınmıştır. İlk siber saldırıların ortaya çıkması daha sonrasında ise siber saldırıların dış politika temelli hedefler üzerinde değerlendirilmesi ile 2007 Estonya, 2008 Gürcistan, Litvanya, Stuxnet siber saldırıları ile 2021 yılında Microsoft siber saldırıları gibi bazı temel saldırılar analize dahil edilmiştir.

Bu çalışmada realist teori ve siber alan kavramlarının ikili karşılaştırılması ile literatür taraması yapılmış ve yaşanmış olaylar analiz edilerek çalışmaya dahil edilmiştir. Ayrıca 2019 yılında Amerika Birleşik Devletleri seçimlerinde Rusya destekli grupların siber saldırıları ile seçim sürecini sabote etmesi ve devletlerin iç işlerine müdahalesi olarak egemenlik haklarını zedelemesi yönünde yaşanan büyük kriz değerlendirilmiştir. Siber alan son çeyrek asırda çok ciddi ilerleme kaydetmiştir. Devletlerin iç ve dış politikalarında son derece önemli bir pozisyon olan siber alan uluslararası ilişkilerde son dönemlerde etkisini açıklayabilmek için realist teori tercih edilmiştir. Realist teoriye göre temel aktör devletlerdir. Devletler günümüzde de varlıklarını korumakta ve siber alanın değişime zorlaması karşısında egemenliği korumak istemektedirler. Buna karşın kripto paralar, siber saldırılar gibi etmenlere karşı çeşitli stratejiler geliştirmektedirler.

Küreselleşmenin getirdiği iletişim ağlarının dünya geneline yayılmasıyla birlikte Uluslararası İlişkiler Disiplinin içerisine birçok faktörün dahil olmasıyla sonuçlanmıştır. Bu alanlardan biri olan siber uzay, uluslararası ilişkiler disiplinini çok boyutlu olarak etkilemiştir. Devletler siber güvenliği sağlamak için çeşitli politikalar oluşturmakta ve stratejiler geliştirmektedirler. Kara, deniz, hava alanlarına ek olarak siber alanın uluslararası ilişkiler disiplinine dahil olması değişen güvenlik boyutunu ve savaş alanlarının çeşitlenmesine sebep olması yönüyle çalışmada incelenmiştir. (Yılmaz & Sağiroğlu, 2013). Savaş alanlarının siber alanda da karşımıza çıkması güvenliğin değişen boyutunu gözler önüne sermektedir (Tuncer, 2022). Siber uzayın etki ettiği alanların çeşitliliği ve büyüklüğü göz önünde bulundurulduğunda siber alanın çok kapsamlı bir şekilde incelenmesi gerektiğini göstermektedir.

Bu çalışmada realist teorinin kökeni ve ne zaman ortaya çıktığı, sonrasında bir teoriye nasıl dönüştüğü, önemli görülen bazı temsilcileri ile birlikte açıklanmaya çalışılmıştır. Ayrıca çalışmada realist teorinin temel özellikleri dikkate alınarak teorinin amacının ve bakış açısının detaylı analizine yer verilmiştir. Çalışmada realist teorinin alt bir çıktısı olan ve genellikle realist teori ile aynı özelliklere sahip olan neo-realist teorinin özelliklerine de değinilmiştir. Bunlara ek olarak neo-realist teorinin, realist teoriden ayrılan yönlerine de değinilmiştir. Teorik ve kavramsal bir çerçevede

realist teori ele alınmış olup teoride önem arz eden güç ve güvenlik kavramları detaylı bir şekilde açıklanmıştır.

Çalışmanın ikinci bölümünde uluslararası politikada siber alanın etkilerine değinilmiştir. Siber alanın gelişim evreleri internetin başlangıç sürecinden detaylı bir şekilde açıklanmaya çalışılmıştır. Ayrıca siber uzay, siber saldırılar, siber casusluk, siber güvenlik ve siber caydırıcılık kavramları açıklanmaya çalışılmıştır. Ek olarak dünya genelinde yaşanmış olan önemli bazı siber saldırılar ve Türkiye özelinde yaşanan önemli görülen siber saldırılar detaylı bir şekilde analize dahil edilmiş ve bu saldırıların amaçlarına değinilmiştir. Burada siber alan değişerek nesnelerin internetinden çıkıp giyilebilir nesnelerle birlikte bedenlerin internetine dönüşmüştür. Her alanda insan güvenliğini etkileyen siber güvenlik sorunu çeşitli şekillerde önem derecesini arttırarak karşımıza çıkmaktadır.

Çalışmanın üçüncü ve son bölümünde realist teori açısından siber politikanın yeri ve önemi açıklanmaya çalışılmıştır. Bu bölümde ayrıca siber uluslararası sistem analize dahil edilmiş ve siber alan ile birlikte değişen uluslararası güvenlik algısı açıklanmıştır. Siber alan ve realist teorinin güç ve güvenlik gibi kavramlar üzerindeki tanımları analiz edilerek çalışmaya dahil edilmiştir. Yine son bölümde önemli bir çalışma alt başlığı olan uluslararası güvenliğin kısıtlılıklarına da değinilmiş ve çalışmaya eklenmiştir. Bu bölümde realist teori algısı ile siber alan incelenerek çeşitli sonuçlar elde edilmiştir. Realist teori geleneğinde olduğu gibi devletler kendileri dışında başka bir devletin kendisine faydası olmayacağını bilmektedir. Realist teorideki, başka bir devletten medet umulmaması gerektiği düşüncesi siber alandaki saldırı ve güç yarışı içinde geçerli bir varsayım halini almıştır. Devletler günümüzde siber alanda birlikler ve ekipler oluşturarak bir güç mücadelesine girmişlerdir. Bu noktada uluslararası örgütlerden ziyade devlete yardım edecek olan yine devletin kendisidir algısı önem kazanmaktadır. Klasik anlamda nükleer caydırıcılık algısı siber alan için de geçerlidir. Bu kapsamda realist teori geleneği siber alanın bu örneğinde olduğu gibi bazı ortak noktaları ortaya çıkarmaktadır.

Realist teoride uluslararası hukukun sağlanamadığını iddia eden düşünce siber alandaki anarşi durumundan dolayı bu noktada da benzerliğini sürdürmektedir. Siber

alanın yüksek öneme sahip konuları arasında varlığını devam ettirmesi devletleri de çeşitli önlemler almaya zorlamıştır. NATO gibi askeri örgütler bünyelerinde siber savunma merkezleri kurmuşlardır. Önem düzeyi gün geçtikçe artan siber alanın geleceği nasıl şekillendireceği merak konusudur. Bu minvalde, çalışmada yüksek önem düzeyine sahip alanlarda ortaya çıkan ve önünde siber kelimesi bulunan kavramlara karşı klasik anlamda söylemden çıkıp devletler için bir strateji niteliği kazanmasındaki rolü araştırılmak ve analiz edilmek istenmiştir. Ayrıca birey, toplum ve kurumlar da eklenerek çalışmanın kapsamı genişletilmek istenmiş ve böylece yapılan analiz güçlendirilmeye çalışılmıştır.



BİRİNCİ BÖLÜM

ULUSLARARASI İLİŞKİLER DİSİPLİNİ ÇERÇEVESİNDE REALİST TEORİ

1.1 Teorik ve Kavramsal Çerçeve

Bu bölümde çalışmanın teorik ve kavramsal çerçevesi anlatılmaya çalışılmıştır. Bu açıdan birinci bölümde çalışmamız için önem arz eden realist teori ve realist teorinin tarihsel bağlamdaki yerine ve önemine değinilmiştir. Realist teorinin ortaya çıkmasını sağlayan siyasal ve tarihsel unsurlara değinilmiş ve teorinin oluşumuna giden süreç detaylı bir şekilde ele alınmıştır. Realist teori ve güvenlik ilişkisini ele alan teorisyenler açıklanmaya çalışılmış ve bu konuda önemli katkıları olan isimler referans verilmiştir. Realist teori bağlamından hareketle devletlerin hayatta kalma mücadelesinden, güç ve güvenlik daha sonra da çıkar ilişkisi bağlamında politikalar oluştururken nelere dikkat edildiğine atıfta bulunulmuştur. Literatürde realist teoride birçok isim ve teorisyen yer almaktadır fakat metodolojik olarak tezimizde bu isimlerden önemli olduğunu düşündüğümüz teorisyenlere yer verilmiştir.

Özellikle realist teorinin başat teori olarak ortaya çıktığı iki savaş arası dönem ve sonrası çalışmamızda titizlikle ele alınmıştır. Ayrıca çalışmada objektif olarak realist teorinin eleştirilerine de yer verilmiştir. Biliyoruz ki I. Büyük Tartışmanın bir tarafında realist teori yer almaktadır. Uluslararası İlişkiler disiplini adına I. Büyük Tartışma dediğimiz tartışmanın da disiplinde aslında ne kadar büyük bir yere sahip olduğunu göstermesi açısından önemlidir. Realist teori Uluslararası İlişkiler disipliniinde neredeyse yarım asırlık bir süreçte öncü teori olarak birçok çalışmada yer almıştır. Dönemin siyasi şartları çerçevesinde iki büyük savaşı geride bırakan insanoğlu bu savaşlar sonrasında tekrar bir savaşın yaşanmaması için gerekli olan ve alınması gereken tedbirler doğrultusunda realist teorinin ilkelerine sıkı sıkıya tutunmuşlardır.

Modern anlamda Uluslararası İlişkiler disiplini I. Dünya Savaşı süreci sonlarını kapsarken, realist teorinin bu disiplinindeki yeri de II. Dünya Savaşı sürecindeki yaşanan gelişmeler ve oluşumları kapsamaktadır. I. Dünya Savaşı dönemi disiplinde İngiliz

teorisyenlerin (İdealizm) idealist yaklaşımları egemen olurken, II. Dünya Savaşı sonrası süreçte disipline Amerikalı (realizm) teorisyenler ağırlık kazanmıştır.

Temelde uluslararası ilişkiler savaşların önlenmesi, barışın sürdürülebilirliği ve bu sürecin korunması gibi temel varsayımlar üzerine idealizm terminolojisi ile bir fırsat yakalamış fakat siyasi ve politik süreç idealizmin ideallerini sağlayamadığı gerçeği ile karşılaşınca realizm ciddi eleştirileri ile disiplindeki yerini almıştır. Bu çerçevede literatürde de kabul edildiği gibi ilk büyük tartışma ortaya çıkmıştır. Uluslararası İlişkiler disiplini diğer sosyal bilimlere nazaran daha genç sayılsa bile hızlı bir ivme yakalamış ve gelişimini sürdürmektedir. Gelişimini sürdüren Uluslararası İlişkiler disiplini kendi şahsına münhasır olarak doğmamış olsa da kazanımları ve argümanları ile sosyal bilimlerde özgün bir yer yakalamıştır. Bu disiplin içinde ise güncelliğini çeşitli yaklaşımlarla devam ettiren ve sürekli gelişerek derinleşen en önemli teorilerden olan realizm ele alınmıştır. Bu tez bu perspektiften ele alınmalı ve değerlendirilmelidir.

1.2 Realist Teori

“Realizm” en az iki alanda kullanıldığı bilinen bir kavramdır. Bir tarafta tarihsel bir süreç olan Soğuk Savaş’ın başlangıcı ve sonunu kapsayan süreyi uluslararası ilişkiler teorisine atıf yapmak için ifade etmektedir. Diğer tarafta ise gerçeklik, bir politika ve strateji olarak veya askerî açıdan güvenlik ve doktrin olarak atıfta bulunur. İlk perspektifte devletlerin davranışlarını ve uluslararası ilişkileri anlamada kullanılan bir bakış açısıdır. İkinci perspektifte ise asıl aktör olanın eylemlerini anlamlandırmamızı sağlamaktadır (Guzzini, 2017).

Realist teori uluslararası ilişkilerde ilk temsilcilerinin de atıfta bulunduğu gibi öncelikle felsefi kavrayış olarak kabul edilen belirli sorunlar çerçevesinde tarihsel deneyim olarak adlandırılmıştır. Bu teorisyenler var olan sorunları çözme, savaşları kazanma, hayatta kalma ve güvenliğin sağlanması olarak yorumlamışlardır. Aynı gelenek içindeki ikinci nesil olarak kabul edilen realist teorisyenler ise devleti açıklamak için sosyal bilimlerde kullanılan bir bakış açısı olarak ele almışlardır (Mohanty, 2007).

Kökenlerini Tzu, Thucydides, Machiavelli ve Hobbes'un düşüncelerine dayanan realist paradigmanın öncüleri arasında E. H. Carr, Hans Morgenthau, Kenneth Waltz, John Mearsheimer, John Vasquez, George Kennan, Joseph Grieco, Robert Gilpin, Barry Buzan, Hedley Bull, sayılabilir. Realizm farklı yaklaşımları (neo-realizm, savunmacı, saldırgan) barındırmakla birlikte bütünsel olarak temelde uluslararası sistemi ve politikayı ele aldığı ileri sürülebilmektedir (Dursun, 2017).

Realist teorinin kökenini daha iyi anlayabilmek adına realist teori tarihsel açıdan sınıflandırılarak ele alınacaktır. İlk olarak eski Yunan tarihçisi Thucydides, daha sonra 17. yy. teorisyenlerinden olan İtalyan Niccolo Machiavelli, son olarak ise 20. yy.'ın klasik realist düşünürleri ele alınacaktır. Özellikle 20.yy.'da realist teoriye bir nevi kimlik kazandıran Hans J. Morgenthau ve E. H. Carr üzerinde detaylı olarak analiz edilecektir (Jackson & Sorensen, 2013, s. 67).

Modern anlamda realist teori her ne kadar yirminci yüzyılda tanımlansa da realist teorinin kökenlerinin çok daha eskilere dayandığı bilinmektedir (Aydın, 2004). Realist teorinin özelliklerinin görüldüğü önemli bir eser olan Sun Tzu'nun Savaş Sanatları adlı eseridir. Bu eser yaklaşık 2500 yıl önce yaşamış olan Çinli bir komutan tarafından kaleme alınmıştır. Eserde devlet yöneticilerine nasıl hayatta kalınacağı tavsiyeler şeklinde anlatılmıştır. Tzu bu eserinde devlet yöneticilerine ve ordu komutanlarına çıkarlarını sağlamaları ve hayatta kalmaları için gücün önemine dikkat çekmiş ve nasıl kullanmaları gerektiği hakkında bilgiler vermiştir. Bu eserde temel kaygı devletin bekasıdır (Goldstein & Pevehouse, 2012, s. 44).

Milattan önce 400'lü yıllarda Realist teorinin kökenlerinin Thucydides'in Atina ile Sparta arasındaki güç mücadelesine kadar götürmek mümkündür (Dursun, 2017). Pleponeyza Savaşı, uluslararası ilişkiler literatüründe realist teorinin ilk örneklerinden biri olduğu algısı uzun yıllar boyunca realist teorinin kökeni olarak kabul görmüştür (Garst, 1989). Pleponeyza Savaşları adlı çalışmasıyla realist literatüre yaptığı katkıyla bilinen Thucydides M.Ö. 471-400 yılları arasında yani Sokrates ve Aristo arasındaki dönemde yaşamıştır (Arı, 2004).

Thucydides'in M.Ö. 400'lerde yaşadığı bilinmektedir. Tzu gibi realist teorinin kökenlerini beslediği bilinmektedir. Thucydides devlet ile insan doğasını birbirine benzetmiş, insanı ilkel bir varlık olarak tanımlamıştır. Thucydides bir asker ve bir teorisyen olarak Pleponeyza Savaşlarına katıldığı bilinmektedir. Thucydides'e göre Pleponeyza savaşının başlıca nedeni Atina ile Sparta arasında birbirlerinin müttefikleri ile ilişkiye girme yetkileri konusundaki görüş farklılığıdır. Bu ilişkiler her iki devletin çıkarlarının ve dengelerinin bir bakıma bozulması anlamına gelmektedir (Turan, 2018). Çünkü Sparta karada güçlü bir konuma sahip iken Atina denizlerde donanma gücünü elinde bulundurmaktadır. Bu iki farklı alandaki güç ve çıkar mücadelesi savaşa dönüşmüştür (Turan, 2018). Savunması için kendisine verilen şehri kaybeden Thucydides önce sürgüne gönderilmiştir. Sürgün yıllarında savaşı neden kaybettiği üzerine birtakım çalışmalar yapan Thucydides, gözlemleri sonucunda yeni fikirler üretmiştir. Thucydides'e göre yenilginin yegâne sebebi var olan güç dengesinin bozulması ve bunun sonucu olarak ortaya çıkan güvenlik kaygısıdır. Thucydides'in gözlemleri sonucunda ortaya çıkardığı silahlanma yarışı, güç dengesi, strateji ve göreceli güç gibi kavramları görmek mümkündür (Keyik & Erol, 2019, s. 15). Pleponeyza Savaşlarının asıl sebebi ve sonucu güç ve çıkar mücadelesi sonucu bozulan denge siyasetinin savaşa yol açmasını oluşturmaktadır.

Thucydides'in Pleponeyza savaşı özelinde öne sürdüğü bir başka düşüncesi ise, iki taraf arasındaki 30 yıllık huzur ortamının bozulup tekrar savaşımaya başlamalarının nedeni Atinalıların güçlerini arttırdıkları ve Lakedamonyalıların da bu güçten korkmaları ve bu sürecin savaşa sürüklemesidir (Çıtak, 2014, s. 39). Bu savaşın sonucunda Thucydides'in en önemli söylemlerinden biri olan "güçlüler yapabileceklerini yaparlar ve zayıflar kabul etmeleri gerekeni kabul ederler" söylemi realist teorinin köklerini oluşturmaktadır (Goldstein & Pevehouse, 2012, s. 44).

Thucydides ek olarak Pleponeyza Savaşları adlı eserinde temel olarak şehir devletlerini tüm eylemlerin aktörü olarak görmüş ve bu algı zamanla özellikle 1648 Westphalia ile modern anlamda devlet merkezli yaklaşım haline gelmiştir (Çıtak, 2014, s. 34). Pleponeyza Savaşı isimli eserin hem güç hem de adalet ve ahlak üzerine dersler veren bir metin özelliği taşıdığı bilinmektedir (Walker, 1987). Realist

geleneğin kökenlerini oluşturan bu yaklaşım zaman içerisinde çeşitlenerek gelişmiştir. Robert Gilpin ise Pleponeyza Savaşları'na atıf yaparak Thucydides'in uluslararası politikada ilk bilimsel öğrenci olduğunu ileri sürmüştür (Garst, 1989).

Realist teori geleneğini düşünceleri ile etkileyen bir başka teorisyen ise Niccolo Machiavelli olmuştur. 16.yy.'da yaşayan İtalyan asker, diplomat ve teorisyen olan Niccolo Machiavelli'nin yazarlarında realist teoriyi etkilediklerini söylemek mümkündür. Machiavelli "Prens" adlı eserinde dönemin Floransalı etkin ailelerinden olan Medici'leri övmesinin altında aslında onları eleştirmesi gerçekliği bu realist teorinin gelişimi açısından örnek oluşturmaktadır (Çakmak, 2019).

Niccolo Machiavelli 'nin Prens adlı çalışmasını Floransa yöneticisi olan Lorenzo di Meccini (Muhteşem Lorenzo) için kaleme aldığı bilinmektedir. Realist teori geleneği açısından "iktidarın nasıl kazanılacağı", "devletin bekası", "gücün sürdürülmesi", "ittifak ve karşı ittifak oluşumu" üzerine bir kılavuz niteliğindedir (Keyik & Erol, 2019). Aslında Machiavelli prensleri, kamu ve askeri ittifakların manipölasyonları da dahil olmak üzere iktidarda kalmak için gereken eylemlerin yapılmasını savunmuştur (Goldstein & Pevehouse, 2012, s. 44).

Machiavelli çalışmasında güç, güç dengesi, ittifak ve karşı ittifak oluşumu üzerinde durmuştur. Ayrıca kent devletleri arasındaki çatışmaların nedenlerine de değinmiştir. Machiavelli Prens'in iktidarını sürdürebilmek için içeriden ve dışarıdan gelebilecek tehditlere karşı egemenliğini koruyacak güce sahip olması düşüncesini savunmaktadır (Arı, 2004).

Machiavelli'nin gerçekçiliği uluslararası politikanın bir "teknolojisi", yani uluslararası arenada ustalaşmak için kullanılabilecek bilimsel temelli bir teknik olarak tasvir eden ilk kişi olduğu bilinmektedir (Forde, 1995). Machiavelli'nin: "Amaca giden her yol mubahtır" sözünün detaylandırılmış ve günümüze uyarlanmış versiyonu olarak değerlendirmek mümkündür (Çakmak, 2019). Machiavelli için en yüksek amaç ise güçlü bir devlet oluşturmak ve idame etmektir (Waltz & Quester, 1982, s. 39). Ayrıca uluslararası ilişkiler doğası gereği önceden tahmin edilemeyen politikalar ve askeri stratejilerle doludur. Bu durumda devletler güçlerini maksimum seviyeye

çıkarmaları gerektiğini savunan Machiavelli, felaket gelmeden önce tedbir alınması gerektiğini savunmaktadır. (Çıtak, 2014, s. 40).

Thomas Hobbes, 17. yy.' da yaşamış realizmi etkileyen önemli düşünürlerden biridir. Hobbes, uluslararası siyasi durumu doğa durumuna benzetmektedir. Doğa durumunu ise tabii yasaların varlığı, çerçevesinde uluslararası sistemin temel niteliği olarak tanımlamaktadır (Ateş, 2009). Hobbes, 1651 yılında kaleme aldığı “Leviathan” isimli eserinde insanın doğasının kötü olduğunu ve insan doğası gereği birbiri ile bir mücadele içinde olduğunu savunmuştur (Keyik & Erol, 2019).

İngiliz teorisyen Hobbes “Leviathan” adlı eserinde devletin oluşum sürecini anlatmaktadır. Ayrıca insanın doğası gereği çıkarıcı olduğunu ve insan doğasının kötü olduğuna vurgu yapmıştır. Bu sebeple insanlar egemenlik devirlerini devletlere devrettiklerini savunmaktadır. Bu açıdan toplumsal bir sözleşmenin olduğunu savunur. Bu savunulan görüş ise dönemin realist düşünce mantığının temellerini oluşturması ve klasik realist düşünce ile örtüşmesi sebebiyle önemlidir (Çakmak, 2019). Hobbes 'in çalışmaları realist teori için oldukça önemlidir. Eseri olan Leviathan siyaset alanındaki ilk teori geleneği olarak kabul edildiği bilinmektedir. Hobbes'a göre insan doğasında kötülük vardır ve üst otoritenin olmaması anarşiye zemin sağlamaktadır. Bu yüzden eserinde tüm insanlık için güçlerini Leviathan adı verilen merkezi otoriteye devretmesini savunmaktadır.

Hobbes'un eserinde “doğa durumu” veya “savaş durumu” olarak adlandırdığı bu siyasal sistemde insanların kendi çıkarları peşinde koştuğunu savunmuştur. Hobbes, günümüzdeki hukukun üstünlüğü ilkesine karşı olarak “orman kanunu” şeklinde betimlemiştir. Bu durumu daha iyi bir hale getirmek için Leviathan'ı güçlü bir monarşiye benzetmektedir. Bu durumda realist gelenek açısından güç politikasının önemine atıf yapılmasını sağlamıştır. (Goldstein & Pevehouse, 2012, s. 44).

Ayrıca Hobbes'un doğa durumunda söyleminden hareketle devletler maddi mülkiyet için “rekabet, güvensizlik, korku ve zafer arayışı” gibi çeşitli sebeplerle sahip oldukları değerleri koruma altına almaya çalışmakla birlikte bu durum uluslararası

alandaki doğa durumu olarak kabul edilmektedir. Bu nedenle eşitler arasında yalnızca kendini koruma doğal hakkı oluşmaktadır (Walker, 1987).

Thucydides, Machiavelli, Hobbes ve aslında tüm klasik realistler az ya da çok iktidarı elde etmenin, elinde bulundurmanın, konuşlandırmanın ve gücün kullanımı olarak bu görüşü “doğa durumu” paylaşmaktadır. Uluslararası siyaset böylece her şeyden önce "güç siyaseti" olarak tasvir edilmektedir. Ulusal çıkarları savunmak ve güvenliği sağlamak gibi aynı temel sorunları yaşayan devletler, devletin bekası ve halkının güvenliği konularında aynı görüşte birbirlerini tekrar etmektedirler (Jackson & Sorensen, 2013, s. 66).

Şekil 1: Klasik Dönem Realist Teorisyenler Tablosu

THUCYDIDES	MACHIAVELLI	HOBBS
Siyasi kader	Politik çeviklik	Siyasi irade
Gerekliklik ve güvenlik	Fırsat ve güvenlik	Güvenlik ikilemi
Politik hayatta kalma	Politik hayatta kalma	Politik hayatta kalma
Güvenlik	Sivil erdem	Barış ve mutluluk

Kaynak: Jackson, R., Sorensen, G. (2013). Introduction to International Relations Theories and Approaches. United Kingdom: Oxford University Press.

Thucydides, Machiavelli, Hobbes ve klasik realizmin temellerini oluşturan yazarların önemine dikkat çekerler ve siyasal hedeflerin başarılablmesini güç ile açıklarlar (Aydın, 2004). Bu tablodaki yazarların bir diğer ortak noktası ise klasik realizmi oluşturmalarıdır. Bu teorisyenler uluslararası politikayı bir güç mücadelesi olarak görmektedir. Güç mücadelesi, iki ülke arasında bir rekabet, çatışma ve siyasi arena olarak tanımlanmaktadır.

Realist teori modern uluslararası ilişkiler disiplininde idealist teorinin I. Dünya Savaşı sonrası süreçteki yaklaşımı ve özellikle II. Dünya Savaşı'nı öngörememesi gibi birtakım eksiklikler sonucunda ortaya çıkmış ve idealist teoriye yoğun bir şekilde eleştirel yaklaşım ile önem kazanmıştır. Böylece literatürdeki Birinci Büyük Tartışma başlamıştır. Bu tartışmanın kazananı hiç şüphesiz uluslararası sistemin anarşik yapısını açıklayan birey ve devlet üzerinden analiz geliştiren realistler olmuşlardır. Realist teori için I. Dünya Savaşı sonrası süreçten Soğuk Savaş sonrası sürece kadar olan zaman diliminde literatürdeki baskınlığını koruduğunu ve nerdeyse mutlak hâkim olduğunu söylemek yanlış olmayacaktır (Aydın, 2004).

Realist teori yirminci yüzyılda yaşanan üç büyük gelişme (I. ve II. Dünya Savaşları ve Soğuk Savaş, uluslararası alanda faşist ve diktatörlüklerin artması) sonucunda temel özelliklerini koruyarak geçerliliğini korumayı başarabilmiştir. Realist teorinin en etkin yönü ise uzun yıllar boyunca kabul görmesi olmuştur. Yıllar içerisinde yeni gelişmeler ve eklemeler olsa da realizmin temel unsurları değişimden kalmayı başarabilmiştir (Arı, 2004).

Siyasi tarih açısından realizm modern anlamda özellikle 1930'larda Almanya'da iktidara gelen Nazi yansılı sosyalist parti ile dünyada otoriter devletlerin varlığının arttığı gözlemlenmiştir. Bu otoriter devletlerin artmasıyla birlikte uluslararası arenada liberalizmin düşüşe, realizmin ise yükselişe geçtiği bilinmektedir (Keyik & Erol, 2019). Kısacası I. Dünya Savaşı'nın yaşanması ve kısa bir süre sonra dünya tarihinde daha büyük ölçekli bir savaşın patlak vermesi ile uluslararası konjonktürde liberallerin savunduğu düşünceye olan inancın azalması ile kendilerini "realistler" olarak adlandıran bir grubun teorileri güç kazanmış ve zaman içerisinde başat konuma yükselmiştir.

Birinci Dünya Savaşı sonrası süreçte yaşanan gelişmeler ve kısa bir süre sonra adına İkinci Dünya Savaşı dediğimiz daha büyük bir savaşın yaşanması, Soğuk Savaş süreci ve sonrası, kutuplaşmaların artması ve Vietnam Savaşı-Petrol Krizi süreçlerinin yaşanması siyasi tarih açısından realist teorinin gelişimini desteklemektedir (Özlük, 2009).

20. yy.'ın ilk çeyreğinde uluslararası ilişkilerde egemen olan idealist düşüncenin gelişimi ve temel önermeleri disiplinin oluşumu için çok önemlidir. Uluslararası ilişkiler disiplini çok yeni bir tarihe sahiptir. Bu disiplin altında üretilen bilimsel çalışmalardan çok büyük bir kısmı realist teori etkisi altında olduğu bilinmektedir (Kanat, 2011).

İdealistlerin kalıcı barışı temin etme yolundaki politikaları ve bu politikaların tam olarak uygulanamaması ve bazı başarısız girişimleri sonucunda İkinci Dünya Savaşı'nın patlak vermesi üzerine disiplinde yeni bir teorinin doğuşuna sebep olmuştur. Adına realizm dediğimiz modern anlamda realist teori böylece ortaya çıkmıştır (Ateş, 2009). Birinci ve İkinci Dünya Savaşları arası dönemde idealistlerin uluslararası konjonktürü anlamada ve açıklamada yetersiz kalması ayrıca meydana gelen İkinci Dünya Savaşını öngörememesi uluslararası arenada artan realist düşünce teorisyenleri ve taraftarlarınca sıfır toplamli oyun olarak tanımlanmıştır (Özlük, 2009). Örneğin, 1945'e kadar olan dönemde "idealist" yazarların Uluslararası İlişkiler disipliniinde "güç" gibi temel kavramları göz ardı ettiği görüşü tartışmalı olmasına rağmen çok yaygındır (Aydın & Açıkmeşe, 2015, ss. 4-5).

İkinci Dünya Savaşı, birçok sosyal belirsizliğe yol açan geniş kapsamlı değişiklikleri beraberinde getirmiştir. Bu nedenle, sosyal istikrarsızlığı önlerken yaygın sosyal değişime izin verebilecek yeni bir düzenin kurulması gerektiği açıktır. Toplumun yapısal hegemonyasının temelinde yatan değişimlere değinmeden bu dönemi ve grupların faaliyetlerini incelemek mümkün değildir. Bu aynı zamanda Gramsci'nin yalnızca belirli bir aktörler grubunun konjonktürel bir projesi değil, bütün bir tarihsel dönem için tasarlanmış bir tarihsel blok kavramıyla ve yaygın yapısal değişiklikleri geliştiren pasif devrim fikriyle ilişkilendirilebilmektedir (Joseph, 2000).

19. ve 20. yüzyılın ütopyacılığına (idealizm) karşı siyaset teorisinde gerçekçilik (realizm), devletçilik, uluslararası ilişkilerde bir tepki olarak ortaya çıkmıştır. Totalitarizmin yükselişi ve büyük savaşın (I. Dünya Savaşı) gelişi ütopycıların umudunu paramparça etmiştir. Modern realist teori, realistlerin idealizm olarak adlandırdıkları liberal bir geleneğe tepki olarak gelişmiştir. İdealizm, uluslararası olaylar üzerindeki kilit etkiler olarak tek başına güçten ziyade uluslararası hukuku,

ahlakı ve uluslararası örgütleri vurgulamaktadır. İdealistler, insan doğasının temelde iyi olduğunu düşünmektedir. Uluslararası sistemi, karşılıklı sorunların üstesinden gelmek için birlikte çalışma potansiyeline sahip bir devletler topluluğuna dayalı bir sistem olarak görmüşlerdir. (Goldstein & Pevehouse, 2012, s. 43).

Realist teorisyenler, idealist teorinin aşırı ütöpik olduğunu ve bazı açılardan imkânsız olduğunu iddia etmişlerdir (Galston, 2010). Realistler, idealistlerin "dünyanın somut gerçeğini hesaba katmadıklarını" iddia etmişlerdir.

Realist teoriye bakıldığında temelde insan doğasının kötü olduğu ve her an suç işlemeye meyilli olduğu savunulmaktadır. İnsan doğası gereği gücü sever ve güç için çalıştığını kabul etmişlerdir. (Dursun, 2017). Realist teori insan doğasının iyi olduğunu bilir fakat olabildiğine kötü olabileceği gerçeğini de bilmektedir. (Morgenthau, 1970, s.2). Augustinian geleneğini izleyen realistler, insan doğasına ilişkin karamsar bir görüşe bağlıdır. Böyle bir görüş, Hristiyanlığın ilk günah doktrini tarafından desteklenmektedir. Toplum hakkında felsefe yapmaya girişen herkesin bir insan görüşüne katılması, ayrıntılarını açıklamaktan çekinmeyen realistler tarafından tamamen kabul edilen bir aksiyondur (John, 1993).

Realizme bakıldığında rasyonelliğin yanında birtakım insani özelliklerin de (hırs, istek ve mücadele) yüklendiği görülmektedir (Ereker, 2010) Bu bakış açısıyla uluslararası ilişkileri bir güç mücadelesi olarak nitelendirmişlerdir. Realistler, uluslararası sistemin bir anarşi durumunda var olduğuna inanmaktadır. Bu, tam bir kaos veya yapı ve kuralların yokluğunu değil, daha çok kuralları uygulayabilecek merkezi bir hükümetin yokluğunu ima eden bir terimdir. (Goldstein & Pevehouse, 2012, s. 50).

Realist teoriye göre devletler de tıpkı insanlar gibi doğası gereği güç için rekabet etmektedir. Bu nedenle hem klasik hem de neo-realistler bu anlayışın değişmeyeceğini savunmaktadır. Bu noktada ise klasik realistler insan doğasının kötülüğünü temel alırken neo-realistler ise anarşik uluslararası sistemin yapısını dikkate almaktadır (Çakmak, 2006). Bu anarşik ortamda devletler kendi güvenliklerini korumak ve sağlamak zorundadır. Realizm en başından beri güvenliğe yönelik tehlikelerin her

zaman mevcut olduğu ve hatta hayatta kalmanın kendisinin bile garanti edilemediği anarşik bir ortamda siyasi birimlerin (devlet) kendilerini nasıl koruduklarına dair açıklamalar sunmuştur (Frankel, 2013). Uluslararası politikacılar ve teorisyenler realist teoride geleneksel olarak dikkatlerini devlet üzerinde yoğunlaştırmışlardır. Devleti temel birim olarak analizlerine dahil etmişlerdir (Nye & Keohane, 1971, s. 329).

Realist teoriye göre uluslararası ilişkilerde güvenlik özellikle de ulusal güvenlik en üst düzeyde yer alır ve devletlerin “survivalı” hayati öneme sahiptir. Realist yaklaşımda güvenliği sağlamak için olmazsa olmaz askeri güç ve askeri konular “high politics”, bireysel ve ulusal örgütler ve sosyal konuları ise “low politics” olarak tanımlanmıştır (Aydın, 2004). Realistler, gücün uluslararası politikanın para birimi olduğuna inanmaktadır. Realistlerin ana aktörleri olan büyük güçler, birbirlerine göre ne kadar ekonomik ve askeri güce sahip olduklarına dikkat etmektedir. Sadece önemli miktarda güce sahip olmak değil aynı zamanda başka hiçbir devletin güç dengesini keskin bir şekilde kendi lehine değiştirmemesini sağlamak da önemlidir. Realistler için uluslararası siyaset, güç siyasetiyle eş anlamlıdır. (Mearsheimer, 2007, s. 77). Realistler için yüksek öneme sahip konular ve daha az öneme sahip konular böylece daha belirgin olarak dillendirilmiştir.

Realist teoriye göre uluslararası sistemde aktör olan devletler hayatta kalmaları için gereken tüm tedbirleri almak zorundadır. Varlığını sürdürmek isteyen devlet anarşik ortamda yalnızca kendi gücüne güvenebilmekte (self-help) ve gücü ölçeğinde hareket edebilmektedir (Dursun, 2017). Bu noktada ise her devletin kendi güvenliğini kendisinin sağlamak zorunda olduğu kabul edilmektedir. Güç dengesiyle ilgili sorun, işleyişinin idealden daha az olmasını sağlayan istikrarsızlığıdır. Güç dengelerinin yapıları hem birimler açısından hem de ilgili birimlerin amaçları açısından uyumlarının dengelerin işleyişinde merkezi olması bakımından önemlidir (Molloy, 2004).

Her devletin kendi güvenliğini sağlaması ve hayatta kalması için gereken tedbirleri alması sonucu uluslararası arenada bir güvensizliğin oluştuğu iddia edilmektedir. Realistler, Uluslararası İlişkiler kurallarının genellikle bir güvenlik

ikilemi yarattığını kabul eder; bu durum, devletlerin kendi güvenliklerini sağlamak için yaptıkları eylemlerin (daha fazla askeri güç) diğer devletlerin güvenliğini tehdit ettiği bir durumdur. (Goldstein & Pevehouse, 2012, s. 52).

Güç realist teorisinin ilk varsayımı Realist varsayımla yaygın olarak ilişkilendirilen ikincisi, devlet-merkezciliktir (Kostagiannis, 2014). Realizm, uluslararası ilişkilerde devleti baskın aktör olarak kabul etmektedir. Bununla birlikte teori devletlerin kendileri tipik olarak nihai güce sahip olarak kabul edilmektedir. Bu, başka bir ulusa savaş ilan etmek gibi kararları uygulama kapasitesini veya tersine, devletleri belirli anlaşmalara bağlayabilecek anlaşmaları içermektedir (Gold & McGlinchey, 2017, s. 49).

Bu anarşik dünyada realistler, dış politikada ihtiyatlılığın büyük bir erdem olduğunu vurgulamaktadır. Bu nedenle devletler, diğer devletlerin niyetlerine değil, onların yeteneklerine dikkat etmelidir. (Goldstein & Pevehouse, 2012, s. 50). Çoğu realist, Uluslararası İlişkilerin bir anarşi durumundan kaçamayacağını ve sonuç olarak tehlikeli olmaya devam edeceğini düşünmektedir (Goldstein & Pevehouse, 2012, ss. 50-51). Realist teori için benzer bir tanım da devletleri bilardo topu olarak görmekte ve bu bakış açısını güç mücadelesi çerçevesinde anarşik bir ortam olarak tanımlamaktadır (Ereker, 2010).

Uluslararası konjonktür diğer bütün çalışma alanları gibi bir mücadele alanıdır. Buradaki temel mücadele ise güç ve iktidar mücadelesidir. Uluslararası politikanın bakış açısı ve temel esasları ne olursa olsun nihai amaç “güçlü” olmaktır. Güç sıradan insan veya bir kral açısından da çok büyük önem atfetmektedir. Bu örnekteki gibi birbirinden farklı iki insanın bakış açısı değişse de güç bu amaçları sağlamak için en önemli adım olarak görülmektedir. Devletler de tıpkı insanlar gibi anarşik ortamda güç mücadelesi içindedir (Morgenthau, 1970, ss. 30-32). Gilpin realist teorisinin özelliklerinden hareketle gerçeklik ampirik temellere dayanarak bize daha bilimsel bir uluslararası politika anlayışı sağladığını savunmuştur (Forde, 1995).

Realist teoride devletler uluslararası alanda herhangi bir tehditle karşılaştığında bu tehdidi yok etmek için iki yol seçmektedir. İlk olarak devletler tehdit olarak

algıladıkları gücü dengeleme yoluna gitmektedir. Bir başka seçenek ise Bandwagoning olarak adlandırılan üstün olan güç karşısında birkaç farklı devlet ile oluşturulan ittifaklar çerçevesinde yeni bir oluşuma gitmeleridir. Ayrıca realist teoriye göre Bandwagoning zayıf olan devletin güçlü olan devlete karşı tek başına mücadele etmesinin daha maliyetli olacağını savunmaktadır. Bandwagoning ile devletler maliyetlerini bölüşmektedir (Çakmak, 2006).

Realist teoriye göre devletler dış politikalarındaki hedeflere ulaşmak için askeri güçleri çerçevesinde hareket ederler. Bir başka deyişle ele alınan yöntemde belirleyici unsur askeri güçtür. Realizmin devletler arası ilişkilerin ahlakçı veya idealist anlayışına karşı doğduğunu hatırlatmakta ve realizmin özünün bir şekilde bu karşıtlıkta yattığı görüşünü paylaşmaktadırlar (Forde, 1995).

J. Samuel Barkın'a göre realist teori devletlerin uluslararası alanda sahip oldukları güç çerçevesinde önem kazandığını iddia etmektedir (Barkın,2010). Realizm ve idealizm arasındaki fark metodolojik olmaktan çok teoriktir (John, 1993). 1930-1940'larda yaşanan İdealizm-Realizm tartışması Uluslararası İlişkiler disiplininde yaşanan birinci büyük tartışmadır. Gerçekçilik ve idealizm aslında felsefidir. İnsanın doğasına ilişkin farklı görüşlere dayanan görüşler, dünya ve siyasette merkezi öneme sahip konular teori Uluslararası ilişkilerde önemli olan tüm paradigmalar arasında realizm belki de en köklü, gelişmiş ve tarihsel olarak köklü olanıdır (John, 1993).

20. yy.' da liberalizme en ağır eleştiriler yönelten kişi Edward H. Carr olmuştur. Carr 1919-1939 Yirmi Yıl Krizi (The Twenty Years Crisis) eserinde realizmin çağdaş bir tanımını yapmıştır. Carr realist kuramın, uluslararası ilişkiler disiplinindeki yerini ve önemini belirginleştirmiştir (Keyik & Erol, 2019). İkinci Dünya Savaşı sonrası tarihsel süreçte ise realist teorinin önemine değinen teorisyenler ise Edward H. Carr, H. Morgenthau, K. Waltz, Raymon Aron, George F. Kennan ve Henry Kissinger olduğu bilinmektedir. Bu teorisyenler realist teoriye katkıda bulunurken kendilerinden önce realist teorinin kökenlerini oluşturan, Thucydides, Machiavelli ve Hobbes 'in fikirlerinden faydalanmışlardır (Dursun, 2017).

Literatürde de ilk büyük tartışma olarak geçen idealizmi ütopyacılık olarak nitelendiren, 20. yy. başlarındaki teorisyenlerden olan Edward H. Carr en sert eleştirileri idealizme yöneltmiştir. Böylece literatürde idealizmin savunduğu gibi değil realizmin savunduğu gibi dünyayı olması gereken gibi değil olduğu gibi anlatmamız gerektiği savunulmuştur (Barkın, 2009). 20. yy.'ın ortalarına gelindiğinde bu görüş iyice destek bulmuş ve uluslararası ilişkiler alanında en iyi teori olduğu savunulmuştur (John, 1993).

Carr İkinci Dünya Savaşı'nın bitmesiyle birlikte en önemli eserlerinden olan Yirmi Yıl Krizi adlı eserinde kendi ülkesinin dış politikasını eleştiren ve aynı zamanda uluslararası ilişkileri anlamaya çalışan bir yaklaşım kaleme almıştır. Bu eserinde Carr I. Dünya Savaşı sonrası sürecin neden yirmi yıl gibi çok kısa bir süreyi kapsadığı sorusuna ise idealizmin dünya gerçeklerinden uzak ütopyacı bir yaklaşımla uluslararası politikayı anlamlandırmaya çalıştığını savunmuştur (Dursun, 2017). Bir başka deyişle E. H. Carr'ın Yirmi Yıl Krizi adlı kitabında idealist (ütopyacı) teorisyenlere karşı eleştirel bir yaklaşımla yeni bir alternatif olarak ortaya çıkmıştır.

Carr idealistlere uluslararası konjonktürün yapısını ve güç mücadelesini anlayamadığı gerekçisi ile eleştirmiştir. Bunun en büyük dayanağını ise II. Dünya Savaşı'nın öngörülememesi ya da önlenememesi oluşturmuştur. Buna karşın İdealist teorisyenler iki savaş arası süreçte kendi teorilerini tam anlamıyla uygulayamadıklarını savunmaktadırlar (Aydın, 2009). Carr'a göre ilk önemli siyasi realist olarak kabul ettiği Machiavelli'nin fikirlerinden hareketle idealizme çok ciddi eleştiriler yönelmiştir. Bu eleştirisini ise realizmin üç temel maddesi olarak sınıflandırmıştır. Birincisi, tarih idealistlerin inandığı gibi hayal gücü ile anlaşılamaz. İkincisi, idealistlerin iddia ettikleri gibi teori pratiği oluşturmaz fakat pratik teoriyi oluşturur. Sonuncusu ve üçüncüsü ise, politikalar etiğin fonksiyonu değil, etik politikanın fonksiyonudur. (Şen, 2014, ss. 16-17).

Edward H. Carr uluslararası ilişkiler disiplininde realist teorinin modern anlamda ilk değerlendirmesini yapan teorisyen olarak bilinmektedir (Keyik & Erol, 2019) Edward H. Carr'a göre güç temel olan bazı unsurları kapsamaktadır. Bu unsurlar askeri, ekonomik ve propaganda şeklinde tanımlanmıştır. Ayrıca bu unsurlar arasından

da askeri güce daha fazla önem vermektedir (Çakmak, 2006). Carr, güce önem verirken gücün caydırıcılığı üzerindeki etkinin önemine dikkat çekerken en son çarenin ise savaş olması gerektiğini savunmuştur (Özdemir, 2008).

İdealizmin temel varsayımlarını (hukuk, etik değerler ve adalet algısı) reddeden Carr, realizmin olağan uluslararası politikayı belirleyen faktör olmasını savunmaktadır (Aydın, 2004). Bu bağlamda Carr'a göre realizm Uluslararası İlişkiler'i olgunlaştırmaya götürecek ve normatif yaklaşımlar yerine çözümlemeye ağırlık vermeyi sağlayacak bir yaklaşım tarzı olarak savunmuştur. (Daban, 2017). Edward H. Carr modern yapısıyla devletlerin gelecekte temel birim olarak kalacağını savunmaktadır. Bu anlayışa göre realistler disiplindeki başat teori olarak kalacaklarını diğer teorilerin ise gerçek hayatla uyuşmayacağını savunmaktadır (Çakmak, 2006).

Hedley Bull'a göre 20. yy. başlarında realist teorinin sistematikleştirilmesi Alfred Zimmern, E. H. Carr, Hans Morgenthau, Raymond Aron ve Martin Wight gibi teorisyenlerin katkıları ile olmuştur (Bull, 1964). Carr'ın Uluslararası İlişkiler disiplini modern anlamda realizmin öncülüğünü yaptığı kabul edilmektedir. Bununla birlikte bir diğer önemli isim özellikle İkinci Dünya Savaşı sonrası süreçte realist düşünceye büyük katkılar sağlan 20. yy. teorisyenlerinden olan ve realist okulun babası olarak adlandırılan Hans J. Morgenthau' dur. (Çıtak, 2014, ss. 17-18). Morgenthau özellikle II. Dünya Savaşı'ndan sonra uluslararası siyasetin bir güç mücadelesi alanı olarak tanımlaması ve ulusal çıkarlara göre hareket edildiğini savunması açısından önemli bir teorisyendir. (Goldstein & Pevehouse, 2012, s. 44).

Yirminci yüzyılın önde gelen realistlerinde H. Morgenthau siyasi aktörlerin öngörülemeyen şekillerde hareket edebileceklerini söylemiş ve insan hareketlerinin önceden tahmin edilemeyeceğini savunmuştur. Ayrıca Morgenthau bireylerin güç peşinde hareket edecekleri için uluslararası politikadaki bazı genel kalıpların önceden tahmin edilebileceğini savunmuştur (Barkın, 2009). Realistler için insanlar bencildir ve başkalarının ihtiyaçlarını dikkate almadan kendi ihtiyaçlarına göre davranmaktadırlar. Realistler, çatışmanın kaçınılmaz ve savaşın yaygın olduğuna inanmaktadır. Bunun insanlığın doğasından hareketle elde edilmiş nesnel bilgi

olduğunu savunmaktadır. Hans Morgenthau, ünlü “tüm politikalar bir güç mücadelesidir” sözüyle tanınmaktadır (Gold & McGlinchey, 2017, s. 48).

Amerikalı Profesör Hans Morgenthau tarafından (1948) *Politics Among Nations* (Uluslararası Politika) adında yazılan eser realizm için önemli bir kaynaktır. Morgenthau uluslararası ilişkilerde tek gerçeği güç olarak tanımlamıştır. Güç üzerinden de realist politikayı savunmuştur. Güçlü olan üstün duruma geçip ve sözünü dinletebilmektedir. Bu yüzden uluslararası politikayı bir güç mücadelesi olarak tanımlamaktadır. Bu sebeple devletler sürekli olarak güçlerini arttırmak isterler böylece de uluslararası alanda bir güç dengesinin olduğunu savunmaktadır.

Uluslararası alanda olan bir güç yine farklı bir güç tarafından dengelendiği zaman güç dengesi sağlanmış olmaktadır. Farklı bir şekilde barışı sağlamanın da mümkün olmadığını savunmaktadır. *Morgenthau, Milletler Arasındaki Siyaset: Güç ve Barış İçin Mücadele* isimli eserinde “uluslararası siyasetin realist teorisini” ortaya koymaktadır. Morgenthau’ ya göre tüm siyasi faaliyetlerin amacı, iktidar peşinde koşmaktır. Durum böyle olunca, Milletler Arasında Politikanın bariz anlamı, uluslararası ortamda güç peşinde koşmalarıdır (Molloy, 2004). Politika, esas olarak bir güç mücadelesi olarak tasavvur edilmiş ve felsefe, "öncelikle, açık bir şekilde düşünmeye yönelik alışılmadık derecede inatçı bir girişim" olarak tasavvur edilmiştir (Frankel, 2013).

Morgenthau’ ya göre insan en net haliyle kaçınılmaz bir şeytandır (Kanat, 2011). İnsan doğasına olan olumsuz yaklaşım H. Morgenthau’nun 1948 yılında uluslararası ilişkiler disiplinine kazandırdığı “*Politics Among Nations*” isimli eserinde açıkça görülmektedir. Morgenthau bu eserinde insanların güç peşinde koştuklarını vurgulamaktadır. Öte yandan, Morgenthau’ ya göre, güç peşinde koşma uluslararası politikanın ayırt edici özelliğidir. Morgenthau bu eseri ile klasik realist düşüncenin kavramsallaştırılması ve sistematik hale gelmesi noktasında büyük katkısı bulunmaktadır (Dursun, 2017).

Hans J. Morgenthau için hayat; insan, politika ve insan kaderi arasındaki bitmeyen bir hakikat arayışı olarak tanımlanmıştır. Ayrıca Morgenthau insan doğası

ve insanlar ile milletler arasındaki kaçınılmaz rekabete ekstra olarak önem atfetmiştir (Thompson, 1980-1981). İnsan doğasını gerçekte nasılsa öyle, tarihsel süreci ise gerçekte nasıl oluşmaktaysa öyle ele alan bu kuramsal anlayışa Morgenthau realizm demektedir. (Morgenthau, 1970, s. 2).

Politik etkinliğin kaynağı olarak insan doğasında kök salmış güç arzusu fikri, Morgenthau'nun siyaset kavramının temelini oluşturmuş ve Morgenthau bu konudaki ilk düşüncelerini savaş sonrası özellikle Milletler Arasında Siyaset. Güç ve Barış için Mücadele ve Uluslar Arasında Politika kitabında geliştirmiştir. Ulusal Çıkarları Savunma, güç arzusu kavramını izleyen Morgenthau, birey düzeyinde “animus dominandi”ni ifadesini, kişinin gücünü artırma ve bu gücü elinde tutma veya gösterme arzusu olarak tanımlamıştır (Wieclawski, 2012).

Kısacası, animus dominandi, hükmetme arzusu, siyasi faaliyeti belirleyen toplumsal güç olarak tanımlayan Morgenthau uluslararası düzlemde, bu davranış kalıpları statüko, emperyalizm ve prestij politikalarına dönüştüğünü ileri sürmektedir. Sonuç olarak Morgenthau, çıkarların tüm siyasetin merkezinde olduğunu ve bu nedenle uluslararası sahnede her devletin genellikle güç olarak tanımlanan ulusal çıkarlarının peşinden gitmesi gerektiğini savunmuştur (Pham, 2008). Morgenthau bu görüşünü ise siyasi gerçekçilik, siyasetin kökleri insan doğasında olan nesnel yasalar tarafından yönetildiğini belirtmektedir. Hindistan, Çin ve Yunanistan'ın klasik uygarlıklarının onları ilk kez analiz etmeye teşebbüs etmesinden bu yana aynı kaldığını iddia ederek savunmuştur (Molloy, 2004).

Morgenthau 'ya göre güç çıkar için kullanılır. Fakat çıkarın net bir tanımı olmadığını savunmaktadır. Morgenthau gibi klasik realistler uluslararası politikayı sadece devletler arasında olan bir süreç olarak tanımlamaktadır. Bu sebeple devletlerin çıkarları için mücadele ettiğini savunmaktadır (Çakmak, 2006). Morgenthau, ilgi ve gücü "insan gücünün doğasında bulunan" güçler olarak tasavvur etse de bunlar için "bir kez ve sonsuza kadar sabit" bir anlam talep etmemiştir (Pham, 2008). Güç kullanımında ise rasyonel bir hesabın olması gerektiğini savunan Morgenthau iyi hesaplanmamış güç kullanımı olumsuz sonuçlar yaşatabileceğini iddia etmiştir (Kostagiannis, 2014).

Güç ve güvenlik insan motivasyonunda önemli bir etkidir. Uluslararası siyasette belirleyici faktör güçtür. Güç dengesini "yaşamın yasası" olarak kabul eden Morgenthau, "bağımsız gücün kontrol altında tutulabilmesi için, yaklaşık olarak eşit güçteki bağımsız güç tarafından karşılanması gerektiğini" söyler. 'Güç dengesi', kavramını savunur ve devletlerin bağımsızlığını korumak için başkalarına olduğu kadar kendine de sınırlamalar getireceğini iddia etmektedir (John, 1993).

Morgenthau, şunu savunmaktadır: “Dünyada meydana gelen derin değişikliklere rağmen her zaman doğru olduğu gibi, diğer ulusların düşmanca emelleriyle karşı karşıya kalan bir ulusun tek bir birincil yükümlülüğü kendi çıkarlarını gözetmek olduğu gerçeği hala doğrudur” (Pham, 2008). Hans Morgenthau tarafından ifade edildiği şekliyle bu temel iç görüş, dünyayı olmasını istediğimiz gibi değil, olduğu gibi görmemiz gerektiğidir (Barkın, 2009).

Morgenthau 'ya göre ulusal ahlakın realizm açısından devletler tarafından tam olarak sağlanması mümkün değildir. Bu görüşünü ahlaki evrensel ilkelerin soyut koşullarını devletlerin somut ilişkilerinde geçerli olmayacağını savunarak iddia etmektedir. Ek olarak bireylerin kendileri için “fiat justitia, pereat mundus” (dünya yok olsa bile adalet yerini bulsun) diyebilmekte ama devletin, himayesindekiler adına bunu söylemeye hakkının olmadığını savunmaktadır (Jackson & Sorensen, 2013, s. 73).

Morgenthau, uluslararası hukuk belgelerinin rolünü göz önünde bulundurarak uluslararası hukukun uygulanmadığı ve caydırıcı bir yetkisinin olmadığını örneklerle savunur, ayrıca uluslararası evrensel örgütlerin ve her şeyden önce Birleşmiş Milletlerin rolü konusunda şüpheci yaklaşımda bulunmuştur (Wieclawski, 2012). Bu uluslararası hukuk kurallarının uygulanması sorunu günümüz uluslararası yapısında da aynıdır. Devletler anarşi ortamında güçleri ölçüsünde uluslararası hukuk kurallarının yaptırımlarından ve normlarından kaçınmaktadır.

Hans J. Morgenthau'nun siyaset kavramını, savaş sonrası ikinci ve aslında en önemli kitabı olan *Politics Between Nations*'da daha da geliştirmiştir. Kitabın 1954'te yayınlanan ikinci baskısı Morgenthau'nun güç ve siyaset anlayışına katkıda bulunan

politik gerçekçiliğin altı ilkesini içermektedir (Wieclawski, 2012). Alman kökenli Amerikalı düşünür Morgenthau realizmin altı unsuru (güç, çıkar, ahlak, siyasal gerçekçilik, ılımlılık, siyasal olan ile olmayan arasındaki ilişki) olduğundan bahsetmiştir (Çakmak, 2019).

H. J. Morgenthau siyasal gerçekliğin temelleri nelerdir? Sorusuna altı temel ilke ile cevap vermektedir.

1- İnsan doğasının kötü olduğu algısından hareketle siyaset yasalarının derinliklerinde yatan kötü huylardan hareketle realizm belli bir dış politikanın karar alıcılarının karakterlerinin sadece yapılan incelemeler sonucunda ön kestirimlerinin bazı analizlerle açıklanabileceğini savunmaktadır. Fakat bu yapılan analizlerin tamamen yeterli olmadığını da eklemiştir. (Morgenthau, 1970, ss. 2-3). Realistler düşüncenin temelinde insan doğası ele alınmaktadır. Bu yaklaşıma göre toplumun genel özellikleri insan doğasının kökeninden beslenmektedir. Bir başka deyişle siyaset dediğimiz olgunun kökleri de insanın özünde var olan tarafsız yasalarla yönetilmesidir. Bu yasaları insanoğlunun gelişimi için kullanılması da temelde birey ve toplumun doğasında var olan yasaların özümsemesi anlamına gelmektedir.

2- Uluslararası politika denilen anarşi ortamında realizme yol gösterecek olan en önemli unsur güç kavramı ile tanımlı yapılan çıkar unsurudur. Çıkar kavramı siyaseti diğer alanlardan bağımsız olarak ele aldığını savunmuştur (Keyik & Erol, 2019, s. 17). Geniş anlamda uluslararası politikada en önemli nokta ise güç terimi ile uyumlu hale getirilen çıkar kavramıdır. Uluslararası siyaseti akıl yolu ile anlamaya çalışan gerçeklerle bağlantı kurulmasına yardımcı olmayı sağlamaktadır.

3- Realistler en temel kavramlardan biri olan güç kavramı ile tanımlanan çıkar teriminin sabit bir anlam içermediğini aksine değişkenlik gösterebileceğini savunmaktadır. Çıkar terimi böylece realist teorinin özünü oluşturduğu gibi zaman ve mekândan da farklılık gösterebilmektedir. Bu görüş Max Weber'in gözlemiyle daha geniş yankı bulmuştur. "İnsan eylemlerini, fikirler değil, çıkarlar dolaysız olarak etkilemektedir" diyerek savunmuştur. (Morgenthau, 1970, s. 10). Weber aynı zamanda Protestan Ahlakı ve Kapitalizmin Ruhu adlı kitabında "unutma ki itibar paradır

'demektedir. Ayrıca “en iyi miktarı öneren, herkesin cüzdanının efendisidir” atasözünü de eklemektedir (Weber, 2014, s. 51). Özellikle Alman ulus devleti örneğinden hareket eden Max Weber ve Friedrich Meinecke gibi teorisyenler uluslararası siyasal gerçeklik ve değişime yapılan vurguyu realist teoriye aktarmışlardır (Walker, 1987).

4- Realist teoriye göre devletler uluslararası arenada ahlaki kurallara göre hareket etmeyeceğini savunmuştur. Ek olarak devletlerin sıradan vatandaşlar gibi doğru olanı yapma gibi bir özgürlüğünün olmadığını eklemiştir (Dursun, 2017). Realistler siyasal eylemin moral öneminin farkındadır. Buna karşın ahlak ile politika arasındaki hassas dengenin sağlanmasının güç bir iş olduğunu kabul etmektedirler. Böylece hem moral hem de siyasal yasaların önemine dikkat çekmektedirler. Ayrıca realist teorisyenler ahlak kurallarının, politik ahlak kuralları ile aynı şey olmadığını düşünmüş ve çoğu zaman bu ahlak kurallarının çelişebileceğini savunmuşlardır (Galston, 2010).

5- Realizm bir devletin uluslararası alanda ahlaki hareket edip etmediğini anlamak için dünya çapındaki ahlak kurallarının bir ölçüt olarak değerlendirilmesini kabul etmemektedir. Ulusların moral kurallarına uymak durumunda olduklarını bilmek ile ulusların aralarındaki ilişkilerde neyin iyi neyin kötü olduğunu tam olarak bilir gözükmek ayrı şeylerdir (Morgenthau, 1970, ss. 12-13). Burada temel nokta ise bir ulus kendi çıkarlarını temel alarak diğer devletlerin de çıkarlarını gözeterek hareket ederse ahlaki davranmış olacağını iddia etmektedir (Çıtak, 2014 s. 33).

6- Siyasal realizm ile diğer düşünce okulları arasında ciddi bir fark vardır. Bu bağlamda her alan kendi kriterlerine göre analiz edilmesinin daha doğru olacağı savunulmuştur (Dursun, 2017). Siyasal realizm ve diğer düşünce okulları arasındaki farkı görmemiz için en güzel örnek Theodore Roosevelt’in, 22 Ocak 1915’te Edward Grey’e yazdığı mektuptur. Mektupta, “... Sözleşmelere iyi niyetle uyulması gerektiğine ve uluslararası ahlak diye bir şeyin mevcudiyetine inananlara iyi bir örnek teşkil etmiş bulunduğunuz için, girmiş olduğunuz eylemin yerinde olduğunu belirtmek isterim...” bu yazıdan hareketle kendi çıkarlarını diğer tüm gerçeklerden ayırarak diğer devlet temsilcilerine vurgulandığı görülmektedir (Morgenthau, 1970, ss. 16-17).

Bu genel ilkeler ışığında realizm özellikle II. Dünya Savaşı sonrası süreçte uluslararası ilişkilerin tarihini ve gelecekteki halini anlatması için etkili olduğu söylenebilmektedir (Çıtak, 2014 s. 33). Realist teorinin Uluslararası İlişkiler disiplinine en önemli katkılarından biri de Morgenthau'nun yöntem bilimi açısından uluslararası ilişkileri kurumlar (etik, hukuk vb.) veya olgulardan çok kavramlar aracılığıyla incelemenin bilimsel açıdan liderliğini yapmasıdır. Böylece teori geleneksel olan tarih, felsefe ve hukuktan uzaklaşarak daha bilimsel bir alana doğru yönelmiştir (Aydın, 2009).

Morgenthau realist gelenek içinde devletlerin temel politikalarının güç arayışı olduğunu ve güç mücadelesi ile devletlerin çıkarları için rasyonel hareket etmesini savunması diğer kuramlardan bağımsız bir şekilde realizmi ele aldığı kanıtını oluşturmaktadır (Özdemir, 2008). Ek olarak Morgenthau realist teoriyi güç kavramı ile açıklarken caydırıcılık yeteneğini de eklemiştir. Bu da gücün doğru kullanılması ve devletlerin rasyonelliği için önem arz etmektedir. Morgenthau güç kullanımının doğru zamanlaması olduğu gibi kullanılacak gücün de doğru bir güç unsuru (siyasal ve askeri) olması gerektiğini savunur. Böylece güç unsuru olan askeri ve siyasal güç arasında ayrım yapmıştır (Özdemir, 2008).

Realizm ya da diğer adıyla politik gerçeklik uluslararası ilişkileri devlet temelli ve devletler arasındaki güç mücadelesi ile açıklamaya çalışan bir düşünce okuludur. Teorik bir çerçeve olarak uluslararası ilişkiler çalışmalarında tarihsel olarak merkezi bir konuma sahiptir (Goldstein & Pevehouse, 2012, s. 43). Devlet merkezli bu görüşün sofistike teorisyenleri, uluslararası etkileşimleri izlemiş ve devlet dışı aktörlerin varlığını görmemezlikten gelmemişlerdir (Nye & Keohane, 1971, s. 343).

Realistler Birleşmiş Milletler'i tamamen yok saymamış fakat realitede otoritesi çok az olan uluslararası veya ulus üstü örgütlerin çabalarına rağmen dünyanın anarşik bir sistemde düzenine devam ettiğini savunmuşlardır. Uluslararası kuruluşlar için genel olarak güçlü devletlerin politik hedefleri yönünde çalıştıklarını iddia etmişlerdir. Bu çerçevede ise II. Dünya Savaşının çıkmasında Milletler Cemiyetinin başarısızlığını ve büyük güçler üzerinde etkisinin olmamasını sıklıkla kullanmışlardır (Gold & McGlinchey, 2017, s. 48).

Realistler 1648 Westphalia ile modern anlamda ulus devletin uluslararası politikalarını izlemiş ve genellikle karar verme yetkisine sahip “devlet adamlarından” bahsetmişlerdir. Realistler; iç siyasetin doğası gereği ve anarşik uluslararası sistemde devletlerin hayatta kalmasının önem taşıdığını vurgulamıştır (Mastanduno, vd., 1989, ss. 459-460). Realist teorinin en önemli özelliği uluslararası ilişkiler disiplini bağımsız bir disiplin haline getirmesi konusundaki büyük etkisidir. Realist teori uluslararası arenada siyasi, kültürel ve ekonomik ilişkileri rasyonel bir bakış açısıyla ele almıştır (Çakmak, 2006). Realist teori elli yılı aşkın bir süreyle uluslararası ilişkiler de hâkim teori olmuştur. Realistler olanı değil, olması gerekeni izah etmektedir.

Realizm sadece gözlemcilerin uluslararası siyaseti anlamak için yaptıkları gözlemler değil aynı zamanda politika uygulayıcıların da dünya politikasını anlamlandırmaya çalıştığı bir teoridir. Kısaca realizm uluslararası ilişkilerin gözlem dili ve pratik dili olarak tanımlanabilmektedir. Realizm, uluslararası ilişkilere özel olarak 'siyasi' bir yaklaşım geliştirdi. Bu nedenle, dünya siyasetinin doğasında algılanan herhangi bir değişikliği ve yeniliği açıklamaya çalışmıştır (Guzzini, 2017).

Realist geleneğin temel varsayımlarını kısaca açıklamak gerekirse;

- İnsan doğasına ilişkin kötümser bir görüş ve suç işlemeye meyilli olduğu düşüncesi vardır (Jackson & Sorensen, 2013, s. 66).
- İnsanın diğer insanlar üzerinde kontrol sağlama (animus dominandi) isteği vardır. Bu özellik hem ulusal hem de uluslararası politikanın temel özelliği olarak değerlendirilmiştir (Dursun, 2017).
- Uluslararası politikada temel yapı devletlerdir, devletler bencil bir şekilde sadece kendi çıkarlarını düşünmektedir (Çakmak, 2006).
- Uluslararası politika ulusal politikadan farklı olduğunu kabul etmekte, Uluslararası politika da anarşinin hâkim olduğunu ve yaşanan sorunların temelde güç (askeri güç) ile çözülebileceğini savunmaktadır. Güç kavramı askeri olan ve askeri kavram dışında kalan güç unsurları olarak ikiye ayrılmasıdır (Mastanduno, vd., 1989, s. 459).
- Ulusal güvenlik değerlerine yüksek saygı ve devletin hayatta kalmasının öncelikli olmasıdır (Dursun, 2017).

- Devletler arasında anarşi durumu olduğundan bir sistem vardır ve bu sistem güç dengesi ile açıklanabilmektedir (Keyik & Erol, 2019, s. 19).

- Dış politika high politics ve iç politika low politics birbirine karıştırılmamalıdır (Aydın, 2009). Bir başka deyişle yüksek öneme sahip dış politika da etkili olan askeri ve devletler arası ilişkileri etkileyen stratejik konular ile daha düşük öneme sahip yani ekonomik ve sosyal konular birbirinden ayrılması gerekmektedir.

- Devletler uluslararası politikada diğer devletleri caydırıcı güç kullanarak kendi çıkarları doğrultusunda hedefler uygularlar. (Mearsheimer, 2007, s. 79).

Yukarıdaki genel varsayımlar realizmin klasik anlamda kabul edilen görüşlerini oluşturmaktadır. Realizm modern anlamda hem ortaya çıktığı dönemin teorisyenlerini etkilemiş hem de yıllar sonrası için bir ışık kaynağı olarak sonraki teorisyenlere yol gösterici olmuştur. Michael Mastanduno, David A. Lake ve G. John Ikenberry 1989 yılında ele aldıkları “Realist Bir Devlet Eylemi Teorisine Doğru” isimli çalışmalarında devleti analizin merkezine yerleştirirken bunu devletin iç ve dış politikadaki sistemlerin kesişme noktasındaki eşsiz konuma sahip olmasından kaynaklandığını savunmuşlardır. Ayrıca bu anlayış çerçevesinde analizlerini realist geleneğin içine yerleştirmişlerdir (Mastanduno, vd., 1989, ss. 458-459).

Benzer bir örnek ise 2002 yılında Amerika Birleşik Devletleri’nin Irak’ı işgalinden önce yaşanan bir reklam tartışması olmuştur. Otuz üç uluslararası ilişkiler akademisyeninin başlatmış olduğu reklam ve bildiri realizmin yıllar sonra etkilediği ve varsayımlarının bazılarının kabul bulduğunu kanıtlamıştır. (Goldstein & Pevehouse, 2012, s. 44).

Realistler, son yarım yüzyılın uluslararası siyasette üç büyük değişime tanık olduğunu ileri sürmüşlerdir. Bu değişimlerden en önemlisi olarak realistler, II. Dünya Savaşı sonrasında çok kutupluluktan iki kutupluluğa geçişin son derece önemli olduğunu savunmuşlardır. Realistler, benzer şekilde, nükleer silahların dünyayı daha fazla veya daha az güvenli hale getirip getirmediği konusunda farklı görüşlere sahiptir ancak bunların devlet politikalarında, pazarlık taktiklerinde, ittifak ilişkilerinde ve statükoyu değiştirme fırsatlarında önemli değişiklikler getirdiği konusunda bir kez daha hemfikirlerdir (Jervis, 1998). Realist teori uluslararası siyaset anlayışına ve daha

genel olarak siyasete, güç ve güvenlik için sürekli bir mücadele ve bu konudaki çatışmalar olarak dayanır (Frankel, 2013). Tüm bu genellemelere rağmen değişen uluslararası konjonktür realist teorinin de eleştirilmesine zemin hazırlamıştır. Realizm teorisi güncelliğini korumaya çalışsa da ciddi eleştiriler karşısında birtakım yenilikleri kabul ederek kendi içerisinde de farklı görüşler ortaya çıkmıştır.

1.5 GÜÇ

Çalışmada realist teori klasik anlamda ele alınmıştır. Bu kapsamda klasik realist teorinin siber alanı açıklamada kullandığı iki kavram olan güç ve güvenlik kavramları analize dahil edilmiştir. Klasik realist teorinin uluslararası ilişkileri açıklamada kullandığı güç ve güvenlik kavramları realist teorinin siber uzayı açıklamada kullandığı kavramlar olduğu için analize dahil edilmiştir.

Literatürde güç kavramı genellikle askeri güç ile ilişkilendirilmiştir. Realistler her ne kadar hukukun ve ahlakın dünya siyasetinin ayrılmaz bir parçası olduğunu kabul etseler bile bunu uygulayabilmek için yine güce olan ihtiyaca dikkat çekmektedirler (Aydın, 2004). Realist teori devletlerin çıkarlarını maksimize etmek için güç unsurunu kullandıklarını ve bunu anarşik bir ortamda rasyonel kararlar doğrultusunda yaptıklarını savunmaktadır. Steven Lukas güç kavramını üç farklı boyutta sınıflandırmıştır. Lukas güç kavramını, çıkar kavramı üzerinden değerlendirmenin daha doğru olacağını savunmuştur. Lukas’a göre güç; bir aktörün (A), isteyerek yapmayacağı şeyleri, bir başka aktöre (B), yaptırabilme yeteneği olarak tanımlamıştır (Özdemir, 2008).

Literatürde güç kavramına yönelik en önemli katkılar yapan teorisyenlerden biri de Joseph Nye’dir. Nye “yumuşak güç” olarak tanımladığı kavramı sert güç ile karşılaştırarak oluşturmuştur. Yumuşak güç bir devletin var olan kapasitesini anlatmak için kullandığı ve gücün geleceği olarak tanımlamak mümkündür. Kısaca yapmak istediklerinizi zorlayıcı güç unsurlarını kullanmadan yaptırabilme yeteneği olarak tanımlanabilmektedir (Keyik & Erol, 2019, s. 25).

Güc birçok bileşenin bir karışımıdır. Bir aktörün uzun vadede yararlanabileceği unsurlar arasında toplam GSYİH, nüfus, bölge, coğrafya ve doğal kaynaklar yer alır.

Daha az somut uzun vadeli güç kaynakları arasında siyasi kültür, vatanseverlik, nüfusun eğitimi ve bilimsel ve teknolojik temelin gücü yer alır. (Goldstein & Pevehouse, 2012, s. 47).

Gücü ikiye ayırmak mümkündür. Bunlar, bir devletin elinde bulundurduğu zengin güç unsurlarıdır buna “potansiyel güç” denir. Bir diğeri ise, potansiyel gücün diğerk aktörler üzerinde sonuca yönelik kullanılması “gerçek güç” olarak tanımlanabilir (Keyik & Erol, 2019, s. 24). Güç mücadelesi içinde olan devletler diğerk devletler karşısında daha baskın konumda olmak için çeşitli birtakım araçlardan faydalanırlar. Bir başka deyişle güç unsurunu oluşturan bazı unsurlar bulunmaktadır. Bunlar kısaca;

1- **Coğrafya;** bir ulusun ya da devletin güç unsurunun temel taşlarından birini oluşturmaktadır. Coğrafyalar ülkelerin dünya üzerindeki konumunu belirleyen sürekli ve değişmez bir unsurdur (Morgenthau, 1970, s. 141). Örnek olarak Birleşik Devletler’in kıta genişliği doğu yönünde üç bin kilometre, batı yönünde ise altı bin kilometre uzunluğunda olmak üzere geniş bir şekilde denizlerle çevrilidir (Morgenthau, 1948). Bu karasal sınırlar dünya üzerindeki konumunu belirlerken Birleşik Devletler için de dış politikadaki uygulamalarına yansıdığı bilinmektedir. Bir başka örneği ise Süveyş Kanalı üzerinden vermek mümkündür. Süveyş Kanalı uzun ince bir deniz hattı ile trans geçişleri kolaylaştıran aynı zamanda bölgedeki varlığı sebebiyle yıllar boyunca güç mücadelesinde önem arz etmiş bir unsurdur. Bu kanalın güç unsurundaki coğrafi etkisi ile açıklanabilmektedir. Rusya Federasyonu (RF) üzerinden örnek verilecek olursa Rusya konumu sebebiyle dünya üzerinde bulunan karaların yaklaşık yedide birine sahip çok büyük bir alanı kaplamaktadır (Morgenthau, 1970, s. 142). Rusya’nın devasa genişlikteki topraklara sahip olması ve aynı zamanda topraklarının belirli bir kısmının kutuplara yakın bölgelerde bulunması savunma olarak Rusya için zor olsa da caydırıcılık açısından daha etkili bir konumdadır. Kutuplara yakın olan sınırların yılın belirli dönemlerinde buz ile kaplı olması ayrıca işgal etmek isteyen devletlerin çok büyük bir alanda başarısız bir girişim olarak sonuçlanacağı tarihsel süreçte örnekleriyle yaşanmıştır. Buna karşın Rusya’nın batı yönündeki toprakları ise Polonya ve diğerk ülkelere kadar adeta düz bir ova görünümündedir. Bir başka deyişle sıradağlar

ve çeşitli su yolları ile ayrılmadığı için Rusya'nın batı kanadı savunması güç bir coğrafya özelliği göstermektedir (Morgenthau, 1948).

2- **Doğal Kaynaklar;** Güç unsurunun bir diğer yapı taşı ise doğal kaynaklardır. Doğal kaynakları yiyecek ve ham madde olarak ikiye ayırmak mümkündür. Yiyecek açısından kendi üretimi kendi tüketimini karşılayan devletler bunu yapamayan devletler karşısında güçlü bir konuma sahiptirler. İngiltere tarihsel süreçte savaş zamanlarında kendi üretimi, kendi tüketimini karşılayamayan bir devlet olarak II. Dünya Savaşı dönemine kadar bu yönüyle zayıf kalmıştır. Bu sebeptendir ki İngiltere savaş dönemlerinde hayati derecede öneme sahip deniz yollarına ekstra önem atfetmiş ve bu deniz yollarının kontrolü için çokça çaba sarf etmiştir (Morgenthau, 1948). Ukrayna örneğinde ise kendi yiyecek ihtiyaçlarını karşılayan ve fazlasını da dünya ticaretine kazandıran bir ülke olma özelliği taşımaktadır. Ayrıca bilinmektedir ki Ukrayna tahıl üretimi ve ihracatı konusunda dünya da önemli bir güce sahiptir. Rusya-Ukrayna Savaşında tahıl koridorunun açılması ise bunun en güzel örneğidir (Acer, 2022). Doğal kaynaklar açısından önem arz eden bir diğer faktör ise ham maddedir. Tıpkı yiyecek ve içecek gibi ham madde de büyük öneme sahiptir. Ham madde kaynakları endüstriyel üretim için ve asıl önemli nokta ise savaş araçlarının temini ve yapımı konusunda büyük öneme sahiptir. Ayrıca ham maddenin işlenmesi açısından teknolojik araçların ve endüstrinin varlığı da hayli önemlidir (Morgenthau, 1970, s. 147). Doğal kaynaklar; bir ulusun gücü üzerinde önemli bir etkiye sahip bir başka unsur da doğal kaynaklardır. Doğal kaynaklardan en önemlisi tarih boyunca defalarca kendini kanıtlamış olan hiç şüphesiz gıdadır. Günümüzde de Rusya Ukrayna Savaşında görüldüğü üzere gıda açısından güçlü olan Ukrayna belirli şartlar altında ticaretine devam edebilmektedir (Keyik & Erol, 2019, s. 25).

3- **Endüstriyel Kapasite;** Bir devletin gücünü belirleyen önemli unsurlardan biridir endüstriyel kapasite. Bir ulus zengin ham madde kaynaklarına sahip olsa bile bu maddeleri işleyecek kendi lehine kullanacak bir kapasiteye sahip değilse kısaca endüstrisi gelişmemiş ise bu o devlet için büyük bir kayıptır. Kongo Demokratik Cumhuriyeti örneği endüstriyel kapasite için çok önemli bir kaynaktır. Bilindiği üzere uranyumdan askeri ve diğer endüstriyel araçlar için çok kıymetli bir madendir. Kongo

devleti çok zengin uranyum kaynaklarına sahiptir. Bu zengin kaynakların varlığı Kongo ulusal gücü için çok büyük bir kazançtır. Kongo Cumhuriyeti bu kaynaklar sayesinde diğer çevre ülkelere nazaran ulusal gücü bakımından göreceli olarak daha güçlü bir konumdadır. Kongo devleti zengin uranyum kaynaklarını işleyecek endüstriyel kapasiteye sahip değildir. Bu endüstriyel kapasitenin yoksunluğu ise Kongo ulusu için çok büyük bir kayıptır (Morgenthau, 1948).

4- Askeri Hazırlık Derecesi; Yukarıda sayılan coğrafya, doğal kaynaklar ve endüstriyel kapasite doğrudan askeri güce hizmet etmektedir. Askeri kapasite ise güç unsuru için önemli bir diğer faktördür. Askeri kapasite; teknolojik gelişme, liderlik ve silahların nitelik ve nicelik önemleri açısından değer kazanmaktadır. Teknolojik gelişmişlik özellikle I. Dünya Savaşı sırası ve sonrasında askeri kapasite bakımından silah sanayinde olan gelişmeler çerçevesinde önem kazanmaktadır. Teknoloji kitle imha silahları, nükleer silahlar ve günümüzde ise siber silahlarla daha etkili ve yıkıcı bir boyut kazanmıştır. Tarihsel süreçte savaş teknolojisine sahip ulusların güçlü olduğu görülmektedir. Bu özellikle on beşinci yüzyıldan on dokuzuncu yüzyıla kadar olan tarihsel süreçte Avrupa'nın diğer bölgelere (Afrika, Orta Asya, Orta Doğu, Yakın ve Uzak Doğu) oranla daha gelişmiş bir savaş teknolojisine sahip olması Avrupa'yı daha üstün bir konuma getirmiştir (Morgenthau, 1948).

Teknolojik gelişmelerin zamanında ve koordineli bir biçimde kullanılmasına ek olarak askerî açıdan liderliğin niteliği de çok önemli bir faktördür. Askeri liderliğin önemi 18. yy. 'da Prusya'nın askeri yönetimini elinde bulunduran Büyük Frederick'tir. Büyük Frederick, Prusya'yı birçok savaşta üstün konuma getirmiş ve başarı sağlamasında etkili olmuştur. Frederick'in bu liderlik vasfı askeri hazırlık derecesi açısından önemli bir örnek teşkil etmektedir (Morgenthau, 1970, s. 155).

Silahlı kuvvetlerin nitelik ve niceliksel özellikleri de askeri hazırlık derecesi açısından önemlidir. Silahlı kuvvetlerin nitelik ve niceliklerin önemi hem teknolojik gelişmeyi hem de askeri liderlik vasfını derinden etkilemektedir. Bir ulus teknolojik olarak ileri bir seviyede olabilmekte ve yönetici olarak iyi bir askeri dehaya sahip olabilmektedir. Buna karşın silahlı kuvvetlerin nitelik ve niceliklerinin yeterli olamaması büyük bir dezavantaj oluşturacaktır. Bir ulusun coğrafyasına uygun olarak

donanımlı ve gelişmiş bir orduya sahip olması gerekmektedir. Bir ordu da ülkesinin sınırları gereği hava, kara ve denizlerde hâkim konuma gelebilmek için niteliklerini arttırması gerekmektedir (Morgenthau, 1970, ss. 156-157).

5- Nüfus; Ulusal gücü belirleyen faktörlerden biri de nüfustur. Beşerî bir faktör olan nüfus niceliksel açıdan önemlidir. Bir ülkenin nüfusunun büyüklüğü ile gücü arasında doğrudan bir bağ bulunmamaktadır. Bir ülkenin diğer ülkelere oranla daha büyük bir nüfusa sahip olması o devleti daha güçlü olarak tanımlamanın yanlış bir yaklaşım olduğu gibi bir ülkenin de az bir nüfusa sahip olması onu güçsüz bir devlet olması anlamına gelmemektedir (Morgenthau, 1970, s. 158).

Thomas Hobbes'un Leviathan isimli eserinde insanların kudretlerinden bahseder. Bu kudreti ise devletin sahip olduğu kudret ile bağlantılı kurmaktadır. Devleti insanların iradelerine bağlı olarak bir grubun veya büyük bir toplumun bir araya getirilmiş her bir üyenin devlete olan inancı olarak açıklamaktadır. Böylece Hobbes hem topluluk olarak nüfusa hem de bu topluluğu oluşturan tüm bireylere önem vermiştir (Hobbes, 2007, s. 68). Kısaca toplumun, birlikteliğin veya grubun büyüklüğünün ve birbirlerine olan bağlılıklarının önemi üzerinde durulmuştur.

Buradan hareketle nüfusun niceliğinden çok niteliğinin önemine dikkat çekmenin daha doğru olduğu kabul edilmektedir. Nüfusun kabaca bir hesapla sayı olarak görmek yerine nüfusun eğilimlerinin ve niteliğinin varlığı daha doğru bir değerlendirme olarak karşımıza çıkmaktadır. Yetişmiş ve kalifiyeli nüfusun daha fazla öneme sahip olduğu bilinen bir gerçektir (Morgenthau, 1948).

6- Ulusal Karakter; Beşerî bir niteliğe sahip ulusal karakter ve moral bir ulusun güç unsurları üzerinde etkiye sahip bir başka önemli ögedir. Ulusal karakter ulusal gücü önemli şekilde etkiler. Herhangi bir devlet savaşta ya da barışta olursa ulusal karakteri canlı tutacak destekler ve politikalar üretmekten geri durmamalıdır (Morgenthau, 1948). Ulusal karakter kavramında Rusya örneğine yer verilmiştir. İkinci Dünya Savaşı yıllarında iki farklı olay (hikâye) anlatılarak Rusların ulusal hayatının pratikte aslında aynı olduğu üzerinde durulmuştur (Morgenthau, 1970, ss. 167-168).

Her ulusun karakteristik özelliğinin kendi ulusal gücünü yansıttığı anlatılmaktadır. Örneğin İngiliz ve Amerikan ulusunun zorunlu askerliğe karşı tutumu ile Türk ulusunun zorunlu askerliğe bakışı farklıdır. İngilizler ve Amerikalılar bu konuda anti-militarizm duygusu ile nefretle hareket ederlerken Türkler askerliği kutsal bir görev olarak görmekte ve bu kanıyı her Türk asker doğar cümlesi ile özetlemektedirler. Bu örnekten hareketle, bir ulusun gücü hesaplanırken ulusu oluşturan bireylerin ulusal karakterinin de hesaplanması gerekmektedir. Ulusal karakter ve moral güç üzerinde doğrudan etkiye sahip olduğu unutulmamalıdır.

7- Diplomasi ve Hükümetin Niteliği; Bir ulusun gücünü meydana getiren faktörler arasında istikrarsız da olsa en önemli etmen diplomasidir. Ulus gücünü belirleyen diğer tüm faktörleri bir araya getiren ve koordineli bir şekilde çalışmasını sağlayan ve nitelikli olmasını sağlayan diplomasidir. Ulusal moral, ulusal gücün ruhu olduğu gibi diplomasi de ulusal gücün beyni olduğu savunulmaktadır. Diplomasıyı yapan ve yöneten hükümetin varlığını basite indirgememek gerekmektedir. Diğer tüm güç unsurları birlikte ve uyumlu bir diplomasi altında çalıştırmak ancak temelde iyi bir yönetimin varlığının sonucudur. Maddi güç unsurlarını ve dış politikası arasındaki hassas dengeyi sağlayan iyi bir yönetim kaçınılmaz bir gerekliliktir (Morgenthau, 1970, ss. 181-186).

Diplomasi, devletlerin uluslararası ilişkilerini ve politikalarını yönetmesi açısından oldukça önemli bir konuma sahiptir. Burada ise iki büyük dünya savaşları arasında Romanya örneği üzerinde durulmaktadır. Romanya uluslararası ilişkilerde ülkesinin fiili kaynaklarından çok daha üstün bir rol oynamasını o dönemdeki dış işleri bakanının profesyonelliğine ve liyakatinden kaynaklandığı savunulmuştur.

Bir başka örnek ise Almanya üzerinden verilmiştir. Bismarck ve Hitler Almanya'nın en kötü dönemlerinde Almanya'yı uluslararası konumda yükseltmişler ve yine Hitler yükselttiği ülkesini kendi hırsları yüzünden dolayı çok kötü bir konuma geri düşürmüştür. Burada ise kişilerin liyakatlerinin önemi olduğu üzerinde durulmuştur (Morgenthau, 1970, ss. 184-185). Ek olarak bir dış politika ne kadar kusursuz bir temel üzerine kurulmuş her ne kadar maddi ve beşerî zengin kaynaklara dayanırsa dayansın liyakatsiz bir hükümetin varlığı her şeyi ortadan kaldırmaya

yetecektir (Morgenthau, 1970, s. 186). Bir devletin bürokrasisinin kalitesi, devletin bilgi toplamasına, uluslararası ticareti düzenlemesine veya uluslararası konferanslara katılmasına izin veren başka bir yetenek türü olup güç kavramı için önemli bir husustur (Goldstein & Pevehouse, 2012, s. 48).

Kısacası karar alıcıların ve uygulayıcıların özellikle dış politikada eğitimli ve yetkin kişilerden oluşması gerektiği savunulmaktadır. Ancak böyle bir anlayışta hareket edilirse gücün diğer unsurlarından olan diplomasi ve hükümetin niteliği kavramının gerçek anlamı ortaya çıkmış olmaktadır. Almanya örneğinde olduğu gibi Hitler hem bir devletin yükselmesi noktasında etkin rol alırken hem de aynı devletin neredeyse yok olması noktasında da o kadar etkin bir rol aldığı söylenebilmektedir. Bu da bizlere devletlerin uluslararası alanda yetkin kişiler tarafından yönetilmesi gerektiği gerçeği ile yüzleştirmektedir.

Yukarıda tanımlanan unsurlar, güç mücadelesinde etkin rol oynamaktadırlar. Devletler uluslararası arenada daha baskın konuma sahip olmak için tüm bu kavramları dikkatli ve özenli bir şekilde kullanmaları gerekmektedir. Devletler realist teori gereği güçlü olurlarsa kendilerini güvende hissederler. Böylece realist teoride güç bizleri bir diğer önemli kavram olan güvenlik kavramı ile tanıştırmaktadır.

1.6 Güvenlik

Klasik anlamda realist teorinin uluslararası ilişkileri açıklamada kullandığı kavram olan güvenlik kavramı siber uzayı açıklamak için çalışmada yer almıştır. Realistler, Uluslararası İlişkiler kurallarının genellikle bir güvenlik ikilemi yarattığını kabul etmekte ve bu durum, devletlerin kendi güvenliklerini sağlamak için yaptıkları eylemlerin (daha fazla askeri güç konuşlandırmak gibi) diğer devletlerin güvenliğini tehdit ettiği bir durum olarak tanımlanmaktadır (Goldstein & Pevehouse, 2012, s. 52).

Güvenlik kavramına yönelik bir başka tanım ise; devletlerin içinde bulunduğu siyasi ortam anarşik bir düzene sahip olduğundan her devletin kendi güvenliğini kendisinin sağlaması beklenmesi durumu olarak tanımlanmaktadır (Çalış & Özlük, 2007, ss. 232-233). Realist teoriye göre devletlerin içinde bulunduğu ortam kaotik olarak tanımlandığı için her devlet kendi güvenliğini kendisi sağlaması gerektiği

şeklinde tanımlanmıştır. Böylece anarşik ortamda güvenlik en önemli sorunsal olarak karşımıza çıkmaktadır. Devletler de sahip oldukları güç oranında kendi güvenliğini sağlamayı sürdürmektedir (Ateş, 2009).

Realist teorisyenler uluslararası barışın korunması için kolektif güvenlik mekanizmasının önemine değinmiştir. Böylece devletlerin hem kendi güvenlikleri hem de uluslararası sistemin güvenliği sağlanacağı savunulmuştur (Sandıklı & Kaya, 2012, s. 144). Booth'a göre, Soğuk Savaş sürecinde uluslararası politikaya hâkim olan güvenlik anlayışı, güvenliğin temel yaklaşımlarının devlet merkezci, askeri kaygıları dikkate alacak şekilde tanımlamıştır (Yavuz, 2009). Devletler mevcut kabiliyetlerini güvenlik kaygılarını giderecek şekilde kullanmaya çalışırlar böylece devletlerin kendi güvenliklerini sağlamaları ve sistemde var olan dengenin devamı şeklinde tanımlanmıştır (Sandıklı & Kaya, 2012, s. 145). Realist teoride güvenlik hayati öneme sahiptir. Buna karşın neo-realist teori güvenlik ikilemi kavramı ile varlığını sürdürmek istemiştir.

Uluslararası İlişkiler disiplini çerçevesinde ortaya çıkan teorilerin büyük bir bölümünde güvenlik önemli bir yer kaplamaktadır. Fakat teoriler güvenliği sağlarken çeşitli yollar ya da farklı araçlar kullanarak güvenliği sağlamayı amaçlamışlardır. Realist teori doğrudan askeri araçlar kullanılarak güvenliği sağlamayı hedeflemiştir. Bunu realist teorinin kökleri olarak nitelendirilen Hobbes ve Machiavelli'nin yaklaşımları ile daha net anlaşılmaktadır (Gözen, 2008). Realist teori kökenlerinden beslenen neo-realist teori ise güvenliği askeri güvenlik araçlarını bir amaç olarak tanımlamakta ulusal güvenliği öne plana çıkarmaktadır. Neo liberal teori ise ulusal güvenliği sağlama yolunda ekonomik politik anlayışı ön plana çıkararak güvenliği belirli bir sistem üzerinden sürdürmeyi amaçlamışlardır (Daban, 2017).

Güvenlik kavramı hem insanlar hem de devletler için hayati öneme sahiptir. Bu çalışmada realist teori güvenlik anlayışı çerçevesi ile analize dahil edilmiştir. Güvenlik ilk insandan günümüze çeşitliliği artarak ve derinleşip geliş göstererek varlığını ciddi şekilde hissettirmektedir. Güvenlik ilk çağlarda insanlar tarafından sadece vahşi hayvanlardan korunma şeklinde tanımlanırken bu algı günümüzde askeri, ekonomi, politik, siber gibi birçok alanda varlığına devam etmektedir. Çalışmada güvenlik

kavramının siber alanda devletler açısından önemine değinilecektir. Böylece güvenliğin realist teori çerçevesinde siber alandaki etkisi üzerinde durulacaktır.



İKİNCİ BÖLÜM

ULUSLARARASI İLİŞKİLERDE SİBER POLİTİKA

20. yüzyılın son dönemlerinde sosyal bilimler disiplini içinde çalışma alanı bulan siber alan internetin yaygınlaşması sonucu daha geniş bir alana yayılmıştır. Uluslararası İlişkiler disiplini çerçevesinde yer bulmuş olan siber alanı daha iyi analiz edebilmek için öncelikle “siber alan” ve “siber savaş” gibi teknik terimleri ayrı ayrı tanımlamamız gerekmektedir. Bu iki kavramı tanımlamadan önce “siber” kelimesinin anlamına değinmekte faydalı olacaktır. Siber kelimesi internet ağlarının bilgisayar ve diğer teknolojik ağlar yardımıyla kullanılması olarak tanımlanabilmektedir. Joseph Nye’a göre siber kelimesi elektronik sistemler ve bilgisayar ile ilgili faaliyetlerin oluşturduğu bir içeriktir (Nye, 2011). Siber politikanın sosyal alanda yarattığı değişimleri ve etkilerini daha iyi analiz edebilmek için öncelikle internetin gelişimine değinmek ve analize dahil etmek daha doğru olacaktır.

2.1 İnternetin Gelişimi

21. yüzyıl şüphesiz dijital gelişimin ve dijital çağın bir yansıması olarak karşımıza çıkmaktadır. Bu dönem bilgi ve iletişim araçlarının en gelişmiş ve etkili olduğu dönemdir. İnternetin tarihi çok eski olmamakla birlikte siber teknolojinin temellerinin yaklaşık olarak 1000 yıl öncesinde iki İslam bilim insanı olan El Heysem (965-1040) ve El Cezeri (1136-1026) tarafından yapılan çalışmalara dayandığı bilinmektedir (Akyeşilmen, 2018).

İnternet Soğuk Savaş döneminde iki kutuplu dünyanın güç mücadelesi sonucu ortaya çıkardığı bir üründür. Bu ürün ABD ve Sovyetler Birliği arasındaki askeri güç mücadelesi sonucunda ortaya çıkmıştır. Sovyetlerin uzaya uydu göndermesi sonucunda (Sputnik-1) Birleşik Devletlerin, askeri konu bakımından Sovyetler Birliğinin gerisinde kaldığı algısı yaratmıştır. Bu algıyı yıkmak isteyen Birleşik Devletler 31 Ocak 1958¹ yılında uzaya bir uydu gönderdi ve kendilerini uluslararası alanda daha güçlü göstermek için askeri alanda kullanılmasını düşündüğü bir ağ

¹ Daha fazla bilgi için; California Institute of Technology,
<https://www.jpl.nasa.gov/missions/explorer-1>

geliştirmiştir. (California Institute of Technology, 2023). 1958 Birleşik Devletler açısından Uzay Çağı'nın başlangıcı olarak kabul edilmektedir.

1969 yılında Amerika Savunma Bakanlığı'na hizmet amaçlı Larry Roberts tarafından icat edilen ağa ARPANET (Advanced Research Projects Agency Network) ortaya çıkmıştır (Marson, 1997). Bu ağ literatürde, günümüzde milyarlarca insanın kullanmış olduğu internet ağlarının atası olarak kabul edilmektedir. Bu ağ ilk önce dört farklı alanda bulunan bilgisayarlar arasında kurulmuştur. Bu alanlar Los Angeles Kaliforniya Üniversitesi, Stanford Üniversitesi, Utah Üniversitesi ve Santa Barbara Kaliforniya Üniversitesi arasında konumlandırılan bilgisayarlar arasındaki iletişim amaçlı geliştirilmiştir. Temelde askeri amaçlar olduğu için bu ürünün geliştirilmesi amaçlı fonlanma Pentagon tarafından karşılanmıştır (Akyeşilmen, 2018).

ARPANET öncelikli olarak askeri alanda kullanıma açılmıştır. Nihai amaç dönemin koşulları göz önüne alındığında (high politics) askeri politika çerçevesinde ordu içi haberleşme olarak kullanılmıştır. Soğuk Savaşın bitmesiyle birlikte değişen dünya koşulları ve özellikle 1980'li yılların başından itibaren Amerika merkezli kişisel bilgisayarların (personal computer) yaygınlık kazanmasıyla askeri bir ağdan sosyal ağa doğru geçiş süreci başlamıştır (Puyvelde & Brantly, 2019, s. 15).

1983 yılına gelindiğinde Amerika'daki kişisel bilgisayarlar üç yıl gibi kısa bir sürede o kadar çok artmıştır ki artık savunma bakanlığı yetkilileri Military Network, (MILNET) sadece askeri siteleri kullanmak için geliştirmişlerdir. 1980'li yılların sonuna gelindiğinde ise sosyalleşen ağlara yeni bir web tarayıcısı eklenmiştir. 1989 yılında Tim Berners Lee ilk web tarayıcısı olan World Wide Web adını alan (www) geliştirmiştir (Britannica Dictionary, 2023). 1998 yılında Google arama motoru kurulmuştur. Bu arama motorunun kurulması, bilgisayar kullanımının yaygınlık kazanması ve internet kullanıcı sayılarındaki artış etkileşimi oldukça arttırmıştır. 1990 yılında yaklaşık 3 milyon (Barbosa, 2006). İnternet kullanıcısı varken bu rakam 2012 yılında milyar 2022 yılı sonu itibariyle yaklaşık 5 milyar kişidir (Recro Digital Marketing, 2022). Özellikle 2000'li yıllarla birlikte cep telefonlarının ve akıllı elektronik ürünlerin kullanılmaya başlanması internet dünyasındaki gelişimin baş döndürücü etkisini açıkça gözler önüne sermektedir.

Bilindiği gibi internet siber alanın genişlemesinde çok etkili bir konumdur buna karşı internet tamamıyla siber alanı kapsadığı bilgisi doğru değildir. İnternet siber ağın yalnızca bir parçasını oluşturmaktadır (Nye, 2014). İnternet özellikle günümüz dünyasında hayatın olağan akışı içerisinde yer edinmiş bir durumdur. İnternet kullanıcı sayısı dünya toplam nüfusunun 3/2'sinden fazladır. İnternette geçirilen süre, sosyal medya kullanıcı sayısı ve daha birçok alanda karşımıza çıkmaktadır. İhtiyaç için geliştirilen bir ürün 7'den 70'e tüm yaş aralığındaki insanların toplu veya bireysel zaman harcadığı bir alan haline gelmiştir. Günümüzde hayatımızı tüm yönleri ile etki altına alan internet dünyasına siber uzay denilmektedir. Siber uzay milyarlarca insanın uzaktan birbirleri ile olan sosyal, siyasi ve ekonomik gibi birçok etkileşimi içinde barındırmaktadır. Her geçen gün gelişimini sürdüren internet tabanlı bu alan akıllı cep telefonlarında akıllı ev aletlerine, savaş araçlarından iletişim ve haberleşme araçları gibi birçok alanda karşımıza çıkmakta ve derinleşerek etkisini arttırmaktadır.

2.2 Siber Uzay

Siber alanın yeni bir etki alanı oluşturduğu herkes tarafından kabul edilen bir gerçektir. Bu noktada ise en büyük açık ve benzerlik ise uluslararası politika ile olan benzerliğidir. Uluslararası politika gibi anarşik bir sisteme sahip olan siber alan; devletler, kurumlar, ulus üstü kuruluşlar ve bireyler gibi birçok etki unsurunu içermektedir. Bu büyüklükte bir etki alanına sahip olan alanın herhangi bir kural koyucu veya denetleyici ile sınırlandırılmamış olması ise anarşik yapısına olan etkisini göstermektedir.

Cambridge sözlüğüne göre siber kelimesini sanal bir alanı kapsayan özellikle bilgisayar ve internet aracılığıyla ilgili özellikleri içeren ya da kapsayan alan anlamına gelmektedir (Cambridge Dictionary, 2023). Bu tanımdan hareketle siber kavramı bilgisayar ve internetle ilgili olan alanı tanımlamak için kullanılmaktadır.

2000'li yılların başından itibaren çok yaygın bir kullanım alanına sahip olan siber kelimesi ülkemizde gelişmekte olan alanların başında gelmektedir. Siber kavramı literatürde birçok çeşitli disiplin çatısı altında çalışma alanı bulmakta ve gelişimini sürdürmektedir. Uluslararası İlişkiler ya da Siyaset Bilimi çatısı altında birçok farklı kavramla birlikte kullanıldığı görülmektedir. Bu kavramlara örnek verilecek olursa;

Siber Uzak, siber savunma, siber savař, siber saldırı, siber caydırıcılık, siber istihbarat, siber güvenlik ve siber politika gibi birçok kavramla birlikte farklı anlamlarda kullanılmıştır.

Siber uzak son yıllarda popülerlięi artan bir kavram haline gelmiştir. Siber uzak kavramı Cambridge sözlüğünde “dünyadaki bilgisayar kullanıcılarının herhangi bir amaçla birbirleri ile iletişim kurmasına veya bilgilere erişmesine olanak sağlayan elektronik bir sistem” olarak tanımlanmıştır (Cambridge Dictionary, 2023). Fakat siber kelimesinin literatürde bilimsel bir kavramın karşılığında girmediğini biliyoruz. Edebiyat ve edebi eserler aracılığıyla literatürde yer edindięi bilinmektedir.

Siber kavramı 1948 yılında Norbert Wiener’in “Cybernetics” adlı eserinde hayvanların ve makinelerin kontrol veya makinelerle iletişim kurulması anlamında kullanılmıştır (Akyeşilmen, 2018). Siber uzak kavramı ise 1984 yılında bilim-kurgu yazarı William Gibson’un yazdığı “Neuromancer” adlı eserde karşımıza çıkmaktadır. Bu eserde siber uzak kavramı “*Siber uzak. Her ulustan milyarlarca meşru operatörün, matematiksel kavramları öğreten çocukların günlük olarak deneyimledięi rızaya dayalı bir halüsinasyon... İnsan sistemindeki her bilgisayarın bankalarından soyutlanan verilerin grafik bir temsili. Akıl almaz karmaşıklık. Işık çizgileri, zihnin uzaysızlığında, veri kümelerinde ve takımyıldızlarında uzanıyordu. Şehir ışıkları gibi, uzaklaşan...*” olarak tanımlanmıştır (Gibson, 1984). Literatürde ortak bir siber uzak tanımı mevcut değildir. Birçok teorisyen tarafından farklı şekillerde tanımlanan siber uzak her geçen gün yeniliğini ve derinlięin arttırarak devam ettięi için birçok tanım eksik kalmaktadır.

Nazli Choucri siber uzayın uluslararası ilişkilerde birçok yenilik ve özellięi sebebiyle artık göz ardı edilemeyecek kadar önemli olduğunu savunmaktadır. Çağdaş politika ve pratik aracı olarak modern uluslararası ilişkileri yeniden şekillendiren bir alan olarak betimlemektedir. Choucri siber uzayı tanımlarken bu alanın birçok katmandan oluştuğunu kabul etmektedir. Siber uzayı hiyerarşik olarak tanımlamakta ve siber uzayı David Clark gibi farklı katmanlardan oluştuğunu savunmaktadır. Choucri siber uzayın katmanlarını; tanımlarken “zamansallık (temporality), fiziksellik (physicality), nüfuz etme (permeation), deęişkenlik (fluidity), katılımcılık

(participation), dayandırma (attribution) ve yükümlülük (accountability)” gibi karakteristik özelliklerinin olduğunu ileri sürmektedir (Choucri, 2012).

David Clark ise siber uzayı dört katmanlı bir etkileşim olarak tanımlamaktadır. Birinci katmanda insan faktörü yer almakta, ikinci katmanda saklanan, dönüştürülen ve iletilen bilgi, üçüncü katmanda hizmetleri oluşturan ve platformu destekleyen mantıksal alt yapı, son katmanda ise var olan mantıksal unsurları destekleyen fiziksel temeller olarak açıklamıştır (Clark, 2010). Clark ayrıca siber uzayı tanımlarken bilgisayarların birbirine bağlı olma durumu ve bu durum içindeki insanların davranışlarının siber uzayın karakterini belirlemesi olarak tanımlarmıştır (Clark, 2010). Siber uzay çok geniş bir çalışma alanı imkânı sunmaktadır ayrıca bu alanların sınırlarını tam olarak bilmek neredeyse imkânsız olup her geçen gün yetenek alanları keşfedilmektedir. Bir başka deyişle siber uzay coğrafi sınırları aşarak yetki sınırlarını genişletme ve aktörlerin kimliklerini gizleyerek eylemler yapmalarına izin veren bir alan olarak tanımlanabilmektedir (Choucri, 2012).

Siber alanı kapsamlı ve net bir tanımının anlaşılabilmesi için siber uzayın bileşenlerine değinmekte faydalı olacaktır. Nezir Akyeşilmen’e göre siber uzay dört farklı bileşen tarafından oluşturulmaktadır. İlk faktör siber uzayda kullanım sağlayan ve siber uzata kendi karakteristik özelliğini yansıtan insandır. İkinci faktör ise siber uzayda kullanıcılar arasında paylaşılan veya iletilen bilgidir. Üçüncü bileşen ise bu eylemlerin kullanılmasını veya iletişimin sağlanmasında gerekli etkiye sahip kodların oluşturduğu mantıksal kapsamdır. Son bileşen ise kullanıcı faktörü insan ile bilgi, iletişim veya herhangi bir işlemin kodlar vasıtasıyla işleyişini oluşturan mantıksal çerçevenin kullanılmasının yolunu açan bilgisayar ya da telefon gibi fiziksel alt yapıdır (Akyeşilmen, 2018).

Salih Bıçakçı siber uzayı en geniş haliyle insanların birbirleri ile bağlı olan bilişim sistemleriyle etkileşim sağladığı fiziksel olmayan alan olarak tanımlamıştır (Bıçakçı, 2014). Hasan Çiftci siber uzayı “*Siber ortam, her türlü yazılım, donanım ve iletişim altyapısından meydana gelen, birbirine bağlı veya birbirinden bağımsız bilgi sistemlerinin oluşturduğu ortamdır.*” olarak tanımlamıştır (Çiftci, 2017).

Daniel T. Kuehl ise siber alanda yaptığı çalışmalarla literatürde önemli bir yeri vardır. Kuehl ise siber uzayı tanımlarken, kara, hava, deniz ve uzay alanının dışında bir alan olduğunu savunmuştur. Siber uzay, ayırt edici ve benzersiz karakteri oluşturmak, depolamak için elektronik ve elektromanyetik spektrum kullanımıyla çerçevelenen bilgi ortamı içindeki küresel bir alan olarak tanımlamıştır (Kuehl, t.y.). Bu tanımda siber uzayı hava, kara ve diğer alanların dışında tanımlaması veya siber uzayı farklı kılan tanım, siber uzay yaratmak ve "girmek" ve elektromanyetik spektrumun enerjilerini, özelliklerini kullanmak için elektronik teknolojilerinin kullanılması olduğunu savunmuştur (Kuehl, t.y.).

Siber uzay bilgi ve teknoloji çağında bir bilgi alanı oluşturması ve uluslararası ilişkilerde devlet dışı varlıkların da yer edinmesi sebebi ile NATO, AB Komisyonu, Beyaz Saray ve diğer ulus üstü kuruluşların tanımlarına bakıldığı zaman genellikle kritik alt yapıların, devletlerin ulusal iç güvenlik stratejileri ile doğru orantılı olan yüksek öneme sahip kurum ve kuruluşların internet ve yazılım ile ilişkili olarak gerçekleşebilecek olumsuz bir olaya karşı kendi varlıklarını korumaları şeklinde tanımlanmıştır. Yine ortak tanımlarda internet, insan faktörü, elektro manyetik alan ve bilgisayar gibi fiziksel alt yapılar dikkate alınarak tanımlanmaya çalışılmıştır (The White House, 2009).

Türkiye'nin 2020-2023 Ulusal Siber Güvenlik Strateji Belgesinde siber uzayın tanımı; *“Doğrudan ya da dolaylı olarak internete, elektronik haberleşme ve bilgisayar ağlarına bağlı olan tüm sistem ve hizmetler”* olarak tanımlanmıştır (Ulaştırma ve Altyapı Bakanlığı, 2020, s. 10). Bu tanımda donanım, yazılım ve sistem üzerinde durulurken, interneti kullanan birey (insan) varlığı nispeten gözden kaçırılmıştır. Özellikle internet ve teknoloji alanında gelişmiş olan Japonya, Amerika Birleşik Devletleri, Hindistan gibi ülkelerin siber uzay ya da siber ortam olarak geçen tanımlarına bakıldığı zaman; internet, sistem, yazılım ve tüm bu süreci kapsayan ortam üzerinde durulduğu görülmektedir (The Government of Japan, 2015, s. 5).

Yukarıda devletler, teorisyenler, ulus üstü kurum ve organizasyonlar tarafından yapılan tanımlardan anlaşılacağı üzere siber uzay insanlar tarafından kullanılan, sistemsel yazılım ve elektromanyetik ağların oluşturduğu tüm dünyayı kapsayan ve

henüz net bir sınırının olmadığı sanal bir ağ olarak görülmektedir. Belirli bir sınırlarının olmaması ve ortamın tamamen sanal olması sebebiyle de kontrol edilmesi oldukça zordur. Devlet, birey ya da herhangi bir kurum tarafından kontrol edilememesi sebebiyle çeşitli tehlikeleri barındırdığı söylenebilmektedir. Siber uzay tanımlardan da anlaşılacağı üzere içinde interneti kapsayan bir alandır ancak tamamen internet ile sınırlı olmadığı anlaşılmaktadır.

Siber uzay ya da siber alan ulusal devletler, devletlerarası kuruluşlar, istihbarat örgütleri, özel sektörde yer alan tüm kurumlar, belirli bir toplumsal grup ve bireyleri kapsayabilecek faaliyetleri ile zarar veya fayda verebilecek sanal bir ortamdır. Siber alanın sınırları belli olmayan geniş imkanlar sunan ortamından çeşitli şekilde faydalanılmakta ya da zarar verilmektedir.

Bu süreçte siber uzayda kullanıcının amacına göre çeşitlilik göstermektedir. Yakın geçmişe kadar siber uzay devletler için düşük politika (low politics) olarak görülmüş ve yeteri kadar önem atfedilmemiştir. Buna karşın 2000’li yılların ortalarında yaşanan casusluk olayları ve zararlı yazılımlar sonucunda devletler ve stratejik öneme sahip kurumlar siber alandaki gelişmeleri yakından takip etmeye başlamışlardır. Böylece düşük öneme sahip bir alan olmaktan çıkan siber uzay günümüzde yüksek politika (high politics) konularından biri haline gelmiştir. Bu gelişmeyi devletlerin ve ulus üstü kurumların yayınladıkları siber güvenlik strateji belgeleri ile kanıtlamak mümkündür.

Siber uzayın özellikleri dikkate alındığında geleneksel uluslararası ilişkiler teorilerinin siber uzayı anlama ve açıklamada yetersiz kaldığı anlaşılmaktadır.

Şekil 2, Siber Uzayın Özellikleri Tablosu;

Zamansallık (Temporality)	Geleneksel zamansallığın yerini neredeyse anlık olarak değiştirir.
Fiziksellik (Physicality)	Coğrafya ve fiziksel konum kısıtlamalarını aşar.
Geçirgenlik (Permeation)	Sınırlara ve yetki alanlarına nüfuz eder.
Akışkanlık (Fluidity)	Sürekli değişimleri ve yeniden yapılandırmaları gösterir.
Katılım (Participation)	Aktivizm ve politik ifade önündeki engelleri azaltır.
Atıf (Attribution)	Aktörlerin kimliklerini ve eylem bağlantılarını gizler.
Hesap verebilirlik (Accountability)	Sorumluluk mekanizmalarını atlar.

Kaynak: Choucri, N. (2012). *Cyberpolitics in International Relations*. USA: The MIT Press.

Siber uzayın anlık gelişmeler göstermesi ve zamansallık bağlantısının çok kısa sürelerle indirgenmesi uluslararası politikada derin etki yaratmıştır. Bu sadece zamansallık açısından değil yukarıda bulunan özelliklerin tümü hem devletlerarası ilişkilerde hem de devletlerin iç işlerinde geleneksel alışılmış durumların aksine yeni birtakım durumlarla karşılaşmasına zemin hazırlamıştır. Değişen algılar sadece devletler üzerinde değil birçok kurum ve özel sektör için de geçerlidir.

Her geçen gün etkisini geliştiren siber uzay başta birey olmaz üzere, diğer tüm aktörler üzerinde etkili olmaktadır. Siber uzayın nevi şahsına münhasır özelliklerine her geçen gün bir yenisinin eklenmesi ise an meselesidir. Bu dinamik ve stratejik

özelliği dikkate alındığı zaman siber uzayın ne denli büyük bir etkisi olduğu daha kolay anlaşılabilmektedir. Siber uzayın birçok özelliğinin yanı sıra birçok tehdit ve risk faktörü bulundurduğunu da belirtmek gerekmektedir. Siber uzayın özellikleri birtakım avantaj sağlarken aynı zamanda birçok tehdit ve güvenlik açığını da barındırmaktadır. Bunlar kısaca;

- Anlık gelişmelere tepki vermesi ve hızlı olması bakımından siber uzay çok etkili bir alan oluşturmaktadır. Fakat bu durumun aksine anlık kaotik bir ortama sebep olması açısından kötüdür. Örneğin 2022 yılında Akbank'ta yaşanan sistemsal sorun veya siber saldırı olarak nitelendirilen gelişme yaklaşık olarak üç gün sürmüş ve bu süreçte Akbank sistemleri kilitlenmiş atm, kredi kartı ve diğer birçok bankacılık işlemleri askıya alınmıştır. Milyonlarca kullanıcı mağdur olmuş ve kısa bir zaman dilimince milyonlarca kullanıcıyı olumsuz yönde etkilemiştir.

- Siber uzayın doğasına özgü çok geniş (sınırsız) bir alana sahip olması bakımından veya uluslararası yapılacak olan herhangi bir çalışmadan kimseden izin (vize, vb.) veya talep olmadan siber uzayda toplantı, görüşme, fotoğraf ya da posta göndermek gibi durumlar için oldukça cazip bir imkân sunmaktadır. Bu özelliğinin aksine uluslararası veya devlet içinde oluşturulacak olan terör grubu, yasadışı bahis, insan kaçakçılığı ve istihbarat bilgilerini sabote etmek ve/ veya bu gibi bireyi ve devletleri olumsuz etkileyecek içeriklere ev sahipliği yapması bakımından kötü bir alanı kapsamaktadır.

- Siber uzayın yapısına özel kodlama, blok zinciri (Blockchain) ve özel yazılımlar içermesi güvenliğin yüksek öneme sahip olması açısından iyi; buna karşın zararlı yazılımlar veya kötü niyetli kişilerce kullanılması bakımından büyük bir tehdit oluşturmaktadır.

- Günümüz teknoloji çağında siber alanda baş döndüren gelişmelere tanık olmaktayız. Her geçen gün siber uzayda daha şaşırtıcı özelliklerle tanışmamız, başta birey, toplum ve devlet güvenliği açısından ciddi sorunları da beraberinde getirmektedir.

Siber uzayın belirsizliklerinin ve içinde bulundurduğu özelliklerinden dolayı kişi, toplum ve devletin hak ve menfaat kaybına uğramaması içten bile değildir.

Özellikle nükleer tesisler, enerji alt yapı tesisleri, bilgi ve denetim kontrol sistemleri, sağlık sistemleri, barajlar, askeri bilgi sistemleri, istihbarat özel sistemleri, iletişim ve haberleşme sistemleri ve kısaca insanlar, kurumlar ve devletler açısından kritik öneme sahip alt yapılara yapılacak olan saldırıların siber uzayda güvenlik hassasiyetinin önemini ifade etmektedir (Gorge, 2007). Siber uzayda güvenlik etkeninin önemine dikkat çekerken diğer taraftan ise sosyal medya sayesinde uluslararası ilişkiler alanında birçok yeni gelişmelerle de karşılaşmaktadır. Örneğin son yirmi yılda popülerlik kazanan sosyal medya bireyler tarafından benimsenmesi ile artık dünya genelinde milyarlarca insan tarafından kullanılmaktadır.

Kullanımı artan iletişim ve sosyal aktivite araçları uluslararası politikada kullanıldığı bilinmektedir. İlk örnekleri 1994 yılında e posta ile başlayan sosyal iletişim araçları günümüzde Twitter, facebook ve linkedln gibi mecralar üzerinden etkinliğini devam ettirmektedir. 1994 yılında kullanılan e posta İsveç Başkanı Carl Bild'in, ABD Başkanı Bill Clinton'a gönderdiği e-posta ilk sosyal iletişim araçlarının kullanıldığı diplomasi olma özelliğini oluşturmaktadır (Bildt, 2016). Günümüzde bireyler gibi devlet kurumlarının da sosyal medya araçları kullandığı bilinmektedir. Sosyal medya kullanıcılarının sayısı Ocak 2023 verilerinde 4,76 milyar kullanıcı sayısı olduğunu ve bunun toplam dünya nüfusuna oranı ise yaklaşık yüzde 60'tır.

Dünya genelinde sosyal medya kullanıcıların günlük olarak sosyal medyada ortalama iki saat otuz dakika süre geçirdiği göz önüne alındığında siber alanın kapasitesi ve kullanıcıları tarafından ne kadar benimsediğini göstermesi açısından önemlidir (Datareportal, 2023). Ek olarak bu kadar kullanıcının olması ise günümüzde sosyal medyanın etkinliğinin büyüklüğünü göstermektedir. Günümüzde bireyler gibi devlet kurumları ve özel sektör kuruluşları da sosyal medyayı tanıtım, reklam ve sorun çözme amaçlı kullanmaktadır. Kırsal olarak muhtarlıktan genel olan bakanlığa kadar tüm devlet dairelerinin sosyal medya sayfaları olduğu bilinmektedir. Özel sektör açısından ise normal bir şubeden genel müdürlük düzeyinde merkezi yönetiminde birer sosyal medya sayfaları bulunmaktadır.

Siber uzayda sosyal medya araçlarının haberleşme, randevu talep etme veya bir sorun gibi birçok anlamda kullanıldığı görülmektedir. Günümüzde böyle özellikleri

barındıran siber uzay uluslararası ilişkilerde bizleri yeni bir kavram ile tanıştırmıştır. Adına dijital diplomasi (e- diplomasi) dediğimiz yeni bir kavram literatüre kazandırılmıştır (Karabulut, 2021). Dijital diplomasi kavramı bürokratlar ve yöneticiler tarafından farklı amaçlar için kullanılabilir. Dış politika yapımında veya liderler tarafından yönetim açısından etkili kararlar almak için sosyal medyanın kullanılması olarak tanımlanabilmektedir (Baştan & Karagül, 2021). Burada William Gibson'un 2013 yılında yayınladığı "Cyberpunk" adlı eserinde yer alan aklın yeni sahibinin siber uzayın oluşturduğu kurgusu akıllara gelmektedir (Doctorow, 2013, s. 404).

Günümüzde teknoloji ve siber uzay hayatımızın merkezinde yer almaktadır. Siber alanda yaşanan gelişmeler siyasi ve sosyal alanda hayatımızı etkilemektedir. Siber uzay özellikle uluslararası gelişmeleri de etkilemektedir. Özellikle Soğuk Savaş sonrası dönemde Marshall McLuhan'ın söylediği "Küresel Bir Köy" tabiri (1989 Berlin Duvarı'nın yıkımından sonra daha fazla önem kazanmıştır.) siber uzayı da kapsar niteliktedir. Küresel bir Köy kısaca sınırların ve duvarların olmaması, insanların hep beraber ortak yaşamı olarak açıklanabilmektedir (Arıboğan, 2023). Bu tanım günümüzde bizlere siber uzayı anımsatmakta sınırlarının olmaması ve tüm dünyayı tek bir ortak alanda birleştirmesi ise buna örnek oluşturmaktadır.

Siber uzayda kullanıcılar internet vasıtasıyla her türlü bilgiye ulaşım sağlayabilmektedir. Kullanıcıların bu bilgilere yasal veya yasal olmayan yollarla ulaşması devlet, birey ve kurumların güvenliği açısından tehdit oluşturmaktadır. Yasa dışı bilgi edinme yolları ise siber uzayın doğasından kaynaklanmaktadır (Clarke & Knake, 2011, ss. 45-47). Siber uzayın doğası gereği var olan özelliklerin hem gerçek hem de yapay bir alanı kapsadığı bilinmektedir. Kullanıcılar arasında olan haberleşme ve birçok yapay alanda sağladığı fayda gibi fiziksel dünyanın gerçek bir tamamlayıcısı olduğu da bilinmektedir.

Siber uzay geleneksel yöntemleri hızlı bir şekilde geliştirmiş ve değişimini sağlamıştır. Bu gelişim ve değişimler uluslararası ilişkilerde devletlerin davranışlarında da etkisini göstermiştir. Uluslararası ilişkilerde mevcut anarşik yapıyı değiştirdiği söylenebilir. Askeri, ekonomik ve siyasi açıdan güçlü olmak yerini

teknolojik alandaki yenilikleri ve gelişmeleri de kapsayacak şekilde genişlemiştir. İletişim ve haberleşme alanında yaşanan bilgiye dair hızlı hareket kabiliyeti devletlerin kurumları arasındaki etkileşimi arttırmıştır. Bu yaşanan gelişme güç algısı üzerinde etkili bir faktör oluşturmaktadır. Siber uzayın eşsiz ve limitsiz özellikleri benzersiz bir istihbarat ve bilgi imkânı sunmaktadır. Bu bakımdan siber uzay fiziksel alanda neredeyse tüm sektörlerde karşımıza çıkmaktadır (Erdem, 2020)

2.3 Siber Savaş

Tarihsel süreçte yaşanan olayların kaçınılmaz bir eki olan savaş kavramı günümüzde de bazı değişiklikler varlığını sürdürmektedir. Neredeyse insanlık tarihi kadar eski bir kavram olan savaş; insanların, kabilelerin, şehir devletleri ve günümüz modern devletlerinin temel konularından biri olduğunu söylemek yanlış olmayacaktır. Literatürde ortak bir savaş kavramı bulmak zordur. Savaş kavramını tanımlamak için M.Ö. 2000’li yıllarda Sun Tzu’ ya kadar dayandırmak mümkündür.

Habil ile Kabil’in kavgasından, mağarada yaşanan döneme, tarımdan, kentsel hayata kadar olan süreç içerisinde insanoğlunun yaşadığı bu uzun süreçte var olan savaş kavramları farklı da olsa temele bakıldığı zaman aynı olduğu bilinmektedir. Savaşın tanımını yapabilmek için öncelikle savaşın olmadığı güvenliğin olduğu alana bakmamız gerekmektedir. Güvenlik kavramı Türk Dil Kurumu Sözlüğünde “toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi, emniyet” olarak tanımlanmaktadır (Türk Dil Kurumu, 2021). Bu tanıma göre savaş kavramı ise toplumsal hayatta düzenin aksaması, korku ortamının hâkim olması ve emniyetsizlik olarak tanımlanabilir. Literatürde siber savaş kavramı birçok teorisyen tarafından farklı bakış açılarıyla farklı şekillerde tanımlanmıştır.

Literatürde hâkim olan teorisyenlerin ortak tanımlarından hareketle internet, bilgisayar sistemleri, kritik öneme sahip veri tabanları ve alt yapılara yönelik oluşturulan sabote, zarar verme ve engelleme amaçlı yapılan saldırılar olarak tanımlanabilmektedir. Buna karşın literatürde siber savaş ile siber çatışma ayrımından doğan farklılıkları açıklayan teorisyenlerden olan P. Lorents ve R. Ottis bu iki kavramın farklılıklarına odaklanmışlardır. Bu iki araştırmacı siber savaşı devletler

arasında olan çatışmalar şeklinde tanımlamışlardır. Çünkü bazı teorisyenler savaş gibi büyük bir olayın yalnızca devlet aktörleri arasında olabileceğini savunmuştur. Bu düşünce sistemine sahip teorisyenler bireyler arasında ise çatışma olabileceğini savunmuşlardır (Dayton, 2010). M. Murphy ise siber savaş hava, kara, deniz ve uzay alanından sonra beşinci boyut savaş alanı olarak tanımlamıştır (Economist, 1 Temmuz 2010).

Nazli Choucri siber savaş kavramını açıklarken bu alanda yapılan siber saldırıların amaçlarını değerlendirmiştir. Bir savaştan bahsedebilmek için bir saldırının olması gerektiğini savunmuştur. Siber alanda yapılan saldırıları siber savaş olarak değerlendirebilmesi için gerekli olan özellikler üzerinde durmuştur. Bu saldırıları ise fiziksel alanda meydana gelen ve siber alanda meydana gelen saldırılar olarak ayırmış ve bu saldırıların sonuçlarını da aynı şekilde siber ve fiziksel hedefler olarak ikiye ayırmıştır.

Siber Hedefler:

- Bir ağın veya sistemin çeşitli bileşenlerini kontrol etmek için radyo frekans cihazlarının kullanılması
- Ağları farklı şekillerde kullanılmasını engellemek
- Önemli bir bilgisayar ağına veya sistemine sızmak
- Truva atları veya diğer kötü amaçlı virüsler oluşturmak ve bunları bir ağ üzerinden göndermek

Fiziksel Hedefler:

- İletişim ağlarının veya kablolarının kesilmesi
- Bir bilgisayarı veya ağ sunucusunu sert bir cisimle kırmak
- Önemli bir elektrik şebekesini veya su arıtma tesisini kontrol eden bir ağa veya sisteme girmek
- Uçuşları yönlendirmek için bir hava trafik kontrol sistemini taklit etmek (Choucri, 2012).

Bu özelliklerden hareketle siber savaşın siber alanda ve fiziksel alanda bulunan araçlar arasında fiziksel ve siber araçlar kullanılarak meydana geldiğini savunmaktadır. Siber savaş tanımını çeşitlendiren teorisyenler de bulunmaktadır. Bu teorisyenler stratejik siber savaş, hibrit savaş ve operasyonel siber savaş olarak farklı gruplar altında açıklamışlardır.

2.3.1 Stratejik Siber Savaş

Devletler veya birtakım gruplar belirli amaçlar çerçevesinde özellikle stratejik siber savaşlarda provokasyon ve dezenformasyon şekilleriyle farklı araçlar kullanarak farklı yollardan taktikler kullanmasıdır. Martin C. Libicki stratejik siber savaşı bir devletin topluma karşı yürüttüğü ancak öncelikli amacının devletin davranışını etkilemeyecek bir siber saldırı türü olarak tanımlamıştır (Libicki, 2009). Siber alanda hâkim olan devlet dışı aktörlerin varlığıyla stratejik siber savaş daha karmaşık olmaktadır. Karmaşık olmasının sebepleri ise karşılık bulma, tepki verme ve saldırıların amaçları açısından karmaşık bir hal almaktadır.

Rusya'nın Estonya ve Ukrayna'ya karşı yapmış olduğu siber saldırılar stratejik siber savaşın birer örneğini oluşturmuştur. Stratejik siber savaşta devletlere ve toplumlara yönelik yapılan saldırıların etkisi daha kısa sürede çözüldüğü bilinmektedir (Güntay, 2017).

2.3.2 Hibrit Siber Savaş

Elektro-manyetik tekniklerin kullanılarak, geleneksel savaş yöntemleri kullanılarak sürdürülen savaşa hibrit savaş denilmektedir. Literatürde hibrit savaş kavramı farklı başlıklar altında ya da doğrudan operasyonel siber savaş kavramı içerisinde kullanılmıştır. Soğuk Savaş sonrası süreçte NATO uluslararası konjonktürün belirsizliği sebebiyle geleneksel savaş yöntemlerine ek olarak hibrit savaş yöntemlerini de geliştirmeye başlamış ve imkanlarını geliştirmeye başlamıştır (Bıçakçı, 2012). Kısaca hibrit savaş 21. Yüzyılın gelişen teknolojisi ile siber savaş yöntemleri kullanılarak sürdürülen karma bir savaş stilidir.

Gelişen teknolojiye ayak uydurmak isteyen NATO değişen tehditlerin yapısını da dikkate alarak ortaya çıkması muhtemel tehditleri önleyebilmek adına ve oluşabilecek olan hibrit savaş kabiliyeti kazanmak için çeşitli müzakereler düzenlemiştir. Bu müzakerelerden biri olan ve NATO'nun hibrit savaş kabiliyeti için önemli sayılan 1998 yılında "Harekât Sistemlerine Enformasyon Teknolojilerinin Uygulanması" ve 1999'da düzenlediği "21. Yüzyılda NATO Enformasyon Sistemlerini Korumak" temalı müzakereleri NATO'nun yeni sisteme uyum sağlaması olarak kabul edilmektedir (Bıçakçı, 2012). Değişen koşullara uyum sağlamaya çalışan NATO hibrit savaş kapsamında tehdit oluşturabilecek olası unsurlara karşı bazı önlemler almak istemiştir. Bu sebeple 1999 yılında Washington Zirvesi icra edilmiştir. NATO üyesi ülkelere karşı yapılabilecek saldırı ihtimali üzerinde durulmuş ve aynı zamanda ittifak oluşturan üye devletleri askeri ve askeri olmayan güç unsurları tarafından muhtemel tehditler konusunda bilgilendirmiştir (Güntay, 2017). Literatürde hibrit savaş için en genel tanım olarak düzenli ve düzensiz güçlerin birleştirilerek kullanılması olarak tanımlanmıştır (Bıçakçı, 2019). Siber hibrit savaşta bu tanıma uymaktadır.

Teknolojik gelişmelerin varlığı ve klasik savaş teknikleri ile birlikte kullanılması hibrit savaşın en temel unsurlarından birini oluşturmaktadır. Siber alan geleneksel savaş alanlarını (hava, kara, deniz ve uzay) kapsayan bir alan olduğu için hibrit savaş modelini kapsamaktadır. Hibrit Siber Savaş siber alanda kullanılan teknolojik aletlerin silah olarak kullanılmasını kapsadığı gibi gayri nizami harp unsurlarını da içermektedir. Hibrit savaşın bir diğer özelliği olan sonuç odaklı olmaması bunun yerine uzun bir sürece yayılan savaş durumunda maksimum çıkar sağlanması amaçlanmaktadır (Bıçakçı, 2019). Özetle siber hibrit savaş karşı tarafa saldırılar düzenleyip yıpratma ve dezenformasyon amaçlı saldırılar yaparak uzun süreli bir zaman dilimine yayılarak kazanç sağlanması olarak tanımlanabilmektedir. Düzensiz ve konvansiyonel yöntemler kullanılarak hibrit savaş yöntemi uygulanmaktadır. Burada dikkat edilmesi gereken nokta ise kısa süreli olmayıp daha uzun soluklu bir süreci kapsadığıdır (Güntay, 2017).

2.3.3 Operasyonel Siber Savaş

Siber savaş kavramı ile operasyonel siber savaş kavramı arasındaki en önemli nokta yapılacak olan saldırıların çok gizli bir şekilde yürütülmesidir. Siber savaş kavramı ile operasyonel siber savaş kavramını birer örnek ile açıklamak gerekirse siber savaş basit sıradan toplumsal olaylara müdahale eden bir grup ekip olarak örneklendirilirken, operasyonel siber savaş kavramı ise çok daha özel ve daha gizli, yurt dışı operasyonlara katılan çok daha profesyonel bir ekibin oluşturduğu müdahale olarak örneklendirilebilmektedir.

Martin C. Libicki operasyonel siber savaşı; “*Askerî hedeflere ve askerî bağlantılı sivil hedeflere savaş zamanı yürütülen siber saldırılar.*” olarak tanımlamıştır (Libicki, 2009). 2008 yılında Rusya’nın Gürcistan’a yönelik olarak yürüttüğü siber müdahaleler operasyonel siber savaş örneği olarak gösterilebilmektedir. Bu örneklerden hareketle operasyonel siber savaşın tek bir amacının olmadığı ve birçok karakteristik özelliği olduğu söylenebilmektedir (Güntay, 2017).

Yukarıdaki tanımlardan hareketle kullanılan savaş kavramının teknolojik gelişme ile derinleşerek geliştiğini gözlemlemek mümkündür. 21. yüzyılda teknolojinin baş döndürücü bir şekilde gelişim göstermesi ile birlikte yaşanan gelişmeler birer devrim niteliği taşımaktadır. Günümüzde savaşlar sadece askeri alanla veya askeri alanı kapsayan teknoloji ile sınırlı kalmamaktadır. Sosyal bilimlerde adına siber alan denilen bu devasa boyuttaki teknolojik düzlem beraberinde birçok etki alanı oluşturmaktadır. Siber alan insan hayatının birçok alanına etki ettiği gibi savaş alanında yaşanan gelişmeleri de çok boyutlu olarak çeşitlendirmektedir. Devletlerin kamu hizmetleri (e-devlet), ulaşım, iletişim, enerji tesisleri, robotik askeri sistemler, insansız hava araçları ve kritik öneme sahip altyapılar gibi devletler ve bireyler için hayati öneme sahip alanlarda yaşanan teknolojik gelişmeler birçok farklı nedenle sabote edilebilmektedir. Bu alanlara uzaktan bir müdahale ile etki edildiğinde asıl amaçlarının dışında farklı amaçlar için hizmet etmekte ya da tamamen yararlı hizmetlerini sıfırlanabilmektedir. Bu olaylar kamu hizmetlerinin aksaması olağan hayat akışının dışında gelişmeler yaşanması ve birçok insanı olumsuz etkileyebilmektedir.

Birleşmiş Milletler sözlüğüne göre “*Savaş kelimesinin gerçekten iki tanımı vardır: savaşın silahları, tankları ve ilerleyen orduları çağrıştıran gerçek tanımı ve savaşın suça karşı savaş, yoksulluğa karşı savaş, uyuşturucuya karşı savaş ve teröre karşı savaş gibi retorik tanımı. "Siber savaş" teriminin hem gerçek hem de retorik savaş yönleri vardır, bu da onu siber güvenlik ve siber saldırıları tartışırken çok yüklü bir terim haline getirir.*” olarak tanımlanmıştır (Schneier, 2013).

NATO siber saldırılara karşı savunma kalkanı oluşturmak için ilk kez 2002’de Prag’da yapılan Zirve toplantısında bu durum ele alınmıştır. Bu tarihten itibaren siber konusu NATO gündeminde daha fazla yer almaya başlamıştır. 2008 yılında NATO’nun ilk siber savunma politikası benimsenmiştir. 2014 yılında Müttefikler, siber savunmayı toplu savunmanın ayrılmaz bir parçası haline getirmiş ve herhangi bir siber saldırının NATO’nun temelini oluşturan antlaşmanın toplu savunma maddesinin (5. madde) yürürlüğe konmasına yol açacağını beyan etmiştir. Ayrıca 2016’da siber uzay askeri operasyonlar alanı olarak kabul edilmiş ve ulusal ağlarının ve altyapılarının siber savunmasını öncelikli olarak güçlendirmeye yönelik ortak beyanda bulunulmuştur (Brent, 2019). Böylece siber alanda oluşabilecek savaşa karşı güçlü bir alt yapı oluşturulması planlanmıştır.

Literatürde siber savaşın olabileceğini savunan teorisyenlerin bulunduğu gibi aslında gerçekte böyle bir siber savaşın olmayacağını savunan teorisyenler de bulunmaktadır. Siber saldırıların bir savaş eylemi olup olmayacağı yönünde çeşitli görüşler bulunmaktadır. J. Stone siber saldırıların amacının bir casusluk, sabotaj eylemi veya bir suç unsuru oluşturduğu net olarak bilinmediği için ayrıca siber saldırı girişimlerin bir savaş olup olmadığı bilinmediğinden dolayı siber saldırıları savaş tanımlamanın zor olduğunu savunmaktadır. Stone savaş kavramını zor kullanmak, öldürme eylemi ve şiddet unsuru ile bağdaştırmıştır. Böylece siber savaşın da bu üç unsur ile açıklanabileceğini iddia etmiştir (Stone, 2013).

T. Rid siber savaş kavramının bir savaş eylemi oluşturmadığını iddia etmiştir. Rid savaş kavramını tanımlarken klasik anlamda savaşın tanımını yapmış ve savaşın şiddet unsuru, politik amaç ve işlevselliği üzerinden analiz etmiştir. Rid’e göre siber

savaşların henüz böyle bir etkinliğinin olmadığını savunarak siber saldırıları bir savaş olarak görmediğini iddia etmiştir (Rid, 2012).

Siber savaşın etki ettiği unsurlar kritik öneme sahip bilgi ve hizmet sistemleridir. Bu bakımdan siber savaşlar, fiziki dünyada etki alanı oluşturan fakat gerçekleşmesi itibariyle siber uzayı kapsayan bir etkileşimdir. Literatürde siber savaşın olmayacağı yönünde görüş bildiren teorisyen ve akademisyenlerin var olduğu bilinse de siber savaşın varlığını savunanların daha ağır bastığı söylenebilmektedir. Bu bakımdan devletler ve devlet dışı aktörlerin varlığı ile her geçen gün daha komplike hale gelen saldırılar bütünü savaş olarak tanımlanmaktadır. Siber savaş kavramı ise her geçen gün gelişmekte ve yeni etkileşim unsurları ile yeni anlamlar kazanmaktadır.

2.4 Siber Saldırıları

Tarihsel süreç içerisinde 19. yüzyıla kadar kara ve deniz savaşları hakimiyetini korurken 20. yüzyıl ile insanoğlu hava araçlarının savaş alanında kullanıldığına şahit olmuştur. Teknolojik gelişmelerle birlikte 21. yüzyılda siber savaş araçlarının kullanıldığına tanıklık edilmektedir (Köker, 2021). Literatürde birçok siber saldırı tanımı bulunmaktadır. En genel anlamıyla siber saldırı; siber alanda meydana gelen bilgisayar ve internet ağlarının imha edilmesi, geçici süre ile kullanılamaz hale getirilmesi, bozulması ve kısıtlanması olarak tasvir edilmektedir (Erdem, 2020). Siber saldırıların genel olarak bilgisayar sistemlerini, büyük veri tabanlı kontrol sistemlerini, donanım ve altyapılarını hedef aldığı bilinmektedir (Güntay, 2014). Bilinen ilk siber saldırı altyapılara yönelik olarak 1982 yılında ABD Başkanı R. Reagan'ın onayı üzerine Sibirya'da bulunan Rus boru hattına yönelik gerçekleştirilmiştir (Yenal & Akdemir, 2020). Bu saldırı sonucunda boru hattına patlama olmuş ve tahribat gerçekleşmiştir. Büyük veri sistemlerine yönelik yapılan siber saldırılarda en ufak bir zarar ya da hasar tüm bir süreci veya tesisi tamamen durdurabilmektedir (Krepinevich, 2012). Bu boru hattı örneğinde olduğu gibi patlayıp ciddi bir zarara da sebep olabilmektedir.

Bu yapılan siber saldırının amacına ulaştığı ve siber saldırının doğası gereği olan etkinliğini sağladığı söylenebilmektedir. Bu örnekten hareketle siber saldırıların

sadece siber alanda etkili olabileceği algısı eksik kalmaktadır. Siber saldırılar siber alandaki ağ, yazılım, donanım ve veri sistemlerini etkileyebileceği gibi fiziksel hayata da etki edebilmektedir. Siber alanda meydana gelen teknoloji destekli değişimler uluslararası alanda aktör ve saldırı algısının değişmesine sebep olduğu açıktır. Yeni teknolojik gelişmelerin fikirleri ve algıları değiştirebileceği algısı askeri konular için nadiren de olsa tam olarak yeterlidir (Valeriano & Maness, 2018, ss. 263-264). Siber alanda yaşanan gelişmeler devletler arası etkileşim ve devlet dışı aktörlerin saldırıları siber gücü artırma yolunda adımlar atmaya zorlamıştır. Bir başka deyişle devletler siber alanda siber güvenlik kapasitelerini artırma yolunda politikalar izlemişlerdir (Darıcılı, 2017). Geleceğe bakıldığında, devletlerin ve devlet dışı kuruluşların otonom siber saldırı silahları geliştirme olasılığının yüksek olduğu öngörülmektedir (Krepinevich, 2012). Siber saldırıların savaşa dönüşme olasılık veya siber saldırıların bir savaş olgusu mu? Bu soruya cevap veren John Stone'a göre siber saldırıların suç, sabotaj, casusluk ya da savaş eylemi mi olduğunu belirleme çabası var olan savaş olgusunun ne olduğunu anlamayışımız tarafından bir sorun oluşturmaktadır. Ancak Stone siber savaşın şiddet içermesi, ölümcül olayların yaşanması ve zor kullanımı olması sebebi ile savaş olarak sayılabileceğini savunmuştur (Stone, 2013). Daha geniş anlamda, siber saldırılar uluslararası hukuk kapsamında nasıl sınıflandırılır? Yoksa siber uzayda gerçekleştirilen eylemler tamamen farklı, tamamen yeni kurallarla mı ele alınmalı? Bu gibi sorular çerçevesinde Matthew C. Waxman' a göre "savaş eylemi" sorusunu çerçelendirmenin yasal olarak daha kesin bir yolu, bir siber saldırının BM Şartı'nın güç yasaklarını ihlal edip edemeyeceği veya silahlı bir saldırı anlamına gelip gelemeyeceğidir (Waxman, 2017). Siber saldırıların ekonomik, siyasi ve askeri olarak siber uzayda arttığını savunmaktadır. Bu sebeple siber savaş yeteneklerinin daha da önemli hale geldiğini savunmaktadır (Möckli, 2010). Möckli siber saldırılarda önemli olan noktanın hasarın potansiyel boyutu olduğunu savunur ve potansiyel zarara göre merdiven şeklini kullanarak siber saldırıları sıralamaktadır.

Möckli siber çatışma düzeyini merdiven şeklinde tasarlamış ve siber saldırıların önem sıralaması yaratacağı potansiyel zarara göre sıralanmıştır. En çok hasar verebilecek olan ve potansiyel olarak en yoğun olan siber savaş ilk sırada yer almaktadır. Siber savaşı sırasıyla, siber terörizm, siber casusluk, internet suçu ve

potansiyel olarak en az zararı verecek olan, merdiven şeklinin en alt kısmında ise siber vandalizm yer almaktadır (Möckli, 2010).

Siber saldırı kavramının genel olarak özellikleri;

- Siber saldırıların geçici olması
- Kısa vadeli hedefler doğrultusunda hareket etmesi,
- Kalıcı bir hasarın oluşturulabilmesi için fiziksel müdahale alanı ile birleştirilmesi gerekir,
- Caydırıcılık ve zorlama etkisinin kullanılabilmesi,
- Zamansallık açısından ne zaman tam olarak yapılacağına bilinmemesi,
- Zarar verme ve tahrip etme yetkinliği (Gartzke, 2013).

Siber saldırıların özellikleri dikkate alındığında bir siber saldırının niteliğini belirlemedeki zorluk, siber savaşın önemli ve belki de kalıcı bir karakteridir (Krepinevich, 2012). Siber saldırılar özelinde siber uzayda yaşanan gelişmeler fiziksel hayata etki ettiğinden dolayı uluslararası düzenlemelerde siber saldırı ve çatışma hukukuna yönelik çalışmalara ihtiyaç olmuştur ancak bu alanda net olarak bir belirginlik yoktur. Uluslararası hukuk kurallarının dahi günümüzde uygulamadaki sorunları göz önüne alındığında siber alanda yaşanan gelişmeler için yapılacak olan hukuk kurallarının uygulanabilirliği bir başka sorunu oluşturmaktadır. Bu soruna ek olarak siber alanda yapılan siber saldırılarda, yapılan saldırının kaynağı net olarak bilinmediği için hukuk kurallarının suçlu üzerindeki işlevselliği olumsuz olabilmektedir. Siber saldırıların kaynağını bulmaya yönelik teknolojik gelişmelere karşın yapılan saldırının anonim olmasına yönelik teknoloji de gelişmektedir (Güntay, 2019). Siber saldırıların varlığının ve yaratmış olduğu etkilerinin daha detaylı olarak anlaşılabilmesi için dünya üzerinde farklı alanlarda yapılan siber saldırılara değinmek gerekmektedir.

2.4.1 1999 Kosova Krizi

1999 yılında bağımsızlığını kazanmak isteyen Kosovalılar ile Sırp'lar arasında yaşanan bağımsızlık yolundaki kriz olayı sonucunda yaşanan siber saldırılar olarak bilinmektedir. Bu krizin hem siber alana hem de fiziki alanda ciddi etkileri olmuştur.

Yaşanan soykırım neticesinde her iki ülkenin vatandaşlarından da hayatını kaybedenler olduğu bilinmektedir. Aynı zamanda siber alanda da yaşanan siber saldırıların varlığı bilinmektedir. Yaşanan soykırım olaylarından sonra NATO olaya müdahil olabileceği sinyali vermiştir. NATO açık bir şekilde Sırp milliyetçilerini uyarmış ve yaşanan şiddet olaylarına son verilmesi gerektiğini açıklamıştır. Buna karşın Sırp birlikleri şiddet olayından geri adım atmayınca NATO kuvvetleri yaşanan olaya bir son vermek istemiştir (NATO, 1999). NATO kuvvetleri olayları bastırmak için harekete geçince kendilerini “Kara El” olarak adlandırılan Sırp hackerler tarafından NATO’nun farklı ülkelerde bulunan alt yapılarına yönelik siber saldırıları başlatmışlardır. Yaşanan bu siber saldırı olayında NATO tarafından yapılan açıklamada erişilen bilgilere göre Sırp milliyetçileri tarafından yapıldığı söylenmiştir (Verton, 1999). Bu saldırı sonrasında yaşanan gelişmeler NATO açısından oldukça önemlidir. NATO bu siber saldırı sonrasında siber uzayın ilerleyen yıllarda ne gibi tehdit oluşturacağı yönünde çeşitli çalışma alanı imkânı bulmuştur. Kosova üzerindeki ihtilaf, internetteki ilk savaş olarak nitelendirilmektedir. Anthony Pratkanis, Kosova sonrası yaşanan siber saldırılar hakkında şu gözlemlerde bulunmuştur: "Şu anda gördüğümüz şey, son derece önemli ve sofistike hale gelecek olan şeyin yalnızca ilk turu. Henüz devletler bu konuda endişelenmedilerse, savaş stratejistleri bu konuda endişelenmeli” diyerek siber alanda yaşanacak gelişmelerin önemine dikkat çekmiştir (Denning, 1999).

2.4.2 2007 Estonya Siber Saldırısı

2007 yılında Estonya’da yaşanan siber saldırılar aslında bir heykelin yerinin değiştirilmesi kararının alınması ile başladığı bilinmektedir. Estonya hükümetinin, Nazilere karşı savaşmış Sovyet birliklerinin kahramanlıklarını anlatan II. Dünya Savaşı’ndan kalmış bir heykelin yer değişikliği yapması sonucunda ortaya çıktığı bilinmektedir (Goodman, 2010). Bronz asker heykeli 1947 yılından itibaren Estonya’nın başkenti Tallinn’deki meydanda bulunuyordu. Bu anıt heykelin caddeden kaldırılıp Tallinn askeri mezarlığına taşınması kararı alınması olaylarında yaşanan toplumsal protestolar yerini siber alandaki saldırılara bırakmıştır. Estonya anıt heykeli taşımak istemesi bir nevi Rusya’ya karşı ayrılıkçı hareket alanı oluşturmuş ve artık

Rus hükümeti yörüngesinde hareket etmek istemediğinin bir göstergesi olarak algılanmıştır. Yaşanan bu olay ayrılıkçı halk tarafından protestolar ile başlayan siber saldırılar yaklaşık 23 Mayıs'a kadar sürmüş ve Estonya'nın bankacılık ve medya sitelerine yönelik ciddi saldırılar yapılmıştır (Kurtul, vd., 2019, s. 16). Estonya hükümeti tarafından verilen kamu hizmetleri verilemez hale gelmiştir. 1991 yılında bağımsızlığını kazanan Estonya, nüfusunun yaklaşık yüzde 40'ı Rus kökenli azınlıklardan oluşmaktaydı (Yener, 2015). Nüfus üzerinden Estonya'ya hakimiyet kurmak isteyen RF zaman zaman bu azınlık grup üzerinden çeşitli politikalar izlemiştir. Yaşanan Bronz Asker heykeli taşıma kararı alınması Rus yanlısı grubun protestoları ve Rusya Federasyonu'nun çeşitli yaptırımları dikkat çekmektedir. Yaşanan krizin hemen ardından gelen siber saldırıların gözlerin Rusya'ya çevrilmesine sebep olmuştur. Siber saldırıların Rus yanlısı grup veya hükümet destekli birimler tarafından yapıldığına dair çok fazla haber vardır. Bu olay sonucunda Estonya NATO'dan yardım talep etmiş ve çeşitli özel sektör kuruluşlarından da yardım aldığı bilinmektedir. Siber uzayın şahsına münhasır özelliği sebebiyle yaşanan bu siber saldırıda isnat-ispat ilişkisinin kurulması hususundaki zorluklar bilinmektedir. Bu sebeple yapılan siber saldırıların kesin olarak RF tarafından yapıldığı itiraf edilmediği sürece kimin yaptığının bilinmesi imkansızdır (Darıcılı, 2017). Ancak dönemin politik koşulları düşünüldüğünde yapılan saldırıların arkasında Rus hükümetinin desteğinin olduğu aşıkardır. Çünkü yapılan siber saldırıda bazı IP adreslerinin RF kaynaklı olduğu tespit edilmiştir (Yener, 2015).

2.4.3 2008 Gürcistan Siber Saldırısı

Rusya Federasyonu ve Gürcistan arasında yaşanan savaş öncesi ve sonrasında dönemde yaşanan gelişmeler olarak siber alanda yapılan saldırıların bütünüdür. 08.08.2008 savaşı olaraktan bilinmektedir. 2008 yılında, Rusya'nın Gürcistan'ı işgalinden kısa bir süre önce, Rusya'nın web sitelerine ve ağ altyapısına yönelik siber saldırılar başlamıştır. Bu saldırılar, Gürcistan'ın dış dünya ile iletişimini etkili bir şekilde devre dışı bıraktığı bilinmektedir (Goodman, 2010). Siber saldırıda en önemli nokta ise Estonya saldırısından farklı olarak Gürcistan siber saldırısında ekonomik temelli bir saldırı olduğudur. Gürcistan siber saldırılara karşı daha savunmasız bir

devletti bu saldırıda ise özel sektör ve diğer ülkelerin önemli yardımları olmuştur. 2008 Gürcistan siber savaşının yöntemi web sunucularına yönelik saldırılar sonucunda bu sitelerin çevrimdışı durumuna getirilmesidir. Ayrıca Gürcistan'ın 2008 yılındaki Cumhurbaşkanı Mihail Saakaşvili'nin Adolf Hitler ile karşılaştırılan resimler web sitelerinde yayımlanarak amaçlanan yöntemlerini kullanmışlardır (Danchev, 2008). Bazı analistler bu saldırıların Gürcistan hükümetinin konumunu oldukça sarstığı ve zayıflattığı yönündedir. Yaşanan siber savaş sonrası dönemde Deutsche Telekom tarafından işletilen Alman sunucuları sayesinde geçici olarak Gürcistan web siteleri yeniden kullanıma açılmıştır (Keizer, 2008). Gürcistan siber saldırıları senkronize askeri operasyonlarla bağlantılı olarak başlatılan geniş ölçekli siber saldırıların bilinen ilk örneği olması bakımından önem arz etmektedir (Connel & Vogler, 2017).

2.4.4 Litvanya Siber Saldırısı

Temmuz 2008'de Rusya Federasyonu destekli olduğu iddia edilen siber saldırılara maruz kalmıştır. Litvanya komünist sembolleri yasakladıktan sonra DDoS (Distributed Denial of Service) saldırılarına maruz kalmıştır. Litvanya'nın bu yasak kararına karşı çıkan RF destekli gruplar tarafından yaklaşık 300 tane Litvanya web sitesini hacklemişlerdir. Bu saldırıların, yanı sıra ulusal etik kurumu, menkul kıymetler ve takas komisyonu, Litvanya Sosyal Demokrat Partisi'nin Web sitelerini kapatmıştır. Bu web sitelerinde orak-çekiç amblemleri kullanılarak yasağa karşı bir atak yapılmıştır. Bazı web sitelerinde ise orak-çekiç amblemlerinin yanında Litvanya karıştı şarkılar da eklenmiştir (Kelley, 2016).

Yaşanan bu siber saldırıların arkasında büyük oranda RF destekli grupların olduğunu iddia etmek mümkündür. Çünkü Litvanya ve RF arasında yaşanan politik anlaşmazlığın sonucunda bu saldırıların yaşanması iddiaları güçlü kılmaktadır (McLaughlin, 2008). Olayların perde arkasında yatan temel politik anlaşmazlık ise Litvanyalı vatandaşların Sovyetler Birliğinin çalışma kamplarında ağır koşullar altında çalıştırılmasıdır. Bu çalışma esnasında hayatlarını kaybeden Litvanyalılar olmuştur. Hayatını kaybedenler için tazminat almak isteyen Litvanya halkına yönelik sözünde durmayarak RF tazminat ödemeyi reddetmiştir. Buna karşın Litvanya politikalarında farklı yönelmeler yaşamış ve RF ile AB arasında ilişkileri engellemeye yönelik

tutumlar sergilemiştir. Bu politik karşı çıkışa RF enerji akışını kesmiş ve ikili ilişkilerin kopma noktasına gelmesine sebep olmuştur. Politik olarak yaşanan bu çatışma yerini siber alandaki saldırılara bırakmıştır (Darıcılı, 2017). Bu siber saldırının da Estonya ve Gürcistan örneğinde olduğu gibi Rus hükümeti ile çatışan çıkarlar sonrasında yaşanmış olması, temelde RF'nun diğer tüm ülkelere politik bir mesajı olarak algılanabilmektedir.

2.4.5 Kırgızistan Siber Saldırısı

21. yüzyılın başlarında politik anlaşmazlıklar sonucunda Rusya Federasyonu destekli olduğu iddia edilen bir diğer siber saldırı örneği ise Kırgızistan'dır. 18 Ocak 2009 tarihinde Kırgızistan'a ait iki internet sağlayıcı ağın DDoS saldırıları sonucunda ülkeye ait web siteleri ve e-posta haberleşmeleri kesintiye uğramıştır (Rhoads, 2009). Siber saldırıların arka planında ise yaşanan politik anlaşmazlık olduğu bilinmektedir. Kırgızistan'a ait Manas şehrinde bulunan Amerikan Hava üssü ile ilgili olan tartışmadır. Bu hava üssünü bir tehdit olarak gören RF üssün kaldırılması için Kırgızistan'a siyasi baskılar yapmıştır (Darıcılı, 2017). Yaşanan bu politik kargaşa sonrası süreçte Kırgızistan siber saldırılara maruz kalmıştır. Siyasi baskılar sonucunda Kırgızistan üssün kira sözleşmesini artırmıştır ancak Amerikan hükümeti Asya jeopolitiğinde etki alanı oluşturmak için tüm maliyetleri kabul etmiştir. 2014 yılına gelindiğinde Kırgızistan üssü kapatmıştır (TRT Haber, 2014). Kırgızistan siber saldırısı, Litvanya, Estonya ve Gürcistan saldırılarının ortak özellikleri RF'nun çıkarları doğrultusunda istediği hedeflere ulaşmak için diğer devletlere karşı siber alanı bir baskı aracı olarak kullanmasıdır.

2.4.6 2010 Stuxnet Saldırısı

Stuxnet saldırısı, Temmuz 2010 yılında İran'ın Natanz nükleer üretim yaptığı tesisleri hedef alan zararlı virüsler yardımıyla gerçekleştirilen bir siber saldırıdır (Şenol, 2016). Bu siber saldırı aynı zamanda siber güvenlik için tarihi bir dönüm noktası olarak kabul edilmektedir. Stuxnet adı verilen bu zararlı yazılım insanlığın günümüze kadar üretmiş olduğu en zararlı ve en karmaşık yazılımdır. Dört tane sıfır gün (Zero Day) kullanması kısaca daha önce denenmemiş ve bilinmeyen bir açıklığı

kullanan bu yazılım sadece bilgisayarlara değil aynı zamanda makinalara da fiziki zarar veren ilk kod olma özelliği taşımaktadır (Akyeşilmen, 2018).

Stuxnet İran'ın Natanz nükleer üretim ve geliştirme tesisine saldırmak için ABD ve İsrailli hackerler ve uzmanlar tarafından geliştirildiği iddia edilen, endüstriyel SCADA (Gözetleyici Kontrol ve Veri Toplama) sistemlerini hedef alan zararlı bir yazılımdır (Sağıroğlu & Alkan, 2018). Bu iddia ABD'nin İran'ı nükleer silah üretmekle suçladığı yıllara denk gelmesi bakımından iddianın olasılığı güçlüdür.

Almanya'nın Münih şehrinde uluslararası gazetecilerle yaptığı güvenlik konuşmasında Eugene Kaspersky, Stuxnet'i pandoranın kutusunun açılışı olarak nitelendirmiştir. Ayrıca *“bu zararlı yazılım para çalmak, spam göndermek ya da kişisel bilgi çalmak için yazılmadı. Bu yazılım tesislere sabotaj düzenlemek endüstriyel sistemlere zarar vermek için oluşturuldu. Korkarım ki bu yeni dünyanın başlangıcı, 1990lar siber vandalların, 2000ler ise siber suçluların on yılıydı. Korkuyorum ki artık siber terörizmin ve siber savaşların başladığı yeni bir çağdayız”* şeklinde tanımlamıştır (Kaspersky, 2010).

Stuxnet ilk başta sıradan bir virüs olarak görünse bile karmaşıklığı, çalışma yöntemi ve kodlanmasının yapısı sebebiyle devletler tarafından yapıldığını güçlendiren karmaşık bir yazılımdır (Akyeşilmen, 2018). Stuxnet'in özellikleri ve yapısı dikkate alındığında detaylı keşfi (casing), uzun süreli bir zamanda mimlenmiş olması (spotting), yaklaşım (approaching), angaje (recruiting) ve sevk/idare (running) edilmiş bir veya daha fazla elaman (HUMINT kaynağı) vasıtasıyla üretildiği anlaşılmakta olup bu uzun soluklu ve komplike olan yazılımı ancak devlet destekli gruplar tarafından yapılabileceği düşünülmüştür (Darıcılı, 2017). Birçok akademisyen ve uzman görüşü bu saldırının arkasında devlet veya devlet destekli grupların olduğu yönündedir (Lupovici, 2016). Stuxnet saldırısı hibrit savaş kavramında literatürde kabul gören başarılı bir siber savaş örneğidir (Sağıroğlu & Alkan, 2018).

Stuxnet endüstriyel kontrol sistemlerini ele geçiren zararlı bir virüs olması sebebiyle ilk defa siber alanda yaşanan saldırının fiziki alanda zarar vermesi açısından önem arz etmektedir. Bu sebeple Kaspersky'in siber saldırılar için geleceğe yönelik

düşüncesi korkutucu boyutlara ulaşabileceği düşüncesini destekler niteliktedir. Stuxnet virüsü kapsamı ve etkisi boyutunda bir ilk olmakla birlikte geleceğe yönelik bunun bir son olmayacağı da açık bir şekilde ifade edilebilmektedir

2.4.7 Türkiye’de Yaşanan Siber Saldırı Vakaları

20. yüzyıl sonları ve 21. yüzyıl başlarında diğer pek çok ülkede olduğu gibi Türkiye’de sürpriz siber saldırı olayları ile karşılaşmıştır. Bu saldırıların zaman içerisinde devam edeceği de su götürmez bir gerçektir. Türkiye’de yaşanan siber saldırıları kısaca değinmek gerekirse;

- Ağustos 2008 yılında Bakü, Tiflis ve Ceyhan boru hattında meydana gelen patlamada enerji akışı sekteye uğramıştır. Yapılan araştırmalar sonucunda bu patlamanın teknik bir arızadan dolayı meydana geldiği açıklanmış bunun da bir siber saldırı olduğu anlaşılmıştır (Şenol, 2016).

- Ocak 2009 yılında Atatürk Havalimanında özellikle dış hatlar bölümündeki bilgisayarları etkileyen “Conficker” adlı virüs sebebiyle verilen hizmetler aksamıştır. Bu olayın sonradan çok daha geniş bir siber saldırı olduğu birçok ülkeyi etkilediği anlaşılmıştır (Kurnaz & Karatepe, 2019).

- Aralık 2015 yılında yaşanan siber saldırı ise Türkiye’nin özellikle bankacılık ve finans alanında ciddi aksamlar yaşanmasına sebep olmuştur. Yaşanan saldırı üstlenen Anonymous, Türkiye’deki birçok bankaya yönelik saldırılarına devam etmiştir (Kurtul, vd., 2019, s. 17).

- Kasım 2015 tarihinde Türk hava sahasını ihlal eden ve uyuğu bilinmeyen savaş uçağı Hatay’ın Yayladağı ilçesinde Türk Hava kuvvetleri tarafından düşürülmüştür (BBC News, 2015). Uçak düştükten sonra Rus Hava kuvvetlerine ait olduğu ortaya çıkan savaş uçağı ikili devlet ilişkilerini kopma noktasına getirmiştir. Kopma noktasına gelen ilişki Türkiye’nin Moskova Büyükelçiliği tarafından yapılan açıklamada da görülmektedir². Türkiye’ye yönelik yaptırım yapacağı tehdidinde bulunan Rusya Federasyonu çeşitli alanlarda (turizm ve gıda) Türk mallarına yönelik ambargo uygulamıştır (Girit, 2016). Bu gelişmelerden sonra Türkiye tarihinde

² Rus uçağının düşmesi sonucu yaşanan diplomatik krize ait açıklama. Daha fazla bilgi için; <http://moskova.be.mfa.gov.tr/Mission/ShowAnnouncement/246277>

yaşadığı en büyük siber saldırılarla karşılaşmıştır. Bu siber saldırılar hem devlet kurumlarına ait web sitelerini hem de bankalar gibi özel sektör kuruluşlarının web sitelerini hedef almıştır (Darıcılı, 2017). Bu siber saldırılar Estonya, Gürcistan ve Kırgızistan siber saldırıları gibi RF ile olan politik kriz sonrasında yaşanması bakımından benzerlik taşımaktadır. Türkiye yaşanan bu siber saldırılara önlem amaçlı Orta Doğu Teknik Üniversitesi (ODTÜ), Ulusal Siber Olaylara Müdahale Merkezi (USOM), Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile Telekomünikasyon İletişim Başkanlığı (TİB) ile anında gerekli önlemleri aldığı bilinmektedir (Darıcılı, 2017). Türkiye bu yoğunlukta siber saldırı ile karşılaşması sonrasında 2016 yılında Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı kabul etmiştir (Darıcılı, 2019). Türk yetkililer gerekli önlemleri aldığı yönünde açıklamalar yapmıştır ancak siber saldırılar web adreslerini ve bazı finans şirketlerinin çalışmasını aksatmıştır.

Örnekleri verilen siber saldırılar dikkate alındığında siber alanın geleceğin güç ve mücadele alanı olduğu aşikardır. Dünya geneli yayınlanan internet güvenliği raporlarına bakıldığında yaşanan siber saldırıların giderek arttığı bilinmektedir. Siber tehdit haritasına bakıldığı zaman 28 Mart 2023 tarihinde günlük olarak ortalama 400.000.000 siber saldırının yapıldığı görülmektedir (ThreatCloud AI, 2023). Şubat 2019 Symantec İnternet Güvenliği Tehdit Raporunda Türkiye 2016-2018 yılları arasında hedeflenen siber saldırıları gruplarından etkilenen önemli on ülke arasında bulunmaktadır (Internet Security Threat Report, 2019, ss. 50-54). Artan saldırılar dikkate alındığında Türkiye gibi gelişmekte olan ülkeler teknoloji alanında daha fazla yatırım yapması gerekmektedir. Siber saldırılar ancak üst düzey teknoloji ile kısmen engellenebilmekte ya da caydırıcılığı tartışılabilmektedir. Aksi halde her ülke, kurum, birey önlemini almazsa siber saldırı için açık bir hedef haline gelmektedir.

2.5. Siber Casusluk

Ulusal ve uluslararası alanda yaşanan teknolojik gelişmeler güvenliğin önemli bir bileşeni olan istihbarat/casusluk faaliyetlerini de etkilemiştir. Casusluk ve istihbarat süreçleri siber uzayda çeşitli şekillerde yer almıştır. İstihbarat kavramı anlamsal olarak Türk Dil Kurumuna göre bilgi toplama, haber alma anlamında olup casusluk kavramı ise ajan olma, casus olma durumu olarak tanımlanmıştır (Türk Dil

Kurumu, 2022). Birey, toplum, devlet ve uluslararası alan için önemli bir faktör olan bilgi toplama ve bilgiye erişme siber uzayda özgün yer bulması, teknolojinin gelişmesiyle siber casusluk ya da istihbarat kavramı olarak karşımıza çıkmaktadır. Siber alanda casusluk, tipik olarak açık kaynak istihbaratından ve sosyal medya üzerinden çeşitli şekillerde uzun süre zarfında uzman kişilerce bilgi toplanmak kaydıyla yürütülen süreçtir (Marchetti, vd., 2016, s. 244). Siber casusluk kısaca siber alanda stratejiler kullanarak bilgi, belge ve veri toplanmasıdır (Erdem, 2020). Bir başka ifade ile siber istihbarat ekonomik, siyasi ve kritik öneme sahip alanlarda üstünlük elde etmek için koordineli olarak uzman kişilerce bilgi toplama olarak tanımlanabilir. Siber alanda casusluğun bilinen örnekleri mevcuttur. Siber casusluğun önemli bir örneği ABD'de yaşanmıştır.

ABD hükümetinin iddiasına göre siber casusluk olayı ilk olarak 1998'de keşfedildi ve saldırılar 2001 yılına kadar devam ettiği yönündedir. Bu saldırılar tamamen siber casusluk yoluyla bilgi toplama girişimlerinden oluşmaktadır (Goodman 2010). İlk casuslukta izinsiz girişleri, saldırganların programlar aracılığıyla "tünelle açarak" sistemlere girerek güvenlik analistlerinin izinsiz girişleri tespit etmesini zorlaştırdığı hükümet ve askeri siber ağları hedef alarak siber casusluk oluşturduğu bilinmektedir (Goodman, 2010). İlk yaşanan casusluk olayı ABD istihbarat yetkilileri tarafından yönetilen 2001 öncesi en büyük siber casusluk operasyonunu oluşturmaktadır. İlk örnek olay gibi, bir başka ikinci örnek olan siber casusluk yoluyla ABD sırlarını toplama girişimlerinden oluşmuştur. İkinci örnek casusluk olayı, hackerler tarafından hassas bilgiler içeren NASA'yı hedef almışlardır. İkinci olayda Sandia Ulusal Laboratuvarlarını ve diğer hükümet ağları ve askeri ağlar dahil olmak üzere birçok gizli bilgi toplandığı iddia edilmektedir. Bu casusluk olayında çok farklı spekülasyonlar ortaya çıkmıştır. Bu spekülasyonlar bir devlet olan Çin'i hedef alarak açıklama yapmış ve Çinli casusların bunu yaptığını iddia etmiştir (Graham, 2005). Şubat 1998'de, İsrailli bilgisayar korsanı Ehud Tenenbaum ve Kaliforniyalı iki genç, DoD ağlarına izinsiz girdi ve basında çıkan haberlere göre ise bunu zevk için yaptıklarını iddia etmişlerdir (Goodman, 2010). Edward Snowden'in ifşa ettiği ABD Milli Güvenlik Ajansının kullandığı birçok gizli teknoloji ve takip metodu bilinir hale gelmiştir. Ayrıca Haziran 2019'da Rusya Federal Güvenlik Ajansının bilgi ve

dokümanları da internete sızdırılmıştır (Bıçakcı, 2019). Bu yaşanan olaylar devletler açısından güvenlik zafiyetinin oluşmasına ve casusluk olaylarına karşı tedbir almasına sebep olmuştur. Siber casusluk için güncel bir örnek ise Ocak 2023 yılında Ukrayna'nın 89 Rus askerini sinyal operasyonu ile öldürmesidir. Bu örnekte işgal altındaki Ukrayna hükümeti yetkilileri, Rus askerlerinin sosyal medya üzerinden fotoğraflar paylaşması ve aynı askerlerin akıllı telefonları aracılığıyla sinyal verilerinin tek bir binadan geldiği bilgisine ulaşılmıştır. Bunun üzerine Ukraynalı askerler, binayı bombalamış ve bu saldırı sonucunda en az 89 Rus askeri hayatını kaybetmiştir (A. B., Darıcılı, 2023). Yaşanan saldırı sinyal operasyonu olarak değerlendirilmiştir. Bu saldırıda önemli nokta ise sosyal medya sayfaları üzerinden fotoğraflar paylaşılması ve Rus askerlerinin kendi yerlerin ifşa etmelerine ek olarak kullandıkları akıllı telefonların baz istasyonları aracılığıyla sinyal verilerinin konum olarak doğruluğunu sağlamıştır. Teknolojik olarak gelenen bu noktada siber casusluğun fiziki alandaki etkisinin büyüklüğünü göstermektedir.

Teknolojinin gelişmesi ile istihbarat ve casusluğun siber alanda önemli bir şekilde etki alanı oluşturması uluslararası ilişkilerde aktör olan devletler açısından çeşitli zorluklar oluşturmaktadır. Siber alanda varlık gösteren casusluk örnekleri, devletlere karşı siber alanda yaşanacak olan terör eylemleri için birer tehdit oluşturmaktadır. Devletler siber alanda yaşanabilecek herhangi bir siber terör olayına karşı siber istihbarat servislerini oluşturmakta ve çeşitli kurumlarında bu alanda yenilikler yapmaktadır. Kritik öneme sahip alt yapılara yönelik siber alanda bilgi toplanması ve bu alanlara yönelik saldırılar siber terör kavramını ortaya çıkarmıştır. Bu bakımdan siber terör, bilgisayar ağları kullanılarak kritik öneme sahip alt yapıları, enerji, ulaşım, iletişim ve diğer devlet hizmetlerine yönelik yapılan saldırılar olarak tanımlanmıştır (Erdem, 2020). Bu bağlamda siber terörizmin devletlere ve toplumlara yönelik zarar etkisi büyüktür. Zarar verme etkisi, sosyolojik ve psikolojik etkisi de dikkate alındığında siber terörizmin günümüz internet çağındaki etkisi terör gruplarında cazip hala gelmektedir.

Siber casusluk alanında önemli bir çalışma olan Talinn El Kitabı'dır (Güntay, 2014). Uluslararası alanda siber casusluğa yönelik hukuki bir adım atılmış olsa bile

uygulama konusundaki tartışmalar yapılan çalışmadan daha çok tartışılmaktadır. Sonuç olarak siber casusluğun yıllar içinde daha da büyük çaplı istihbarat olaylarında kullanılacağı düşünülmektedir. Bu sebeple devletler ve siber alandaki diğer aktörler alt yapılarını, sistemlerini ve verilerini casusluk olaylarına karşı koruyabilmeleri için bu alanda çeşitli yatırımlar yapmaları gerekmekte ve kurumlarını güçlendirmeleri gerekmektedir.

2.6.Siber Güvenlik

Amerika muhtemel bir sıcak çatışma durumunda ordu içerisindeki iletişimi kesintisiz sağlamak için bulduğu interneti 1990'lı yıllarda interneti sivilleştirilmesi ile küresel boyutta yeni bir bilgi sürecini başlatmıştır (Öğün & Kaya, 2013). Sivilleşmeye açık hale gelen internet devletler için hem iç politikada hem de uluslararası politikada siber güvenlik sorununu da beraberinde getirmiştir. Devletler için uluslararası alanda en etkili örneği 1991 yılında yaşanan Körfez Savaşı'nın internet üzerinden yayınlanması yeni düzenin çok farklı olacağının sinyallerini vermiştir. Böylece siber alanda devletler birer aktör haline gelmişlerdir (Bıçakcı, 2012). Siber uzay devletler için 21. yüzyılda en büyük tehdit konusu olarak karşımıza çıkmaktadır. İlk siber güvenlik sorunu olarak algılanacak olan girişim Elk Cloner tarafından 1982 yılında "bilgisayar virüsü"³ icat edilmiştir. 1988 yılında ise büyük ölçekli etki yaratan Moris kurtçuğu ortaya çıkmıştır. Bu kurtçuğun internete bağlı bilgisayarların yaklaşık olarak üçte birine zarar verdiği bilinmektedir. Bu iki gelişme siber tehdit algılanması ve siber güvenliğin oluşturulması için algılanan ilk örneklerdir. Moris kurtçuğunun bilgisayarlara zarar vermesi bu alanda kişisel bilgi güvenliği olarak algılanmıştır (Akyeşilmen, 2018). 2001 yılında ise 15 yaşında bir çocuğun Yahoo, amazon ve diğer küresel çaptaki şirketlere yönelik siber saldırı yaparak bu şirketleri milyarlarca dolar zarara uğratması ile sonuçlanmıştır (Geers, 2011). Bu olaydan sonra siber güvenlik geniş çaplı bir güvenlik sorunu halini almaya başlamıştır. Siber alan ya da siber uzay şeklinde tanımlanan bu yeni ortamın gelişmesiyle birlikte literatürde güvenlik çalışmaları altında siber güvenlik çalışmaları başlığı adı altında kendine yer bulmuştur.

³ İlk virüs hakkında daha detaylı bilgi için; Neuromancer kitabı ss. 65-70 okunabilir. Bu kitapta ilk defa siber virüsten bahsedilmektedir.

Siber güvenlik, kara, hava, deniz ve uzay güvenliğinden sonra devletler için kritik öneme sahip güvenlik alanı haline gelmiş ve beşinci boyut güvenlik alanını oluşturmaktadır (Nye, 2016-2017). Siber güvenlik sorunu siber alanın dışındaki alanları da etkileyebileceği anlaşıncı ulusal ve uluslararası güvenlik sorunu olarak algılanmıştır (Bayraktar, 2014). James Adams interneti anarşik bir sistem olarak görüyor ve siber uzayın yeni bir uluslararası savaş alanı haline geldiğini savunmaktadır (Petallides, 2012). Yeni bir savaş alanı haline gelen siber uzay aktörler açısından oldukça tehlikeli bir hal almaktadır. Bu sebeple aktörler siber uzayda güvenliklerini arttırmanın yollarını çeşitli şekillerde sağlamak istemişlerdir. Güvenli ve emniyetli bir siber uzaya duyulan ihtiyaç daha da önemli bir hale gelmiştir. Güvenliğin iç politikada başladığını bilen devletler öncelikle bilgi kontrolü ve bilgi yönetimi açısından birtakım tedbirler almışlardır (Geers, 2011). Siber güvenlik alanında tedbirler alan devletler öncelikle kendi halkına yönelik tedbirler almışlardır. Siber alanda alınan güvenlik önlemleri başta Hollywood olmak üzere sinema sektöründe de etkisini göstermiştir.

1983 War Games, 1995 Hacker Movie, 2000 Takedown, 2008 Untraceable ve 2016 Snowden adlı filmlerde siber alanın filmler üzerindeki etkilerini görmek mümkündür. Fimler aracılığıyla bu alana dair kurgusal mesajlar verilmiştir (Çalışkan, 2019). Ek olarak 1999 The Matrix filmi ise tam bir bilim kurgu filmi olma özelliği taşımaktadır. Matrix sözcüğü ilk kez 1984 yılında William Gibson tarafından Neuromancer adlı kitabında bilgisayar sisteminin karmaşıklığını anlatmak için kullanılmıştır. Bu film ayrıca siber alanı tarihsel süreç açısından bağlamaktadır.

İnternetin gelişmesi ile bilgi ve iletişim sektörleri ortaya çıkmıştır. Bu sektörler ise casuslar, hackerler ve bilgisayar korsanları artık bu alanda suç işlemeye ve çatışmaya başlamışlardır. Bu bağlamda teknolojinin ortaya çıkardığı değişim tüm dünyayı etkisi altına almış siber alanda, siber silahlarla yaşanan çatışmalar siber güvenlik kavramını doğurmuştur (Köker, 2021). Siber güvenlik algısı klasik güvenlik algısının aksine zaman ve mekân kavramında farklı şekillerde karşımıza çıkmıştır. Literatürde siber güvenlik terimi üzerinde net bir görüş birliği bulunmamakla birlikte çok boyutlu bir süreci içerdiği kabul edilmektedir (Rolf, H., Weber, 2019). Güvenlik kavramı kendi başına çok komplike bir terimdir. Güvenlik kavramı esastan tartışmalı

bir kavram olduđu gibi güvenlik terimi çok stratejik bir terim olup çok boyutlu olduđu bilinmektedir (Açıkmeşe, 2008).

Uluslararası Telekomünikasyon Birliği'nin (ITU) siber güvenlik tanımı, "korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamı" şeklindedir (Rolf, H., Weber, 2019). Birçok modern ulus devlet siber uzayda güvenliğin sağlanması için uluslararası anlaşmalar ve iş birliği yoluna gitmektedir. Siber güvenlik stratejileri ve siber güvenlik eylem planları ile bu kararlılığı vurgulamaktadırlar. Siber güvenlik kapsamında yapılan uluslararası seviyede ilk çalışma NATO Siber savunma mükemmeliyet merkezi ve uluslararası bağımsız uzmanlar grubu tarafından hazırlanan "siber savaşta uygulanacak hukuk hakkında Tallinn El Kitabı"dır. Bu el kitabı, tamamen uzman grubu görüşlerinden oluşmaktadır (Tallinn El Kitabı, 2013). Bu noktada asıl önemli sorun ise NATO'nun siber saldırılara nasıl karşılık vereceği sorunudur. NATO müttefiklerine karşı yapılacak olan bir siber saldırıda siber güvenlik açısından bunun bir savaş sebebi olarak mı yoksa sadece siber güvenlik desteği verilerek yapılan saldırıların azaltılması mı sağlanacağı konusunda net bir görüş birliği bulunmamaktadır. NATO her ne kadar siber güvenlik alanında önemli ölçüde tedbirler almış olsa da temel sorun yaşanacak olan bir siber saldırıda ortak savunma koşulu olan 5. maddenin siber saldırıyı kapsamaması sorunudur (Yayla, 2013). Estonya'ya yapılan siber saldırılarda ortak savunma koşulu işlevsiz kaldığı bilinmektedir. NATO 2008 yılında Bükreş Zirvesinde tanımlamış olduđu savaş kavramında yaşanan değişikliğe ayak uydurmak için yeni bir strateji belgesi oluşturmuştur. Bu zirvede değişime ayak uydurulması için gereken kaynağın sağlanacağını bildirmiştir. Bu zirve sonrasında ise NATO Siber Savunma Yönetimi Otoritesi ve Estonya Tallinn merkezli bir NATO Siber Savunma İş birliği Mükemmeliyet Merkezi'nin kurulmuştur (Robinson, 2017).

Bir diğer çalışma ise Avrupa Birliği özelinde gerçekleşmiştir. Avrupa siber güvenlik alanında sınır ötesi düzenlemelerin benimsenmesinde en gelişmiş bölge olarak görünmektedir. Önemli yasama araçları olarak Avrupa Konseyi Budapeşte Sözleşmesi karşımıza çıkmaktadır (Rolf, H., Weber, 2019). Avrupa Konseyi

bünyesinde siber suçlarla ilgili hazırlanan ilk resmî belge olma özelliği taşıyan Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi, 23.11.2001 tarihinde Macaristan'da imzalanarak 01.07.2004 tarihinde yürürlüğe girmiştir. 2004 yılında yürürlüğe giren Budapeşte Sözleşmesi en eski bağlayıcı ve en geniş kabul görmüş yasal düzenleme olarak kabul edilmektedir. Bu bağlamda siber uzaya yönelik küresel olarak hukuksal düzenlemeler artmaktadır (World Economic Forum, 2017). Budapeşte Sözleşmesi tüm dünyaya açıktır. Bugüne kadar, aralarında Arjantin, Avustralya, Kanada, Şili, İsrail, Japonya ve Amerika Birleşik Devletleri'nin de bulunduğu birkaç önemli AB üyesi olmayan Devlet de dahil olmak üzere 63 Devlet sözleşmeyi onaylamıştır. Eylül 2017 Avrupa Komisyonu “Siber Güvenlik Paketi” açıklamıştır. Bu pakette Avrupa Birliği düzeyince operasyonel iş birliği, kapasite geliştirme, bilgi ve enformasyon çalışmaları ve uluslararası iş birliği hedefleri doğrultusunda siber güvenliği arttırmayı amaçlamaktadır (Rolf, H., Weber, 2019).

Siber güvenlik alanında yaşanan gelişmeler özellikle 21. yüzyılın başlarında devletlerin yapmış olduğu birtakım çalışmalarda görmek mümkündür. Devletler kendi içinde kurmuş olduğu birtakım birimler, orduları içinde kurmuş olduğu yeni yapılar veya vatandaşlarını korumak için daha sivil bir halde yapmış oldukları siber güvenlik çalışmaları bulunmaktadır. Günümüzde devletler klasik anlamda savaş planları ve hazırlıklarının yerine siber güvenlik alanında da savaş, savunma, caydırıcılık ve siber güvenlik alanında birtakım çalışmalar yapmaktadırlar.

Amerika kıtasında bulunan gelişmiş bir ülke olan Kanada yüzde 97,67 skoru ile ve Amerika Birleşik Devletleri ise yüzde 100'lük skoru ile kendi kıtalarında siber güvenlik alanında ileri bir düzeye sahip olduklarını 2020 Global Siber Güvenlik indeksi ile kanıtlamışlardır. Orta Doğu bölgesinde ise yüzde 98,06'lık skoru ile Birleşik Arap Emirlikleri ve yüzde 99,54 skoru ile bölgesinde zirveyi tutan Arabistan bulunmaktadır. Asya-Pasifik bölgesinde ise Rusya, Güney Kore, Japonya, Malezya, Singapur, Çin, Hindistan, Avusturalya ve Endonezya gibi siber alanda gelişmişlik seviyesi yüksek ülkeleri ilk sıralarda yer almaktadır. Siber güvenlik ve teknoloji alanında dünyada gelişmiş ülkeler arasında bulunan ülkelerin olduğu bölge Avrupa olarak kabul edilmektedir. Avrupa bölgesinde ise 99,48'lik skor ile Estonya ve

99,54'lük skor ile İngiltere ilk sıralarda yer alırken Türkiye'de 97,50'lik skoru ile üst sıralarda yerini almayı başarmıştır (International Telecommunication Union, 2020, ss. 33-107).

Günümüzde siber güvenlik öncelikle özel düzenleyici faaliyetler ve savunma stratejileri yoluyla güvence altına alınmıştır. Bu faaliyetler bazı sınırlı uluslararası iş birliği ve düzenlemeler ile sağlanmaya çalışılmaktadır. Devletler de özel olarak yasalar çıkararak siber saldırı ve istismarı önleyici siber güvenliği sağlayıcı adımlar atmışlardır. Bu devletlerden biri olan Türkiye çeşitli suçları içeren yasa çıkardığı bilinmektedir (Sofaer, vd., 2010, ss. 182-184). Siber alanda işlenen suçlara ilişkin güvenliğin sağlanmasını hedefleyen Türkiye ilk olarak 6 Haziran 1991 tarihli 3756 Sayılı Türk Ceza Kanunu'nun bazı maddelerinin değiştirilmesi ile hukuksal olarak gerekli tedbirleri almayı amaçlamıştır. 3756 sayılı kanunun 20. maddesi ile "Bilişim Alanında Suçlar" bir ek oluşturulmuştur. Eylül 2004 yılında 5237 sayılı kanun ile siber suç kavramı ceza kanununa dahil edilmiştir. İlerleyen yıllarda ilgili kanunlar tanımları genişletilerek veya yeni eklemeler ile birlikte siber alanda güvenliğin sağlanması ve suçun önlenmesine ilişkin ve suçun caydırıcılığı açısından ceza kanunları yenilenmiştir (Bıçakcı, vd., 2015, s. 4). 2006 yılındaki Terörle Mücadele kavramının genişletilerek siber alanın dahil edilmesi ve 2008 yılında "Kişisel Verilerin Korunması Kanunu" bu alanda bilinen örnekleri oluşturmaktadır. Türkiye hem hukuksal alanda hem de teknolojik alanda yenilikler yaparak değişen teknolojik çağa ayak uydurmak için birtakım yenilikler yapmıştır. Bu yeniliklerden biri olan 2003 yılında Başbakanlık altında bilgi güvenliğinin sağlanması amacıyla Adalet, Milli Savunma, İçişleri, Dışişleri, Ulaştırma, Sanayi ve Ticaret Bakanları ile Milli Güvenlik Kurulu Genel Sekreteri, Genel Kurmay Muharebe Elektronik ve Bilgi Sistemleri Başkanı, Millî İstihbarat Teşkilâtı (MİT) Müsteşarı ve TÜBİTAK'ın oluşturacağı bir Ulusal Bilgi Güvenliği Üst Kurulu'nun kurulması öngörülmüştür. Zaman içerisinde bu üst kurul kurumlar içerisinde kritik öneme sahip alanlarda gelişim göstermiştir. Kritik öneme sahip kurumlar olarak Ocak 2000 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) kurulmuş ve Kasım 2008'de Telekomünikasyon İletişim Başkanlığı (TİB) kurumuna dönüştürülmüştür. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) birçok teknolojik araçlar geliştirerek kurumlarla olan bağıını güçlü

tutmakta ve devlet kurumlarının güvenlik ihtiyaçları doğrultusunda yazılım ve ekipman gelişimini sağlamaktadır. 2012 yılında Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile birlikte, 81 ilde gerekli tedbirleri almak için kurulmuştur. Ayrıca Türkiye’de Siber Kriz Yönetimi ve Kritik Altyapı Koruması görevi 5902 sayılı kanunla Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı’na (AFAD) verilmiştir. Estonya’da yaşanan siber güvenlik sorunu dikkate alınarak Türk Silahlı Kuvvetleri içerisinde (TSK) de Haziran 2012’de Siber Savunma Merkezi Başkanlığını kurmasına karar verilmiştir. Millî İstihbarat Teşkilâtı (MİT) ise 6532 sayılı kanun dahilinde “Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu” çerçevesinde MİT’in görev ve yetkileri tanımlanmıştır (Bıçakçı, vd., 2015, ss. 5-21). Türkiye özelinde görüldüğü üzere siber alanda aktör konumunda olan devletler yeni kanunlar çıkararak ve birtakım teknolojik gelişmelerle yazılım oluşturmuş ve danışma kurumları oluşturmuştur. Yaşanacak siber güvenlik sorunu için bazı uluslararası kuruluşlar ise bünyesinde siber güvenlik birimleri kurmuş ve uluslararası iş birlikleri yapmışlardır (Ünver, vd., 2011).

Uluslararası siber güvenlik çalışmalarına örnek olacak Birleşmiş Milletler ise birtakım kurallar dahilinde siber güvenliği sağlamaya yönelik adımlar atmıştır. Siber güvenlik faaliyetleriyle ilgili uluslararası anlaşmalar arasında anlaşmalar (BM Şartı ve Cenevre Sözleşmeleri) ve evrensel olarak kabul edilen davranış kuralları yer almaktadır. Örneğin, fiziksel güç kullanımına eşdeğer kinetik etkileri olan siber saldırılar, fiziksel güç kullanımıyla aynı ölçüde BM Şartı kapsamında "silahlı saldırılar" olarak kabul edilmesi şartı bu örnek dahilindedir (Sofaer, vd., 2010, s. 185).

Yapılan tüm düzenlemeler ve anlaşmalar düşünüldüğünde, siber saldırılar stratejik tehdit düzeyine çıkma potansiyeline sahip olduğu anlaşılmaktadır. Bu nedenle, ulusal güvenlik planlamacıları tarafından ele alınmış ve siber güvenlik, yüksek öneme sahip konulardan biri haline gelmiştir (Geers, 2011).

2.7 Siber Caydırıcılık

Bilgisayarın icadı ile bilgisayar üzerinden diğer elektronik araçlara ve ağlara bağlanarak çeşitli siber saldırılar yapılmaktadır. Özellikle 1960’lı yıllardan sonra

Soğuk Savaşın bir çıktısı olarak siber uzayda güç mücadelesine giren ABD ve Rusya Federasyonu arasında ideolojik ve teknolojik birçok alanda yaşanan güç mücadelesi caydırıcılık alanında önemli bir şekilde karşımıza çıkmaktadır (Akyeşilmen, 2018). Siber uzayın tüm iletişim ağlarını barındırması, veri tabanları ve çeşitli bilgi kaynaklarını kapsayan küresel bir sistem olması bu alanda yaşanacak olan saldırıların büyüklüğünü ve yıkıcı etkisini gösterirken bu alanda alınacak olan tedbirlerin ve caydırıcılığın önemini göstermektedir (Liaropoulos, 2013, s. 15). Soğuk Savaş sonrası süreçte güç mücadelesi alanına dönüşen siber uzay beraberinde birtakım zorlukları da barındırmaktadır. Siber uzayın çok geniş bir alanı kapsaması siber güvenliğin sağlanmasında önemli bir etken olan caydırıcılığın sağlanması için de büyük zorluklar barındırmaktadır. Siber alan hakimiyetinin karasal ve denizel alan savunmasından daha zor olmasından kaynaklanan birtakım sorunlar çerçevesinde teorisyenler siber caydırıcılık teorileri geliştirmişlerdir (Tuncer, 2021).

Siber saldırılar sadece zarar vermek değil aynı zamanda politik ve ideolojik hedefler için de çeşitli siber saldırılar yapılmaktadır (Kugler, 2009). Bu sebep doğrultusunda başta devletler ve devletler üstü kurumlar olmak üzere birçok kurum ve kuruluş, özel sektör kurumları ve birey temelli birçok alanda siber caydırıcılık stratejileri geliştirilmektedir. Literatürde birçok teorisyen siber caydırıcılık stratejileri geliştirmiştir. Christopher Haley siber caydırıcılık teorisi analizinde üç yöntem üzerinden açıklamıştır. İlk olarak maliyetleri ve sonuçları analiz etmiş, ikinci yöntem misilleme üzerine odaklanarak yaşanmış siber saldırılar dikkate alınarak bu siber saldırıları yapanların ağır cezalar almasını önermiştir. Üçüncü yöntem ise saldırının saldırı yapan tarafa dayatılmasının önemi üzerinde durmuştur (Haley, 2013).

Eric T. Jensen “Siber Caydırıcılık” adlı eserinde Christopher Haley’e karşıt görüş olarak siber caydırıcılık alanında ceza uygulamalarının uygulanamayacağını savunmaktadır. Bu görüşünü destekler nitelikte atıfta bulunduğu nokta ise siber alanın esnek olan noktalarıdır (Jensen, 2012). Siber caydırıcılık karşı tarafın yapacağı saldırı sonucunda yaşanacak olan ağır maliyetler ile karşılaşacağına inandırmak ve yapacağı muhtemel bir saldırıdan vazgeçirmeye ikna etmek şeklinde tanımlanmıştır (Iasiello, 2018). Caydırma, bir düşmanı ilk etapta saldırgan eylemi başlatmamaya ikna etmeyi

içerir (Lin, 2012). Siber caydırıcılık temel olarak klasik caydırıcılık temelleri üzerinden hareket ederek siber alanın doğasına uygun bir şekilde teoriye aktarılmıştır (Youd, 2014). Siber alanda yapılacak olan saldırılara karşı muhtemel bir ceza yaptırımını uygulanma ihtimalinin olmamasına karşın bu saldırının ağır bir maliyet sonucu olacağına ilişkin görüşü destekleyen teorisyenler bulunmaktadır. Bu görüşü savunanlardan biri olan Amerikan Genelkurmay başkanlığı eski yardımcısı James Cartwright'tır. Cartwright'a göre siber caydırıcılık yapılan saldırıların bize yapmak istedikleri ölçüde karşı tarafa bunu yapabilme yeteneği olarak tanımlamıştır (Libicki, 2009).

Literatürde siber caydırıcılık konusunda iki farklı görüşün hâkim olduğunu söylemek mümkündür. Bu görüşlerden ilki siber caydırıcılığın siber alanın kendi doğası ve zorlukları gereği yapılan teorinin pratikte işe yaramayacağını savunmuşlardır. İkinci grup teorisyen ise geliştirmiş oldukları siber caydırıcılık teorisinin, teoride olduğu gibi pratikte de işe yarayacağını savunmuşlardır (Sağıroğlu & Alkan, 2018).

Siber caydırıcılık ile hukuksal açıdan mücadele etmek için ulus devlet olan ABD kendi hukuksal yapısı içerisinde adalet bakanlığında siber tehditlere ve siber suçlara yönelik hukuksal altyapı oluşturulmuştur. Bu sebeple savunma bakanlığı içerisinde Amerika Birleşik Devletleri Siber Komutanlığı (USCYBERCOM) kurulmuştur (Youd, 2014). Bu kurulan siber komutanlık sayesinde siber tehditler ve siber suçlarla hukuksal olarak mücadele etmek isteyen ABD dünyaya örnek olmuştur. Yapılan tüm bu düzenlemelere rağmen siber alanın doğası gereği olan özellikleri düşünüldüğünde yapılan düzenleme ve caydırıcılık önlemlerinin eksik ve yetersiz kaldığını savunan teorisyenlerin varlığı bilinmektedir. Bu teorisyenlerden biri olan Will Goodman 2007 ve 2008 Estonya- Gürcistan siber saldırılarından hareketle 2010 yılında yazmış olduğu "Siber Caydırıcılık Pratikte Teoriden Daha Zor" adlı çalışmasında siber caydırıcılığın pratikte uygulanma sorunu ve zorluğuna dikkat çekmiştir (Goodman, 2010). Bir diğer teorisyen Amir Lupovici ise 2014 yılında Sonny şirketinin yaşadığı siber saldırılar sonucunda Kuzey Kore lideri ile ilgili olan filmi yayından kaldırması analizinden hareketle yapmış olduğu çalışmasında siber caydırıcılığın başarısızlığı ve zorluklarına

dikkat çekmek istemiştir (Lupovici, 2011). Bu grubu oluşturan teorisyenler siber caydırıcılığın zorlukları ve karmaşıklığının da üzerinde durulmuştur. Siber alanın karmaşıklığı ve zorlukları ise genelde siber alanın büyüklüğü ve ilişkilendirilme problemi ile açıklamışlardır. Yine ABD örneği üzerinden hareket ederek nükleer caydırıcılığı sağlayan ABD'nin aynı başarıyı siber caydırıcılık alanında sağlayamayacağını iddia etmişlerdir (Şenol, 2017). Siber caydırıcılığı sağlamak ya da en aza indirmek için hukuksal bir çerçeve oluşturulması gerektiğini savunan teorisyenler Birleşmiş Milletler Hükümet Uzmanları Grubu'nun norm ve kurallar çerçevesinde anlaşmaya varılması gerektiğini savunmuşlardır. Bu çerçevede Talinn El Kitabı ve siber uzayda sivillerin korunmasına yönelik IV. Cenevre Sözleşmesi siber saldırıları azaltmaya yönelik yapılan uygulamalardır (Bendiek & Metzger, 2015).

Özellikle 2000'li yıllar siber alanın hızla gelişim gösterdiği zamanlardır. Bu yıllarda siber caydırıcılık alanında stratejik hedefler izleyen NATO ve Avrupa Birliği gibi devlet üstü kurumlar bazı hamleler yapmışlardır. Bu amaç doğrultusunda NATO Portekiz ve Oberammergau'da siber akademi okulları kurmuş ve müttefiklerine eğitim vermiştir (NATO, Dergisi, 2016). Akademide temel amaç siber güvenliğin sağlanması ve caydırıcılık eksenli savunma oluşturmaktır. Bu doğrultuda Türkiye'de 2017 yılında Türk Silahlı Kuvvetleri içerisinde Siber Savunma Harekât Merkezi Komutanlığı kurulmuştur (Savunma Sanayi Bakanlığı, 2017). NATO siber caydırıcılık konusuna çağın gereklilikleri doğrultusunda gereken önemi vermektedir. Güncel olarak 2023 yılında NATO Siber Savunma Mükemmeliyet Merkezi (Estonya/Talin) koordinatörlüğünde 17-21 Nisan tarihleri arasında Kilitli Kalkan-2023 (Locked Shields-2023) Tatbikatı yapmıştır. Söz konusu tatbikata otuz sekiz ülkenin katıldığı bilinmektedir (T. C. Millî Savunma Bakanlığı, 2023). Dünyanın en büyük canlı siber tatbikatı olması açısından önem arz etmektedir. Tatbikatta temel amaç siber varlık ve kritik altyapılara karşı gerçekleştirilebilecek farklı siber saldırı senaryolarının test edilmesi ve siber alandaki yeteneklerin arttırılması olmuştur.

Her geçen gün gelişim gösteren siber alan önemini de arttırmaktadır. Siber caydırıcılığın sağlanabilmesi ve geliştirilmesi için siber güç unsurlarının inşasını ve eğitiminin sağlanması, kritik öneme sahip altyapıların güçlendirilmesi, muhtemel siber

saldırıları için caydırıcılığın attırılması ve önlemler alınması gerekir (Harding, 2016, s. 15). Bu önlemler zamanında alınabilirse siber caydırıcılık stratejisi uygulanabilmekte ve yapılacak olan siber saldırıları önlenebilmektedir. Ancak realite de günümüze kadar yapılan siber saldırılardan hareketle siber saldırıları durdurmak neredeyse imkansızdır. Buna karşın yüksek teknolojiye sahip devletler veya kurumlar yapılacak siber saldırılar sonucunda yaşanan zararlar kısmen minimize edilebilmekte ya da potansiyel zararların etkisini azaltmaktadır. (Tuncer, 2021). Siber alanın doğası gereği bulunan birtakım zorluklar çerçevesinde ABD'nin Soğuk Savaş dönemindeki nükleer caydırıcılık başarısından hareket eden Libicki, ABD'nin aynı başarıyı siber alanda sağlayamayacağını düşünmektedir (Libicki, 2009). Bu düşünceyi destekler nitelikte yapılan siber saldırı sonucunda 2011 yılında ABD Savunma Bakanlığı raporlarından sızan bilgilere göre “siber saldırıların savaş sebebi sayılacağı ve askeri operasyonlarla karşılık verilebileceğinin açıklanması” ile savunulmaktadır (Nacita & Reith, 2018). Literatürde bir diğer görüş ise henüz çok büyük bir siber savaşın yaşanmadığı ve bu savaşta da en gelişmiş siber savaş araçları kullanılmadığından dolayı siber caydırıcılığın sonucunun önceden tahmin edilmesinin zor olduğunu savunmuşlardır (Sağıroğlu & Alkan, 2018).

Literatürdeki görüş farklılıkları siber alanın önemini göstermektedir. Yapılan iş birlikleri ve hukuksal düzenlemeler ise siber caydırıcılığın önemini ve hassasiyetine dikkat çekmektedir. İnsan hayatı ile iç içe geçen siber alan her konuda olduğu gibi insan hayatını etkilemekte ve zararlarından korunması için çeşitli stratejiler geliştirmeye zorlamaktadır.

ÜÇÜNCÜ BÖLÜM

RELİST TEORİ AÇISINDAN SİBER POLİTİKA

3.1 Siber Uluslararası Sistem

Westphalia sistemi ile devletler zaman içerisinde uluslararası aktörler olarak kendi egemenliklerini oluşturduktan sonra karşılıklı olarak müdahaleleri genellikle askeri güç kapasitesine dayanan bir şekilde gerçekleşmiştir. Günümüzde bu klasik anlamda uygulanan savaş, çatışma veya caydırıcılık eksenli askeri güç unsuru siber alanla birlikte dönüşüm yaşamış ve siber silahların kullanımı ile baş döndüren bir etki aracı haline gelmiştir (Aktaş & Güntay, 2016).

Soğuk Savaş'ın sonu ve küreselleşme ile dünya siyasetinde yeni bir dönüşüm ortaya çıkmıştır. Modern dünyada iletişimin en önemli özelliği artarak devam ediyor olmasıdır. Bu artış küresel boyutta olup iletişimin gelişmesi ile dünyanın modern bir köy haline geldiği söylenebilir. İletişim ağlarındaki yaygınlık ile birlikte bireyler çok uzak mesafelerden anlık olarak haberdar olabilmekte, sosyal medya ya da canlı yayınlar sayesinde yer ve zaman arasındaki bağlantı ortadan kalkmaktadır (Thompson, 2014). Bu sayede insanlar birbirleri ile nerede olursalar olsunlar etkileşime geçebilmekte veya etkileşim içinde hareket etme imkânı bulabilmektedir. İletişimin bu denli gelişmesi ve sosyal medyanın ivme kazanması uluslararası sistemde birey ve devlet açısından çeşitli imkanlar sunmaktadır.

Yirminci yüzyılın sonlarına doğru iletişimin küreselleşmesi ve iletişimde yaşanan kablolu haberleşme, elektronik kodlama ile iletişim ve bilgiyi işleme ve depolama özelliği uluslararası sistemde geniş yankı uyandırmıştır (Thompson, 2014). Yirminci yüzyıl sonları ve yirmi birinci yüzyıl başlarında depolanan bilgi ve bilginin işlenmesi ile elektronik alanda ortaya çıkan yeniliklerin siber alana dönüşmesi ile sonuçlanmıştır. Uluslararası sistemde yaşanan bu değişim ve gelişimler devletler arasındaki ilişkilere de yansımıştır. Uluslararası ilişkiler disiplininde yer edinen siber politika güncelliğini korumakta ve gelişimine devam etmektedir.

Küreselleşme, kavramsal olarak dikkate alındığında farklı ülkelerde yaşayan insanlar arasında etkileşim ve karşılıklı bağımlılığın artışı ifade etmektedir (Scholte, 2014). Günümüzde küreselleşmenin siber alanla birlikte daha da hızlandığını söylemek mümkündür. Uluslararası ilişkiler mesafeler arasında bir çalışma iken, küreselleşme ise sınırların ortadan kalkması ile sınır-ötesi alanlara erişme yetkinliğidir (Scholte, 2014). Bu fırsatı geliştiren siber alan sınırları kaldırarak devasa bir kapasite oluşturmaktadır.

Siber alanın etkisiyle birlikte uluslararası sistemin transformasyon değişim yaşadığı bir zaman diliminde küresel uluslararası sistem de büyük değişimler yaşamıştır. Siber alanın gelişmesi ve içerisinde birçok farklı kavramların oluşması devlet ve sistem açısından önemlidir. Siber alanın yirminci yüzyılın sonlarından, içinde bulunduğumuz zamana kadar gelişme ve büyüme göstermesi açısından oldukça önemli olmakla birlikte geleneksel anlamda uluslararası ilişkiler sistemini yeniden tasarlaması bakımından da önem arz etmektedir. Özellikle siber alanda yapılan saldırılarla birlikte Rusya'nın yeni bir referans noktası olarak ortaya çıkmasını sağlamıştır. Rusya'nın Estonya, Gürcistan ve Ukrayna' da yapmış olduğu siber saldırılar referans olmasının temel özelliğini destekler niteliktedir. Uluslararası sisteme hükümetler açısından bakılacak olursa gelecekte devletler arası gerilimlerden önce siber saldırıların yaşanabileceği düşünülmektedir (Steiger, 2022). Yine bu düşüncenin oluşmasında Rusya'nın izlemiş olduğu politikalar örnek oluşturmaktadır. Yirmi birinci yüzyılda teknolojik olarak oldukça gelişmiş olmasına rağmen devletler halen uluslararası sistemde temel analiz birimi olarak varlıklarını korumaktadır (Darıcı, 2017). Ancak Siber politikalar ile birlikte Uluslararası İlişkiler Disiplini yeni bir etkileşim alanı haline gelmiştir. En belirgin özelliği ise küreselleşme ve siber politikalar ile birlikte devlet dışı aktörlerin varlığıyla birlikte, bu aktörlerin siber güç unsurlarını kullanarak çeşitli tehdit unsurları oluşturmaları sonucunda klasik anlamda uluslararası ilişkiler disiplinini etkilemiş ve değişime zorlamıştır (Erdem, 2020).

Klasik anlamda Uluslararası İlişkiler disiplinini değişime zorlayan siber politikalar Nazlı Choucri ve Robert Reardon 2012 yılında yapmış oldukları literatür taramasında siber uzay çalışmalarının henüz istenilen seviyede bir çalışma alanına ve

yetkinliğine sahip olmadığını savunmuşlardır (Reardon & Choucri, 2012). Günümüzde popüler bir çalışma alanı haline gelen siber uzay klasik olarak değerlendirilen güvenlik algısının ötesine geçememiştir. Uluslararası sistem siber alanın etkisi ile birlikte savaş ve teknoloji kavramları arasında değişen bir algı oluşturmuştur. Günümüz teknolojisi kullanılarak türetilen savaş silahları uluslararası sistemi derinden etkilemiş ve algısal olarak değişime zorlamıştır (Köker, 2021).

Siber uzayın yaygınlık kazanması uluslararası sistemde yaşanan değişimlerin bir çıktısıdır. Siber alanda yapılacak olan bir saldırının klasik anlamdaki saldırıya kıyasla daha ucuz ve erişilebilirliğinin kolay olması bu değişimin yaşanmasında etkili olan faktörlerden bazılarıdır (Nye, 2011).

Siber uzayın etki alanı her geçen gün artmaktadır. Dijitalleşen dünyada siber alanın büyümesine teknolojik aletler hizmet etmektedir. Ekonomi, askeri, sağlık ve birçok alanda teknolojik aletler insan yaşamıyla iç içe geçmiş durumdadır. Çeyrek asır önce literatürde siber alanın sanal ortamda bir canlıya nasıl zarar vereceği, nasıl bir kan akıtacağı tartışılırken günümüzde bu tartışma yerini giyilebilir araçların insan sağlığı ve kişisel verileri konusundaki tartışmalara evrilmiştir. Yaşanan acı tecrübeler siber alanın gerçek hayata etki ettiği siber savaş araçlarının ortaya çıkardığı tahribatın bir sonucudur. İnsan hayatıyla kusursuz bir etkileşim sağlayan siber alan teknolojik cihazların etkisiyle dijital alanda etkileşimi arttırmaktadır. Bu gelişmeler dikkate alındığında siber güvenlik ve siber alanın etkisinin büyüklüğünün artarak devam edeceği düşünülmektedir (Bıçakcı, 2019). 2022 sonu itibarıyla Apple 90 milyar Amerikan doları (Apple Inc, 2023). Microsoft 52 milyar dolar (Bloomberg HT, 2023). Google ise 76 milyardan (Investing, 2023). Fazla büyüklükte ticaret hacimleri bulunmaktadır. Bu şirketlerin toplam ticaret hacmi büyüklüğü dünyada bulunan birçok devletin ticaret hacminden daha büyük olduğu bilinmektedir. Bu veriler dikkate alındığında teknoloji-insan ilişkisi daha kolay anlaşılabilir.

Teknolojik gelişmelerin bir diğer önemli çıktısı ise diplomasi faaliyetlerinde kendini göstermesidir. Uluslararası ilişkilerin yapı taşlarından olan diplomasi kültürü de dijitalleşme yaşamış ve bu kapsamda dijital diplomasi (Diplomasi 2.0) konsepti ile karşımıza çıkmaktadır (Karabulut, 2021).

Siber alanda meydana gelen deęişim ve dönüşümler uluslararası ilişkileri ve sistemin yapısını doğrudan etkilemekte ve uluslararası sistem daha fazla anarşik hale gelmektedir. Bu anarşik sistem yapısı ise devletlerin egemenlik başta olmak üzere güvenlik, ekonomik ve diplomatik her alanda dönüşüme zorlamaktadır (Darıcılı, 2017). Teknolojik gelişme ile birlikte sosyal medya araçlarının yeni bir etkileşim aracı olarak kullanıldığı bilinmektedir (Baştan & Karagül, 2021). Bunun en güncel örneęi ise dünya tarihinde ilk defa sosyal medya araçları üzerinden e miting yapılması olmuştur. Rusya’da dünyanın ilk dijital siyasi mitingi gerçekleştirilmiştir.⁴ Siber alanın etki alanı haline gelmesine verilecek bir başka örnek ise 17 Aralık 2010 tarihinde Tunus’ta başlayan gösterilerin sosyal medya araçları kullanılarak ülke içinde ve ülke dışındaki diğer alanlarda etki göstermesi ile sonuçlanması olmuştur (Baştan & Karagül, 2021).

Günümüzde siber alanın etkisinin özellikle covid-19 etkisi ile daha da arttığını söylemek mümkündür. Bu doğrultuda Silikon Vadisine elçilik açan Danimarka gerekçe olarak toplumsal deęişimlerin teknoloji ile gerçekleştiğini vurgulamıştır. Bir başka deyişle siber alan gün geçtikçe etkisini arttırmakta ve derinlik kazanmaktadır. Siber alanın bu denli etki alanı oluşturmaları ve beraberinde getirdiğı birçok yenilik aynı zamanda birer risk faktörü olarak karşımıza çıkmaktadır. Yapan zekanın öncü isimlerinden olan bilim insanı Geoffrey Hinton yapay zekanın insanlardan daha akıllı olabileceğini hatırlattı ve insanlığı bekleyen tehlikelere değinmiştir (BBC News, 2023). Bu örneklerden hareketle Daniel W Drezner’in, 2019 yılında yapmış olduğı Teknolojik deęişmelerin Uluslararası İlişkileri etkisi çalışmasında; Teknolojinin, uluslararası sistemde normların yayılması üzerinde doğrudan bir etkiye sahip olduğı varsayılmıştır. Bu çıkarımdan hareketle siber saldırıların ekonomik büyüme ve ulusal güvenlik için büyük bir tehdit oluşturma potansiyeline sahip olduğunu savunmuştur (Drezner, 2019). Yaşanan teknolojik gelişmeler dikkate alındığı zaman siber uzayın insan yaşamına kolaylık sağlamanın yanı sıra kötü niyetli saldırılara açık olduğı bilinmektedir. Bu güvenlik zafiyeti sebebiyle güvenlik ve savunma harcamalarında yaşanacak olan artış kaçınılmaz olacaktır (Yalman, 2018, ss. 270-271).

⁴ Daha fazla Bilgi için Bakınız; <https://www.zaks.ru/new/archive/view/238723>

3.2 Siber Alan ile Birlikte Değişen Uluslararası Güvenlik

Uluslararası güvenlik, devletler ve sistem açısından oldukça önemlidir. Literatürde İkinci Dünya Savaşı, Soğuk Savaş dönemi ve öncesine kadar devletlerin güvenlik algısı realist teori temelinde olan askeri güç odaklı bir algı baskındır (Köker, 2021). Realist perspektifte on yedinci yüzyılda Hobbes'in adına anarşi dediği ve böylece uluslararası sistemin güvenliğinin sağlanacağını düşündüğü toprağı koruyabilme becerisi, günümüz modern devlet sisteminde siber alanın güvenliğinin sağlanması olarak açıklanabilmektedir (Keohane, 2014).

Güvenlik kavramı 1940-1980 arası dönemde genellikle stratejik çalışmalar altında değerlendirilmiştir. 1980-1990 arası süreçte ise askeri tehditlerin ötesinde çevre, ekonomi, insani güvenlik ve siyasi güvenlik başlıkları dahilinde ele alınmıştır (Açıkmeşe, 2008). 1990 sonrası süreçte ise güvenlik kavramına ön bir ek olarak uluslararası sistemde yer edinen “siber” zaman içerisinde derinlik kazanmış ve gelişmeye devam etmektedir. Günümüzde ise siber güvenlik olarak farklı bir çalışma alanı haline gelmiştir.

Siber politikaların nevi şahsına münhasır özellikleri sonucunda ortaya çıkan değişimler uluslararası ilişkiler alanında özellikle güvenlik konsepti çerçevesinde ele alınmıştır. Güvenlik kavramı çerçevesinde değişen algılar sonucunda yaşanan değişiklik sistemi etkilemiştir. Uluslararası güvenlik algısı günümüze kadar anarşi, düzen ve sistem üzerinden analiz edilmiş ve çeşitli teorilerle açıklanmaya çalışılmıştır. Bilgi çağının etkisi ile bu kavramlar derinlik kazanmış ve analize yeni kavramlar dahil edilmiştir (Kello, 2013). Klasik anlamda güvenlik anarşi, düzen ve sistem gibi bağımlı değişkenler üzerinden analiz edilmişlerdir. Siber politikaların sisteme dahil edilmesiyle birlikte bağımsız değişken kavramlar analize dahil edilmiştir.

Uluslararası terörizmin önlenmesi 2000'lerden itibaren biçimlendirici bir şekilde gelişim göstermiştir. Stuxnet saldırısından sonra, gelişmiş olan devletler, siber saldırı tehlikesine dikkat çekmişlerdir (Steiger, 2022). İçinde bulunduğumuz yüzyılda değişen parametreler doğrultusunda ortaya çıkan güvenlik algısı uluslararası ilişkilerin temelini oluşturmaktadır. Devletler güvenliğe dayalı bir sistem içerisinde egemenliğe

ve güce dayalı politikalar izlemektedirler. Yaşanan gelişmeler neticesinde siber güvenlik hızla teknik bir disiplinden stratejik bir konsepte dönüşmüştür. Küreselleşme ve internetin etkileşimiyle beraber gelişen ağ teknolojisi bireylere, kurumlara ve devletlere benzersiz bir güç vermiştir (Geers, 2011). Bu bağlamda günümüzde ulusal güvenlik, uluslararası ilişkilerin temelini oluşturmaktadır. Burada dikkat edilmesi gereken önemli bir diğer husus ise siber uzayın kendisinin gerçek güvenliği ile ilgilidir (Choucric & Clark, 2019).

Uluslararası alanda güvenlik algısı 21. yy'da yaşanan siber saldırılarla birlikte tehditlerin yeni boyutlar kazanarak devam ettiği bir yüzyıl olmuştur (Barlas, 2020). Ulusal güvenliğin boyut deęiştirdiđi yirmi birinci yüzyılda siber uzay ile birlikte güvenlik konsepti de anlam derinleşmesi yaşamıştır. Klasik anlamda ulusal güvenlik o devletin sınırları ve kurumları olarak tanımlanırken bu algı siber uzayın getirdiđi birtakım yeniliklerle birlikte devletin kurumları, sınırları, elektrik ve internete bađlı kritik alt yapıları da güvenlik konseptinin içine dahil edilmiştir (Geers, 2011). Alman federal hükümeti, 2007'de ilk siber saldırı kapasiteleri oluşturulduktan sonra bile siber uzayda bir kısıtlama kültürü olması gerektiđini savunan bir açıklama yapmıştır (Steiger, 2022). İngiliz Hükümeti'nin, 2013 yılında Belgacom'a (Belçika Telekomünikasyon Şirketine) düzenlediđi saldırıyla, müttefiklerine karşı bile siber yeteneklerini kullanmaktan çekinmediđini göstermiştir (Der Spiegel, t.y.). Böylece uluslararası güvenlik için öncü bir adım atılması gerektiđini göstermiştir.

Siber alanın uluslararası ilişkilere en büyük etkisinden biri de var olan temel aktörlere ek yeni aktörlerin ortaya çıkması ve bu sebeple uluslararası sistemde yaşanan deęişim ve istikrar sorunu olmuştur. Siber alanda devlet dışı aktörlerin varlığı ve terörist eylemlerde bulunan başta Irak Şam İslam Devleti (İŞİD), Tamil Elam Kurtuluş Kaplanları ve El Kaide⁵ gibi grupların siber uzayın getirdiđi yenilikleri terörist amaçlarla kullanması ulusal ve uluslararası güvenliđi tehlike altına almaktadır. Siber alanda yaşanan gelişmeler düşük maliyetli savaş stratejilerinin ortaya çıkmasına zemin

⁵ İŞİD, EL Kaide ve Tamil Kaplanları hakkında daha fazla bilgi için sosyal medya ve internet adreslerine bakabilirsiniz. Bu terör örgütleri militan kazanımı ve kendi eylemlerini haklı göstermek için birçok yayın yapmaktadır. <https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/>

hazırlamıştır. Klasik anlamda milyon dolarlık füze ve silahların yerini siber alandaki saldırıların alması açısından önem arz etmektedir.

Yurt içi ve yurt dışındaki hedeflere yönelik örtülü operasyonlar sadece askeri siber güçler tarafından değil, istihbarat servisleri tarafından da gerçekleştirildiği bilinmektedir. Ağustos 2022 İngiltere Başbakanlık seçimlerinin olası bir siber saldırı sebebiyle ertelendiği bilinmektedir (Savunma TR Haber, 2022).

2016 yılında AB şirketlerinin %80'inin en az bir siber güvenlik olayı kaydedildiği bilinmektedir. Bu oranın günümüzde arttığı tahmin edilmektedir. Yaşanan bu saldırılar ise uluslararası güvenliğin değişen boyutunu gözler önüne sermektedir. Siber suçların neden olduğu ekonomik hasar 2013 ile 2017 yılları arasında beş kat arttığı bilinmektedir. Siber sigorta primlerinin 2018'de 3 milyar Euro'dan 2020'de 8,9 milyar Euro'ya çıkması bu gelişmenin bir ifadesidir (Avrupa Sayıştay Kurumu, 2019, s. 10).

Klasik anlamda güvenliği sağlamak isteyen devletler uluslararası ilişkilerde anarşi ortamında egemen olma arzusu ve kazanma dürtüsüyle hareket etmektedir. Uluslararası güvenlik alanında yaşanan zafiyet tam olarak bu nedenle ortaya çıkmaktadır. Anarşi ortamında güvenlik, güç ve çıkar için hareket eden devletler savaşların çıkmasının en büyük sebebini oluşturmaktadır. Bir başka ifadeyle anarşi ortamı savaşlara zemin hazırlamaktadır (Açıkmeşe, 2008). Uluslararası ilişkilerde var olan anarşi durumu siber alan için de geçerliliğini korumaktadır. Siber alanda ek olarak devlet dışı varlıkların da bulunması siber alandaki ilişkileri düzenleyen bir üst otorite bulunmadığından siber güvenlik ciddi bir tehlike olarak karşımıza çıkmaktadır.

Devletler başta egemenliklerini sağlamak için siber alanda güvenlik odaklı denetleme ve düzenlemek istemektedirler. Bu da realist teoride devlet olmanın bir çıktısı olarak siber alana uyarlanması oluşturmaktadır. Buna karşın siber alanda devlet dışı varlıkların egemen olduğu ve siber alanda tam anlamıyla düzenleyici ve denetleyici kurum-kuruluşun egemen olmadığı gerçeği ise devletler için olumsuz bir durum oluştururken, devlet dışı aktörler için olumlu bir çıktıdır.

Siber alanın getirdiği yenilikler sonucunda karasal sınırların ortadan kalktığı ve gücü klasik anlamda askeri güç kapasitesi değil donanım, yazılım ve inovasyonun belirlemesi olmuştur (Geers, 2011). Siber uzayın uluslararası ilişkileri etki sahası içine almasıyla beraber başta NATO ve BM gibi ulus üstü kurumlar siber güvenlik için çeşitli çalışmalar yapmışlardır (Çelik, 2018). Siber alanın göstermiş olduğu gelişim karşısında harekete geçen devletler ve devlet üstü kurumlar (AB, NATO, Amerika, Çin, Rusya ve İngiltere) siber savunma için ayırdıkları bütçeler ve siber güvenlik stratejileri kapsamında uluslararası sistemin dönüştüğünün görülmesi mümkündür (Kurtul, vd., 2019). Bir başka deyişle siber alanın uluslararası ilişkileri etkilemesiyle birlikte klasik anlamda savunma harcamaları yapan devletler ek olarak siber güvenlik harcamaları da yapmışlardır.

AB'nin siber ekosistemi, adalet ve içişleri, dijital tek pazar ve araştırma gibi bir dizi iç politikayı etkileyen karmaşık ve çok yönlüdür. Dış ilişkilerde siber güvenlik, diplomasi ve AB'nin gelişmekte olan savunma politikasının giderek artan bir parçası haline gelmiştir (Avrupa Sayıştay Kurumu, 2019, s. 13). Choucri ve Clark'ın daha iyi bir siber güvenliğin maliyetinin olduğunu savunmasının bir çıktısı olarak devletlerin harcamalarında görmek mümkündür (Choucri & Clark, 2019).

Siber alanda yaşanan bilimsel gerçeklikleri ve teorik çalışmaları açıklamak için yapılan çalışmalardan birini de Joseph Nye yapmıştır. Nye 'ın "siber güç" temelli çalışması bilgi devrimi alanında yaşanan gelişmeleri açıklamak için yaptığı teorik temel çalışmalardan biridir. Nye'e göre siber alanda oluşacak topluluklar bölgesel yargı sınırlarını aşarak kendilerine has bir şekilde ortaya çıkacaklardır. Bu oluşan grupların bölgesel sınırlamaları aşması ise siber alanın ulusal hatta uluslararası güvenliği tehlikeye atacağını düşündürmektedir (Nye, 2011).

Siber uzayın etkisi ile devletler uluslararası alanda egemenliklerini sürdürecektir fakat yeni aktörlerin varlıkları da artarak devam etmesi düşünülmektedir. Bu sebeple devletler sistemi kontrol etmesi zorlaşacak ve güvenliklerini kısıtlayıcı faktörlerle karşılaşabilmektedirler (Nye, 2011). Siber uzayda devletlere karşı kullanılan siber saldırılar uluslararası ilişkilerde küresel sistemi ve devletler arası politikaları derinden etkilemiştir (Çelik, 2018).

3.3 Siber Alan ve Realist Teorideki Tanımlar

Realist teori, uluslararası ilişkilerde güç, güvenlik ve ulusal çıkarların uluslararası sistemdeki devletlerin davranışlarını şekillendirmedeki önemini vurgulayan bir bakış açısıdır. Realist yaklaşım, devletlerin uluslararası ilişkilerde birincil aktörler olduğu ve davranışlarının kendi güvenliklerini en üst düzeye çıkarma ve kendi çıkarlarını geliştirme arzusu tarafından yönlendirildiği fikrine dayanmaktadır.

Realist teori ayrıca uluslararası sistemin doğası gereği anarşik olduğunu ve kuralları uygulayacak veya çatışmayı önleyecek daha yüksek bir otoriteye sahip olmadığını ileri sürmektedir. Siber arenada bu, devlet davranışını yöneten yolun net kurallarının olmadığı ve devletlerin siber yetenekleri, normları ihlal etmek veya saldırgan davranışlarda bulunmak anlamına gelse bile çıkarlarını ilerleteceğine inandıkları şekillerde kullanacakları anlamına gelmektedir. Genel olarak gerçekçi teori, siber arenanın uluslararası ilişkilerde devletlerin avantaj ve güvenlik için rekabet etme olasılığının yüksek olduğu önemli bir savaş alanı olduğunu ileri sürmektedir. Siber arenada devlet davranışını şekillendirmede güç ve güvenliğin rolünü anlamak, siber tehditleri yönetmek ve uluslararası sistemde istikrarı desteklemek isteyen politika yapıcılar için çok önemlidir.

Realist teori, uluslararası ilişkilerde uluslar arasındaki ilişkilerde güç ve güvenliğin rolünü vurgulayan bir düşünce okuludur. Gerçekçilik, ulusların öncelikle kendi çıkarları tarafından motive edildiğini ve kendi güvenliklerini ve güçlerini geliştirecek şekillerde hareket edeceklerini öne sürmektedir. Realistler dünyayı, ulusların çıkarlarını korumak için güç kullanmaya hazır olmaları gereken, rekabetçi ve tehlikeli bir yer olarak görmektedir. Realist teori devletlerin siber yeteneklerini kendi çıkarlarını ilerletmek ve rakiplerine karşı avantaj elde etmek için kullanacaklarını öne sürüyor. Siber yetenekler, casusluk yapmak, fikri mülkiyeti çalmak, kritik altyapıyı bozmak ve bir devletin gücünü ve güvenliğini artırabilecek diğer gizli faaliyet biçimlerini gerçekleştirmek için kullanılabilir. Gerçekçi teori, siber arenaya gelince, ulusların siber operasyonları çıkarlarını sürdürmek ve güvenliklerini artırmak için kullanacaklarını öne sürmektedir. Siber

operasyonlar istihbarat toplamak, diğer ulusların operasyonlarını bozmak ve hatta kritik altyapıya saldırılar başlatmak için kullanılabilir. Realistler bu eylemlerin ulusal güvenliği sağlamak ve uluslararası sistemde gücü sürdürmek için mevcut tüm araçları kullanma şeklindeki daha geniş bir stratejinin parçası olduğunu iddia etmektedir.

Realist paradigmada güç kavramı teorinin temelinde yer almaktadır. Bu teoriye göre devletlerin kendi güvenliklerini sağlayabilmeleri için güçlerini maksimum seviyede tutmaları gerekmektedir. Güç kavramı realist teoride sahip olunması gereken doğal kaynaklar adı altında tanımlanmıştır.

Realist görüşe göre insan doğası kötüdür ve bu amaçla insan güç peşinde koşmaktadır. Sürekli güç için uğraşan insanların kötü davranışlarda bulunabildiğini kabul gören görüşün siber alan için de geçerli olduğunu söylemek mümkündür. Siber alanda daha çok ekonomik ve bilgi elde etme temelli siber saldırı yapan korsanlar bu kategori altında değerlendirilmektedir. Bu kategoride değerlendirilen siber korsanlar için realist teoride insan doğası algısının geçerli olduğunu söylemek yanlış olmayacaktır (Barlas, 2020).

Siber uzayla birlikte uluslararası sistemde var olan anarşik durumun devam ettiği algısıdır. Günümüzde siber alanda denetleyici ve düzenleyici bir üst otorite olmadığından siber ortamın anarşik bir yapıda olduğu görüşü realist bakış açısıyla örtüşmektedir.

Siber uzay kısa bir süre öncesi sürece kadar low politics olarak görülmekte iken günümüzde siber saldırılar sonrası süreçte Anonymous, Wikileaks ve Panama Belgeleri gibi hassas bilgilerin sızdırılması sonucunda yaşanan kriz ortamı sonucunda, siber uzayın yüksek öneme sahip konular arasında yer almasıyla sonuçlanmıştır (Güntay, 2014). Bir başka deyişle devletlerin bilişim alanında güvenlik sorunlarıyla karşılaşması siber uzayın ulusal ve uluslararası alanda önemli bir faktör haline gelmesi ile neticelenmiştir. Ek olarak küreselleşme olgusunun beraberinde getirdiği siber uzay çeşitli güvenlik zafiyetlerine de sebep olmaktadır. Artan bu güvenlik zafiyetleri devletler açısından ciddi sonuçlar çıkarmaktadır. Egemenliklerinin zedelenmesini

istemeyen devletler artık siber alandaki çalışmalara ağırlık vermiş ve siber alanı da önem düzeyi yüksek konular arasına almışlardır.

3.4 Siber Alanda Uluslararası Güvenliğin Kısıtlılıkları

Günümüzde uluslararası güvenlik politikaları bilgi devrinin zorlukları ile karşı karşıyadır. Bunlardan en önemlisi siber alanda kullanılan siber silahların uluslararası teoriler ışığında doğru değerlendirilememesidir.

Bilgi çağının getirdiği yenilikler politika yapıcılarının ve teorisyenlerin güvenlik hakkındaki düşüncelerinde yenilik veya değişiklik gerektiriyor mu? Teorisyenler ve karar alıcılar bu soruyu ele alırken çeşitli zorluklarla karşılaşmaktadırlar. Siber alan bu konuda zorluklar ile karşılaşmamıza neden olmaktadır. Siber alanın doğası gereği oluşan birtakım kısıtlılıklar oluşan zorlukların çıktısıdır (Kello, 2013).

Realist teori siber alanda uluslararası iş birliğinin zor olduğunu savunmaktadır. Bu düşünce ise iki temel faktör üzerinden analizine dahil edilmektedir. İlk olarak devletlerin hileli politikalar ve güvenme sorunundan kaynaklandığını savunmaktadır. Bir diğer temel faktör ise devletlerin göreceli kazanca yönelik olan algılarıdır. Bunun bir çıktısı olarak günümüzde de siber alanda bir ortak görüşün ve hukuksal zeminin olmayışı olarak açıklamaktadır (Köker, 2021).

Diğer güvenlik alanlarında olduğu gibi uluslararası güvenliğin de özellikle siber arena söz konusu olduğunda, sınırlamaları vardır. Siber alan açısından uluslararası güvenliğin sınırlamalarından bazıları şunlardır;

- Küresel fikir birliği eksikliği: Siber alanda neyin kabul edilebilir davranış oluşturduğu konusunda küresel bir fikir birliği eksikliği vardır. Bazı ülkeler açık, özgür ve güvenli bir siber alanı savunurken diğerleri serbest bilgi akışı yerine ulusal güvenlik ve egemenliğe öncelik vermektedir. Bu fikir birliği eksikliği, siber alanda davranış için uluslararası normlar ve kurallar geliştirmeyi zorlaştırmaktadır.

- İlişkilendirmede olan zorluk: Siber saldırıları belirli bir ulusa veya aktöre atfetmek zor hatta imkânsız olmaktadır. Özellikle bazı tekniklerin kullanılarak yapılan bir saldırının gerçek kaynağını gizlemek mümkündür. Bu, etken aktörün siber alandaki

eylemlerinden sorumlu tutmayı zorlaştırmaktadır. Bir başka deyişle siber alanda yapılan eylemlerin kimin ya da kimler tarafından (gerçekte) bilinmesinin zorluğu uluslararası güvenliğin kısıtlılıklarını oluşturmaktadır (Egan, 2017).

- Siber uzayda caydırıcılık ve cezalandırma olanağının çok ciddi maliyetler gerektirdiği bilinmektedir. Yapılan bir siber saldırıya anında karşılık vermek ya da cezalandırmak pek mümkün olmamakla birlikte geçerli net bir imkânın olmaması siber alanın doğası sonucunda ortaya çıkan kısıtlılıktır. (Brantly, 2018).

- Uluslararası İlişkileri oluşturan ve etkileşimi sağlayan ana aktör olan devletler siber alanı net olarak kontrol edemiyor olması da uluslararası güvenliğin kısıtlılıkları arasında yer almaktadır (Vaishnav, vd., 2013).

- Hızla gelişen teknoloji: Teknoloji sürekli gelişmekte ve bu da siber alandaki potansiyel tehditlerin bir adım önünde olmayı zorlaştırmaktadır. Yeni teknolojiler geliştirildikçe yeni güvenlik açıkları ve saldırı vektörleri de keşfedilmektedir. Bu, uluslararası güvenlik çabalarının değişen teknolojiye ayak uydurmadaki zorluğunun bir çıktısıdır. Ayrıca teknolojinin sürekli olarak gelişti düşünülüğünde aktörler, siber alanda savunma yerine saldırı kapasitesinin artırılması yönünde hedefler izlemektedirler.

- Sınırlı kaynaklar: Uluslararası güvenlik çabaları genellikle finansman, personel ve teknolojik ekipman gibi sınırlı kaynaklar tarafından kısıtlanmaktadır. Bu, küresel ölçekte etkili siber güvenlik önlemlerinin geliştirilmesini ve uygulanmasını zorlaştırabilmektedir.

- Devlet ve devlet dışı aktörler: Siber alanda hem devlet hem de devlet dışı aktörler uluslararası güvenliğe tehdit oluşturabilmektedir. Geleneksel güvenlik çabaları devletlerin eylemlerine odaklanırken bilgisayar korsanları ve siber suçlular gibi devlet dışı aktörlerin de uluslararası güvenlik üzerinde önemli bir etkisi olabilmektedir.

- Siber uzayda yapılan saldırıların klasik anlamda yapılan saldırılardan farkı hızlı olması ve çok boyutlu olmasıdır. Buna ilaveten çok geniş alanda daha fazla zarara uğratmasını da bir diğer faktör olarak değerlendirmek mümkündür. Özellikle gelişmişlik seviyesi ve internet (teknoloji) kullanımı yüksek olan ülkelerde meydana gelebilecek zararın boyutları daha da fazla olabilmektedir. Uluslararası alanda siber saldırıları engelleyecek bir üst otorite olmadığından ulusal ve uluslararası güvenliği kısıtlamaktadır (Gürkaynak & İren, 2011).

- Uluslararası siber güvenliği sağlamaya yönelik hukuksal olarak birtakım çalışmalar yapıldığı bilinmektedir. Yapılan hukuksal sözleşmeler ve anlaşmaların doğrudan siber güvenlikle ilgili çok az sayıdadır. Bu kapsamda Tallinn El Kitabı, Avrupa Birliği Siber Güvenlik Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü oluşturulmuştur. Bu hususta yapılan hukuksal düzenlemelerin doğrudan bir yaptırımı veya doğrudan bir bağlayıcılığı olmadığı göz önüne alındığında uluslararası güvenliğin kısıtlı olduğu sonucuna varılmaktadır (Günay, 2019).

- Siber alanın bir diğer kısıtlılığı ise siber uzayın sınırlı alanı tarafından kısıtlanmış olmasıdır (Geers, 2011).

- Siber alan temel olarak internet ağlardan oluşmaktadır ve bu ağlar ile bağlantılı araçlar her an sızma girişimlerine açık olması da siber alanın kısıtlılıklarını oluşturmaktadır (Liaropoulos, 2013, s. 158).

- Siber savunmanın algılanan zorluğu nedeniyle çekici bir seçenek gibi görünse de siber caydırıcılığı baltalayan birkaç konu vardır. İlk olarak, siber silahların sanal doğası ve gizliliği nedeniyle bir devletin misilleme yeteneğinin fiziksel olarak test edilememesi siber uzayda uluslararası güvenliğin kısıtlılıklarını oluşturmaktadır (Orsı, vd., 2018)

- Gelişmişlik düzeyleri farklı ülkeler arasındaki görüş farklılıkları da siber alanda uluslararası güvenliğin kısıtlılıklarını ortaya çıkarmaktadır. Teknoloji seviyesi

daha düşük bir ülkenin siber saldırılara karşı daha duyarsız tutumu uluslararası alanda oluşturulması muhtemel iş birliğinin önüne geçmektedir (Trachtman, 2004).

Genel olarak, uluslararası güvenlik çabaları siber tehditleri ele almada ilerleme kaydetmiş olsa da güvenilir bir siber alan sağlamak için ciddi kısıtlılıkların ve zorlukların varlığı bilinmektedir.



SONUÇ

Bu çalışma küreselleşmenin getirmiş olduğu siber uzay alanında realist teorinin bu alanı açıklama yetkinliğine, yaklaşık bir asırdır literatüre egemen olan realist teorinin siber alan ile birlikte literatürde hâkim olan koltuğunu koruyup koruyamadığına ve realist teorinin siber uzayı açıklamadaki eksikliklerinin neler olduğuna geçerli bir yanıt aramıştır. Literatürde bu soruya yönelik doğrudan çok sayıda yanıt bulunmamaktadır. Lakin bu yanıtların konuyu açıklamadaki gücü sadece realist teorideki güvenlik şemsiyesi altında açıklamaları nedenlerinden dolayı eksik kalmaktadır. Bu bakış açısı da siber alan gibi devasa büyüklükte interdisipliner bir alanı sadece güvenlik ve güvenlikleştirme çalışmaları adı altında kısıtlanması ile sonuçlanmıştır.

Literatürde sadece güvenliğe odaklanılmış ve realist teorinin diğer ilkeleri göz ardı edilmiştir. İlgili açığı kapatmak amacıyla bu çalışma realist teori özelinde, siber güvenlik kavramını ele alarak literatürdeki hâkim yaklaşımlardan farklı bir argüman ortaya koymaktadır. Bunu da yaşanmış siber saldırılar, siber casusluk olayları, siber güç kapasitesi ve siber savaş silahları kavramında yaşanan değişimler üzerinden tartışmaktadır. Realist teori siber alanda yaşanan gelişmeleri tam olarak açıklamakta yetersiz kalmaktadır. Buna karşın güç, güvenlik ve anarşi gibi temel kavramlar üzerinde siber uzay ile ortak bir noktada yer almaktadır. 2007 Estonya siber saldırıları olayından başlayarak 2022 başında vuku bulan Rusya/Ukrayna Savaşı'nda yaşanan siber saldırılara kadar önemli görülen bazı temel siber vakalar üzerinden değerlendirme yapılmıştır.

İnterdisipliner bir özelliğe sahip olan Uluslararası İlişkiler Disiplini değişime ve yenilgiye açık olmasıyla bilinmektedir. Ancak bu özelliğini siber alanda net bir şekilde gösterememiştir. Çeyrek asırı aşan sürede teknolojik gelişime ve siber alana tam olarak adapte olamamıştır. Bunun en bariz örneği ise uluslararası ilişkiler teorilerinde siber alanın net olarak özgün bir yer edinememiş olmasıdır. Siber alan internet ile gelişme göstermiş uluslararası ilişkiler alanında bir aktör olmamasına rağmen zaman içerisinde uluslararası ilişkileri ve politikayı derinden etkilemiş ve değişime zorlamıştır. Uluslararası İlişkiler disiplini devlet dışı aktör olarak sisteme müdahale etmiştir.

Siber alanın uluslararası politikadaki etkisi ile birlikte uluslararası güvenlik, kavramsal ve pratik açıdan çağın gerisinde kalmış ve değişime yenik düşmüştür. Lucas Kello da uluslararası ilişkiler disiplindeki temel teorilerin siber alanı açıklamakta yetersiz kaldığını savunmuştur. Bir başka deyişle siber alanın temelinde var olan teknolojik gelişmelere ve bilgi çağının getirdiği yeniliklere uluslararası ilişkiler teorileri yeterince açıklayamamış ve eksik kalmıştır (Kello, 2013).

Siber uzay söz konusu olduğunda realist teori devletlerin bu sorunları nasıl algıladığı ve nasıl yaklaştığına dair çeşitli perspektifler sunmaktadır. Realistler, siber uzayı geleneksel güç ve mücadele alanının bir uzantısı olarak görmektedir. Realistler klasik anlamdaki güç mücadelesinin siber alanda da geçerli olduğunu savunmaktadır. Stratejik bir araç olarak siber güç, ucuza elde edilebildiği ve diğer araçlarla birlikte veya tek başına kullanılabildiği için çekici ve avantajlıdır (Kugler, 2009). Bu yönüyle realist teori ile bağdaşmaktadır. Buna güzel bir örnek ise İsrail devletinin casus yazılımı olarak dünya piyasasına satışa sunduğu “Pegasus” yazılımıdır. İsrail dış politikasına uyumlu bir şekilde bu yazılımı satması siber alanda da her durumun mubah görülmesi realist geleneğin siber alandaki bir göstergesidir.

Realistler ayrıca siber alandaki güç eşitsizliklerinin rolünün de farkındadır. Sofistike siber operasyonlar yürütme yeteneği gibi daha gelişmiş teknolojik yeteneklere sahip devletlerin az gelişmiş devletlere göre bir avantaja sahip olduğunu ileri sürmektedir. Bu güç asimetrisi, siber hakimiyet ve siber savunma yarışı potansiyeli hakkında klasik anlamda caydırıcılık faktörünün nükleer caydırıcılık ile olan bağlantısı gibidir. Bu açıdan da realist teori ile örtüşmektedir.

Siber alanın etkileşiminin artması ile uluslararası alanda güvensizlik ortamı devam etmiştir. Bu güvensizlik ortamında realist teorisyenlere göre devletler güvenliklerini sağlamak istemektedir. Siber alanın devlet dışı aktörleri de etkilemesi ile neo-realist teori siber güvenlik çalışmalarında daha uygulanabilir bir bakış açısı sunmaktadır. Çünkü güvenlik perspektifinden neo-realist teori temel aktör olarak devletleri ele alsa bile devlet dışı varlıkların sistemde bulunduğunu kabul etmektedir (Güntay, 2016).

Siber uzayın devletlerin askeri güç kapasiteleri bağlamında da siber merkezli değişim ve dönüşümler yapması konusunda özellikle siber orduların kurulması kapsamında devletleri etkilediği bilinmektedir (Darıcı, 2017). Bir başka deyişle siber alanın uluslararası ilişkiler kapsamında devletler arası politik etkilerinin olduğunu gözlemlenmektedir. Klasik anlamda caydırıcılığı sağlamak isteyen devletlerin oluşturmuş oldukları askeri birliklerin artık siber savunmada alanında da oluştuğunu görülmektedir. NATO, AB, BM gibi ulus üstü kurumların bünyelerinde siber savunma merkezlerinin kurulması bunun bir çıktısıdır. Siber alanın uluslararası sistemdeki etkisi devletlerin güvenlik stratejilerine yansımıştır. Klasik anlamda sınır güvenliğini askerler aracılığıyla koruyan devletler günümüzde siber alanda güvenliği, gizli bilgileri ve kritik alt yapısını korumak için siber savunma ekipleri oluşturmuştur.

Uluslararası İlişkiler disiplin olarak içinde bulunduğu dönemin gerekliliklerinden beslenen bir bilim dalıdır. Bu sebeple günümüzde de siber alandan beslenmekte ve içinde bulunduğumuz çağın gelişmelerinden hareket etmektedir. İçinde bulunduğumuz yüzyılda başında siber olan olaylar çokça gündemde etkinliğini korumaktadır. Birey, toplum ve devlet tarafından yaşanan siber olaylar güvenlik, güç, silah sanayi ve egemenlik alanında değişimler için aşındırmalar yapmıştır. Örnek olarak devletler ve bireyler için siber güvenlik artık bir zorunluluk olmuştur. Bu çerçevede siber alana yönelim sağlanmıştır. Güç, güvenlik, silah teknoloji ve egemenliği en iyi açıklayan realist teori olduğundan dolayı bu iki kavram bir arada incelenmiştir.

Atina ile Sparta şehir devletleri arasında ortaya çıkan savaşın Thucydides'e göre en önemli nedeni iki şehir devleti arasında ortaya çıkan güç dengesinin bozulmasıdır. Bu eşitliğin bozulması savaş ile sonuçlanmıştır. Günümüzde siber alanda ortaya çıkan teknolojik gelişim farkı da uluslararası politikada son derece etkili olmaktadır. Siber alanda ortaya çıkan göreceli güç kavramı realist teori kökeninden beslenmesi açısından analizde yer almıştır.

Realist teori kökeninden bir başka örnek ise Machiavelli'nin realizmi uluslararası politikanın bir teknolojisi olarak tasvir etmiştir (Forde, 1995). Bu çalışmada siber alanı bilimsel temelli bir teknik olarak teknolojinin teknolojisi olarak

tasvir etmek mümkündür. Günümüzde uluslararası arenada yaşanan gelişmeleri anlamak için bu tasvirin kullanılması gerekmektedir.

II. Dünya Savaşı, Soğuk Savaş, Vietnam Savaşı ve Petrol Krizi realist teorinin gelişmesini desteklediği gibi siber uzayda yaşanan gelişmeler de realist teorinin gelişmesini devam ettirmektedir. Burada dikkat edilmesi gereken nokta realist teorinin bazı temel analiz ilkeleri haricinde olduğudur. Bir başka deyişle devletlerarası ilişkilerde savaşın doğası değil siber alanın gelişmesi ile savaş konu olan savaşın karakterinin değiştiği gerçeğidir. Savaşan taraflar arasında sıcak çatışma olmadan milyarlarca dolar zarar vermek amaçlı siber saldırıların yapılması ya da siber alanda etki düzeyi yüksek insansız araçların kullanılarak fiziki alanda da kullanılan araçların varlığıdır.

İçinde bulunduğumuz yüzyıl ve geçmiş yıllar ne yazık ki bizlere savaşlar, çatışmalar, göçler ve askeri operasyonlarla baskın bir geçmiş yaşatmış ve yaşatmaya devam etmek olup bunun bir çıktısı olarak realist paradigmayı baskın bir şekilde karşımıza çıkarmaktadır. Buna karşın diplomasi, uluslararası hukuk ve idealist teorilerin önemi azaltmıştır. Uluslararası İlişkiler disiplini olarak çağın içinde bulunduğu dönemin konjonktürel şartlarından etkilenerek oluştuğu bilinmektedir. Bu durumda siber alanın siyaset bilimi ve uluslararası ilişkiler boyutunda güvenlik çalışmaları altında sıkça karşılaşılan bu algının bir sonucunu oluşturmaktadır.

Realist teori, uluslararası ilişkilerde güç ve güvenliğin önemine vurgu yapmaktadır. Siber alanda devletler, gelişmiş siber yetenekler geliştirerek ve kritik altyapılarını güvence altına alarak gücü elinde tutmaya çalışmaktadır. Neo-realist teoride var olan self-help ilişkisi devletlerin birbirlerine güvenmediği bir ortam oluşturmakta ve devletler de böyle bir ortamda güvenliklerini arttırmak için askeri kapasitelerini arttırmak istemektedir (Açıkmeşe, 2008). Bu var olan algı siber alanda devlet ve devlet dışı kurumların güvenlik algısı çerçevesinde siber imkanlarını geliştirmesi ile örtüşmektedir. Siber alandaki tehditler devlet dışı kurumları da derinden etkilemektedir. Solar Winds saldırısı, Colonial Pipeline Saldırısı, Microsoft Exchange Saldırıları ve Ransomware Saldırıları 2020 ve 2021 yıllarında yaşanan bu saldırılar sonucunda global şirketler, sağlık kurumları ve kamu kurumları dahil olmak

üzere birçok kuruluş bu tür saldırılarla karşılaşmış ve fidye talepleriyle mücadele etmek zorunda kalmıştır.

Siber alan için de güçlü bir teknolojik ağı sahip olmak gerekmektedir. Realist teoride sadece ulusal güvenlik konusu yüksek önem sahiptir ancak siber alanda birey, toplum ve özel kurumlarında siber güvenlikleri yüksek öneme sahiptir. Realistler, uluslararası sistemin kapsayıcı bir otoritenin olmadığı anarşi ile karakterize edildiğini iddia etmektedir. Benzer şekilde, siber uzayda merkezi bir yönetim organı yoktur, bu da nispeten merkezi olmayan, anarşik bir ortama yol açmaktadır. Kendi çıkarları doğrultusunda hareket eden devletler, kendi siber alanlarını güvence altına almayı ve kritik varlıklarını korumayı amaçlayarak genellikle ulusal çıkarlarını küresel iş birliği veya normlardan üstün tutmaktadır. Neo-realist paradigmada güvenlik algısının oluşumu açısından anarşi durumu temel belirleyici etkidir (Açıkmeşe, 2008). Bu bakımdan siber alanda hâkim olan anarşi durumu realist teori ile uyumaktadır.

Güvenlik ikilemi, realist teoride kilit bir kavramdır ve devletler güvenliğini artırma çabalarının başka devletler için artan güvensizliğe yol açabileceğine dikkat çekmektedir. Siber uzayda devletlerin ağlarını güvence altına almak veya algılanan tehditlere yanıt vermek için aldığı önlemler, istemeden gerilimleri artırabilmekte ve bir misilleme amaçlı siber saldırı döngüsünü tetikleyebilmektedir. Siber alanda güvenlik ikilemi potansiyel saldırılara karşı caydırıcı olması amaçlanan yüksek teknolojik araçlara sahip olmaktır.

Fiziksel dünyadaki tehditlerin aksine siber uzayda fiziksel veya doğal sınırlar yoktur. Böylece, iki potansiyel düşman arasındaki fiziksel mesafe ne olursa olsun sanal ortamda aralarında akabilecek bilgi ve bunun sonucunda ortaya çıkan tehditler sadece saniyeler kadar uzaklıktadır. Bu durumda, çıkarlarına yönelik tehdit algılayan devletlerin kendi siber güçlerini artırmak için harekete geçmeleri için potansiyel bir hasım güçlerin gerçek niyetleri ve olasılıkları hakkındaki belirsizliğin ortaya çıktığı sanal bir güvenlik ikilemi kurulur (Rocha & Fonseca, 2019).

İçinde bulunduğumuz yüzyılda Dünya siyasetinde önemli konuma gelen devlet dışı aktörlerin varlığı dikkat çekmektedir. Değişen uluslararası sistemde etki unsuru

olarak özel sektöründe dahil olduğu bilinmektedir. (Choucri, 2012). Neo-realist teorinin siber alanla uyum sağladığı aktör analizidir. Bir başka deyişle günümüzde siber alan teknolojik gelişmelerin en önemli özelliği olarak ortaya çıkmıştır. Egemenlik ilkesiyle hareket eden modern devletler siber alana tam olarak hâkim olamamıştır. Siber alanın uluslararası sistemde özel sektör (birey) faktörüne önemli bir şekilde etki ettiği bilinmektedir (Vaishnav, vd., 2013).

Realist teori uluslararası ilişkilerde gücün, çıkarların ve devletlerin mücadelesini ulusal çıkar olarak vurgulayan bir düşünce okuludur. Devletlerin uluslararası sistemde ana aktör olduğunu ve eylemlerinin kendi güçleri ile doğru orantılı olarak güvenliklerini sağladıklarını ve her an güçlerini arttırma amacıyla hareket eden devlet anlayışını savunan bir düşünce okuludur. Realistler, uluslararası sistemin anarşik olduğunu, yani uluslararası sistemde kural koyacak ve bu kuralları uygulayacak veya devletler (ana aktörler) arasındaki meydana gelebilecek potansiyel çatışmaları önleyecek merkezi bir otorite bulunmadığını savunmaktadır.

Uluslararası sistemin anarşik yapısına ve iki kutuplu veya çok kutuplu olabilen güç dengesi etrafında dönen sistem boyunca yeteneklerin dağılımına dayanan devlet merkezli sistemik bir uluslararası siyaset teorisidir. Realist teoride devletlerin temel amacının hayatta kalmak olduğu uluslararası sistemin anarşik olduğunu varsaymaktadır. Realizm devletlerin sistem içerisinde birbirlerine tam olarak güvenememesiyle birlikte devletlerin rasyonel aktörler olduğu varsayımı onlar adına önem teşkil etmektedir (Pashakhanlou, 2018, ss. 29-36).

Uluslararası İlişkileri oluşturan ve tanımlayan ana aktör olan devlet, siber alanı anlamlı bir ölçüde kontrol edememekte ya da kendisini yeni siber gerçekliklerin olumsuzluklarından yalıtamamaktadır (Vaishnav, vd., 2013). 1990'lardan bu yana, silahlı kuvvetlerini siber uzayda koruma görevini devreden ülkelerin sayısının artması dikkat çekicidir. Bu kısmen, kurumların bu alanda yeterli korumayı sağlamak istediklerinin bir çıktısıdır. (Rocha & Fonseca, 2019).

Güvenliğe yönelik siber tehditlere ilişkin artan kanıtlar, Siber uzayın siyasallaşmasını ve ortaya çıkan politika söylemlerindeki önemini pekiştirmektedir.

Bugün güvenlikle ilgili sorunlardan biri, tehditlerin kaynakları, yerleri veya hedefleri hakkında henüz tam bir anlayışa sahip olunamamasıdır. Ayrıca “siber güvenlik” kavramının kendisi konusunda da ortak bir mutabakat yoktur. Sonuç olarak, bilinen ölçütlerden yararlanma ve bunları muhtemelen daha etkili yollarla yeniden birleştirme eğilimi vardır (Vaishnav, vd., 2013).

Yeni aktörlerin yaratılması kimlikler ve diğerleri ile birlikte onların siber yetkilendirmesi, geleneksel uluslararası karar ortamını potansiyel olarak önemli şekillerde değiştirmektedir. Yeni asimetri türü, özellikle daha zayıf aktörlerin güçlülere ne ölçüde etkileyebileceği ve hatta tehdit edebileceği ortaya çıkan bir gerçek olarak uluslararası sistemi etkilemiştir. (Vaishnav, vd., 2013).

Sonuç olarak yukarıdaki analizlerden hareketle realist anlayış çerçevesinde devletlerin siber uzaydaki davranışları Uluslararası Sistem'deki davranışlarının bir benzeri olarak yorumlanabilmektedir. Siber uzayın ve doğal çevrenin iki yeni etkileşim alanı olarak öne çıkması göz önüne alındığında, dünya siyasetinde artan önemi, teoremin parametrelerini yeniden çerçevelemek için esastır (Choucri, 2012). Bir başka deyişle siber alanın artan önemi teorilerin kavramsal çerçeveleri yeniden ele alacaktır.

Realist teoremin evrensel olduğu iddiası, siber alanın evrenselliği ile uyushmaktadır. Bu kapsamda küreselleşme sonucunda ortaya çıkan internet ciddi katkıları vardır. Devlet sistemi uluslararası alanda kritik olmaya devam etmekte ancak artık gücü ve nüfuzu elinde tutan tek aktör devletler değildir (Choucri, 2012). Bu bakış açısı da siber alanın anlaşılması açısından realist perspektif ile uyumsuzluk göstermektedir.

Siber uzayı yönetmek için kurulan yeni kurumlar (ICANN, IETF ve diğerleri) ile geleneksel uluslararası kurumlar ITU veya diğer Birleşmiş Milletler ve Avrupa Birliği kuruluşları gibi arasında siber mekanlar üzerinde artan etki ve kontrol mücadelesi, yeni meşruiyet ve sorumluluk gerilimleri, zaten çetrefilli olan uluslararası hesap verme sorumluluğunu daha da karmaşık hale getirmektedir. Bu da uluslararası ilişkiler üzerinde siber uzayın kısıtlılıklarını arttırmaktadır (Vaishnav, vd., 2013).

Şimdiden gelecekte teknolojik gelişimin ne derece bir ilerleme kaydedileceğinin bilinmemesi bu çalışma açısından bir kısıtlılık oluşturmaktadır. Clark'a göre Siber uzayın doğası sonucu ortaya çıkan güçlerin karmaşık bir etkileşimi tarafından yönlendirilerek gelişmesi ve mutasyona uğraması beklenen bir durumdur. Clark ayrıca gelecekte internetin kendisinin bile bir mutasyona uğrayabileceğini düşünmektedir (Clark, 2010). Clark'ın bu öngörüsü gelecekte doğru bir şekilde ortaya çıkarsa çalışmanın siber alan üzerindeki bir diğer kısıtlılığı olacaktır.

Dünya genelinde sıcak bir siber savaş yaşanmamış olması ve sonuçlarının tahmin edilememesi bu çalışmanın kısıtlılıklarından bir diğerini oluşturmaktadır. Siber güvenliğin doğası gereği ulusal ve uluslararası hukukun uygulanmasına karşın zorluklar barındırmaktadır. Bu sebeple siber güvenliğin sağlanmasına yönelik ulusal ve uluslararası hukuk kurallarının uygulanmasını zorlaştırmakta ve karmaşık hale getirmektedir. Böylece siber alanda ortaya çıkan birtakım özellikler hukuksal kuralların uygulanmasını engellemekte veya zorlaştırmaktadır (Fidler, vd., 2013).

Realizm ideolojik olarak siber alanın felsefi boyutuyla uyuşmadığı bilinen bir gerçektir. Bu çerçevede realizm temelde siber alanın dinamiklerinin yanında güncel parametrelerle yoğrulması gerekmektedir. Bu siber alana realist perspektiften daha iyi bir bakış açısı kazandırmak için gereklidir. Siber alanın da realist teorinin klasik ilkelerini değişime zorladığı ortadadır. Siber alanda devlet merkezli bir algı söz konusu olmamakla birlikte, siber alanı sadece güç ve güvenlik açısından değerlendirmekte yanlış olmaktadır. Siber alan sonucunda güç kavramı farklı şekilde karşımıza çıkmaktadır. Siber alanda oluşan kripto para gibi devletlerin egemenliklerini etkileyen oluşumlar ortaya çıkmış bu durum devletler açısından çeşitli güvenlik tehlikeleri barındırmaktadır. Devletlerin iç işlerindeki olaylara siber alan üzerinden dış müdahalelerin yapılması devletlerin egemenlikleri üzerinde olumsuz bir durum oluşturmaktadır. Bu duruma en güzel örnek ise Biden-Trump seçimleri örnek olarak gösterilebilir.

Realizmin uluslararası ilişkiler alanındaki teorilerden yalnızca biri olduğunu unutmamak gerekmektedir. Realist teori eksikliklerine rağmen siber alanın anarşi doğasında var olan siber silahlar ve siber saldırılar oldukça hakimiyetini koruyacağı

öngörülmekte buna karşın realist teorinin siber alanı sadece belli ilkeler üzerinden analiz etmesi de realist teorinin siber uzay ile olan uyumsuzluğunu göstermektedir. Buna karşın liberalizm ve inşacılık gibi diğer teorilerin perspektifleri ile siber uzayın daha detaylı olarak anlaşılabilmesi mümkündür. Her teori farklı bir perspektif sunduğu için bir diğer teorinin açık bıraktığı alanı tamamlaması açısından önemlidir. Siber alan kendi başına çok büyük bir çalışma alanı sunmaktadır Bu minvalde siber alanda yaşanan gelişmeleri daha detaylı analiz edebilmek için diğer teorilerin perspektifleri de etkili olacaktır. Bu denli büyük ve karmaşık bir alanı en iyi şekilde analiz edebilmek için çoklu teorik bakış açılarını ve ampirik düzlemleri esas alarak değerlendirmek daha doğru olacaktır. Çalışma sonucunda realist teorinin siber uzayı açıklamadaki eksikliklerinin daha fazla olduğu böylece realist teorinin siber alan ile olan uyumunun çok az olduğu anlaşılmaktadır.

KAYNAKÇA

Acer, Y. (2022). Rusya-Ukrayna Savaşının Gıda Arzına Etkileri Ve Tahıl Koridoru Anlaşması. Ankara: SETA Perspektif Sayı 343. <https://setav.org/assets/uploads/2022/07/P343.pdf>

Açıkmeşe, S. A. (2008). *Kopenhag Okulu Ve Realist Güvenlik Çalışmaları 'nda Aktör, Tehdit Ve Politika: Avrupa Güvenliği Üzerine Bir Değerlendirme* [Ankara Üniversitesi Sosyal Bilimler Enstitüsü]. <https://dspace.ankara.edu.tr/xmlui/bitstream/handle/20.500.12575/79966/227999.pdf?sequence=1&isAllowed=y>

Aktaş, H., Güntay, V. (2016). Karadeniz Ülkeleri Güvenlik Konsepti Ve Uluslararası İlişkiler Açısından Siber Caydırıcılık; Türkiye Üzerine Bir Yaklaşım. *TASAM Akademi*, 1. International Black Sea- Caucasus Congress, 21-34. <https://avesis.ktu.edu.tr/yayin/094708c5-8e10-4ad0-af7b-933c484d2a27/karadeniz-ulkeleri-guvenlik-konsepti-ve-uluslararasi-iliskiler-acisindan-siber-caydiricilik-turkiye-uzerine-bir-yaklasim>

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*. Ankara: Orion Kitapevi.

Andrew, L. (2013). Great Power Politics In Cyberspace: U.S.A And China Are Drawing the Lines Between Confrontation And Cooperation (Ed.). PANORAMA of global security environment içinde (ss. 155-166.). Bratislava/ Slovak: Centre for European and North Atlantic Affairs Publications. https://www.researchgate.net/publication/264327157_Great_Power_Politics_in_Cyberspace_USA_and_China_are_drawing_the_lines_between_confrontation_and_cooperation

Apple Inc. (2023). *Condensed Consolidated Statements Of Operations*. Erişim Adresi https://www.apple.com/newsroom/pdfs/FY22_Q4_Consolidated_Financial_Statements.pdf

Arı, T. (2004). *Uluslararası İlişkiler Teorileri Çatışma Hegemonya İş Birliği*. İstanbul: Alfa Yayınları.

Arı, T. (2004). *Uluslararası İlişkiler ve Dış Politika*. İstanbul: Alfa Yayınları.

Arı, T. (2014). *Postmodern Uluslararası İlişkiler Teorileri-2: Uluslararası İlişkilerde Eleştirel Yaklaşımlar*, (ss. 1-45). Bursa: Dora Yayınları.

Arı, T. (2018). *Uluslararası İlişkiler Teorileri Çatışma, Hegemonya ve İşbirliği*, (9. Baskı). Bursa: Aktüel Basım Yayın.

Arı, T. (2018). *Uluslararası İlişkilere Giriş* (5. Baskı). Bursa: Aktüel 16 Basım Yayım Dağıtım.

Arı, T. (2018). *Uluslararası İlişkilere Giriş*, (5. Baskı). Bursa: Aktüel Basım Yayım.

Arı, T. (2021). *Uluslararası İlişkiler Teorileri Modern Ve Post-Modern Teoriler* (10. Baskı). Bursa: Bursa Aktüel 16 Basım Yayım Dağıtım.

Arı, T., Toprak, E. (2016). *Uluslararası İlişkiler Kuramları-I*. Eskişehir: Açık öğretim Fakültesi Yayınları.

Arıboğan, D. Ü. (2023). *Teknolojik Gelişmelerin Siyasal Hayata Etkileri: TESAM VI. Sosyal Bilimler Kongresi*. TESAM Yayınları. <https://tesam.org.tr/wp-content/uploads/2023/02/Deniz-Ulke-Aribogan.pdf>

Ateş, D. (2009). Uluslararası İlişkiler Disiplininin Oluşumu: İdealizm / Realizm Tartışması Ve Disiplinin Özerkliği. *Doğuş Üniversitesi Dergisi*, 10 (1), 11-25. <http://journal.dogus.edu.tr/index.php/duj/article/view/55>

Avrupa Sayıştay Kurumu. (2019). Etkili bir Avrupa Birliği Siber Güvenlik Politikası için Zorluklar. (Mart 2019 Raporu). https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_DE.pdf

Aydın, M. (2004). Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği. *Uluslararası İlişkiler Dergisi*, 1(1), 33-60. <https://www.jstor.org/stable/43925897>

Aydın, M. (2004). Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği. *Uluslararası İlişkiler Dergisi*, 1(1), 33-60. <https://www.jstor.org/stable/43925897>

Aydın, M., Açıkmeşe, S. A. (2015). Uluslararası İlişkiler Kuramlarında Ana Akımlara Yeniden Bakış. *Uluslararası İlişkiler Dergisi*, 12(46), 1-9. <https://www.jstor.org/stable/43926326>

Barbosa, G. T. (2006). *Internet Use 1990*. SASI Group (University of Sheffield) and Mark Newman (University of Michigan), Erişim Adresi http://archive.worldmapper.org/posters/worldmapper_map335_ver5.pdf

Barkin, S. J. (2010). *Realist Constructivism Rethinking International Relations Theory*, New York: Cambridge University Press.

Barkin, S. (2009). Realism, Prediction, and Foreign Policy. *Foreign Policy Analysis*, 5, 233-246. <https://www.jstor.org/stable/24909777>

Barkin, S. (2009). Realism, Prediction, and Foreign Policy. *Foreign Policy Analysis*, 5, 233-246. <https://doi.org/10.1111/j.1743-8594.2009.00091.x>

Barlas, B. (2020). Realist Bir Perspektifte Siber Güvenlik Kavramı. *Academic Social Resources Journal*, 5 (18), 535-548. <https://doi.org/10.31569/ASRJOURNAL.108>

Baştan, Y., Karagül, S. (2021). Diplomasinin Dönüşümü ve Dijital Diplomasi. *Troyacademy*, 6 (3), 777-803. <https://doi.org/10.31454/troyacademy.959312>

Baylis, J. (2008). Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler Dergisi*, 5(18), 69-85. <https://dergipark.org.tr/tr/pub/uidergisi/issue/39260/462353>

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. *Güvenlik Stratejileri*, 10(20), 119-148. <https://dergipark.org.tr/tr/pub/guvenlikstrjtj/issue/7523/99140>

BBC News. (2015, 4 Aralık). *Türkiye-Rusya uçak krizi: 10 Günde neler yaşandı?*. Erişim Adresi https://www.bbc.com/turkce/haberler/2015/12/151204_rusya_krizin_10_gunu

BBC News. (2023, 2 Mayıs). *Google'dan ayrılan yapay zekanın 'babası' Hinton'dan uyarı: Sohbet robotları yakında insanlardan daha zeki olabilir*. Erişim Adresi <https://www.bbc.com/turkce/articles/ce9647177890>

Bendiek, A., Metzger, T. (2015). *Stiftung Wissenschaft und Politik German Institute for International and Security Affairs - Deterrence theory in the cyber-century*. https://www.swp-berlin.org/publications/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

Bıçakçı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler Dergisi*, 10(40), 101-130. <https://dergipark.org.tr/tr/download/article-file/540269>

Bıçakçı, S. (2019). Siber Güvenlik ve Savunma. *Güvenlik Yazıları Dergisi*, 2019 (42), 1-8. <https://doi.org/10.13140/RG.2.2.21435.77601>

Bıçakçı, S., Ergin, F. D., Çelikpala, M. (2016). *Türkiye'de Siber Güvenlik Ve Nükleer Enerji*. İstanbul: Ekonomi ve Dış Politika Araştırmalar Merkezi. Erişim Adresi https://edam.org.tr/wp-content/uploads/2017/10/edam_siber_guvenlik_raporu.pdf

Bıçakçı, S. (2012), Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler Dergisi*, 9(34), 205-226. <https://www.uidergisi.com.tr/wp-content/uploads/2014/12/Yeni-Savas-ve-Siber.pdf>

Bildt, C. (2016, 13 Aralık). *I sent the first email between heads of state-but the real revolution of connectivity is still to come*. Erişim Adresi <https://qz.com/861001/i->

sent-the-first-email-between-two-heads-of-state-but-the-new-era-of-connectivity-will-change-the-world

Bloomberg HT. (2023, 26 Nisan). *Microsoft ve Alphabet gelirlerini arttırdı*. <https://www.bloomberght.com/microsoft-ve-alphabet-gelirlerini-artirdi-2330335>

Brantly, A. F. (2018). *The Cyber Deterrence Problem: 2018 10th International Conference on Cyber Conflict*. NATO Publications. <https://ccdcoc.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf>

Brent, L. (2019, 12 Şubat). “NATO’nun Siber Uzaydaki Rolü”. [NATO Review] Erişim Adresi <https://www.nato.int/docu/review/tr/articles/2019/02/12/natonun-siber-uzaydaki-rolue/index.html>

Britannica Dictionary. (2023). World Wide Web. <https://www.britannica.com/topic/World-Wide-Web>

Bull, H. (1966). The Case for a Classical Approach. *World Politics*, 18(3), 361-377. <https://www.jstor.org/stable/2009761>

California Institute of Technology. (2023). Explorer-1. <https://www.jpl.nasa.gov/missions/explorer-1>

Cambridge Dictionary. (2023). Cyber. <https://dictionary.cambridge.org/dictionary/english/cyber>

Cambridge Dictionary. (2023). Cyberspace. <https://dictionary.cambridge.org/dictionary/english/cyberspace>

Choucri, N. (2012). *Cyberpolitics in International Relations*. USA: The MIT Press.

Choucri, N., Clark, D. (2019). *International Relation In The Cyber Age The Co-Evolution Dilemma*. USA: The MIT Press.

Clark, D., D. (2010). Characterizing cyberspace: Past, present and future ECIR Working Paper No. 2010-3, 1-18. MIT Political Science Department. <https://dspace.mit.edu/handle/1721.1/141692>

Clarke, A. R., Knake, K. R. (2011). Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit. (Çev. Erduran, M). İstanbul; İKÜ Yayınevi.

Clarke, R. A., Knake, R. K. (2011). *Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit*. (Çev. Erduran, M.). İstanbul: İKÜ Yayınevi.

Connel, M., Vogler, S. (2017). Russia's Approach to Cyber Warfare. CNA Analysis and Solutions March 2017. 1-30.

Craig, A. J. S., Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age (Ed.), *Realism in Practice An Appraisal* içinde (ss. 85-101). Bristol/England: E-International Relations Publisng. <http://www.e-ir.info/publications>

Çakmak, C. (2006). Realist Teori, Uluslararası İlişkilere Etkisi Ve Kritiği. *Kamu Hukuku Arşivi*, 9(1), 44-55. <https://kutuphane.dogus.edu.tr/mvt/pdf.php?pdf=0008464&lng=0>

Çakmak, S. (2019). *İdealizm-Realizm Sentezi Ekseninde Türkiye'deki Suriyeli Sığınmacılar*, [Gazi Üniversitesi Sosyal Bilimler Enstitüsü]. <https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=fmeAmNNS4-DgCWwbxHpHNA&no=htZjBO48YgKG2tqLLTI7dg>

Çalış, Ş., Özlük, E. (2007). Uluslararası İlişkiler Tarihinin Yapısökümü: İdealizm-Realizm Tartışması. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (18), 225-243, <https://dergipark.org.tr/tr/pub/susbed/issue/61794/924205>

Çelik, S. (2018). Siber Uzay Ve Siber Güvenliğe Multidisipliner Bir Yaklaşım. *Academic Review of Humanities and Social Sciences*, 1 (2), 110- 119. <https://dergipark.org.tr/tr/pub/arhuss/issue/40217/478931>

Çıtak, E. (2014). Uluslararası İlişkilerde Gerçeklik (Ed.). *Uluslararası İlişkiler Teorileri Temel Kavramlar* içinde (ss. 29-64). Ankara: Kripto Yayınevi.

Çıfci, H. (2017). *Her Yönüyle Siber Savaş* (İkinci Baskı). Ankara: TUBİTAK Yayınları.

Daban, C. (2017). Uluslararası İlişkilerde Teorik Tartışmaların Yönteme Etkisi. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 27 (2), 190-227. <https://dergipark.org.tr/tr/pub/sbe/issue/38545/507007>

Danchev, D. (2008, 11 Ağustos). “Coordinated Russia vs Georgia cyber attack in progress”. [Zdnet]. Erişim Adresi <https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/>

Darıcılı, A. B. (2017). *Amerika Birleşik Devletleri Ve Rusya Federasyonu’nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi* [Uludağ Üniversitesi Sosyal Bilimler Enstitüsü]. <https://acikerisim.uludag.edu.tr/handle/11452/4457>

Darıcılı, A. B. (2019). Türkiye’nin Siber Güvenlik Politikalarının Analizi; Türkiye’nin Potansiyel Siber Güvenlik Stratejisi. *TESAM Akademi Dergisi*, 6 (2), 11-33 <http://dx.doi.org/10.30626/tesamakademi.613517>

Darıcılı, A. B. (2023 Mart 10). Rusya-Ukrayna Savaşı’nın En Kilit Operasyonu- Youtube. <https://www.youtube.com/watch?v=nl-yt6PgPs&t=175s>

Datareportal. (2023, Nisan). *Global Social Media Statistics*. Erişim Adresi <https://datareportal.com/social-media-users>

Denning, E. D. (1999, 10 Aralık). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*", *Global Problem Solving Information Technology and Tools*. Erişim Adresi <https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/>

Der Spiegel. (t.y.). <https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html>.

Doctorow, C. (2013). When Sysadmins Ruled the Earth (Ed.), Cyberpunk içinde (ss. 391-427). USA: Underland Press.

Drezner, D. W. (2019). Technological change and international Relations. *Journal of International Relations*, 1-18. <https://doi.org/10.1177/0047117819834629>

Dursun, H. R. (2017). Realizmin Realist Bir Eleştirisi Olarak Raymond Aron ve Uluslararası İlişkiler Kuramı, 5(2), 67-85. <https://doi.org/10.14782/sbd.2017.66>

Egan, B. J. (2017). International Law and Stability in Cyberspace. *Berkeley Journal of International Law*, 35 (1), 169- 180. <http://scholarship.law.berkeley.edu/bjil/vol35/iss1/5>

Erdem, T. (2020). *21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay* [Trakya Üniversitesi Sosyal Bilimler Enstitüsü]. <https://dspace.trakya.edu.tr/xmlui/handle/trakya/5279>

Ereker, F. (2010). *Dış Politika ve Kimlik: İnşacı Perspektiften Türk Dış Politikasının Analizi* [Ankara Üniversitesi Sosyal Bilimler Enstitüsü]. <https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/33895>

Fidler, D., P., Pregent, R., Vandurme, A. (2013). Nato, Cyber Defense, And International Law. *St. John's Journal Of International* 4 (1), 1-25. <https://www.repository.law.indiana.edu/facpub/1672>

Forde, S. (1995). International Realism and the Science of Politics: Thucydides, Machiavelli, and Neorealism. *International Studies Quarterly*, 39(2), 141-160. <http://www.jstor.org/stable/2600844>

Frankel, B. (2013). *Roots of Realism*. New York: Taylor & Francis.

Galston, W. A. (2010). Realism in political theory. *European Journal of Political Theory*, 9(4), 385-411. <https://doi.org/10.1177/1474885110374001>

Garst, D. (1989). Thucydides and Neorealism. *International Studies Quarterly*, 33(1), 3-27. <http://www.jstor.org/stable/2600491>

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38 (2), 41-73. http://dx.doi.org/10.1162/ISEC_a_00136

Geers, K. (2011). *Strategic Cyber Security*. Talinn/ Estonia: CCD COE (NATO Cooperative Cyber Defence Centre of Excellence) Publication.

Gibson, W. (1984). *Neuromancer*. (Çev. Gülbey, G). İstanbul: Altıkkırkbeş Yayın.

Girit, S. (2016, 1 Ocak). *Rusya ambargoları yürürlükte: Türkiye nasıl etkilenecek?*. https://www.bbc.com/turkce/haberler/2016/01/151231_rusya_turkiye_ambargo

Goodman, W. (2010). Cyber Deterrence Tougher in Theory than in Practice?. *Strategic Studies Quarterly*, 102-135. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-04_Issue-3/Goodman.pdf

Gold, D., McGlinchey, S. (2017). International Relations Theory (Ed.). *International Relations* içinde (ss.46-57). Bristol; England: E-International Relations Publishing. <http://www.e-ir.info/wp-content/uploads/2016/12/International-Relations-E-IR.pdf>

Goldstain, J. S., Pevehouse, C. J. (2012). Realist Theories (Ed.). *International Relations* içinde (10. Baskı). (ss. 42-81). UK: Pearson Longman <https://www.pearsonhighered.com/assets/samplechapter/0/2/0/5/0205780210.pdf>

Gorge, M. (2007). Cyberterrorism: hype or reality?. *Computer Fraud & Security*, 2007 (2), 9-12. [http://dx.doi.org/10.1016/S1361-3723\(07\)70021-0](http://dx.doi.org/10.1016/S1361-3723(07)70021-0)

Gözen, R. (2008). Uluslararası İlişkilerde Güç ve Adalet. *Muhafazakâr Düşünce Dergisi*, 4 (15), 207-227. <https://dergipark.org.tr/tr/pub/muhafazakar/issue/55767/763369>

Graham, B. (2005, 25 Ağustos). "Hackers Attack Via Chinese Web Sites". [The Washington Post]. Erişim Adresi <https://www.washingtonpost.com/archive/politics/2005/08/25/hackers-attack-via-chinese-web-sites/03559eb7-4e56-40bf-b406-8198bd1e1131/>

Guzzini, S. (2017). Realist Theory and Practice- Cornell University/ <https://www.diis.dk/en/research/realism-as-a-critique-of-militarism-and-national-primacy>

Günay, S. Y. (2019). Bir Hukuk Konusu Olarak Siber Güvenlik, *HAVELSAN Dergisi*, 3 (1), 38-40. <https://www.havelsan.com.tr/kurumsal/medya-merkezi/havelsan-dergi#1648>

Güntay, V. (2016). *Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-Cat)* [Karadeniz Teknik Üniversitesi * Sosyal Bilimler Enstitüsü]. https://www.ktu.edu.tr/dosyalar/uls_5aa95.pdf

Güntay, V. (2017). Uluslararası Sistem Ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi*, 6 (2), 81-108. <https://doi.org/10.28956/gbd.354150>

Güntay, V. (2019). 21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk. *Siyaset Bilimi ve Uluslararası İlişkiler Dergisi*, 1 (2), 87-109. <https://dergipark.org.tr/tr/pub/novusorbis/issue/51611/632145>

Gürkaynak, M., İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 16 (2). 263-279.

Haley, C. (2013). A Theory of Cyber Deterrence. *George Town Journal of International Affairs*,

<https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley>

Harding, B. (2016). *Cyber Deterrence*. USA: Air War College.
<https://apps.dtic.mil/sti/citations/AD1037682>

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

Iasiello, E. (2018). Is Cyber Deterrence an Illusory Course of Action?. *Journal of Strategic Security*, 7 (1), 54-67. <http://dx.doi.org/10.5038/1944-0472.7.1.5>.

International Telecommunication Union. (2020). Global Cybersecurity Index 2020. Erişim Adresi https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Internet Security Threat Report. (2019, Şubat). *Symantec Data*. Erişim Adresi: <https://docs.broadcom.com/doc/istr-24-2019-en>

Investing. (2023). *Google verileri*. Erişim Adresi <https://tr.investing.com/equities/google-inc-income-statement>

Jackson, R., Sorensen, G. (2013). *Introduction to International Relations Theories and Approaches*. United Kingdom: Oxford University Press.

Jensen, E. T. (2012). Cyber Deterrence. *Emory International Law Review*, 26, 773-824. https://digitalcommons.law.byu.edu/faculty_scholarship/231

Jervis, R. (1998). Realism in the Study of World Politics. *Journal of International Organization*, 52(4), 971-991. <https://www.jstor.org/stable/2601364>

John, M. S. (1993). Realism Neorealism And Critical Theory: A General Essay. *The Indian Journal of Political Science*, 54(1), 128-154. <https://www.jstor.org/stable/41855644>

John, M. S. (1993). Realism Neorealism And Critical Theory : A General Essay. *The Indian Journal of Political Science*, 54(1), 128-154. L: <https://www.jstor.org/stable/41855644>

JOHN, M. S., (1993). Realism Neorealism And Critical Theory : A General Essay. *The Indian Journal of Political Science*, 54(1), 128-154. <https://www.jstor.org/stable/41855644>

Joseph, J. (2000). A Realist Theory of Hegemony. *Journal fort he Theory of Social Behaviour*, 30(2). 179-202. <https://doi.org/10.1111/1468-5914.00125>

Kanat, S. (2011). Realizm Kapsamında Terörizm, Güvenlik ve NATO’nun Dönüşümü [Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü] <https://acikerisim.sdu.edu.tr/handle/123456789/32438>

Karabulut, B. (2021). Sosyal Medya ve İletişim Alanında Yaşanan Dönüşüm: Twitter Diplomasisi Örneği. *Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10, 105-119. <https://dergipark.org.tr/tr/pub/aksos/issue/66291/997200>

Kaspersky (2010, 27 Eylül). Kaspersky Lab’s experts believe that Stuxnet manifests the beginning of the new age of cyber-warfare. https://www.kaspersky.com/about/press-releases/2010_stuxnet-worm-insight-from-kaspersky-lab

Keizer, G. (2008, 11 Ağustos). “Cyberattaacks knock out Georgia’s Internet presence”. [Computerworld] Erişim Adresi <https://www.computerworld.com/article/2532289/cyberattacks-knock-out-georgia-s-internet-presence.html>

Kelley, B. (2016, 2 Kasım). “A Timeline of Russian Cyber Attacks”. [Cyber Reports] Erişim Adresi <https://ilccyberreport.wordpress.com/2016/11/02/a-timeline-of-russian-cyber-attacks/>

Kello, L. (2013). The Meaning of the Cyber Revolution Perils to Theory and Statecraft. *International Security*, 38 (2), 7-40. http://dx.doi.org/10.1162/ISEC_a_00138

Keohane, R. O. (2014). Uluslararası Toplumda Egemenlik (Ed.), *Küresel Dönüşümler Büyük Küreselleşme Tartışması* içinde. (Çev. Boyraz, C.). Ankara: Phoenix Yayınevi.

Keyik, M., Erol, M. S. (2019). Realizme Göre Güç Ve Güç Dengesi Kavramları. *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, 3(1), 12-49. <https://dergipark.org.tr/tr/download/article-file/723189>

Kostagiannis, K. (2014). Hans Morgenthau and the Tragedy of the Nation-State. *The International History Review*, 36(3), 513-529. <https://www.jstor.org/stable/24703187>

Kostagiannis, K. (2014). *Realist conceptualisations of power and the nation-state* [The University of Edinburgh]. <https://era.ed.ac.uk/handle/1842/15859>

Köker, A. E. (2021). *Siber Güvenliğin Stratejik Bakış Çerçevesinde Konumlandırılması: Tehdit/Caydırıcılık Bağlamında Örnek Kriz İncelemeleri* [Beykent Üniversitesi Lisansüstü Eğitim Enstitüsü]. <https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp>

Krepinevich, A. (2012). Cyber Warfare: A “Nuclear Option”?. Washington: Center for Strategic and Budgetary Assessments.

Kuehl, D. T. (t.y.). From Cyberspace to Cyberpower: Defining the Problem. <https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210>

Kugler, R. L. (2009). Deterrence of Cyber Attacks (Ed.). *Cyberpower and national security içinde* (ss. 309-340). National Defence:

USA.<https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-13.pdf?ver=2017-06-16-115053-773>

Kurnaz, S., Karatepe, S. (2019). Kritik Alt Yapıların Güvenliği Kapsamında Türkiye’deki Hava Alanlarının Siber Güvenliği. *ASSAM Uluslararası Hakemli Dergi*, 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı, 119-129. <https://avesis.sdu.edu.tr/yayin/08c9b914-8f7b-47c6-bb12-52a14316de58/kritik-alt-yapilarin-guvenligi-kapsaminda-turkiyedeki-hava-alanlarinin-siber-guvenligi>

Kurtul, A., Zeyveli, M.F., İnce, Y., Yıldız, K., Yüce, H., Yakaryılmaz, F. (2019). *Siber Güvenlik Raporu*. İstanbul: Bilişim İnovasyon Derneği. <http://www.bilisiminovasyon.org.tr/tr/main/pages/siber-guvenlik-raporu/12>

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. USA: RAND Corporation

Lin, H. (2012). Cyber conflict and international humanitarian law, *International Review of The Red Cross*, 94 (886), 515- 530. <https://doi.org/10.1017/S1816383112000811>

Lupovici, A. (2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. *Military and Strategic Affairs*, 3 (3), 49-62. <https://www.inss.org.il/wp-content/uploads/2017/02/FILE1333533336-1.pdf>

Lupovici, A. (2016). The “Attribution Problem” and the Social Construction of “Violence”: Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives* 17, 322-342. <https://doi.org/10.1111/insp.12082>

Marchetti, M., Pierazzi, F., Guido, A., Colajanni, M. (2016). Countering Advanced Persistent Threats through Security Intelligence and Big Data Analytics (Ed.), 2016 8th International Conference on Cyber Conflict: Cyber Power içinde (ss. 243-262). Tallinn/ Estonia: NATO CCD COE Publications.

Marson, M. S. (1997). A Selective History of Internet Technology and Social Work. *Computers in Human Services*, 14 (2), 35-49. https://doi/10.1300/J407v14n02_03

Mastanduno, M., Lake, D. A., & Ikenberry G. J. (1998). Toward a Realist Theory of State Action. *International Studies Quarterly*, 33(4), 457-474. <http://www.jstor.org/stable/2600522>

Mastanduno, M., Lake, D. A. & Ikenberry, G. J. (1989). Toward a Realist Theory of State Action. *International Studies Quarterly*, 33(4), 457-474. <http://www.jstor.org/stable/2600522>.

Mc Laughlin, D. (2008, 2 Haziran). “*Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites*”. [The Irish Times] Erişim Adresi <https://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after%02collapse-of-over-300-websites-1.942155>

McGLINCHEY, S. (2017). *International Relations*. Bristol/İngiltere: E-International Relations Publishing.

Mearsheimer, J. J. (2007). Structural realism (Ed.). *International relations theories: Discipline and diversity* içinde (ss.77-94). Britania: Oxford university press https://www.commarkschools.org/Downloads/8_mearsheimer-_structural_realism.pdf

Mohanty, S. P. (2007). Realist Theory (Ed.). *International Encyclopedia of the Social Sciences (2. Edition)* içinde (ss. 97-100). USA: Macmillan Reference.

Molloy, S. (2004). Truth, Power, Theory: Hans Morgenthau’s Formulation of Realism. *Diplomacy and Statecraft*, 15, 1-34. <https://doi.org/10.1080/09592290490438042>

Morgenthau, H. J. (1948). *Politics Among Nations The Struggle for Power and Peace*. New York: Alfred A. Knopf, INC.

Morgenthau, H. J. (1970). *Uluslararası Politika-I. Cilt.* (Çev. Oran, B. Ve Oskay, Ü). Ankara: Sevinç Matbaası.

Möckli, D. (2010). Cyberguerre: Concept, État D'avancement Et Limites, Politique de sécurité: analyses du CSS, 71, 1-4. Zurich: Center for Security Studies. <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysen-71-FR.pdf>

Nacita, I., Reith, M. (2018). Cyber War and Deterrence. *Air&Space Power Journal*, 32 (2), 74-83. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-32_Issue2/ASPJ-Summer-2018.pdf

NATO. (1999, 30 Ocak). Statement by the North Atlantic Council on Kosovo, <https://www.nato.int/docu/pr/1999/p99-012e.htm>

NATO. (2020). Duyurular/ NATO Resmi İnternet Sitesi. (15/11/2022). <https://www.natoschool.nato.int>

Nye, J. S. (2011). Nuclear Lessons For Cyber Security?. *Strategic Studies Quarterly*, 5 (4), 18-38. <https://dash.harvard.edu/bitstream/handle/1/8052146/Nye-NuclearLessons.pdf>

Nye, J. S. (2011). *The Future of Power*, US: PublicAffairs.

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series, 1. London, England: Chatham House Erişim Adresi <https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf>

Nye, J. S. (2016). Deterrence and Dissuasion in Cyberspace. *International Security*, 41 (3), 44-71. doi: https://doi.org/10.1162/ISEC_a_00266

Nye, J. S., Keohane, R. O. (1971). Transnational Relations and World Politics: An Introduction. *International Organization*, 25(3), 329-349. <https://www.jstor.org/stable/2706043>

Öğün, M. N., Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri*, 9(18), 145-181. <https://dergipark.org.tr/tr/pub/guvenlikstrtj/issue/7525/99154>

Özdemir, H. (2008). Uluslararası İlişkilerde Güç: Çok Boyutlu Bir Değerlendirme. *Ankara Üniversitesi SBF Dergisi*, 63(3), 113-144. https://doi.org/10.1501/SBFder_0000002075

Özlük, E. (2009). Gelenekselcilik-Davranışsalcılık Tartışmasını Bağlamında Anlamak. *Ankara Üniversitesi SBF Dergisi*, 64(3), https://doi.org/10.1501/SBFder_0000002118.

Pashakhanlou, H., A. (2018). The Past, Present and Future of Realism (Ed.). *Realism in Practice* içinde (ss. 29-42). Bristol; England: E-International Relations Publishing.

Petallides, C. J. (2012, 4 Mart). “Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat” [Inquires] Erişim Adresi <http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat>

Pham, J. P. (2008). What Is in the National Interest? Hans Morgenthau’s Realist Vision and American Foreign Policy. *American Foreign Policy Interests*, 30, 256-265. <https://doi.org/10.1080/10803920802435245>

Polat, D. Ş. (2020). NATO’nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi*, Özel Sayısı, 135-158. <https://doi.org/10.28956/gbd.695973>

Puyvelde, V. D., Brantly, A. F. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, (1. Edition), Cambridge/İngiltere: Polity Press.

Reardon, R., Choucri, N. (2012). The role of cyberspace in international relations: A view of the literature. *Proceedings of the 2012 ISA Annual Convention*, San Diego, CA., 1-34.

Recro Digital Marketing. (2022, 28 Ocak). *We Are Social 2022: Dünyada ve Türkiye’de internet-sosyal medya kullanımı*. Erişim Adresi <https://recrodigital.com/dunyada-ve-turkiyede-internet-sosyal-medya-kullanimi-2022/>

Resmî Gazete/ Bakanlar Kurulu, World Economic Forum- Digital Geneva Convention.

Rhoads, C. (2009, 28 Ocak). “Kyrgyzstan Knocked Offline”. [The Wall Street Journal] Erişim Adresi <https://www.wsj.com/articles/SB123310906904622741>

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32. <https://doi/10.1080/01402390.2011.608939>

Robinson, N. (2017). Spending on Successful Cyber Defense. <https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html>

Rocha, M., Fonseca, D. F. (2019). The Cyber Issue And Realist Thinking. R. Esc. Guerra Nav, 25 (2), 517-543.

Sağiroğlu, Ş., Alkan, M. (2018). Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık (Ed.). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* içinde (ss. 84-104.). Ankara: Grafiker Yayınları <https://www.sasad.org.tr/uploaded/Siber-Guvenlik-ve-Savunma-Farkindalik-ve-Caydiricilik.pdf>

Sandıklı, A., Kaya, E. (2012). Uluslararası İlişkiler Teorileri Ve Barış (Ed.), *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri* içinde (ss. 133-161). İstanbul; Ankara: BİLGESAM Yayınları.

Savunma TR Haber- Haberler. (2022, 3 Ağustos).
<https://www.savunmatr.com/ingilteredeki-secimler-siber-saldiri-tehlikesi-nedeniyle-ertelendi>

Sayın, Y., Oktay, S. (2020). Bir Savaş Yöntemi Olarak “Hibrit Savaş” Ve Dönüşen Ordular: Dünya, Ortadoğu Ve Türkiye (Ed.). Devlet Doğasının Değişimi: Güvenliğin Sınırları içinde (ss. 289-298). TESAM Yayınları: Ankara.
[https://tasam.org/Files/Icerik/File/%C4%B0GK2Kitap_\(6\)_pdf_5e23767f-f7ea-468e-aa23-d7e1692190ab.pdf](https://tasam.org/Files/Icerik/File/%C4%B0GK2Kitap_(6)_pdf_5e23767f-f7ea-468e-aa23-d7e1692190ab.pdf)

Schneier, B. (2013, Ağustos). “*Cyberconflicts and National Security*”. [United Nations Chronicle]. Erişim Adresi
<https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security>

Sofaer, A. D., Clark, D., Diffie, W. (2010). Cyber Security and International Agreements (Ed.), *Proceedings of a workshop on Deterring Cyberattacks Informing Strategies and Developing Options for U.S. Policy* içinde (ss. 179-206). Washington, D.C.: National Academy of Sciences.
<https://cs.brown.edu/courses/cs180/sources/lec17/Sofaer.pdf> 179-206.

Steiger, S. (2022). *Cybersicherheit in Innen- und Außenpolitik*. Berlin: POLLUX – Informationsdienst Politikwissenschaft.

Stone, J. (2013). Cyber War Will Take Place!. *Journal of Strategic Studies*, 36 (1), 101-108. <https://doi.org/10.1080/01402390.2012.730485>

Şen, O. (2014). Uluslararası İlişkiler Disiplininin Gelişimi (Ed.). *Uluslararası İlişkiler Teorileri Temel Kavramlar* içinde (ss. 13-28). Ankara: Kripto Yayınevi.

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl?. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2 (2), 10-17.
<https://dergipark.org.tr/tr/download/article-file/290469>

Şenol, M. (2017). Türkiye’de Siber Saldırlara Karşı Caydırıcılık. *Uluslararası Bilgi Güvenliği Dergisi*, 3 (2), 1-9. <https://dergipark.org.tr/tr/download/article-file/396047>

T. C. Millî Savunma Bakanlığı. [@tcsavunma]. (2023, 21 Nisan). *NATO Siber Savunma Mükemmeliyet Merkezi (Estonya/Talin)*. Twitter. <https://twitter.com/tcsavunma/status/1649853804894887938>

T. C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi 2020-2023*. Erişim Adresi <http://www.sp.gov.tr/upload/xSPTemelBelge/files/HwolM+ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf>

T.C. Cumhurbaşkanlığı Savunma Sanayi Başkanlığı. (2017). Duyurular/SSB Resmi İnternet Sitesi. (). <https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1083&LangID=1>

Tallinn El Kitabı (2013). Tallinn El Kitabı/ Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı/ NATO Mükemmeliyet Merkezi, <https://docplayer.biz.tr/11039588-Siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi.html>

The Government of Japan. (2015). *Cybersecurity Strategy, 2015*. Erişim Adresi <https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf>

Thompson, B. J. (2014). İletişimin Küreselleşmesi (Ed.). *Küresel Dönüşümler Büyük Küreselleşme Tartışması* içinde (Çev. Özçelik, B.). (ss. 295-310). Ankara: Phoenix Yayınevi.

Thompson, K. W. (1980-1981). Hans J. Morgenthau (1904-1980). *International Security*, 5 (3), 195-197. <https://www.jstor.org/stable/2538428>

ThreatCloud AI. (2022, 10 Ekim). *Recently Daily Attacks*. Erişim Adresi <https://threatmap.checkpoint.com/>

Trachtman, J. P. (2004). Global Cyberterrorism, Jurisdiction, and International Organization 1-36. <https://ssrn.com/abstract=566361>

TRT Haber- Haberler. (2014,11 Temmuz). <https://www.trthaber.com/haber/dunya/kirgizistandaki-abd-askeri-hava-ussu-kapandi-135685.html>

Tuncer, O. S. (2021). Siber Caydırıcılık. *Cyberpolitic Journal*, 6 (11), 74-96. <http://cyberpolitikjournal.org/index.php/main/article/view/106>

Tuncer, O., S. (2022). Concepts of Security from a Perspective of Political Science, *Acta Politica Polonica*, 2022 (53), 127-146. <https://wnus.usz.edu.pl/ap/en/issue/1240/article/19747/>

Turan, O. (2018). Thucydides'in Aktarımına Göre Atina Salgınının Gerçek Etkileri. *Tarih ve Gelecek Dergisi*, 4 (2), 89-108. <http://dx.doi.org/10.21551/jhf.450225>

Türk Dil Kurumu. (2021). Güvenlik. <https://sozluk.gov.tr/>

Türk Dil Kurumu. (2022). İstihbarat. <https://sozluk.gov.tr/>

Ünay, S. (1998.) Yapısal realizm ve ötesi Kenneth Waltz'un "Uluslararası Siyaset Teorisi"'ne eleştirel bir yaklaşım. *Divan Dergisi*, 1998 (1), 207-216. <https://divandergisi.com/pdf/38.pdf>

Ünver, M., Canbay, C., Mirzaoglu, A. G. (2011). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Ankara: Bilgi Teknolojileri ve İletişim Kurumu. <https://docplayer.biz.tr/18199804-Siber-guvenligin-saglanmasi.html>

Vahit, G. (2014). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler. *Güvenlik Stratejileri Dergisi*, 14 (27), 79-111. <https://doi.org/10.17752/guvenlikstrtj.432151>

Vaishnav, C., Choucri, N., Clark, D. (2013). Cyber International Relations as an Integrated System. *Environment Systems and Decision*, 33 (4), 561-576. <http://dx.doi.org/10.1007/s10669-013-9480-3>

Valeriano, B., Maness, R. C. (2018). International Relations Theory and Cyber Security Threat, Conflict, and Ethics in an Emergent Domain. *Oxford Handbooks Online*. <https://doi.org/10.1093/oxfordhb/9780198746928.013.19>

Verton, D. (1999, 4 Nisan). *Serbs launch cyberattack on NATO*. Erişim Adresi <https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/>

Walker, R. B. J. (1987). Realism, Change, and International Political Theory. *International Studies Quarterly*, 31(1), 65-86. <https://www.jstor.org/stable/2600660>

Walker, R. B. J. (1987). Realism, Change, and International Political Theory. *International Studies Quarterly*, 31 (1), 65-86. <https://www.jstor.org/stable/2600660>

Waltz, K. N. (2000). Structural Realism after the Cold War. *International Security*, 25 (1), 5-41. <https://www.jstor.org/stable/2626772>

Waltz, K., Ouester, H. G. (1982). *Uluslararası İlişkiler Kuramı Ve Dünya Siyasal Sistemi*. (Çev. Onulduran, E). Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları.

Waxman, C. W. (2017). Cyber Strategy & Policy: International Law Dimensions. *Testimony Before the Senate Armed Services Committee*, 1-6. https://scholarship.law.columbia.edu/faculty_scholarship/2025/

Weber, H. R. (2019). Cyber Security in International Law. https://2019colloquium.aail.org/wp-content/uploads/2019/09/Session_IV_Rolf_H_WEBER.pdf

Weber, M. (2014). *Protestan Ahlakı ve Kapitalizmin Ruhu*. (Çev. Ökten, M.). Ankara: Tutku Yayınevi.

White House National Infrastructure Advisory Council. (2009). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, 2009. Erişim Adresi <https://georgewbush-whitehouse.archives.gov/pcipb/physical.html>

Wieclawski, J. (2012). Hans J. Morgenthau's Concept Of Politics – Its Nuances And Implications For The Contemporary Foreign Policy Making. *Journal of Politeja*, 3(21), 155-176. <http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-48f31849-7c99-4d1c-bcf9-e7a357ad6e09>

World EconomicFoum. (2017). “Why We Urgently Need A Digital Geneva Convention”, Weforum, 29.11.2017, <https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention>

Yalman, Y. (2018). Siber Terör, Terörizm Ve Mücadele (Ed.), *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* içinde (ss. 259-280). Ankara: Grafiker Yayınları.

Yavuz, B. (2009). Critical Security Studies and World Politics. *Uluslararası İlişkiler Dergisi*, 21 (6), 139-145. <https://dergipark.org.tr/en/pub/uidergisi/issue/39267/462417>

Yayla, M. (2013). Hukuki Bir Terim Olarak “Siber Savaş”. *TBB Dergisi* 2013, 104, 177-202. http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf

Yenal, S., Akdemir, N. (2020). Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi. *ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi*, 11(1), 414-450 <https://dergipark.org.tr/en/download/article-file/1114311>

Yener, Y. (2015/26 Nisan). “8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış” [*Siber Bülten*] Erişim Adresi <https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/>

Yılmaz, S., Sağiroğlu, Ş. (2013). *Siber Güvenlik Risk Analiz, Tehdit ve Hazırlık Seviyeleri*, “6. Uluslararası Siber Güvenlik ve Kriptoloji Konferansı”. Proceedings

Published. <https://silo.tips/download/siber-gvenlik-risk-analizi-tehdit-ve-haz-rl-k-seviyeleri>.

Youd, N. (2014). Cyber Deterrence: Is a Deterrence Model Practical in Cyberspace?. *Journal of Space & Defense*, 47-58.

