T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

SİBER GÜVENLİĞİ YENİDEN DÜŞÜNMEK: STUXNET ÖRNEK OLAYI

YÜKSEK LİSANS TEZİ

MESUT KESİK

Tez Danışmanı
Dr. Öğr. Üyesi Görkem ALTINÖRS

BİLECİK, 2020

10297256

T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

SİBER GÜVENLİĞİ YENİDEN DÜŞÜNMEK: STUXNET ÖRNEK OLAYI

YÜKSEK LİSANS TEZİ

MESUT KESİK

Tez Danışmanı
Dr. Öğr. Üyesi Görkem ALTINÖRS

BİLECİK, 2020

10297256

BEYAN

Siber Güvenliği Yeniden Düşünmek: Stuxnet Örnek Olayı adlı yüksek lisans tezimin hazırlık ve yazımı sırasında bilimsel ahlak kurallarına uyduğumu, başkalarının eserlerinden yararlandığım bölümlerde bilimsel kurallara uygun olarak atıfta bulunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, tezin herhangi bir kısmının Bilecik Şeyh Edebali Üniversitesi veya başka bir üniversitedeki başka bir tez çalışması olarak sunmadığımı beyan ederim.

<table>
<tr><td colspan="4">Bu çalışmanın,
Bilimsel Araştırmalar Projeleri (BAP), TÜBİTAK veya benzeri kuruluşlarca desteklenmesi durumunda; projenin ve destekleyen kurumun adı proje numarası ile birlikte beyan edilmelidir.</td></tr>
<tr><td colspan="2">DESTEK ALINMIŞTIR</td><td></td><td>DESTEK ALINMAMIŞTIR</td><td></td></tr>
<tr><td colspan="5">Destek alındı ise;</td></tr>
<tr><td colspan="5">Destekleyen Kurum:</td></tr>
<tr><td colspan="3">Desteğin Türü</td><td colspan="2">Proje Numarası</td></tr>
<tr><td colspan="2">1- BAP (Bilimsel Araştırma Projesi)</td><td></td><td colspan="2" rowspan="3"></td></tr>
<tr><td colspan="2">2- TÜBİTAK</td><td></td></tr>
<tr><td colspan="3">Diğer; ……</td></tr>
</table>

Mesut KESİK

Tarih: …/…/2020

ÖNSÖZ

Bu tezin yazılması aşamasında, bilimsel bir çalışmanın nasıl yapılacağı konusunda verdiği değerli bilgiler ve yol göstericiliği, sabrı ve ilgisinden ötürü tez danışmanım Dr. Öğr. Üyesi Görkem ALTINÖRS'e sonsuz teşekkürlerimi ve saygılarımı sunarım. Görkem ALTINÖRS, bütün bu sürecin en iyi şekilde yönetilmesini sağlamış, ortaya çıkmış olan bu tezin tüm aşamasında bilgi ve birikimleriyle yolumu aydınlatmıştır. Gösterdiği ilgi ve alaka akademiye olan bağlılığımı perçinlemiş ve bu yolda ilerleme hususundaki azim ve şevkimi artırmıştır. Saygıdeğer hocamın üzerimdeki hakkı çoktur. Bunun yanı sıra geleceğin siber dünyada olduğu fikrini bana ilk aşılayan hocam Dr. Öğr. Üyesi Hakan ARIDEMİR'e, tezin henüz fikir aşamasında bilgi ve tecrübelerini şevkle aktaran Arş. Grv. Ramazan GÜREŞÇİ'ye, eğitimim boyunca engin bilgilerinden yararlanma fırsatı bulduğum değerli hocalarım Dr. Öğr. Üyesi Hakan OLGUN ve Dr. Öğr. Üyesi Çağdaş ZARPLI'ya sonsuz teşekkürlerimi sunarım. Eğitim hayatım boyunca maddi manevi hiçbir desteğini esirgemeyen anne ve babama teşekkür ederim.

Mesut KESİK

Tarih: …/…/2020

ÖZET

SİBER GÜVENLİĞİ YENİDEN DÜŞÜNMEK: STUXNET ÖRNEK OLAYI

Bu tezin amacı, siber güvenlik olgusuna anarşi ve uluslararası hukuk bağlamında konstrüktivist bir eleştirel değerlendirme yapmaktır. Siber-güvenlik günümüzde ana-akım uluslararası ilişkiler teorileri olan realizm ve liberalizm tarafından devlet merkezli bir güvenlik problemi olarak değerlendirilmektedir. Bu tezde ise siber güvenlik bağlamında siber uzayın kendinden menkul devlet merkezli bir varlık olarak ele alınmaması gerektiği, aksine bir sosyal yapı olduğu iddia edilmektedir. Tezin temel araştırma sorusu siber güvenlik özelinde, anarşinin ne ölçüde uluslararası sisteme içkin olduğudur. Bu bağlamda anarşi kavramı uluslararası hukuk ile siber güvenliği anlamak için değerlendirilecektir. Beş bölümden oluşan bu tezde giriş kısmında genel bir bilgi verilecektir. İkinci bölüm olan anarşi bölümünde ise anarşinin konusu ve Stuxnet için önemine değinilecektir. Realizm, liberalizm ve konstrüktivizmin anarşiye olan yaklaşımı anlatılacaktır. Üçüncü bölüm olan uluslararası hukuk bölümünde uluslararası hukukun günümüze kadar olan süreci ve siber güvenliği sağlamada neden önemli olduğu anlatılacaktır. Dördüncü bölümde ise siberin tanımı ve siber dünyanın yapısından bahsedilecek ve daha sonra 2010 yılında İran'a karşı yapılan Stuxnet saldırısı okuyucuya aktarılacaktır. Sonuç bölümünde ise genel değerlendirme ve çözüm önerileri sunulacaktır.

Anahtar Kelimeler: Siber Güvenlik, Anarşi, Uluslararası Hukuk, İran, Stuxnet

ABSTRACT

RETHİNKİNG CYBER SECURITY: THE CASE OF STUXNET

The aim of this thesis is to make a constructivist critical evaluation of cyber security in the context of anarchy and international law. Nowadays, cybersecurity is considered a state-centered security problem by realism and liberalism, which are the mainstream theories of international relations. In this thesis, it is claimed that in the context of cyber security, cyber space should not be considered as a self-appointed state-centered entity, but rather a social structure. The main research question of the thesis is to what extent anarchy is inherent to the international system, with regard to cyber security. In this context, the concept of anarchy will be evaluated to understand international law and cyber security. In this thesis consisting of five chapters, general information will be given in the introduction. In the second part, anarchy, the subject of anarchy and its importance for Stuxnet will be discussed. Realism, liberalism and constructivism's approach to anarchy will be explained. In the third part, international law, the process of international law until today and why it is important in ensuring cyber security will be explained. In the fourth part, the definition of cyber and the structure of the cyber world will be mentioned, and then the Stuxnet attack against Iran in 2010 will be explained to the reader. In the conclusion part, general evaluation and solution suggestions will be presented.

Key Words: Cyber Security, Anarchy, International Law, Iran, Stuxnet

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR LİSTESİ

BM: Birleşmiş Milletler

NATO: North Atlantic Treaty Organization

MR: Manyetik Rezonans

VPN: Virtual Private Network

DDos: Distributed Denial of Service Attack

ARPANET: Advanced Research Projects Agency Network

PLC: Programmable Logic Controller

1.GİRİŞ

Bu tezin amacı; günümüzün en büyük potansiyel sorunlarının başında gelen siber güvenliğin, anarşi ve uluslararası hukuk bağlamında analizini Stuxnet örnek olayı üzerinden yapmaktır. Araştırma, uluslararası hukuk ve siber güvenlik alt-disiplinlerini anarşi kavramı ile bir araya getirmeye odaklı olup, bu sayede literatüre katkı sunmak amaçlanmaktadır. Siber dünya dediğimiz yerin neresi olduğunu ve nasıl bir yer olduğunu, bunun yanı sıra anarşi ile olan bağını irdeleyerek bu dünyanın uluslararası hukuk alanında yapılan çalışmalarda ne kadar yer edindiğini ve var olan eksiklerini ortaya koymak amaçlanmıştır.

Bu tezi önemli kılan iki neden vardır. Birincisi 2010 yılında İran'da gerçekleştirildiği tespit edilen ve saldırının merkezi olarak Natanz Nükleer Tesisleri' nin olduğunun Belarus menşeili VirusBlokAda tarafından tespiti ve ardından gelişen uluslararası hukuk sorunsallarıdır. Bu sorunsalların başında BM Antlaşması'nın 2/4'ün ihlalinin söz konusu olup olmadığı ve eğer böyle bir ihlal söz konusu ise 51. maddenin ne ölçüde kullanılabileceğinin belirsizliği gelmektedir. Milletler Cemiyeti'nin başarısız olmasındaki temel etkenlerden biri olan yaptırımların kim tarafından ve ne ölçüde olacağının devletlerin inisiyatifine bırakılması sorunu bugün kendini siber alanda göstermektedir. O gün kurulamayan Güvenlik Konseyi bugün BM'de varlığını sürdürmektedir ancak siber dünyada yapılacak yaptırımların kimlere ve ne ölçüde yapılacağı belirsizliğini korumaktadır. Zira siber alanda devletleri koruyacak, tüm devletler tarafından kabul edilmiş genel bir antlaşma bulunmamaktadır. Toplamda 64 ülkenin imzaladığı ancak yaptırım konusunda herhangi bir etkinliği olmayan Sanal Ortamda İşlenen Suçlar Sözleşmesi, mevcut olan talebi karşılamakta oldukça yetersizdir. BM'de siber suçlarla alakalı olarak bir Güvenlik Konseyi'nin olmayışı her gün yapılan milyonlarca siber saldırıya karşı nasıl güvenlik önlemleri alınması gerektiğinin belirlenmemiş olması devletlerin kendi başlarının çarelerine bakmak zorunda kalmalarına neden olmaktadır. Böylesi bir ortamın giderek anarşik bir hal aldığı gerçeğinin ışığında siber dünyada devletin kontrolü nasıl sağlaması gerektiği, devlet-üstü yapıların -BM, NATO vs.- ne gibi önlemler alması gerektiği araştırmanın bir başka sorusudur. Ancak burada amaçlanan devletin tüm siber dünyayı kontrol altında tutması gerektiğini savunmak veya devletin tümüyle elini siber dünyadan çekmesi gerektiğini savunmak değil, her iki görüşe

alternatif bir yol bulmaktır. İkinci sebep ise birbirinden tamamen bağımsız üç farklı alanın ilk kez bir araya getirilecek olmasıdır. Anarşi; daha çok uluslararası ilişkiler uzmanlarının ilgilendiği bir uluslararası ilişkiler kavramı, uluslararası hukuk; hukukçuların ilgilendiği ve uzmanlaştığı bir alt-disiplin ve siber dünya ise mühendislerin ilgilendiği ve uzmanlaştığı bir alt-disiplindir. Ancak Stuxnet ile beraber bu üç farklı kavram bir araya getirilecek ve konuya geniş bir perspektif kazandırılacaktır. Bunun temel nedeni ise ne uluslararası hukuka değinilmeden ne de uluslararası ilişkilere değinilmeden siber dünyadaki bu karmaşanın anlaşılıp çözüme kavuşturulamayacak olmasıdır. Bu yönden sosyal bilimlerin iki dalı olan uluslararası ilişkiler ve hukuku günümüz teknolojisine uyarlamak adına önemli bir problem olarak ortaya çıkan siber güvenlik konusu ile birlikte işleyerek uluslararası politikaya bir katkı sunma amaçlanmaktadır.

Temel soru siber güvenlik özelinde, anarşi ne ölçüde uluslararası sisteme içkindir? Ayrıca, Stuxnet saldırısı ile beraber uluslararası hukukun siber dünyada mevcudiyeti ve yeterliliği ne ölçüdedir? Anarşinin siber dünyadaki yansıması nedir? Siber saldırıların nasıl yapıldığı, kişilerin ve kurumların kendilerini siber saldırılardan nasıl koruyabilecekleri yardımcı sorulardandır. Tezin her üç sacayağında da Stuxnet'te birleştirici sorular bulunmaktadır. Anarşinin ne olduğu, realizmin ve liberalizmin anarşiye olan bakış açılarının ne olduğunu ve devletin oluşumunda ne gibi etkene sahip olduğu ve sosyal inşacılığın liberalizm ve realizmden farklarının ne olduğu, zayıf ve güçlü yönlerinin ne olduğu ve bu tez için ne öneme sahip olduğu soruları cevaplanacaktır. Bunun yanı sıra uluslararası hukukun ne olduğu ve nasıl işlediği, kuvvet kullanma yasağının ne olduğu ve neleri kapsadığı, meşru müdafaa hakkı ve bu hakkın genişletilmiş versiyonu olan önleyici meşru müdafaanın ne olduğu ve içerisinde barındırdığı problemleri, kuvvet kullanma ve meşru müdafaa kavramlarının siber dünyaya yansımaları ve eksiklikleri, uluslararası hukukun siber dünyayı nasıl tanımladığı, siber saldırıları ne olarak ele aldığı ve saldırı karşısında hukuki olarak yapılabilecek hamlelerin neler olduğu ve bu konudaki eksikliklerin ne olduğu soruları cevaplanacaktır. Akabinde siberin ne olduğu, siber dünyanın nereyi kapsadığı ve içinde neleri barındırdığı, ne gibi tehditlere gebe olduğunu ve siber dünyada neler yapılabileceğini daha önce yaşanan tecrübelerden örnekler vererek Stuxnet'e giden yolda ne gibi gelişmeler kaydedildiği soruları cevaplanacaktır.

Bu tezin yazılmasındaki amaç; literatürdeki eksikliğin giderilmesine katkıda bulunmaktır. Siber dünyada olan gelişmeler yalnızca belli bir kesim tarafından takip edilmektedir. Zira uzmanlık gerektiren bir konu olan siber dünya, aslında hepimizin gün boyu olduğu yerdir. Sosyal medyada gezerken, internetten haberlere bakarken, e-mailleri kontrol ederken, internetten bir şeyler alırken aslında hep oradayız. Hatta artık hastane için randevularımızı bile internet üzerinden almakla kalmıyor ülkemizde uygulamaya konulan e-nabız programı ile kan ve idrar tahlil sonuçlarımız, MR ve tomografi sonuçlarımızı bile elimizdeki akıllı telefonlardan takip edebiliyor, kaydedebiliyoruz. Bununla beraber reçetelerimizi bile barındıran bu uygulama ile doktorumuza kullandığımız ilaçların kutularını götürmek zorunda kalmıyoruz. İnovasyon açısından oldukça önemli bir gelişme bu ancak madalyonun bir de diğer yüzü var. Bu tür bilgiler her an çalınabilir ve bunu fark edemeyebiliriz. Elimizin altındaki her türlü teknolojik cihaz –telefon, tablet, bilgisayar, otomasyon sistemleri vs.- ele geçirilebilir ve bu nedenle bizler için ciddi tehditler içermektedir. Telefonumuzun hacklenerek[1] içindeki bilgilerin başkaları tarafından ele geçirilmesi, fotoğrafların, videoların ve mesajların sızdırılması tehlikesi ile her an karşı karşıyayız. Bu vakalarla ünlü birçok kişi mağdur olmuş ve halen daha da bu mağduriyetlere yenileri eklenmektedir. Bunun yanı sıra sadece bireysel değil, küresel anlamda da birçok sorunla karşılaşılabilmektedir. Örneğin; resmi sitelere yapılan saldırılar ve resmî kurumlardaki sistemlerde saklanan bilgilerin çalınması durumunda devletler zor durumda kalabilmektedir. Bunun en büyük örneği; 2006 yılında kurulan ve 10 yıl boyunca milyonlarca belgeyi yayınlayan Wikileaks'dir. Julian Assange'in kurmuş olduğu bu siteye normal tarayıcılardan giriş yapılamamaktadır. Tor adı verilen tarayıcı ile giriş yapılabilen bu site internetin karanlık yüzü olarak bilinen Darknet veya Deepweb olarak iki farklı isimle bilinen sanal âlemin alt katmanında yer almaktadır. Yayınladıkları bu belgelerle uluslararası birçok skandala sebebiyet veren Wikileaks, siber dünyada neler yapılabileceğinin bir örneğidir. Nitekim tezin örnek olayı olan Stuxnet'te bu örneklerden biridir. 2010 yılında tespit edilen bir virüs ile İran'ın Natanz Nükleer Tesisleri'nde çok ciddi yıkımlara sebebiyet vermiş ancak ne ne zaman yazıldığı ne kim tarafından nasıl bulaştırıldığı ne de kim tarafından yazıldığı halen daha belirlenememiş ve bu olayın arkasındaki sır perdesi halen daha aralanamamıştır. Bunun nedeni ise, siber saldırıları düzenleyenleri tespit etmenin kimi zaman imkânsız

[1] Hack kelimesinin TDK'de bir karşılığı bulunmamaktadır. Ele geçirmek anlamını çağrıştıran hack kelimesinin ele geçirmek şeklinde kullanılması anlam karmaşasına yol açacağından hack kullanılmaya devam edilecektir.

olduğudur. Sıklıkla kullanılan ve VPN[2] (virtual private network) olarak adlandırılan teknoloji sayesinde sürekli IP[3] değişimi sağladığından faillerin yakalanması oldukça zordur. Devletlerarası iş birliği sağlandığı takdirde ise tespiti daha mümkündür. Ancak siber dünyanın kurucusu ve aynı zamanda hegemon devleti olarak kabul edilen ABD'nin kendi hareket alanının kısıtlanması ve kendisinin uluslararası mahkemede yargılanma ihtimalini doğuracak olması nedeniyle bu tür bir iş birliğinde bulunmadığı yönünde oldukça yaygın ithamlar bulunmaktadır. Ancak dünya ne ABD'den ne de Rusya'dan ibarettir. Nitekim Rusya'nın da bu konuda 2008 yılında Estonya'da düzenlenen DDos[4] saldırısından sorumlu tutulmasına karşın ABD ile paralel şekilde reddetmeleri ancak faillerin bulunması konusunda gerekli adımların atılmasında neden iş birliğine gidilmediği dünya kamuoyu tarafından halen daha hatırda kalan bir sorudur.

Bağımsız her devlet kendini koruma hakkına sahiptir ve saldırıya uğraması durumunda meşru müdafaada bulunma hakkı BM Antlaşması'nın 51.maddesi ile korunmaktadır. Ancak siber dünyada gerçekleşen herhangi bir saldırı alışılagelmişin dışında kullanıcılar tarafından önceden fark edilememe ihtimalinin dışında saldırıya uğradığından bile bihaber olabilmektedir. Bunun nedeni kullandığımız teknolojik aletlerin ele geçirilebilir olması ve kullanıcıyı yanlış yönlendirebilir olmasıdır. Böyle bir durumda devletlerin kendilerini nasıl savunacağı ve saldırıyı fark ettikleri anda nasıl karşılık verebilecekleri sorularının cevapları uluslararası hukukta çerçevesi net olarak çizilmiş değildir. Bu araştırmanın amacı bu konudaki eksiklere işaret ederek neler yapılabileceği konusunda literatüre katkıda bulunmaktır. Zira hayatımızın vazgeçilmezi haline gelen akıllı cihazların, otomasyon sistemlerinin ele geçirilmesi yıkıcı etkilere sebep olabilir. Ancak bugüne kadar yapılan çalışmalar incelendiğinde siber güvenlik, uluslararası hukuk ve anarşi kavramları hep birbirinden bağımsız olarak çalışılmış konulardır. Bu tezin amacı siber güvenliğin sağlanmasının önemine Stuxnet örnek olayı üzerinden değinmektir. İkinci olarak siber dünyanın mevcut düzenin anarşik düzene nasıl tekabül ettiğinin fark edilmesi gerekir ki komplo

[2] Türkçeye sanal özel ağ olarak çevrilen bu teknoloji sayesinde sizi bambaşka bir yerde gösterebiliyor ve kimliğinizi gizleyebiliyor. Ayrıntılı bilgi için bkz. https://www.chip.com.tr/haber/vpn-nedir-ne-ise-yarar_45313.html (Erişim 2.12.19)

[3] Açılımı "İnternet Protokolü" olan IP; her internete bağlandığınızda size atanan bir tür kimlik kodudur. Ayrıntılı bilgi için bkz. https://www.chip.com.tr/ip-adresim-nedir (Erişim 2.12.19)

[4] "Distributed Denial of Service Attack" olarak adlandırılan ve Türkçe' ye "Dağıtılmış Hizmet Reddi" olarak çevrilen, kapasitesinin üzerinde yaşanan yoğunluk neticesinde geçici süreyle hizmet sağlayamaması üzerine odaklı bir siber saldırı türü.

teorilerinden ve şehir efsanelerinden arındırılabilsin. Üçüncü olarak siber dünyanın bu anarşik yapısına karşı yapılabileceklerin hiç kuşkusuz hukuk kuralları çerçevesinde olması gerektiği gerçeği ışığında uluslararası hukuk kurallarında ne gibi düzenlemeler yapılması gerektiğine değinmektir. Zira siber dünyanın bağımsız devletler gibi sınırı bulunmamakta her an her yerden etkileşim sağlanabilmektedir. Bu yüzden iç hukuk yollarıyla müdahale ve mücadele sınırlı bir çerçevede yapılabildiğinden konunun uluslararası hukuk bağlamında ele alınması ve gerekli tedbirlerin ve uygulanabilecek meşru müdafaanın uluslararası hukuk tarafından belirlenmesi ve tüm devletlerin buna uyması gerekmektedir. Uluslararası ilişkiler bağlamında siber dünyanın kesin sınırlar içerisinde tanımlanması ve gerek bireylerin gerekse devletlerin yasal haklarının belirlenmesi ve korunması gerekmektedir. Bunu yaparken ne böylesi olaylara sebebiyet verecek bir hukuki boşluğa mahal verilmeli ne de bireyi ve devleti savunma adına kişisel hayatın gizliliğinin ve insan haklarının ihlaline izin verilmelidir.

Araştırma Stuxnet'i her üç alanla ilişkilendirebilecek şekilde ele alınacaktır. Öncelikle anarşi kavramına yer verilerek anarşinin ne olduğu okuyucuya açıklanacaktır. Daha sonra uluslararası hukukun ne olduğu, ortaya çıkışı ve bugüne gelişi anlatılacak ve anarşi ile olan bağı ortaya konulacaktır. Akabinde tezin ana teması olan siber güvenliğe geçilecek ve siber ve siber güvenlikle alakalı kavramlara yer verilerek okuyucunun zihninde kullandığımız teknolojinin ne olduğu ve nasıl çalıştığının okuyucunun gözünde canlanması sağlanacaktır. Son olarak Stuxnet' in bu üç kavram ile olan ilişkisi Stuxnet 'in ne olduğu ve ne gibi zararlar verdiği anlatılarak siber dünyadaki potansiyel tehlike ışığında nelerin yapıldığı, nelerin yapılmadığı ve niçin yapılmadığı uluslararası hukuk çerçevesinde tartışılacaktır. Bunu yaparken anarşi konusu daha öncede bahsedildiği üzere liberalizm, realizm ve sosyal inşacılık çerçevesinde değerlendirilecektir. Anarşinin devletin ortaya çıkışı üzerindeki etkisi Hobbes ve Locke temelinde günümüz teorisyenlerden de faydalanarak açıklanacak ve devlet öncesi durumun mevcut siber dünya ile olan benzerliğine değinilerek konunun uluslararası hukuk ile bağdaştırılabilir hale gelmesini sağlanacaktır. Tüm bunlar yapılırken anarşi ve uluslararası hukuk alanlarında birincil ve ikincil kaynaklara başvurulacak, siber güvenlik alanında ise birincil kaynaklara yer verilecektir. Alınan her kaynak birbirleriyle mukayese edilecek şekilde dizayn edilerek okuyucunun zihninde bir çatışma ortamı yaratmak amaçlanacak ve böylelikle okuyucunun da zihninde kendine ait bir görüş yaratmak amaçlanacaktır.

Anarşi denilince akla ilk olarak kaosa dayalı bir düzensizlik gelmektedir. Yunanca bir kelime olan anarşi; yöneteni olmayan anlamına gelmektedir (Woodcock, 2014:14). İlk olarak 1840 yılında Proudhon tarafında kullanılan anarşizm kavramı (Kropotkin'den aktaran Taylan, 2014:4) 1917 yılında yayınladığı *The European Anarchy* kitabında uluslararası ortamın nihai karar alıcı ve devletlerin bağlayıcı olduğu merkezi bir iktidarın olmaması bağlamında anarşi olarak tanımlayan G. Lowes Dickinson'a (Dickinson'dan aktaran Ersoy, 2014:161) kadar geçen süreçte anarşi kavramı daha çok toplum teorisi olarak kullanılmaktaydı. Ancak bu tezde kullanılacak olan anarşi kavramı toplum teorisi olan anarşi değil uluslararası ilişkiler teorisi olan anarşidir. Bunun nedeni tezin anarşi olarak addettiği şey siber dünyada bir üst otorite olmayışından kaynaklanan anarşidir. Toplum teorisinde kullanılan anarşi ise daha çok bireylerin mutluluğunu baz alan, devleti bireylerin özgürlüğünü gasp etmek için kurduğu sistem olarak görmekte bu yüzden devletin ortadan kaldırılması gerektiğini savunarak devletsiz bir ortam olarak belirtilen kavramdır. Bu kavram tezin siber dünyayı tanımlamada kullanılacak olan kavram olmamakla beraber tezin lanse etmek istediği anarşi devlet öncesi durumdaki anarşidir. Bu anarşi; devletin ortaya çıkış sebebi olan anarşidir ve devletin yok edilmek istenilerek oluşturulmak istenen sistem değildir. Bu nedenle bir uluslararası ilişkiler teorisi olarak anarşi kavramı siber dünyayı anlamlandırmak ve kurulması gereken devlet-üstü otoritenin ne olabileceğini savunabilmek adına realizm, liberalizm ve sosyal inşacılık çerçevesinde ele alınacaktır.

Realizm; uluslararası ilişkiler teorilerinin temel teorisi olarak addedilen teoridir. Bu teoriye göre; devlet bir zorunluluk olarak ortaya çıkmış ve var olan anarşik düzenden bireylerin özgürlüklerinden belli miktarda feragat ederek kurduğu bir sistemdir. Çünkü doğa halinde insan vahşidir. Denetleyici ve düzenleyici bir mekanizmanın olmayışı insanı diğerleri üzerinde hakkaniyetsiz davranışlara kolaylıkla sevk edebilmekte ve bireye karşı yapılan herhangi olumsuz bir davranışın cezalandırılamayacak olması onu bu davranışından alıkoymamakta ve cani bir varlığa dönüştürmektedir. Bu ortamı realizm anarşik olarak tanımlar. Bu nedenle Hobbes kendisiyle özdeşleşen şu deyimi kullanılır: "*homo homini lupus"* yani "insan, insanın kurdudur.". Bunun önüne geçmek amacıyla bireyler bir araya gelerek belli özgürlüklerinden feragat ederek bir üst otorite kurar. Bu özgürlüklerin başında cezalandırma yetkisi gelir. Birey kendisine yapılan herhangi bir haksızlığa karşılık

cezayı kendisinin vermesi durumunda ortaya karmaşa çıkmaktadır. Zira hangi suça ne kadar ceza verileceği belli değildir. Herhangi bir ölçütün olmaması nedeniyle suçlara karşı cezada hakkaniyet uygulanamamaktaydı. Devletin ortaya çıkışıyla beraber düzenlenen yasalarla beraber bu güvence altına alındı. Realizme göre devlet; yaşamın her alanını denetleyen ve düzenleyen bir kurum olarak karşımıza çıkmaktadır. Öyle ki Hobbes bu yüzden devleti bir *Leaviathan'a* benzetir. Bu yaratık o kadar büyük ki kendi ağırlığı altında ezilmekte ve hareket etmekte zorlanmaktadır. Devletin her alanda etkin olması ve her alanda denetleyici olması onu böylesi bir ağırlığa ulaştırmaktadır.

Liberaller, realistlerin bu karamsar yaklaşımını eleştirmektedir. Liberalizme göre devlet öncesi durumda insanlar tam bir özgürlük içerisinde yaşamaktadır ve insanların Hobbes'un tanımladığı gibi bir vahşi hayat sürmemektedir. Bunun nedeni olarak da Locke doğa yasasını göstermektedir. Doğa yasası insanları her eylemi gerçekleştirmekten alıkoymaktadır. Devletin ortaya çıkışına ise liberaller bu doğa yasasını ihlal edenleri ölçülü şekilde cezalandırabilecek bir otoritenin olmayışına bağlamaktadırlar. Böylelikle yapılabilecek ölçüsüz cezalandırmaların önüne geçilerek barış dönemine geçilebileceğini savunmuşlardır. Liberalizmin en önemli yanı iş birliğine açık olmalarıdır. Her alanda iş birliğine açık olan liberaller özellikle ekonomide yapılacak iş birliği ile barışın sonsuza kadar sürdürülebileceğini düşünmektedirler.

Realist teoriye göre uluslararası ilişkiler; devletlerin nihai karar alıcı bir merkezin olmaması ve devletleri bağlayıcı herhangi bir üst merciinin olmamasından ötürü anarşi olarak tanımlanmaktadır (Ersoy, 2014:161). Bu nedenden ötürüdür ki Waltz uluslararası ilişkilerde *self-help* sisteminin hâkim olduğunu belirtir (Waltz, 2015:131). Devletler uluslararası alanda kendi başlarının çaresine bakmak zorunda kalmıştır. Kendi başının çaresine bakma durumu zamanla güç istencine ve ittifaklar yapmaya evrilerek uluslararası ilişkilere tek kutuplu, iki kutuplu ve çok kutuplu sistemlerin yanı sıra güç dengesini kazandırmıştır. Devletlerin kendi içlerindeki güç istenci zamanla güvenlik ikilemine dönmüştür. İlk defa John H. Herz tarafından tanımlanan güvenlik ikilemi (Ersoy, 2014:163) Heywood tarafından şu şekilde tanımlanmaktadır:

> *Bir devletin askeri yapılanmasının, başka devletler tarafından her zaman, potansiyel ya da fiili saldırganlık olarak yorumlanmaya maruz kaldığı ve misilleme niteliğinde askeri yapılanmaya vs. yol açtığı bir durumu tanımlamaktadır* (Heywood, 2018:115).

Neo-realizm ise uluslararası ilişkilerde daha çok kutupluluk aracını kullanır ve iki-kutuplu sistemin neden daha çok istikrar sağladığını açıklamada kullanılır (Heywood, 2018: 179). Bunun yanı sıra neo-realizm denilince akla gelen ilk isim olan Kenneth Waltz, devletlerin doğa durumunda da savaş halinde olduğunu belirterek, bu savaş halinin sürekli olmadığını ancak her an bir yerlerde savaşın patlak verebileceği şeklinde olduğunu belirtmektedir (Waltz, 2015:129). Ayrıca Waltz, realistlerin devletin olmadığı zamanda şiddetin olduğu iddiasını devletin var olmasıyla devam ettiğini şu şekilde belirtmiştir:

> *Eğer hükümetin yokluğu şiddetle ilişkilendiriliyorsa, keza varlığı da ilişkilendirilebilir. Rastgele bir ulusal trajediler listesi bu noktayı fazlasıyla örnekler. Napolyon'un yenilgisini takip eden yüzyılın en yıkıcı savaşları devletler arasında değil, bunların içinde meydana gelmiştir. Çin'de 1851'de başlayıp 13 yıl süren Taiping İsyanı'nda ölen sayısı tahminleri 20 milyon gibi yüksek bir rakam civarındadır. Amerikan İç Savaşı'nda yaklaşık 600 bin kişi yaşamını yitirmiştir. Daha yakın tarihte, zorunlu kolektifleşme ve Stalin'in temizlik hareketi beş milyon Rus'u ortadan kaldırmış, Hitler ise altı milyon Yahudi'yi yok etmiştir. Kimi Latin Amerika ülkelerinde hükümet darbeleri ve ayaklanmalar ulusal yaşamın olağan özellikleri haline gelmiştir. Örneğin, 1948-1957 arasında sivil çatışmalarda 200 bin Kolombiyalı ölmüştür. 1970'lerin ortasında İdi Amin'in Uganda'sı sakinlerinin çoğu hayatlarının, tıpkı Thomas Hobbes'un doğa durumundaki gibi iğrenç, hayvanca ve kısa süreli hâle geldiğini hissetmiş olmalıdır (*Waltz, 2015:130).

Liberalizme göre ise anarşi vardır ve bu anarşi uluslararası örgütler, ticaret ve demokrasi ile aşılabilir. İnsan doğasının kötü olmadığını, iş birliğine yatkın olduğunu düşünen liberaller serbest ticaret, demokratik barış ve uluslararası örgütlerin inşası ile istikrar ve düzenin getirilebileceğini iddia etmektedir (Heywood, 2018:190). Aynı iddiaya Nye da yer vermektedir. Nye; liberallerin ticaretin sınırları aştığı, insanların birbirleriyle temas kurduğu ve BM gibi kuruluşların mutlak anarşi görüşünün yetersiz kaldığı bir bağlam yarattığını iddia etmektedir (Nye ve Welch, 2015:7). Ayrıca Nye liberalizme üç kola ayırmaktadır: ekonomik, sosyal ve siyasi. Ekonomik liberalizmde önemli olanın ticaret olduğunu belirten Nye, örnek olarak ise Richard Rosecrance gibi Japonya'yı verir ve Japonya'nın gelişimini ticaretle ilişkilendirir (Nye ve Welch, 2015:85). Sosyal liberalizmde ise kişisel temasların çatışmayı azalttığını belirten Nye, örnek olarak ise öğrenciler, iş insanları ve turistleri göstererek iletişim sıklığının yabancılık duygusunun ve başkalarına yönelik nefretin azalacağını belirtir (Nye ve Welch, 2015:87). Son olarak bahsettiği siyasi kolu ise günümüzde daha çok neo-liberalizm olarak adlandırılan türü olduğunu belirten Nye, kurumların, anarşiyi sınırlandırdığında etkisini azaltarak istikrar kazandıracağını ve böylelikle barışçı bir ortam oluşacağını belirtir (Nye ve Welch, 2015: 87-88). Liberalizmin 1980'lerin sonunda ortaya çıkan bugün ciddi eleştirilere maruz kalan neo-liberalizme göre ise;

devletlerin egemenliğinin bu karşılıklı bağımlılık ve uluslararası kuruluşlar tarafından kısıtlandığını iddia eder (Nye ve Welch, 2015:471).

Tez hem realizme hem de liberalizme mesafeli yaklaşmaktadır. Alternatif teori olarak sosyal inşacılığın kullanıldığı bu tezde kullanılacak argümanlar sosyal inşacılık üzerinden savunulacaktır. Zira sosyal inşacılık; savunduğu tez gereği uluslararası ilişkilerin de bir sosyal inşa olduğu iddiasındadır (Küçük, 2014:325). Bunun yanı sıra sosyal inşacılık denilince akla ilk gelen Wendt'in *Anarşi; devletler ondan ne anlıyorsa odur* sözüdür. Bu tezde de savunulacak argüman budur. Realizmin bireyler üzerinde kurduğu otoritenin siber dünyada kurulması bireylerin özgürlüğüne müdahale olabilir ve özel hayatın gizliliğinin ihlali sık sık gündeme gelebilir. Bunun nedeni siber dünyada sınırların sanal olması ve bu nedenle herhangi bir verinin gizliliğinin ihlalinin oldukça mümkün olmasıdır. Bunun yanı sıra korumacı bir yaklaşım sergileyen realizmde her alana müdahale sonsuz olasılığın olduğu siber dünyada bir süre sonra devlette paranoya seviyesine ulaşabilir ve herhangi bir saldırıya karşı önlem adı altında bireylerin veya kurumların gündelik işleyen rutinlerine ket vurabilir. Böyle bir durumda yeniden kaos meydana gelebilir. Liberalizmde ise devletin sınırlı yetkilere sahip olması hatta neoliberalistlere göre devletin yalnızca *gece bekçisi* olması durumunda denetlenebilirlik noktasında devletin oldukça aciz kalması tehlikesiyle karşı karşıya kalınma riski vardır. Devletlerin ortaklaşa kuracağı bir devlet-üstü otoritede böyle bir boşluğun oluşmaması gerekmektedir. Siber güvenliği küresel düzeyde sağlamak amacıyla kurulacak bir üst otoritede iş birliğinin de maksimum düzeyde olması gerekmektedir. Eğer bir devlet, bu iş birliğini reddederse ilerleyen zamanlarda birliğin salahiyetinin devamı noktasında ciddi problemlerle karşılaşılabilir. Nitekim 2008 Estonya ve tezin örnek olayı olarak dördüncü bölümde siber güvenlik başlığı altında detaylıca incelenecek olan Stuxnet gerçekleşmeyen iş birliğinin tabii sonucudur. İran'ın egemenliğini ihlal eden bu saldırının faillerini bulmak adına yapılması gereken çalışma ne yazık ki yapılamamıştır. Bu tezin ortaya çıkışı ise buradaki boşluğa dayanmaktadır.

Siber[5] kavramı 20.yy'a ait bir kavram olmakla beraber henüz herkes tarafından üzerinde mutabık kalınmış bir tanımı bulunmamaktadır ancak genel olarak sanal kelimesini çağrıştırmaktadır. İkinci Dünya Savaşı sırasında şifreli mesajların sıklıkla

[5] İngilizce *cyber* kelimesinden türetilen siber kelimesinin TDK'de karşılığı bulunmamaktadır. Bu nedenle metin içerisinde siber kelimesi kullanılmaya devam edilecektir.

kullanılması ve bu mesajların deşifre edilmesine yönelik çalışmaların yoğunlukta olması nedeniyle özellikle matematikçiler tarafından geliştirilen algoritmalar bilgisayarın temelini oluşturmaktadır. Savaşın bitimi ile beraber bu iletişim ağı dünyaya yayılmaya başlamış ve bu sayede Amerika kıtası Asya ve Avrupa ile her an iletişim kurabilir hale gelmiştir. 1969 yılında ABD tarafından geliştirilen ARPANET[6] adlı ağ ile ortaya çıkan (Bidb,2020) internet, 1971 yılında Ray Tomlinson tarafından gönderilen ilk e-posta (Digitalage,2020) ile haberleşme alanında yeni bir çağa geçildi. Zaman içerisinde e-postalardan ziyade kurulan web siteleri ile internet giderek gündelik hayatın bir parçası haline geldi. Özellikle cep telefonlarının yaygınlaştığı 1990lar ve internetin de cep telefonlarına girdiği son 15 yıllık süreç iletişim alanında benzeri görülmemiş değişikliklere neden oldu. İnsanlar artık ellerindeki küçük cihazlarla konuşmanın ötesine geçerek birbirlerini görebilir hale geldi ve telefon yalnızca iletişim kurmak için kullanılan bir cihaz olmanın ötesine geçti. 2004 yılında kurulan Facebook'la beraber bu geçişin ilk sinyalleri verildi. İlk sosyal medya sitesi olma özelliğini taşıyan Facebook'tan iki yıl sonra kurulan Twitter ile beraber iletişim kurmak kulaktan kulağa konuşmanın ötesine geçti ve insanlar artık sadece konuşmuyor, yazışıyor ve paylaşımlar yapabiliyordu. Akıllı telefonlar ile beraber bu eylemler çok daha rahat yapılabilir hale geldi. Çünkü ilk zamanlarda belli bir mekânda yapılabilen eylemlere artık mobil halde iken de aynı eylemleri gerçekleştirme imkânı sunuyordu. Bunun yanı sıra artık insanlar telefonlarına yüklü olan uydu haritaları ile beraber adres sorma ve gideceği yeri bulamama derdinden de kurtulmuş oldu. Her gün çıkan yeni uygulamalar sayesinde artık hayat giderek kolaylaştı ve insanlar bankalarda sıra beklemek yerine ellerindeki cihazlardan istedikleri işlemleri yapabilmektedir. Hatta hastane için randevuları bile akıllı cihazlarla rahatlıkla alabilmektedir. Ancak bu kolaylık arka planda ciddi problemleri de meydana getirmektedir. Bu problemlerin başında güvenlik gelmektedir. Kişilerin yapmak istedikleri birçok eylem beraberinde kişisellik açısından bir oturum açma zorunluluğu ve her yere bir şifre koyma zorunluluğunu getirmiştir. Bu şifreler ise başkaları tarafından ele geçirilebir niteliktedir. Hack[7] olarak adlandırılan bu işlemle beraber herhangi bir kullanıcının tüm bilgileri başkaları tarafından ele geçirilebilmektedir. Bu sorunu aşmak için kullanıcılar

[6] İnternetin atası olarak kabul edilen ve "Gelişmiş Araştırma Projeleri Dairesi Ağı" olarak Türkçe'ye çevrilebilen ağ adıdır.

[7] TDK'de herhangi bir karşılığı olmayan hack kelimesi daha çok ele geçirmek anlamına gelmektedir. Ancak bu tanımın anlamı tam olarak karşılamamasından ötürü hack kullanılmaya devam edilecektir.

belli başlı önlemler almaktadır. Bunun başında kırılması zor şifreler gelmektedir. Özellikle bankalarda şifre olarak rakamların kullanılmasından ötürü doğum tarihinin veya 1900'lü sayıların kullanılmasına izin verilmemesi bu nedenden ötürüdür.

Her ne kadar tahmin edilebilirliği zor olan şifreler seçilse de her halükârda bu sistemler ele geçirilebilir sistemlerdir. Günümüz teknolojisinde asla ele geçirilemeyecek bir sistem şu ana kadar inşa edilememiştir. Hayatımızı devam ettirdiğimiz, her gün içerisinde bulunduğumuz bu dünya siber dünya olarak adlandırılmaktadır. Bu dünyanın sanal oluşu fiziki zaman ve mekânı olmayışı nedeniyle güvenliğini sağlamak oldukça zordur. Nitekim günümüzde sayısız saldırılar düzenlenmekte ve bu saldırılar birçok yere zarar vermektedir. Stuxnet bunlardan biridir. Sadece bireysel ihtiyaçları karşılamanın ötesindeki bu sanal dünya ile beraber fabrikaların ve her türlü tesislerin işleyişi sürdürülmektedir. Buna ket vurmak amacıyla düzenlenen bir saldırı olan Stuxnet İran'ın nükleer santrallerdeki işleyişini aksatmıştır. Düzenlenen bu saldırı ile İran'ın egemenliğinin ihlal edilip edilmediği ve bunun sonucunda ne tür önlemler alabileceği ve meşru müdafaa hakkını ne yönde kullanabileceği tartışma konusu olmuştur ve tez bu bağlamda ortaya çıkmıştır.

BM Antlaşması'nın 2/4.maddesinde her türlü saldırı yasaklanmıştır. 51.maddede ise böyle bir saldırının gerçekleşmesi durumunda devletlerin meşru müdafaa hakkının olduğu belirtilmiştir. Ancak siber dünyanın yeni olması ve her geçen gün büyük bir hızla büyümesi hukukun geride kalmasına neden olmuştur. Bu nedenle siber saldırıların saldırı olarak tanımlanıp tanımlanamayacağı bugün bile belirsizliğini korumaktadır. Bir grup bunun saldırı olarak tanımlanması gerektiği yönünde görüş beyan ederken, bir grup saldırı olarak tanımlanamayacağı yönünde görüş beyan etmektedir. Bu karmaşa bizleri doğa durumuna sürüklemektedir. Siber dünyada bir devletin olmayışı liberallerin de devletin ortaya çıkışını gerekçelendirirken ortaya koyduğu cezadaki ölçüsüzlüğü meydana getirmektedir. Herhangi bir suç işlenmesi durumunda bireylerin cezaları kendilerinin vermesi kaosa yol açmaktadır. Nitekim bu adaleti değil güçlünün güçsüzden iyiden iyiye ayrılmasına neden olmaktadır. Zira güçlü olan; böyle bir ortamda daha da güçlenmekte güçsüz ise hakkını bile savunmaktan aciz hale gelmektedir. Ancak buradaki fark, çatışmanın reel dünyadaki bireyler arası çatışmadan farklı olarak birey, devlet ve devlet dışı organizasyonların oluşturduğu topluluklar arasında gelmektedir. Bu topluluklardan birisi olarak 1990'lı yıllarda bir grup matematikçinin bir araya gelerek kurmuş olduğu Cyberpunk; devletin

bireylerin özgürlüğüne müdahale ederek özel hayatının gizliliğini ihlal ettiğini iddia etmiş ve bunun önüne geçilmesi için algoritmalar geliştirerek dinlenmeyi ve izlenmeyi önleyici tedbirler almaya çalışmışlardır. Bu hareketin bir yansıması olarak 2006 yılında kurulan ve 10 yıl boyunca milyonlarca gizli belgeyi yayınlayan Wikileaks, bu mücadelenin simgesi haline gelmiştir. Ancak her ne kadar kahramanca gibi görünse de belgelerin yasadışı yollarla ele geçirildiği aşikârdır. Siber güvenlikteki açıklardan birini kullanarak ele geçirilen ve yayınlanan belgeler devletlerin egemenliğine bir müdahale olarak görünmektedir. Nitekim Stuxnet'te görülen de budur. Burada gerçekleşen olay santralde ciddi bir yıkımı meydana getirdi. Zararının tazmin edilmesini isteyen İran'ın karşısına uluslararası hukukta yer alan ciddi bir boşluk çıkmaktadır. Bu boşluk, siber dünyanın çerçevesinin hukuki olarak çizilememesinden kaynaklı bir boşluktur.

İran'a yönelik neden böyle bir saldırının yapılmış olabileceği ve failler olarak neden ABD ve İsrail'in -özellikle ABD'nin- gösterildiği sorusunun yanıtı İran'ın nükleer enerji konusundaki geçmişine dayanmaktadır. Şah Muhammed Rıza Pehlevi, ABD ile yaptığı antlaşma ile 1967 yılının Kasım ayında ilk nükleer reaktörüne sahip oldu ve Şah sonraki 20 yıl içerisinde 23 nükleer santralin daha devreye gireceğini duyurdu (Gzt, 2020). ABD'nin İran'a nükleer reaktör vermesinin altında iki neden yattığını belirten Jane, bu iki nedeni şöyle açıklamaktadır:

> *"1949'da SSCB'nin ilk nükleer denemesini yapması ve nükleer caydırıcılığın sağlanması, 1956 Süveyş Krizi'nde İngiltere ve Fransa'nın bıraktığı güç boşluğunun SSCB tarafından doldurulmaya çalışılması."* (Jane, 2017:266).

Ancak işler başlangıçta iyi gitse de Şah Rıza'nın baskıcı yönetimi İran'ı bambaşka bir İran yaptı. Sürgünde olan dini lider Ayetullah Ruhullah Humeyni'nin ülke içerisindeki örgütlenmesi ve yapılan gösteriler sonucu Şah ülkesini terk etmek zorunda kalmış tarihe "Şubat Devrimi" olarak geçen devrim gerçekleşmiş ve Fransa'da sürgünde olan Humeyni'nin gelişi ile İran İslam Cumhuriyeti ilan edilmiş oldu. Başbakan Muhammed Musaddık'ı petrolleri millileştirmeye çalışması sonucunda 1953 yılında yapılan "Ajax Operasyonu" ile görevden uzaklaştıran (AA, 2020) ABD, kendisine Şah ile bir müttefik yaratmıştı ancak yalnızca 26 yıl sonra ülkenin laikleşmeye, batılılaşmaya karşı muhalif kesimi tarafından yapılan devrim sonucunda bölgedeki en önemli müttefiklerinden birini kaybetmiş oldu. 1979 yılında Şah'ın tedavi amacıyla ABD'ye gitmesini protesto eden bir grup öğrencinin ABD büyükelçiliğini basarak 52 elçilik personelini 444 gün süre ile rehin alması (Ekren,

2017:147) ile meydana gelen "Rehineler Krizi" olayı ABD-İran arasındaki ilişkilerin belki de bir daha geri döndürülemez şekilde olumsuz etkiledi. Başkan Carter'ın rehine konusunda başarısız olması sonucunda seçimi kaybetmesinin ardından başa gelen Ronald Reagan'ın 1984 yılında İran'ı terör listesine eklemesinden 2 yıl sonra patlak veren "İrangate" skandalı Reagan'ın da siyasi kariyerini önemli ölçüde olumsuz etkiledi. Hook, bunu şu şekilde açıklar:

"1986 yılında artık Amerika karşıtı İslami bir teokrasi olan İran'a gizli silah satışlarının kârının, Kongre'nin bu amaçla Amerikan fonlarının kullanılmasını yasaklamasını hiçe sayarak, 1984 ve 1986 yılları arasında, Nikaragualı kontraları fonlamak için ortaya çıkınca, Reagan'ın yeterliliği, dürüstlüğü ve değerlendirme anlayışını tartışmaya açık hale getirdi." (Hook ve Spanier, 2014:147)

ABD'nin İran'a karşı bu ofansif tutumuna karşılık İran, 1980'li yılların sonunda İran-Irak Savaşı sonrasında yeniden gündeme gelmiş ve 1990'lı yılların başında SSCB ve Çin ile nükleer reaktör inşası konusunda anlaşmaya varmışlardır (Ekren, 2017:152). Her ne kadar ABD bu duruma karşı çıksa da 2005 yılında imzalanan antlaşma ile Buşehr'e nükleer santral yapılması kararlaştırılmıştır (Ekren, 2017:153). 11 Eylül sonrası Bush halkın da desteğini alarak 2002 yılında Kuzey Kore, Irak ve İran'ı "Şer Ekseni" ilan etti (NTV, 2002). Bu açıklamadan yaklaşık 6 ay sonra 14 Ağustos 2002'de İran muhaliflerinden Ulusal Direniş Konseyi ve Halkın Mücahitleri Örgütü'nden Ali Rıza Caferzade'nin Natanz' da Uranyum zenginleştirdiğine dair açıklaması İran nükleer programının bir krize dönüştüğünün göstergesi olmuştur (Jane, 2017:274). Natanz' a giden yolda ABD ve İran ilişkileri bu şekilde ilerlemiş ve günümüzde de halen tam olarak düzelmiş değildir.

Tezde kullanılacak yöntem nitel araştırma yöntemidir. Değişkenliğin fazla olduğu sosyal bilimlerde nicel araştırma kullanarak doğru sonuca ulaşmak her zaman mümkün olamamaktadır. Zira tezin örnek olayının laboratuvar ortamında gerçekleştirilmesi mümkün olmakla beraber, tezin bütününe hitap etmeyecek olması burada bir eksikliğe sebebiyet verebilmektedir. Araştırma soruları ile sonuca gidilmeye hedeflenen tezde mukayese ön planda tutulacak ve uluslararası hukuk alanında realist veya liberal yaklaşımla neler yapılabileceği ve sonuçlarının ne olacağı üzerine senaryolar oluşturularak sonuca gidilecektir. Mevcut durumun asıl olarak ele alınacağı tezde derinlemesine tanımlamalarla okuyucunun konuyu tam olarak anlaması sağlanacak ve konuyla ilgili uzmanların görüşlerine yer vererek bakış açıları genişletilmeye çalışılacaktır.

Bu tez, daha önce yapılmamış bir şeyi yapmakta ve üç farklı alanı birbirleriyle bağlayarak birbirinden çok farklı ve alakasız gibi görünen üç kavramın aslında birbirleriyle iç içe olduğunu ortaya koymaya çalışmaktadır. Mevcut düzende var olan kaosun sistemin inşacısı olan mühendislerle çözülmesinin oldukça zor olması sebebiyle bu sorunu çözmek adına hukukun mühendislikle arasındaki bağı oluşturmak adına üçüncü olarak uluslararası ilişkiler kullanılacaktır. Uluslararası ilişkiler kullanılmadan sorunun doğrudan hukuki yollarla çözümüne gidilmesi sorunun temelinin anlaşılması noktasında eksikliğe neden olacağından, yapılacak düzenlemelerin günü kurtarmaktan öteye geçemeyeceği savunulmaktadır. Bu nedenle uluslararası ilişkilerde anarşi kavramı mevcut düzeni açıklamak adına kullanılacak ve yapılacak düzenlemelerin kalıcı olabilmesi sağlanacaktır.

Tez; 5 bölümden oluşmaktadır. İkinci bölümde anarşi kavramı anlatılacak ve siber dünyadaki bu kaosun anlaşılması bakımından devlet öncesi durum okuyucuya aktarılarak siber dünyanın mevcut durumunun okuyucunun zihninde canlanması amaçlanacaktır. Üçüncü bölümde uluslararası hukuk anlatılacaktır. Tarihi ortaya çıkışı ve işleyişi hakkında bilgi verilecek ve anarşinin ortadan kaldırılması adına devlet öncesi dönemden ayrı olarak yapılan hukuki işlemlerle düzenin nasıl sağlandığından bahsedilecektir. Günümüze kadar gelen süreçte hangi aşamalardan geçtiği okuyucuya aktarılacak ve anarşiye olan bakış açısı hakkında bilgi verilecektir. Dördüncü bölümde siber güvenlik anlatılacaktır. Kullandığımız teknolojinin ne olduğu ve güvenlik açısından ne gibi gelişmelerle bugüne gelindiğinden bahsedilecek olup Stuxnet'e varan süreçte neler yaşandığı ve hukuki olarak neler yapıldığı okuyucuya aktarılacaktır. Daha sonra Stuxnet hakkında bilgi verilecek ve Stuxnet üzerinden siber dünyada yapılabilecek illegal her eylemin (saldırı, sabotaj, istihbarat, tuzaklama vs.) nasıl yapılabildiği anlatılarak okuyucunun siber dünyayı anlaması amaçlanacaktır. Kullandığımız sistemlerin bizleri nasıl yanıltabildiği, güvenilir olup olmadıklarını belirlemedeki sorunlar ele alınarak tezin üç ana parçasından biri olan teknolojik kısmı okuyucuya en yalın haliyle aktarılacaktır. Uluslararası hukukun var oluş nedenlerinden biri olan savaş ve barış hukuku üzerinden siber eylemlerin uluslararası hukuk nezdinde nerede olduğu ve olması gerektiği tartışılacak, 2/4.maddenin yanı sıra 51.maddeye de değinilerek ülkelerin müdafaa hakları çerçevesinde kendilerini savunabilmeleri gerektiği anlatılacaktır. Sonuç bölümü olan son bölümde ise bu üç kavram ışığında verilen bilgilerin bir genellemesi yapılarak hukuki boşluklara işaret edilecek ve bu

boşlukları doldururken yapılacak düzenlemelerin ne gibi sonuçlar doğuracağı tartışılarak bir üçüncü yol meydana getirilecektir.

2.ULUSLARARASI POLİTİKADA ANARŞİ

2.1. Giriş

Uluslararası politika; devletlerin birbirleriyle her türlü ilişkilerini yürüttüğü bir alandır. Bu alanda gerek ticarete gerek savaşa gerekse barışa karar verilir. Bu kararların alınmasındaki temel etken ise devletlerin ilişkilerinin düzeyidir. Devletin ilk inşasından bugüne değin geçen süreçte birbirleriyle olan ilişkilerini belirleyen en temel etken ticarettir. Sulhun veya savaşın olmasına verilecek kararda ticaretin etkisi oldukça büyüktür. Ticaretin yanı sıra ikinci olarak güç; sulh ve savaş durumunun belirleyicisidir. Her iki etkenin de temelinde yatan neden ise devletin çıkarlarıdır. Bünyesinde barındırdığı vatandaşlarını korumak adına gerektiğinde savaştan bile çekinmeyen devletlerin binlerce yıllık tecrübeleri uluslararası ilişkilere bugünkü politikaları kazandırmıştır.

Devletleri bu davranışlarını sergilerken hesaba katması gereken bazı noktalar vardır. Örneğin; tarihteki ilk yazılı antlaşma olan Kadeş Antlaşması'nın imzalanmasındaki temel etken ortak düşman olan Asurluların güçlenmesi olmuştur (Baysoy, 2015:15). Asurluların güçlenmesi savaş durumunda olan iki devleti (Mısır ve Hitit) barış durumuna getirerek ortak düşmana karşı ittifak yapmaya itmiştir. Gereğinden fazla güçlendiğine kanaat getirilen bir devlete karşı oluşturulan ittifak tarihte birçok kez karşımıza çıkmıştır. Bu ittifaklar sayesinde çoğu dönem "güç dengesi" ile geçmiştir. Ancak devletleri bu davranışlarından alıkoyan veya bunları düzenleyen kurallar genellikle teamüller olmuştur. Bu teamüller binlerce yıllık devletlerarası ilişkilerden edinilen tecrübelere dayanmaktadır. Bu tecrübeler sayesinde devletler varlıklarını sürdürmüşler ya da yok olmuşlardır. Ancak, devletlerin savaşa karar vermelerinde devlet üstü bir karar verici mekanizma olmamasından ötürü tam anlamıyla bir kaos hakimdi. Savaşın ne zaman çıkacağı ve ne kadar süreceğinin bilinmemesi devletlerin ömrünün tahmin edilememesine neden olmaktaydı. Bu yüzden her devlet için öncelik güçlü olmaktır. Güç, beraberinde güvenliği de getirmekte ve bu sayede devletin ömrünü uzun kılabilmektedir. Güçlü olanın sözünün geçtiği bu dönem anarşik bir dönemdir. Her ne kadar günümüzde uluslararası birçok antlaşma ile uluslararası hukuk sağlanmaya çalışılsa da uluslararası ilişkiler teorisyenleri bugün anarşinin halen daha devam ettiğini kabul etmekte ancak çözüm yolu konusunda ayrışmaktadır**.**

Siber dünyadaki anarşi ise denetleyen ve düzenleyen bir kurum olmamasından kaynaklıdır. Doğası gereği siber dünya, kontrol edilmesi oldukça güç bir dünyadır. Bunun yanı sıra bu dünya; yaşadığımız reel dünya gibi bir başlangıcı olmamakla beraber, reel dünyanın geçirdiği tecrübeye dayalı evrimi yaşama imkanını kendinde bulamamıştır. Bu dünya oldukça iyi eğitimli insanlar tarafından oluşturulmuştur ve kısa bir süre sonra devletin siber dünyanın merkezine doğru yol alması neticesinde birtakım kişiler bu duruma karşı çıkarak devletin bu dünyaya egemen olmaması için çeşitli yöntemler geliştirilmiştir. Geliştirdikleri çeşitli algoritmalarla izlenmek, dinlenmek, takip edilmek gibi şeylerin önüne geçmek amaçlanmış ve bu alanda büyük başarılar sağlanmıştır. Ancak bu özgürlük hareketi aynı zamanda çeşitli problemlere de yol açmıştır. İzlenememe durumu çoğu zaman özgürlük açısından oldukça önemli olsa da bu durum suiistimal edilebilmektedir. Nitekim tezin örnek olayı olan Stuxnet saldırısı gerçekleştirilmiş ancak saldırının izini bulma konusunda takip edilmeme özgürlüğünün suiistimaline uğramıştır. Siber dünyadaki anarşi bugün öyle bir boyuta ulaşmıştır ki herhangi bir saldırının failini yakalamak neredeyse imkânsız hale gelmiştir.

2.2. Anarşi 'nin Tanımı

Yunanca bir kelime olan anarşi; yöneteni olmayan anlamına gelmektedir (Woodcock, 2014:14). İlk olarak 1840 yılında Proudhon tarafında kullanılan anarşizm kavramı (Kropotkin'den aktaran Taylan, 2014:4) 1917 yılında yayınladığı *The European Anarchy* kitabında uluslararası ortamın nihai karar alıcı ve devletlerin bağlayıcı olduğu merkezi bir iktidarın olmaması bağlamında anarşi olarak tanımlayan G. Lowes Dickinson'a (Dickinson'dan aktaran Ersoy, 2014:161) kadar geçen süreçte anarşi kavramı daha çok toplum teorisi olarak kullanılmaktaydı. Proudhon, Bakunin, Godwin gibi düşünürler yönetimin olmadığı bir toplum tasarlayarak bireylerin bu sayede mutlu olabileceğini çünkü devletin, bireylerin elindeki imkânları alarak onları köleleştirdiğini iddia etmektedirler. Birinci Dünya Savaşı'na kadar olan süreçte özellikle Fransa'da yaygın bir görüş olan anarşizm, daha sonraları Almanya ve İspanya'da da revaç hale gelmiştir. Hatta İspanya İç Savaşı (1936-1939) sırasında dönemin meşhur anarşisti Emma Goldman'ın bizzat oraya giderek anarşistlere destek verdiği bilinmektedir. Ancak tezimizde bahsedeceğimiz anarşi kavramı sosyal teori olarak anarşiden ziyade uluslararası ilişkiler teorisinde kullanılan bir kavram olan anarşi olacaktır. Zira 4. bölümde anlatılacağı üzere siber dünyanın anarşik olmasının

nedeni olarak bir üst otoritenin bulunmaması ve bununda bir anarşiye sebebiyet verdiğidir.

2.3. Uluslararası İlişkilerde Anarşi

Her ne kadar Birinci Dünya Savaşı sonrasında gelişen ilişkilerin uluslararası ilişkileri başlangıcı olarak kabul edildiği varsayılsa da uluslararası ilişkilerin en başına Kadeş Antlaşması'nı koymak mümkündür. İki devletin yazılı bir metin ortaya koyduğu ve ilk antlaşma olarak kabul edilen Kadeş Antlaşması, uluslararası ilişkilere dair ilk bulgudur. Modern toplum öncesinde yer alan bu devletlerde kontrol kaba kuvvet ile sağlanmaktaydı. Bu toplumlarda devleti ayakta tutan en önemli özellik ise savaşlardı. Fetih politikası tüm imparatorlukların yüzyıllarca kullandığı bir politikaydı. Ancak teknolojinin gelişmesi ve toprakların da genişlemesiyle imparatorluklar tek bir merkezden idare edilemez hale geldi. Bu nedenle feodalite meydana geldi ve imparatorluklar özerk yönetimlere ayrıldı. 1648 tarihine gelindiğinde ise günümüz uluslararası ilişkilerini şekillendiren antlaşma imzalandı. Westphalia ile beraber, halihazırda tek bir merkezden yönetilmekte oldukça zorlanılan imparatorluklar yerini ulus-devletlere bırakmaya başladı. Westphalia, yalnızca imparatorlukların kendi içlerinde yaşadığı bir bölünme değil aynı zamanda küresel siyasetin de gidişatını değiştiren bir olaydı. David Held, bu düzeni şu şekilde açıklar:

> *Kendi içinde hiyerarşik bir otorite düzeni olan merkezi devlet, son kararı veren yüksek mahkemeler ve bürokratik bir yönetimden oluşur. Yasa yapımı, adaletin sağlanması ve şiddet tekeli, merkezi iktidarın elindedir. Bu, düzeni kurmuş olan devletler, askeri ve ekonomik güç düzeyleri ne olursa olsun, uluslararası alanda eşit egemenlerdir. Bu eşitlik, aynı zamanda kendilerinden üstün bir otorite olmadığı anlamına gelir ve sistemi esas olarak anarşik yapar. Uluslararası alanda anarşi belirleyicidir; hukuk, ancak asgari bir arada yaşama ilkelerini belirleyebilir. Devletin uluslararası alandaki özerkliğinin korunması, tüm devletlerin ortak önceliği olmalıdır* (Held'den aktaran Kaygusuz, 2014:35).

Westphalia ile beraber her ne kadar yüksek mahkemeler kurulmuş olsa da devletlerarasısı ilişkileri denetleyecek bir yüksek mahkeme kurulamamıştır. Devletleri ortaya çıkaran şey olan bireylerin feragati, devletlerde ortaya çıkmamış bu nedenle devlet üstü bir otorite kurulamamıştır. Bu durum, savaşların bitmemesine aksine daha fazla kayıplar veren savaşlara neden olmuştur. Bunlardan biri ise Birinci Dünya Savaşı'dır. 1914 yılında başlayan ve 1918'e kadar devam eden 4 yıllık bu savaşta yirmi milyona yakın insan ölmüştür.

Birinci Dünya Savaşı'nın barış görüşmeleri sırasında ABD Başkanı Woodrow Wilson'un bir ulus üstü birlik kurulması gerektiği yönündeki fikrini beyan ettiği *Wilson Prensipleri* olarak anılan 14 maddelik bildiri ile beraber uluslararası politikada

anarşinin önlenmesine yönelik ilk adım atılmış oldu. Her ne kadar Wilson amacına ulaşamamış olsa da attığı bu adımla beraber uluslararası politikada bugünü şekillendiren bir görüş belirttiği aşikârdır. Bugün Wilson'un bu adımı uluslararası ilişkiler teorilerinde liberalizmin –kimilerine göre idealizmin- temelini teşkil etmektedir. Wilson'un attığı bu adım sayesinde bugün halen varlığını sürdüren BM[8], uluslararası problemlere çözüm arayan –her ne kadar işlevselliği sorgulansa da- arabuluculuk faaliyetlerini yürüterek silahlı çatışmaların çıkmasını engelleyen yegâne uluslararası kurum olarak faaliyetlerine devam etmektedir.

4.bölümde anlatılacağı üzere siber güvenliğe büyük oranda ihtiyaç duyulmasının temel nedeni olan siber dünyanın anarşik yapısını anlamak adına anarşinin uluslararası politikada nasıl vücut bulduğu önemlidir. Ancak bunu yaparken az önce de belirtildiği üzere toplumsal teori açısından değil uluslararası ilişkiler teorilerinde anarşi kavramının nasıl işlendiği ele alınacaktır. Zira siber güvenliği sağlayacak olan bireylerin kendileri değil, onların eylemlerini hukuki yollarla kısıtlayacak olan devletler ve devlet-üstü yapılardır.

Uluslararası ilişkiler teorilerinde anarşi kavramı daha çok realizm ve liberalizmin çalışmalarında görülmektedir. Devletin ortaya çıkış sürecindeki ayrılıkların temeli olan bireyin doğası realizmde kötücül, liberalizmde ise iyimser kabul edilmektedir. Buna göre realizm; devletin ortaya çıkışını bir zorunluluk olarak görürken liberalizm ise gönüllülük esasına dayandırmaktadır. Sosyal inşacılık ise uluslararası ilişkilerde en önemli şeyin sosyal olduğunu sosyal ve uluslararası politikanın insan bilincinin dışında bir fiziksel varlık olmadığını iddia eder (Arı ve Kıran, 2011:50).

2.3.1. Realist Teoride Anarşizm

Uluslararası ilişkilerin en temel teorisi olarak kabul edilen realizm; kötümser yanıyla öne çıkmaktadır. Bireyin doğa halinde kötü olduğu, egemen devletler üzerinde nihai karar alıcı ve kararların devletleri bağlayıcı olduğu merkezi bir devlet-üstü iktidarın olmayışından ötürü uluslararası sistemi anarşik olarak nitelendirmesi (Ersoy, 2014:183) realizmin bu yönünü ortaya koymaktadır. En önemli temsilcisi olarak Thomas Hobbes'un gösterildiği realist düşüncede bireyler daima çıkarlarını maksimize etmek için mücadele etmekte ve bu mücadelesini güç ile sağlamaya

[8] Birleşmiş Milletler.

çalışmaktadır. Bu nedenle Hobbes *Leviathan* adlı kitabında devlet olmadan insanın yaşamı yalnız, fakir, mutsuz ve kısa olarak nitelendirmiştir. Bununla beraber Hobbes insanların doğuştan eşit olduğunu ancak bu eşitliğin bedensel ve zihinsel yetenekler açısından olduğunu, zihinsel ve fiziksel eşitliğin olmadığını ve bu nedenle birkaç zayıfın bir araya gelerek güçlü olanı öldürebileceğini belirtir ve bu nedenle eşitliğin güvensizlik ve çatışmayı doğurduğunu (Hobbes, 2018:99) ve çatışmanın var olmasından ötürü devletin var olması gerektiğini belirtmektedir. Devletin ortaya çıkışının nedeni olarak doğa halini öne süren Hobbes, devlet öncesi doğal yaşama döneminin kaos, kargaşa, genel savaş hali olduğunu bunun nedeni olarak da insanın doğası gereği vahşi, saldırgan ve bencil olduğunu belirtir (Uygun, 2019:13) ve böyle bir barbarlığın tek kaçış yolunun egemen ve rakipsiz bir gücün oluşturulmasında yani devletin oluşturulmasında görmektedir (Heywood, 2013:87). Robert Nozick ise Hobbes'un devletin varlığını meşrulaştırmak ve buna zemin hazırlamak adına anarşi durumunu öne çıkarttığını öne sürer (Nozick, 2015:10-11).

Özpek, gerçekten anarşinin devletin ortaya çıkışıyla son bulan bir durum olup olmadığını (Özpek, 2014:124) sorar ve Ponting'den verdiği örnek sonrasında devlet öncesi durumun devleti meşrulaştırmak için kurgulanan bir anti-ütopya olup olmadığını sorgular (Özpek, 2014:125). Ponting, *Yeni Bir Bakış Açısıyla Dünya Tarihi* kitabında MÖ 7500 civarında Ceriko (Eriha)'da 44 dönümlük bir arazide yaşayan 300 kişilik bir kabilenin bulunduğu yerleşim yerinde bulunan oldukça büyük bir duvarın başta savunma için yapıldığının düşünüldüğünü ancak daha sonra yeniden yapılan incelemelerle duvarın asıl amacının sel sularını önlemek olduğunu belirtir (Ponting, 2018:45). Ancak yine aynı kitabında Uruk döneminde elde edilen artı ürünün üretici olmayan ve yakın yerlerde olan gruptan hammadde temini için takas edildiğini ve toplum içinde uzmanlaşmanın artmasının daha büyük sınıflaşma ve dengesizlik yarattığını belirtmiştir ve bununla beraber dini otoritelerin ve dini otoriteler kadar din dışı liderlerin, orduların ve savaşların çıktığını (Ponting, 2018:64) belirten Ponting, kentin askeri ve siyasi otoritesi tarafından haraç ve vergi alındığını belirtir (Ponting, 2018:65). Bu durum Hobbes'un tezini destekler niteliktedir. Gözen, bunun yanı sıra realizmin kendi içinde kısır döngü içerdiğini iddia etmekte ve şöyle demektedir:

> *"Savaş niçin oluyor? Çünkü uluslararası anarşi var. Peki, anarşi niçin var? Çünkü egemen devletlerin güç mücadelesi var. Peki, egemenlik niçin var ve egemenler güç mücadelesi yapıyor? Çünkü insan doğasında kötülük ve rekabet var. Peki, insan veya devlet niye kötü? Çünkü kendini güvende hissetmiyor, mutlak güvenlik olamıyor, güvenlik çıkmazı var. Peki, güvenlik çıkmazı önlenemez mi? Önlenemez çünkü uluslararası anarşi var…"* (Gözen, 2014:84).

Burada dikkat çeken şey; sanki realizmin bilerek bir kısır döngü içerisine sokulduğudur. Savaşın var olmasının nedeninin uluslararası anarşi olduğu savı tam olarak doğru değildir. Zira Waltz, doğa durumunun savaş hali olduğunu ancak burada kastedilenin savaşların durmadan meydana gelmesi değil, kuvvet kullanıp kullanılmayacağına her devletin tek başına karar vermesiyle savaşın her an çıkabileceği olduğudur (Waltz, 2015:129). Egemen devletlerin güç mücadelesi içinde olduğu doğru, hatta Hobbes Leviathan kitabında bunun insanın fiziksel ve zihinsel olarak eşit olmamasına bağlamaktadır. Ancak egemen güç mücadelesi anarşinin sonucu değil nedenidir. Bunun yanı sıra güç mücadelesi egemen devletler arasında değil doğa halindeki insanlar arasındadır. Bireylerin bir araya gelerek belirli haklarından feragat ederek oluşturdukları devlet, güç mücadelesinden ziyade hayatta kalabilme uğraşısı içerisindedir. Herkesin herkesle gerçekleştirdiği bir sözleşmeyle devlet düzenine geçişin sağlanacağını belirten Hobbes, ölüm korkusu ve daha iyi bir yaşam arzusunun insanları rasyonel davranmaya iteceğini ve herkesin her şey üzerindeki haklarından vazgeçerek güçlerini birleştirip bir iktidar yaratacaklarını belirtir (Uygun, 2019:200). Joseph Nye de uluslararası sistemin bilardo topları gibi devletlerin sonu gelmez bir çatışmalar silsilesi içinde birbirlerine çarpa çarpa yuvalandığı bir bilardo masası olmadığını, uluslararası sistemin sosyal olduğunu belirtir (Nye ve Welch, 2015:63).

Doğa halinin anarşik olduğu ve bu nedenle kaosun hâkim olduğu realist görüşe Waltz, devletin varlığının da kaos yaratabileceğini öne sürerek itiraz eder. Ulusal trajediler listesi adı altında Napolyon'un yaptığı savaşları örnek veren Waltz, bunun yanı sıra Çin'de 1851'de başlayıp 13 yıl süren ve yaklaşık 20 milyon insanın ölmesine neden olan iç savaşını ve Amerikan iç savaşını örnek gösterir ve eğer anarşi kaosla, yakıp yıkmayla ve ölümle özdeşleştirilirse, o zaman anarşi ile devlet arasındaki ayrım bize fazla bir şey anlatmaz der (Waltz, 2015:130). Bunun yanı sıra Waltz, devletin meşru kuvvet kullanımında ulusal sistemle uluslararası sistem arasında bir ayrıma giderek devletin uluslararası alanda kuvvet kullanma tekelini elinde bulundurmadığını, sadece ulusal sınırları içerisinde bunu yapmaya muktedir olduğunu belirterek uluslararası sistemin *self-help*[9] sistemi olduğunu öne sürer (Waltz, 2015:131).

[9] Kendine yardım olarak da çevrilen bu terim bazı yerlerde öz-yardım olarak da kullanılmaktadır. Karışıklığa sebebiyet vermemek adına öz-yardım şekliyle kullanılacaktır.

Siber dünyaya realist bir bakış açısıyla yaklaşmak konunun tam olarak anlaşılamamasına neden olmaktadır. Zira realist teorinin merkez olarak aldığı şey devlettir. Ancak siber dünyanın herhangi merkezinde devlet yoktur. Bunun dışında realist açıdan bakacak olursak, Stuxnet anlaşılamaz bir hâl alır. Zira Stuxnet saldırısı kimin tarafından yapıldığı halen netlik kazanmamış bir saldırıdır. Her ne kadar ABD ve İsrail ile ilgili şüpheler olsa da kesin olarak suçlanabilecek kanıt bulunmamaktadır. Stuxnet saldırısı siber dünyada meydana gelen bu zamana kadarki en karmaşık saldırıdır. Bu saldırı ile dışarıdan erişim sağlanamayan bir yere -ki bu yer bir nükleer santral- bir saldırı ilk kez düzenlenmiş ve böylelikle siber dünyada erişilemeyecek yer algısı ortadan kalkmıştır. Buradan da anlaşılacağı üzere siber dünyanın merkezinde devletler değil işletim sistemleri ve ona bağlı sistemler vardır.

2.3.2. Liberal Teoride Anarşizm

Liberalizm deyince akla gelen ilk isim olan John Locke'a göre insanlar doğa halinde tam bir özgürlük ve eşitlik içerisindedir ve kimsenin kimseye bir üstünlüğü yoktur ancak bu otoritesizlik bir başıboşluk anlamına gelmez zira doğa durumundaki özgürlük doğa yasasının çerçevesini çizdiği bir özgürlüktür (Locke'dan aktaran Uygun, 2019:213). Hobbes'un doğa halinde insanların her şeyi yapabilme imkanına doğa yasasıyla karşı çıkan Locke, aklın buyrukları olan doğa yasasının insan davranışlarını sınırlandırdığını söyler (Locke'dan aktaran Uygun, 2019:215). Ancak Locke, doğa yasasını ihlal eden birini ölçülü şekilde cezalandıracak bir otorite olmayışından ötürü bu cezalandırmayı herkesin yapması sonucunda zarar görenin intikam duygusu içerisinde olabilme ihtimalinden ötürü büyük sakıncalar doğabileceği, bu ölçüsüz cezaların barış durumunu bitirerek savaş durumuna geçilebileceği endişesiyle bir üst otorite olan devletin kurulmasını elzem görmüştür (Locke'dan aktaran Uygun, 2019:213-214). Rousseau ise düzenin bozulma nedeni olarak özel mülkiyetin çıkışını göstermiş ve zenginler ve fakirler arasında çıkan çatışmaların bir güvensizlik ortamı yarattığını ve zenginlerin, fakirlerin saldırısından korunmak için devleti kurduğunu iddia etmiştir (Rousseau'dan aktaran Uygun, 2019:231). Bu durumda Rousseau'ya göre devlet yalnızca zenginin mülkünü korumak için ortaya çıkmış bir yapıdır. Aynı zamanda bu anlayış devletin varoluş sebebinin şiddete, hırsızlığa ve dolandırıcılığa karşı korunması ve sözleşmelerin tatbik edilmesi işlevi ile sınırlı olan bir nevi gece bekçisi görüntüsü ortaya çıkarmaktadır (Nozick, 2015:57). Bu anlayış günümüz neoliberal anlayışıyla örtüşmektedir. 1989 sonrası

ortaya çıkan ve kökeninde Milton Friedman'ın kurucusu olduğu Chicago Okulu bulunan bu anlayışa göre devlet yalnızca bir gece bekçisi görevi görmeli bunun dışındaki tüm alanlar özel sektöre bırakılmalıydı. Her ne kadar liberalizmin başlangıcında devletin sınırlandırılması yer alsa da bu kadar küçültülmesi düşünülmüş bir şey değildi. Zira böylesi bir durum ekonomik olarak zayıf olanları elimine etmeye yönelik bir tutum olarak algılanmaktadır. Bunun yanı sıra neo-liberalizmin uygulamada özgürlükçü olarak görülen ancak sonrasında baskıcı rejimlere birçok kere teyit edilmiştir. Örneğin; ABD'de Reagan, Birleşik Krallık'ta Thatcher, Şili'de Pinochet ve Türkiye'de de Özal hükümetleri ekonomik istikrar ve özgürlük ile geldikleri iktidarlarını otoriterleşmeyle perçinlemişlerdir. Bugün halen daha bazı ülkelerde uygulanmaya çalışılan bu model esasında 2008 krizi ile beraber çöküşe geçmiştir.

Devletin varlığı konusunda liberal görüşteki en büyük değişim; klasik liberalizmde devletin iş birliğine dayalı varlığı ön planda iken neoliberalizmle beraber bu gece bekçisi devlet modeline dönüşmüştür. Klasik liberaller devletin müdahalesi konusunda endişeli ve ihtiyatlı iken neoliberaller devlet ile piyasalar arasındaki tüm bağları kaldırmayı devleti bir hakem olarak bırakmayı hedeflemektedirler (Ongur ve Yavçan, 2014:281). Neoliberalizmin klasik liberalizmden bu ayrışmasındaki temel etken devletin ortaya çıkışındaki ekonomik etkenlerdir. Malların serbest piyasada mübadelesi sayesinde insanların tutkuları, ekonomik çıkarlarının maksimizasyonu vasıtasıyla yani şiddetin, piyasanın barışçıl ortamında ekonomik kazanç peşinde koşmakla ilgili bir şey diye yüceltmesiyle dizginleneceği (Carnoy, 2015:35) görüşüyle ortaya çıkan liberalizm, 1989'daki New Orleans kasırgası ile beraber tüm dünyaya Milton Friedman'ın öncüsü olduğu Chicago Okulu ile birlikte yayılan devletin minimalize edilmesi fikri ile farklı bir boyuta evrildi. Bu evriliş; devletin giderek küçüldüğü ve devletlerin öz-yardımı bireyler nezdine indirdiği bir hal almaya başladı. Öyle ki devlet yalnızca sınır güvenliğinden sorumlu bir gece bekçisi durumuna büründü ve bunu yaparken kullandığı ordunun bile özel sektöre devredilmesi gibi uçuk bir görüş ortaya çıktı. Hal böyle olunca devletin varlığı sorgulanır hale geldi. Devlet yalnızca sınır güvenliğini sağlamak için mi kuruldu sorusu akıllara geldi. Baktığımızda bunun doğru olmadığı ve devletin doğa halinde yaşanan anarşiyi ortadan kaldırmak adına bireylerin belli özgürlüklerinden feragat ederek bir üst otorite olan devleti kurduğu genel kabul görür bir savdır. Ortaya çıkan bu neoliberalist görüş Rousseau'yu

haklı çıkarmaktadır. Devletin ortaya çıkışını zenginlerin yoksulların saldırısından korunmak ve mülklerini korumak olduğunu belirten Rousseau'ya göre devletin ve kanunların görünürde herkesin can ve mal güvenliğini sağladığı ancak asıl varlık nedeninin güçlülerin korunması olduğunu yineliyordu ve bunun aynı zamanda çok katı eşitsizliklerin egemen olduğu bir düzen olarak ortaya çıktığını belirtiyordu (Locke'dan aktaran Uygun, 2019:231).

Locke; devletin iktidarının sınırlı olduğunu ve doğa yasasının insan davranışlarını sınırlandırdığını belirtir (Uygun, 2019:204). Buna rağmen devletin can ve mal özgürlüğüne müdahale etmesi durumuna karşılık bireylerin devlete karşı direnme hakkının olduğunu belirtir. Bu yola başvurmak için önce yasal yolların denenmesinin gerekli olduğunu belirten Locke, eğer bu yollar tükenmişse direnme hakkına başvurulabileceğini belirtir (Locke'dan aktaran Uygun, 2019:216). Bunun yanı sıra Locke 'un insan davranışlarını doğal hakların belirlediği görüşüne Nozick, diğerlerinin çerçevelenmiş bölgenin sınırlarını aşması ya da tecavüz etmesi yasak mıdır ya da sınırı geçilen bir kişiye tazminat verilmesi şartıyla bu tür eylemlerde bulunma hakkı var mıdır sorusunu sorar (Nozick, 2015:94). Nozick bunu daha da ileri taşıyarak *eğer kurbanların zararları karşılanıyorsa, bir eylem, neden izin verilmek yerine yasaklansın?* der ve şu örneği verir:

*Y'nin birinin evinin önünde kayarak kolunu kırdığını ve gördüğü zararın karşılığında dava açıp 2000 dolar aldığını öğrenen X, şunu düşünebilir: "Y ne kadar şanslı ki, başına böyle bir şey geldi: 2000 dolar için kolunu kırmaya değer; bu miktar gördüğü zararı fazlasıyla karşılar." Fakat herhangi birinin gelip de X'e, "önümüzdeki ay senin kolunu kırabilirim ve eğer bunu yaparsam sana 2000 dolar tazminat veririm; fakat eğer kırmaktan vazgeçersem sana hiçbir şey vermem" derse, bu durumda X, ne kadar çok para kazanacağını mı düşünür? Yoksa sürekli endişe içinde, duyduğu en ufak sesten irkilerek, ani bir saldırıdan ya da zarardan korkarak mı dolaşmaya başlar? Bu durum, saldırıları yasaklamak için bir sebep teşkil eder mi? (*Nozick, 2015:104).

Bunun yanı sıra Nozick gerçekleştiğinde tam tazminat alacağımızı bildiğimiz halde bazı şeylerden korktuğumuzu ve bu korkuyu bertaraf etmek maksadıyla bu tür eylemlerin yasaklandığını ve cezalar getirildiğini ancak bunun eylemlerin gerçekleşmeyeceğini garanti etmeyeceğini ve insanların kendilerini emniyette hissetmelerini sağlamadığını belirtir (Nozick, 2015:104). Siber dünyada da buna benzer bir durum mevcuttur. Sistemlere sızarak zarar vermeleri ve karşılığında tazminat ödemeleri belki gördükleri zararları karşılar ancak hiç kimse tazminat karşılığı sistemlerine zarar verilmesini kabul etmez nitekim etse bile sisteme zararın verilip verilmediği veya ne zaman verileceği kol kırılması gibi gözle görülür bir olay

değildir. Bununla beraber siber dünyada kolunuzu kırmış olsalar bile bunu fark edememeniz yüksek ihtimaldir.

Nozick 'in bahsettiği yasaklama ve cezanın uluslararası alandaki karşılığı devletler üstü bir oluşumla sağlanabilir. Bunun öncülü ise Woodrow Wilson'dur. Birinci Dünya Savaşı sonrası ulus üstü bir yapı kurmayı hedefleyen Wilson yayınladığı 14 maddelik kendi adıyla anılan Wilson Prensipleri ile bunun temellerini atar. Bu prensipler içinden uluslararası ilişkiler bakımından en önemlisi şu maddedir:

Madde 14. Özel antlaşmalarla, küçük, büyük tüm devletlerin siyasi bağımsızlıklarını ve toprak bütünlüklerini karşılıklı olarak güvence altına alacak bir uluslar birliği kurulmalıdır (Kaymaz, 2007:151).

Wilson'un yayınladığı ve idealizmin temellerini oluşturan bu bildiride yer alan ve yukarıda verilen madde ulus üstü bir mekanizma kurma düşüncesini tüm dünyaya yaymıştır. Wilson'un en büyük hayali olan ve adeta kendisiyle özdeşleşen uluslar birliği fikri bu maddede yer almaktadır. İş birliğinin en önemli göstergesi olan bu birlik, o dönem imzalanan gizli antlaşmaları reddederek diplomasinin açıktan yürütülmesi gerektiği inancıyla bağımsız her devletin şeffaf bir zeminde ilişkilerini yürütmesini amaçlamaktadır. Kâğıt üzerinde kalan antlaşmaların yeterli olmayacağını bilen Wilson, antlaşmaları uygulamak ve kuralları uygulamak için örgüte ve sıkı kurallara ihtiyaç olduğu kanaatindeydi (Nye ve Welch, 2015:151). Günümüz BM Antlaşması'nın temelini oluşturan bu bildiride her türlü saldırı yasa dışı ilan edilerek devletlerin her an saldırıya maruz kalma korkusunu ortadan kaldırmak amaçlanmıştır. Bunun yanı sıra böyle bir durum gerçekleştiğinde birliğin tüm üyelerinin saldırgan devlete karşı ittifak oluşturarak saldırganı bu tutumundan vazgeçirecektir. Ortak güvenlik doktrini, devletlerin güçlü bir koalisyon oluşturarak saldırıdan caydırmaya çalışması ve başarısız olduğunda güç kullanacak olması bakımından güç dengesi politikasıyla benzerdir (Nye ve Welch, 2015:152). Nye ortak güvenlik ile güç dengesi arasında üç fark olduğunu belirtir ve bunu şu şekilde açıklar:

"Birincisi, ortak güvenlik yaklaşımı bir devletin kapasitesi yerine saldırgan politikalarına odaklanıyordu. Bu, fazla güçlenmeye başlayan herhangi bir devlete karşı ittifakların kurulduğu, yani devletlerin kapasitesine odaklanılan güç dengesi politikasıyla karşıtlık oluşturuyordu. İkincisi, koalisyonların önceden kurulduğu bir güç dengesi sistemindekinin tersine, bir ortak güvenlik sisteminde koalisyonlar önceden belirlenemiyordu, zira hangi devletin saldırgan olacağı bilinmiyordu. Bununla birlikte, saldırı bir kez gerçekleştiğinde, tüm devletler saldırgana karşı birleşiyordu. Üçüncüsü, ortak güvenlik tarafsızların ya da hazıra konacakların olmadığı küresel ve evrensel bir sistem olarak tasarlanmıştı. Çok fazla ülke tarafsız olursa, iyiler koalisyonu zayıf görünebilir ve koalisyonun saldırganı caydırma ya da cezalandırma kabiliyetini azaltabilirdi." (Nye ve Welch, 2015:152).

Nye'ın ortak güvenlik konusundaki en büyük endişesi tüm ülkelerin veto hakkının olması durumudur. Uygulamanın oldukça zor olacağı bu durumda

uygulamanın nasıl yapılacağı ve ne tür yaptırım uygulanacağı kararı devletlerin kendilerine bırakılmıştı ve bunu yaparken devletlerin herhangi bir üst otoritesi olmaması devletleri bazı politikaya uymaya mecbur edebileceği dünya hükümetine doğru atılmış bir adım olmadığı yönünde bir değerlendirmede bulunur ve bu durumun anarşik devletler sisteminin sonu olmadığını, bilakis, uluslararası sistemin kurallara uymayan üyelerini devletlerin topluca disiplin altına alma çabası olduğu yönünde bir değerlendirmede bulunur (Nye ve Welch, 2015:153).

Sarf edilen bunca emeğe rağmen Milletler Cemiyeti başarısızlıkla sonuçlandı. Bunun nedenlerinin başında o günlerde böyle bir cemiyet kuracak yeterli tecrübenin olmadığı gösterilebilir. Bunun yanı sıra o günlerde uluslararası hukuk iç hukuktan daha az ilgi gördü. Zira devletler bir üst kurul tarafından kısıtlanmayı o günlerde kabul etmediler ve bunun için gönüllü olmaları gerektiğini savundular ve ne yazık ki gönüllü devlet sayısı oldukça azdı. Bu aslında anarşiye bir nevi gönüllülük olarak görülebilir. Bir üst otorite kurarak mevcut anarşik yapının ortadan kaldırılmasına yönelik gerçekleştirilen bu adımın kendilerini kısıtlayacağını düşünerek reddetmek o dönemki siyasilerin ileri görüşlü olmadığını göstermektedir. Zira İkinci Dünya Savaşı'nın çıkışında Milletler Cemiyeti'nin aktif bir tutum sergileyememesinden ötürü böylesi büyük bir yıkıma sebebiyet verdiği yaygın bir görüştür. Eğer Milletler Cemiyeti'nin ortak güvenlik konusunda karar alma yetkisinin o dönem bugünkü gibi bir Güvenlik Konseyi ile belirlenmesi yönünde bir adım atmış ve diğer devletler de buna destek vermiş olsalardı belki daha savaşın başında Avusturya'yı ilhak etmesi sonucunda çıkartılabilecek bir ortak kararla Hitler durdurabilirdi. Ancak bu olmadı. Zira o dönemin şartlarına bakıldığında çok kutuplu bir sistem hâkimdi ve üst kurulu oluşturacak devletlerin kim olacağı bile belirsizdi. Bununla beraber Nye'ın da bahsettiği üzere saldırgan olabilecek devletin hangisi olduğu bilinmiyordu. Acı bir tecrübeyle bu da öğrenilmiş oldu. İkinci Dünya Savaşı sonrasında ABD daha önce yaptığı hatayı bu sefer yapmadı ve Birleşmiş Milletler'in kuruluşunda daha aktif rol oynadı ve iç politikada aldığı darbeyi bu sefer almadı. Böylelikle en azından bugüne kadar yeni bir küresel savaşın çıkması engellenmiş oldu. Her ne kadar birçok kere savaşın eşiğine gelinmiş olsa da -Küba Krizi bunun en iyi örneğidir- savaştan ziyade barış seçeneği ön plana çıktı. Bunun nedeni de o dönemin siyasilerinin İkinci Dünya Savaşı sırasında yaşanan katliamın Birinci Dünya Savaşı'ndan çok daha fazla olması ve gelişen teknoloji ile beraber konvansiyonel silahların yerini yavaş yavaş kitle imha

silahlarına bırakması ve bu nedenle çıkabilecek bir üçüncü Dünya Savaşı'nda daha öncekilere nazaran daha fazla insan öleceği tehlikesidir.

Her iki teorinin bakış açısına ortak bir değerlendirme yapacak olursak, realizmin insanın doğası konusunda fikrini doğrulanmakla beraber anarşinin yok edilemeyeceği görüşü BM ile yanılgıya uğramıştır. Bununla beraber liberalizmin görüşüne göre devletin birey üzerindeki rolü düşünüldüğünde devletin neoliberalizmde olduğu gibi sadece gece bekçisi olması görüşü dördüncü bölümde anlatılacak olan siber güvenlik karşısında devleti birçok noktada çaresiz bırakacaktır. İlaveten klasik realizmdeki gibi devletin Hobbes'un deyimiyle bir Leaviathan'a dönüşmesi durumunda insan haklarının ihlaline yol açabileceği bir durumun ortaya çıkması tehlikesi de göz önünde bulundurulmalıdır. Zira siber dünyada devletin tamamıyla kontrolü ele alması ve her alanda etkili olmaya çalışması bireylerin davranışlarını takibe varan neticelere sebebiyet vermekle beraber özel hayatın gizliliğinin de ihlaline neden olabilir. Bu alanda devletlerin ve devlet-üstü kuruluşların –özellikle BM ve NATO- önlem alırken insan haklarına halel getirmemeye özen göstermeleri ve bu konuda şeffaf olmaları gerekmektedir.

Stuxnet saldırısı üzerinden liberalizmi değerlendirecek olursak; bu saldırı ile önem kazanan şey iş birliğinin yalnızca devletler ve uluslararası örgütlerle sınırlı kalmaması gerektiğidir. Zira saldırının kesin olarak bir devlet tarafından yapıldığı netlik kazanmış değildir. Her ne kadar güvenlik uzmanları böylesi bir kodun sıradan kişi veya kişilerce yazılamayacağı yönünde görüş beyan etmiş olsalar da sonuç olarak bir siber saldırının kişi veya kişilerce yapılabileceği ve yapılan bu saldırıların etkilerinin yıkıcı olabileceği bilinmektedir. Bu durum bizlere şunu göstermektedir: artık aktör sayısı bir veya birkaç değil yedi milyara kadar çıkabilmektedir.

2.3.3 Sosyal İnşacılık'da Anarşizm

Waltz'un anarşi görüşüne paralel olarak bir görüş Alexander Wendt'ten gelir. Uluslararası ilişkilerde anarşi sorunsalını inşacı bir yaklaşımla ele alan Wendt bir sosyal inşa olarak anarşinin farklı kültürel yapılarını fark etmiştir (Gözen, 2014:27). Wendt, rasyonalist ana akımın maddi unsurlara önem verdiğini, inşacılığın fikir, norm ve kimliklerin birim davranışlarını etkilemedeki önemini vurgulayarak, anarşinin devletlerin kaderi olmadığını ve anarşinin barışçıl toplumsal yaşam biçimlerine dönüşebileceğini öne sürer (Yalvaç, 2014:50). Wendt meşhur makalesi *Anarşi Devletler Ne Anlıyorsa Odur* 'da öz-yardımın anarşiden doğmadığını bunun süreçten

kaynaklandığını ileri sürer (Wendt, 2013:7). Bunun yanı sıra Wendt, makalesinin adında da belirttiği gibi anarşinin devletlerin ondan ne anlıyorsa o olduğunu ileri sürer ve anarşi devletlerin onu nasıl adlandırdığını beyan eder (Wendt, 2013:7). Devletlerin düşmanlarına karşı farklı, dostlarına karşı farklı davrandığını çünkü düşmanların tehdit edici olduğunu ancak dostların öyle olmadığını ileri sürerek İngiliz füzelerinin ABD için Sovyet füzelerine göre farklı bir öneme sahip olması gibi ABD'nin askeri gücünün de benzer şekilde Kanada için farklı Küba için farklı bir öneme sahip olduğunu belirtir (Wendt, 2013:9). Hareketlerimizi şekillendiren yapıları meydana getiren şeyin kolektif anlamlar olduğunu belirten Wendt, toplumun bir üniversitenin ne demek olduğunu unutması durumunda profesörlerin ve öğrencilerin güçlerinin ve uygulamalarının varlıklarını yitireceği gibi Amerika ve Sovyet Rusya artık düşman olmadıklarına karar verirlerse soğuk savaşın biteceğini söyler (Wendt, 2013:10). Bu bize Hobbes'un doğa halinde savaşın sürekli olduğu görüşüne şüpheyle yaklaşmamıza neden olur. Zira Hobbes'a göre doğa halinde sürekli bir savaş var ancak eğer iki taraf arasında Wendt 'in belirttiği gibi böyle bir olay gerçekleşmesi durumunda savaş biter ve anarşi son bulur. Buradaki bir diğer ayrım anarşi kavramına Hobbes'un, Waltz ve Wendt' in farklı yaklaştıklarıdır. Hobbes, anarşi ile kaosu eş tutarken Wendt ve Waltz ayrı tutmuşlardır. Waltz ve Wendt, anarşinin var olduğunu kabul etmekle beraber bunun böyle devam edeceğini kabullenir ancak kaos durumunun daimî olduğunu reddeder. Bu görüşe paralel bir görüş de Nye'den gelmektedir. Nye; anarşinin hükümetsizlik demek olduğunu ama ille de kaos demek olmadığını belirtir ve bazı önemli seçimlerin yeterince düzen sağlayan temel uygulamalar ve kurumların var olduğunu bunların uluslararası hukuk ve uluslararası kuruluşlar olduğunu belirtir (Nye ve Welch, 2015:36). Bunun yanı sıra Nye, neden devletlerin de bireyler gibi bir süper Leviathan oluşturmadığını sorduğunda Hobbes'un devletler arasındaki güç dengesinin belirli bir düzen sağladığını ve devletlerin düşmanca bir potansiyel savaş pozisyonunda dursalar bile uyruklarının günlük çabalarına destek olacaklarını belirtir (Nye ve Welch, 2015:36). Hobbes'un bu söylemi bize liberalizmi çağrıştırmaktadır. Bir önceki başlıkta da incelendiği üzere liberaller uluslararası anarşinin iş birliği ile aşılabileceğini savunurlar ve savaş halinin mütemadiyen devam ettiği görüşüne karşı dururlar. Ancak Hobbes'un bu söylemine Nye itiraz etmektedir. Nye, modern devletler sisteminin beş yüzyıllık tarihinde güç dengesinin korunmadığını ve çıkan savaşların hemen hemen hepsinde en az bir büyük gücün savaşa dâhil olduğunu ve bu savaşların büyük, genel savaşlar olduğunu belirtir (Nye ve Welch, 2015:109). Bunun yanı sıra Nye, gücü,

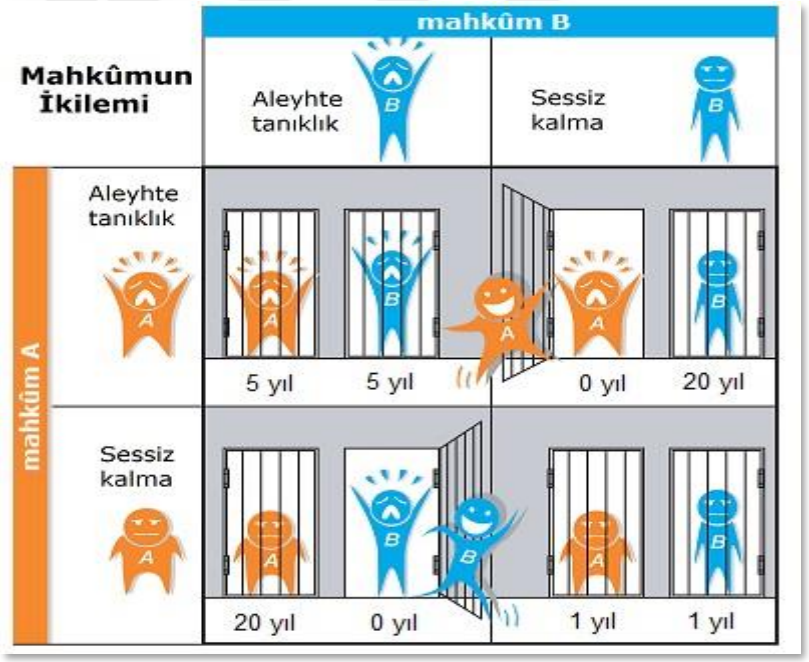
barışı korumak için değil bağımsızlıklarını korumak için dengelediğini söyler ve güç dengesinin ayrı ayrı devletlerden oluşan anarşik sistemin korunmasına yardımcı olduğunu iddia ederek bu iddiasını 18. yüzyılın sonunda Polonya'nın parçalanması ve 1939'da Hitler'in yeniden taksim örneğini vererek güç dengesinin barışı ve her zaman her devletin bağımsızlığını korumadığını ancak anarşik devlet sistemini koruduğunu iddia eder (Nye ve Welch, 2015:109).

Waltz'un da bu yöndeki açıklamasına Wendt devletlerin hâlihazırda sahip olduklarını koruyarak hayatta kalmayı istemektedir ancak ya biri hem hayatta kalabiliyor hem de diğerlerini fethedebiliyorsa (Wendt, 2016:138) diye itiraz eder. Oppenheimer'ın *fetih kuramı* da buna paraleldir. Oppenheimer'a göre devlet örgütlenmesinin temelinde, tahrip gücü yüksek yarı göçebe kabilelerin, savaşma gücü düşük ve tarımla uğraşan yerleşik toplulukların işgal ettikleri topraklarında kalıcı olabilme ve idareleri altına aldıkları insanlardan düzenli itaat ve kazanç elde edebilme isteği yatmaktadır (Oppenheimer'dan aktaran Özpek, 2014:126). Altı aşamada (Seçilmiş ve Türkoğlu, 2006:87) varlığını tamamlayan devletin Oppenheimer'a göre yerleşik toplulukların topraklarını işgal edebilmelerindeki temel sebep olarak nedenli-nedensiz sürekli savaşlar gösterilmiş ve bu savaşlar neticesinde meydana gelen kavga, yağma, soygun ve tecavüz gibi şiddet içerikli olayların devamı neticesinde köylülerin direncinin kırıldığı belirtilmiştir (Oppenheimer'dan aktaran Seçilmiş ve Türkoğlu, 2006:87-88). Oppenheimer'in bu görüşü bize Fransız antropolog Pierre Clastes'in *Devlete Karşı Toplum* eserini hatırlatmaktadır. Oppenheimer gibi Clartes da toplumun ilkel aşamadan başlayarak modernleşmeye doğru giden düz bir çizgi üzerinde ilerleyeceğini ve günün birinde mutlaka devleti kuracağını çünkü devletin tüm toplumların kaderi olduğunu iddia eder (Clartes'dan aktaran Uygun, 2019:14-15). Uygun ise buna karşı çıkarak günümüzde halen varlıklarını sürdüren ilkel toplumları örnek göstermektedir (Uygun, 2019:15).

Realist teoriye göre her ne kadar devlet, anarşinin getirdiği bir zorunluluk olarak lanse edilse de gerçekten de böyle midir bilinmez ancak bilinen şey; siber dünya için bir üst otoritenin ne kadar gerekli olduğudur. Zira üst otoritesiz bir siber dünyada her an yeni bir kaos çıkabilmektedir. Yeni bir saldırının ne zaman geleceği kimse tarafından bilinmiyor iken ve saldırılara karşı savunmanın ne kadar yeterli olduğu belli değil iken olası bir saldırının zararının ne kadar olabileceği kimse tarafından kestirilememektedir. Her gün yapılan milyonlarca siber saldırıya karşı koymaya

çalışan kullanıcılar Wendt'in bahsettiği öz-yardımla sistemlerini ayakta tutmaya çalışmaktadır. Bunun nedeni ise siber dünyayı kontrol altında tutan bir gücün olmayışıdır. Keza böyle bir güç inşa edilebilir mi o bile bir tartışma konusudur. 4. bölümde de değinileceği üzere siber dünya; kontrolü sağlamanın neredeyse imkânsız olduğu bir dünyadır. Bunun nedeni ise siber dünyanın bizleri aldatmaya oldukça müsait olması ve önümüzdeki ekranları güvenmenin bazen imkânsız olduğudur. Nitekim tezin örnek olayı olan Stuxnet'te kontrol ekranları her şeyi normal gösterirken arka planda virüs oldukça hummalı bir çalışma ile santrifüjleri bozmuş ve sistemi aksatmıştır. Ancak yine de böyle bir olay engellenebilir miydi sorusuna ister istemez içimizden evet yanıtını vermekteyiz. Zira eğer İran'ın tesislerinin güvenliğini yeterince sağlayabilecek imkânı olsaydı belki de bu saldırıyı önceden önleyebilirdi. Ya da saldırıya uğradıktan sonra uluslararası bir üst otorite olaya el atmış olsaydı bugüne kadar diğer devletlerin de iştirakiyle bu olayın faili ya da failleri gün yüzüne çıkartılabilirdi. Ancak böyle bir otoritenin olmayışı ve devletlerin bu alandaki öz-yardımı ne yazık ki yeterli gelmemektedir. Bunun yanı sıra siber dünyanın kurucusu ve bugünkü hegemon gücü olarak kabul edilen ABD'nin İran'ın kendi enerjisini üretmesini sağlayabilecek nükleer santrallere "nükleer silah üretebilir" endişesiyle izin vermemesi ve küresel gücünü kullanarak İran'a sürekli olarak ambargo uygulaması bizlere Wendt'in *Anarşi Devletler Ne Anlıyorsa Odur*'u doğrular niteliktedir. Zira dünyada nükleer silaha sahip resmi olarak saptanan 9 ülke bulunmaktayken bunlardan yalnızca Kuzey Kore ABD için tehdit unsuru oluşturmakla beraber bir de İran'ın nükleer silah edinebilecek kapasitede olması ABD için tehdit unsurudur. Onun dışındaki 8 ülke ABD için bir tehdit unsuru olarak görülmemektedir. Sovyet Rusya'nın ABD ile imzaladığı Start I ve Start II antlaşmaları ile ve Sovyetlerin dağılması ile Soğuk Savaş'ın bitmiş olması göz önüne alındığında bu bize anarşinin aslında devletlerin eylemlere yükledikleri kolektif anlamlardan kaynaklandığını göstermektedir. ABD'nin İran konusundaki bu endişesinin kesin olup olmadığı bilinmemektedir. Bunu anlamanın yolu ise diplomasiden geçmektedir. Ancak İran ile ABD arasındaki diplomatik ilişkiler 1979 Devrimi ile beraber askıya alınmış durumdadır. Birbirlerinden yalnızca istihbarat ve müttefikler aracılığıyla uzaktan uzağa diyalog kuran ABD ve İran arasındaki bu iletişimsizlik karmaşaya neden olmaktadır. Bu karmaşa bizi mahkûmun ikilemi teorisine götürmektedir. Merrill Flood ve Melvin Dresher tarafından 1950'lerde ortaya çıkarılan bu oyun; gözaltına alınan iki kişinin birbirleriyle iletişimi olmadan her ikisine de aynı teklifin götürülmesi

ve sonucunda kimin neye karar vereceğine dayanan bir oyundur. Burada amaç iş birliğinin mümkün olup olmadığı ve bireylerin davranışlarının ne yöne seyredeceğidir. 1979 yılında Robert Axelrod'un bir bilgisayar programı aracılığıyla yaptığı test sonucu iş birliğinin her zaman için en karlı yol olduğu ortaya çıkmıştır. Bunun yanı sıra *Nash Dengesi* olarak adlandırılan ve bireylerin diğer bireylerin davranışlarını da göz önünde bulundurarak varabileceği en iyi karara varmalarının bir yolu olan bu dengeye ulaşmak ancak güvene dayalı iş birliği ile mümkün görünmektedir. Hepsinden önemlisi *Pareto Optimumu* olarak adlandırılan bireylerin alabileceği en kârlı karar olan her ikisinin de inkâr etmesine dayalı hamleleri gerçekleşme olasılığı en düşük ihtimal olarak gözükmektedir. Zira inkâr edenin, diğerinin itiraf etmesi sonucu yirmi yıl hapis yatacağı gerçeği bulunmaktadır. Bu nedenle böylesi bir karara varmak için her iki tarafında kesin olarak birbirlerine güven duymaları ve mutlak iş birliği sağlamaları gerekmektedir.



Tablo 1: Mahkûmun İkilemi Oyunu

Kaynak: www.liberteryen.org (Erişim 21.01.2020)

Güven ve güvene dayalı olarak gerçekleştirilen iş birliği realist görüşte pek yer almamaktadır. Zira realistler insanın doğasının kötü olmasından ötürü sürekli olarak çıkar çatışmasının yaşandığını bunun da iş birliğini imkânsız hale getirdiğini düşünmektedirler. Realistlerin bu kötümser yaklaşımına karşılık liberaller bunun

gerçekleşebilir olduğunu savunmaktadır. Bunun nedeni olarak da liberaller insanın doğasının iyi olduğuna anarşinin neden olduğu kaosun iş birliği ile aşılabileceğini düşünmektedirler.

2.4. Bölüm Değerlendirmesi

Bu bölüm ışığında görülmektedir ki, siber dünya realist veya liberalist teori ışığında incelenmesi siber dünyanın tam olarak anlaşılamamasına neden olmaktadır. Zira siber dünya, doğası gereği yalnızca devleti değil veyahut yalnızca bireyi değil, tüm dünyayı birey, toplum ve devlet bütününde tek bir çatı altında toplamayı başarmış bir dünyadır. Bu nedenledir ki siber dünyaya realist teori ışığında yaklaşmak siber dünyada hakimiyetin devlette olduğu izlenimini vermektedir. Ancak siber dünyanın her ne kadar da kurucusu ve hegemonyası olarak ABD kabul edilse de hâkim olduğunu iddia edemeyiz. Zira siber dünyada güç; bu dünyanın dilleri olan yazılım dillerine en iyi hâkim olanlarındır. Aynı şekilde liberal teori ışığında incelendiğinde ise özgürlükler adı altında bazı kişi veya grupların devletleri ve küresel barışı tehlikeye atabileceği birçok kez görülmüştür. Gerek Wikileaks gerekse Snowden olayları bunlara birer örnektir. Bu nedenledir ki siber dünya onu oluşturan sosyal yapı ışığında incelenmeli ve yorumlanmalıdır.

3.ULUSLARARASI HUKUK

3.1. Giriş

Tezde bu bölüme yer verilmesinin nedeni konunun çözümünde uluslararası hukuka duyulan ihtiyaçtır. Ancak bunu yapmadan önce siber saldırıların mevcut uluslararası hukuk çerçevesinde ne tür bir yer edindiğine değinmekte fayda var. Zira bu bölümde saldırı ve meşru müdafaaya ilişkin verilen üç örnek dava siber saldırıların yorumlanabilmesine ışık tutabilecek örneklerdir. Bu davalarda kullanılan ve bugün uluslararası hukukta karmaşaya neden olan vukuu muhakkak ve vukuu muhtemel kavramları siber dünya için de tehdit oluşturmaktadır. Zira siber dünyada vukuu muhtemel durumları tespit etmek mümkün değildir. Böyle bir düşünce ile yapılacak bir siber saldırının sonuçlarının nerelere varabileceği ise muallaktadır. Nitekim Stuxnet saldırısı da yaygın kanıya göre İran'ın nükleer silah üretme ihtimaline karşı düzenlenmiş bir saldırıdır. Ancak İran'ın nükleer silah üretebilecek kapasitede olmadığı herkes tarafından bilinmektedir. İran'a yapılan bu saldırı ikinci bir Irak vakasına dönüşmüştür. Böyle bir olayın bir daha yaşanmaması için gerekli önlemler uluslararası hukuk çerçevesinde alınmalıdır. Ancak ondan önce uluslararası hukukun geçmişten bugüne evrimi ve Stuxnet'in anlaşılmasında yardımcı olacak üç davaya değinmek gerekmektedir.

1648 ile ortaya çıkan ulus-devlet ve uluslararası hukuk, yaşamın bundan sonraki kısmında insanların daha barışçıl bir şekilde hayatlarını devam ettirmesi ve savaş olasılığını düşürmeyi ve hatta sonsuz barışı hedeflemiştir. Her ne kadar bu başarılı olamamışsa da günümüz dünyası belli bir düzene oturmuş bulunmaktadır. Bu düzene kadar geçen süreç, bireylerin ve devletlerin yaşadıkları tecrübelerin bileşkesini oluşturmaktadır. Bu bileşke sayesinde günümüzde ilişkiler daha profesyonel bir şekilde ilerlemektedir.

İkinci Dünya Savaşı sonrasın kurulan Birleşmiş Milletler ve bu örgütün temeli olan Birleşmiş Milletler Antlaşması, uluslararası ilişkilerdeki düzeyi belirlemede önemli bir unsurdur. Bu antlaşmaya göre, devletlerin toprak bütünlüğü korunmuş ve bütünlüğüne halel getirecek eylemler yasaklanmıştır. Ancak günümüz dünyasında bu antlaşmanın yetersiz olduğu görülmektedir. Zira antlaşma metnindeki maddelerin günümüz problemlerine cevap veremediği durumlarda maddelerin yorumlanarak

karara varılması karmaşaya yol açmıştır. Bu karmaşanın en temel nedeni yorumlayıcı devletlerdir. Karara lehine etki edici şekilde maddeleri yorumlayanlar genellikle güçlü devletlerdir. Aşağıda detaylandırılacağı üzere devletlerarasındaki bu anlaşmazlıklar artık maddelerden çok yorumlar ve geçmiş zamanlarda alınan BM kararları ile giderilmeye çalışılmaktadır.

Tezin temelini oluşturan siber dünya ve bu dünyadan alınan örnek olay olan Stuxnet ise BM Antlaşması'ndaki bu yetersizliği göstermektedir. Siber dünyada saldırı veya savunmanın ne olduğu ve nasıl yapılacağı net değildir. Bunun nedeni içinde yaşadığımız dünyanın siber dünya ile kıyaslanamamasından kaynaklanmaktadır. Reel dünyada yapılacaklar zaman ve mekân kısıtlamasında iken, siber dünyada yapılacak herhangi bir şey için böyle bir kısıtlama pek söz konusu değildir.

Bu bölümde, uluslararası hukukun ortaya çıkışı ve bugüne geliş süreci anlatılacaktır. Bölümde incelenecek örnek olayların siber dünyada ne gibi yansımaları olabileceği tartışılacak ve uluslararası hukuka duyulan ihtiyaç belirtilecektir.

3.2. Uluslararası Hukukun Ortaya Çıkışı

Devletlerin ortaya çıkışı sonrası birbirleriyle olan ilişkileri, iç ilişkilerindeki farklılık nedeniyle ortak bir zemine oturtulması zaman almıştır. İç hukukta kullandıkları argümanlar ve olaylara bakışı her devletin farklı olmasından mütevellit birbirleriyle olan ilişkilerinde ortak bir hukuki yolun oluşması Roma Dönemi'nde gerçekleşmiştir. Uluslararası hukukun kurucusu olarak kabul edilen Roma İmparatorluğu, iç hukukta oldukça gelişmiş bir yapıya sahip olmasından ötürü uluslararası hukukun ortaya çıkışında önemli ilkelere imza atmıştır. *Ius Civite* olarak bilinen ve örf ve adetlerden oluşan ve yalnızca sivillere uygulanan bir hukuk olarak M.Ö. altıncı yüzyıla kadar geçerliydi. Yabancılara karşı uygulanamaması nedeniyle yeni bir hukuk arayışına girilen Roma'da *Ius Gentium* olarak adlandırılan Roma vatandaşlarının yanı sıra yabancılara da uygulanabilen bir hukuk geliştirildi (Ceylan, 2004:3). Böylelikle Roma vatandaşı olan ve olmayanların arasındaki uyuşmazlıklara çözüm getirmesi sebebiyle uluslararası hukukun da temelleri atışmış oldu.

Kanunlar ve örf ve adetlerle yönetilen bütün kavimler, kısmen kendi hukuklarından ve kısmen de bütün insanlar için ortak olan hukuktan yararlanırlar; çünkü bir kavmin kendisi için oluşturduğu hukuk, o devlet vatandaşlarına özgü bir hukuktur ve ius civite, yani vatandaşlarına uygulanan hukuk olarak anılır; buna karşılık, doğal akıl gereğince bütün insanlara ve bütün insanlar tarafından aynı şekilde uyulan hukuk ise ius gentium, yani bütün kavimlere ortak olan hukuk anılır. Roma vatandaşları

da kısmen kendi hukukunu kısmen de bütün insanlara ortak olan hukuku kullanır." (Zulueta'dan aktaran Karakocalı, 2016:20).

Ünlü Roma hukukçusu Gaius'un meşhur eseri olan Institutiones'da tanımladığı ve orijinali Latince olan ve 1946 yılında Francis de Zulueta tarafından İngilizce'ye çevrilen eserde yaptığı bu tanımlamadan da anlaşıldığı üzere *Ius Gentium* uluslararası hukukun temel taşı olarak kabul edilebilir.

Modern anlamda uluslararası hukukun temeli olarak 1648 tarihli Westphalia Antlaşması gösterilmektedir. Bu antlaşma ile beraber feodal düzenin yıkılması ve uluslararası bir toplumun inşası ile laik bir düzende ulusların bir arada yaşama ilkesi esas alınmıştır. Westphalia'nın örnek teşkil etmesi sebebiyle bundan sonra uluslararası alanda çıkan tüm uyuşmazlıklar -savaşlar dahil- bir araya gelerek yapılan konferanslarla, toplantılarla çözümlenmeye çalışılmış ve belli oranda başarı sağlanmıştır. Bugün gelinen noktada BM'nin etkin rol oynayabilmesi bu tecrübelere dayanmaktadır. Her ne kadar barış sonsuza kadar sağlanamamış olsa da savaşların azaltılmasında ve çoğu zaman daha henüz savaş çıkmadan yapılan görüşmelerle olası bir savaşın önlenebildiği su götürmez bir gerçektir.

3.3 Uluslararası Barışın Koruyucusu Olarak Birleşmiş Milletler

Birinci Dünya Savaşı sırasında Wilson Prensipleri olarak bilinen bildiride ABD Başkanı Woodrow Wilson barışın sağlanması amacıyla ulus üstü bir organizasyon oluşturulması teklifinde bulunmuştur ve 1919 yılında Milletler Cemiyeti kurulmuştur. Ancak 1920 yılında yapılan başkanlık seçimini Cumhuriyetçi aday Warren G. Harding'in kazanması ile beraber izolasyonist politikaya dönülmesi neticesinde MC'ye üyeliği gerçekleşememiştir. Diğer yandan Sovyetler 'in de kuruluşun dışında bırakıldığından ötürü MC, Avrupa içinde bir güvenlik sistemi kurmayı amaçlayan iki ülke olan İngiltere ve Fransa'nın eline kaldı (Sander, 2013:35). Ancak Fransa bu örgütü Almanya'ya karşı bir garantör kurum, barış antlaşmalarının koruyucusu ve gözden geçirilmelerinin önleyicisi bir güç olarak görmekteyken İngiltere, cemiyeti Almanya ve öbür mağlup devletleri de kapsayacak bir yeni uzlaşma sisteminin merkezi olarak görüyordu (Hasgüler ve Uludağ, 2012:73-74). Cemiyet o zamanlar şimdiki gibi küresel tecrübelere sahip olmamasından ötürü işleyiş konusunda ciddi aksaklıklara neden olmuş ve bunun sonucu olarak İkinci Dünya Savaşı ortaya çıkmıştır. Cemiyetin iki başı olarak görülebilecek ülkeler olan İngiltere ve Fransa'nın

Almanya'ya karşı tutumu Hitler gibi bir diktatörün yükselmesinin adeta önünü açmış ve Hitler'in diplomatik manevralarıyla Avrupa'nın istila edilmesine yol açmıştır. Hitler, özellikle "*kendi kaderini tayin*" hakkı ile Polonya'yı ve Çekoslovakya'yı istila etmiş ve adeta düşmanını kendi silahıyla vurmuştur. Bunu yaparken Avrupa'nın karşı koymamasının temel nedeni yeni bir savaşın çıkmasını istememeleri ve buna bağlı olarak uyguladıkları *yatıştırma politikası*dır. Düşman bir ülkeye taviz vererek tatmin etmek (Roskin ve Berry, 2014:114) olarak tanımlanan bu politikanın mimarı olan Chamberlain'in aynı zamanda siyasi hayatında kapanmayacak yaralar açmasına neden olmuştur. Hitler gibi bir diktatörün giderek hem yerelde hem de küresel ölçekte güçlenmesi neticesinde güç dengesini bozmasının önüne ne yazık ki geçilememiş ve üstüne üstlük düzenlediği harekatlara ses çıkarmayarak savaşa girmeme isteği ve işgal edilen toprakların savaşmaya değmeyeceği yönündeki görüşü ile toprakların Hitler yönetimine bırakılması adeta istediğini yapma fırsatını vermiştir. Oysa ki Wilson, kurduğu bu örgütün barış ve refah getirmesini ummuş ancak pratikte karşılığını alamamıştır.

Milletler Cemiyeti'nin Birinci Dünya Savaşı tecrübesiyle kurulmasına karşılık barışı ancak 20 yıl koruyabilmiş olması büyük hayal kırıklığı yarattı. Cumhuriyetçilerin izolasyonist politikayı benimsemesinin faturasının Japonya'nın Pearl Harbor saldırısı ile kesilmiş olması sonucu ABD Thomas Jefferson'ın *manifest destiny*[10]sine dönmesini sağladı. Savaş sonucunda başta yaptığı hayatı yapmama konusunda kararlı olan ABD, dizginleri eline alarak -Hiroşima ve Nagazaki'ye atılan atom bombalarının bunda payı büyük- uluslararası sistemi yeniden inşa etmeye koyuldu ve Birleşmiş Milletler kuruldu. Birleşmiş Milletler ifadesi ilk olarak Roosevelt tarafından teklif edilmiş ve 1 Ocak 1942 tarihli Birleşmiş Milletler Bildirisinde kullanılmıştır (Gündüz, 2015:107). Resmi olarak 24 Ekim 1945'te kurulan BM, halihazırda 193 ülkenin üye olduğu bir organizasyona dönüşmüştür.

Birleşmiş Milletler' in amaçları arasında en önemli olanı uluslararası barış ve güvenliğin sağlanmasıdır. Bunu hayata geçirmek için en çok kullanılan yol BM Antlaşması'nın 2. maddesidir. BM Antlaşması'nın 2. maddesi gereği kuvvet kullanmak yasaklanmıştır. Ancak bunun istisnasını yine aynı antlaşmanın 51. maddesi oluşturmaktadır. Meşru müdafaayı kapsayan bu maddenin nasıl kullanılacağı ve ne

[10] Açık yazgı olarak Türkçe' ye çevrilen bu terime göre; ABD dünyanın kurtarıcısıdır ve bu görev O'na Tanrı tarafından bahşedilmiştir. ABD, yayılmacı politikanın meşruiyetini bu politikaya bağlamaktadır.

ölçüde kullanılacağı ise yoruma açık bırakılmıştır. Bu tezin ana arterlerinden birini bu iki madde oluşturmaktadır. Kuvvet kullanma yasağı ve bunun istisnası kapsamında devletlerin meşru müdafaa hakkının muğlaklığı sebebiyle devletler arası anlaşmazlıklar bugün had safhaya ulaştı. Bunun yanı sıra siber dünya gibi oldukça yeni ve her geçen gün hızla büyüyen bir alanda gerçekleştirilen saldırıların hukuki boyutu bu iki madde arasında git-gel yaşamaktadır.

3.4. Kuvvet Kullanma Yasağı

Devletlerin kuvvet kullanması için haklı sebeplerinin olması fikri Antik Yunan ve Roma'ya dayanmaktadır (Beyoğlu, 2018:22). Uluslararası hukukta haklı sebep üzerine çalışmaları ile bilinen Hugo Grotius savaşı haklı gösteren nedenleri; bizim olan bir şeyi savunma, bize borçlu olan bir şeyi elde etmeye çalışma, cezalandırma (Grotius, 2011:74) olarak belirtmiştir. Bunun dışında canını korumak üzere savaşa girişilebileceğini belirten Grotius, bu savaşın ancak haksız bir saldırıda bulunana karşı söz konusu olabileceğini, kaçınılmaz ve kesin olması gerektiğini yalnız böyle bir tehlikenin var sayılmasının yeterli olmadığını belirterek şu ifadelere yer verir:

> *Tehlikenin kaçınılmaz ve zaman bakımından önlenemez bir kesinlikte olması gerekir. Saldıran, bizi öldürme niyetini açıkça ortaya koyarcasına silahına davranmışsa, şüphesiz böyle bir suç işlemine karşı durulabilir; bunu ben de kabul ederim. Şu var ki, nesnel şeylerde olduğu gibi, moral konularda da azıcık olsun boyutu olmayan bir nokta da pek bulunamaz. Ancak, kimilerinin yaptığı gibi, kendi canına karşı herhangi bir tehlike yaratan kimseyi, ondan önce davranarak, öldürme hakkını tanıyanlar hem çok yanılmaktadır hem de başkalarını yanıltmaktadır* (Grotius, 2011:75).

Grotius' un bu ifadeleri ilerleyen yerlerde değinilecek olan ve siber saldırılarda ABD'nin ısrarla savunduğu önleyici meşru müdafaa konusunda da fikrini net bir şekilde göstermektedir. Yalnız bunu değil 2003 yılında Irak'a yönelik düzenlediği saldırılarda gerekçe olarak kitle imha silahlarını göstermesi hususunda ise Grotius şöyle demiştir:

> *Bu yazarların bir başka görüşüne de katılmamaktayım. Bunlar şöyle demektedirler: Kendilerine karşı savaş açılması için haklı nedenler yaratanların, bu savaşta kendilerini savunmaları da haklıdır; çünkü, bu yazarlara göre, işlenmiş bir haksızlığın öcünü alırken bu haksızlıkla orantılı davranmakla yetinecek pek az kimse vardır. Oysa, kesin olarak bilinmeyen bir şeyden korku duymak, zorlama yollarına başvurma hakkını vermez; nasıl ki, çok ağır bir cezaya çarptırılma korkusu, bir suçluya da kendisini kamu yöneticisinin buyruğu uyarınca kovuşturan görevlilere karşı direnme hakkını vermez* (Grotius, 2011: 77-78).

BM Antlaşması'nın 2/4 maddesi kuvvet kullanmayı kesin olarak yasaklamaktadır. Kuruluş felsefesinde uluslararası barış ve güvenlik olan BM, yaşanan

acı tecrübelere istinaden bu konu üzerinde özellikle durmaktadır. Ancak bu maddenin istisnası 51. maddedir. Madde şu şekildedir:

> *Bu Antlaşmanın hiçbir hükmü, Birleşmiş Milletler üyeleri tarafından birinin silahlı saldırıya hedef olması dahilinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyelerin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildiridir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez (*İnhak, 2020).

Bu maddede tezin kilit noktalarından birini oluşturan şey "silahlı saldırı" dır. Siber saldırıların birer silahlı saldırı olarak nitelendirilip nitelendirilemeyeceği halen daha üzerinde mutabık kalınamamış bir konudur. BM Genel Kurulu tarafından 14 Aralık 1974 tarihinde kabul edilen 3314 sayılı kararda saldırı şu şekilde tanımlanmaktadır: "Saldırganlık; bir devletin başka bir devletin egemenliğine, toprak bütünlüğüne veya politik bağımsızlığına karşı veya bu tanımda belirtilen Birleşmiş Milletler Şartı ile tutarsız herhangi bir şeklide silahlı kuvvet kullanılmasıdır" (Undocs, 2020). Ancak bu tanım devletleri bağlayıcı değildir. Siber saldırılar bazı uzmanlar tarafından silahlı saldırı olarak kabul edilmekteyken, bazıları tarafından silahlı saldırı olarak kabul edilmemektedir. Michael N. Schmitt'e göre "Tüm silahlı saldırılar kuvvet kullanımıdır ancak tüm kuvvet kullanımları silahlı saldırı değildir" (Schmitt' ten aktaran Çifci, 2017:112). Schmitt'e göre saldırının kuvvet içerdiğini anlamak için 8 kriter önermiştir (Schmitt, 2017:334-335-336):

1. Ciddiyet (severity)
2. İvedilik (immediacy)
3. Doğrudan olma (directness)
4. Yayılabilirlik (invasiveness)
5. Etkilerin ölçülebilirliği (measurability of effect)
6. Askeri karakter (military character)
7. Devlet katılımı (state involment)
8. Karineye dayalı yasallık (presumptive legality).

Schmitt'e göre siber saldırıların kuvvet kullanma olarak nitelendirilebilmesi için fiziksel hasara neden olması gerekmektedir (Schmitt, 2017:334). Bunun dışında Schmitt, tuş vuruşlarını izlemekle örneklendirdiği siber casusluğun, casusluğun uluslararası hukukta doğrudan bir yasaklanma durumu olmadığını bu nedenle bir kuvvet kullanımı olarak görülmesinin olası olmadığını belirtir (Schmitt, 2007:335).

Gerçek şu ki, birincisi siber dünyada fiziksel hasara neden olma durumu gerçek hayattaki gibi fiziksel zararla eşdeğer durumda değildir. Bir yerin bombalanması sonucu verilen fiziksel zarar gözle görülür ve ölçülebilirdir. Ancak siber dünyada verilen fiziksel zararlar etki süresi bakımından bazen ani bazen de yıllar alan bir süreçtir. Bu tamamıyla saldırıyı gerçekleştirenin amacına uygunluğuyla alakalı bir durumdur. Örneğin; bir sabotaj saldırısı düzenlemek için ani bir saldırı ve sonuçlarını da ani şekilde görmek mümkündür. Ancak tezin örnek olayı olan Stuxnet gibi saldırılarda böyle bir beklenti söz konusu değildir. Sızma işleminin gerçekleştirilmesi sonrası uygun zamana kadar sistemde kalma, fark edilmeme ve yayılabildiği kadar yayılma amaçlanabilir. Böyle bir saldırı Schmitt'e göre siber casusluk olarak görülmekte, bu da kuvvet olarak adlandırılamamaktadır. Schmitt' in bu yaklaşımı bu tarz saldırıların merkezi olan ABD'nin çıkarına uygun olacak sübjektif bir görüştür. Merkez olarak kabul edilmesinin nedeni sızma ve uzun yıllar orada kalması durumunun ABD'nin birçok saldırıda kullandığı bir teknik olduğu -özellikle yayınlanan Wikileaks belgeleri ve eski NSA çalışanı Edward Snowden'in açıklamaları- henüz kesin olarak ispatlanamamış ancak bu yönde ciddi ithamların bulunduğu bir durumdur.

Her iki tanımlamada da eksik olan şey siber dünyadaki karşılıklarıdır. Bir eylemin silahlı saldırı olarak tanımlanabilmesi için öncelikle silahın ne olduğunun bilinmesi gerekmektedir. Antlaşma çerçevesinde düşünüldüğünde silah olarak tanımlanmasa da kabul edilen görüş; geleneksel silah olarak bilinen konvansiyonel veya kitle imha silahlarıdır. Birebir orduların veya çeşitli grupların kullandıkları ateşli veya ateşsiz silahlardır. Siber dünyada bir silah bazen taşıyıcı bellek (USB, taşınabilir hard disk, hafıza kartı vs.), bazen de tıkladığımız herhangi bir şeyin içerisine gizlenmiş kodlar dizilimidir. Bu nedenle silahın tam olarak tanımlanabilmesi ve mevcut görüşlerin revize edilmesi gerekmektedir.

Ancak gelinen noktada BM, bu konuda oldukça pasif konumda durmaktadır. Zira BM'nin herhangi bir saldırı olayının gündeme gelmesi sonucu yapılan görüşmeler, oylamalar ve çıkarılan sonuçlar siyasi hamlelerle yapılmakta ve Güvenlik Konseyi'nin çıkarlarına aykırı olarak bir sonucun çıkmasına bir şekilde engel olunmaktadır. Bunun başını ise ABD çekmektedir. Kore savaşı ile başlayan süreçte, Körfez Savaşı ve ABD'nin Irak'a müdahalesine giden yolda alınan kararlar BM'nin ABD'nin amaçlarına hizmet ettiği yönünde eleştirilere neden olmuştur.

Irak'ın 1990 yılında Kuveyt'i işgali sonrası BM'de çıkartılan 660 sayılı karara göre Irak'ın kınanması istenmiş ve 1 Ağustos 1990 öncesi sınırlarına çekilmesi istenmiştir (Bozkurt, 2007:93). Ancak bu kararda 2/4'den bahsedilmemiştir. Bunun nedeni Kuveyt'in 51. madde gereği bir meşru müdafaa yoluna giderek Irak'a karşılık vermesi sonucu çıkacak bir bölge savaşının istenmemesidir. Nitekim böyle bir olay daha önce 6 Gün Savaşları'nda yaşanmış ve çatışma bir bölge savaşına dönüşmüştür. Saddam'ın bu kararı tanımaması üzerine 6 Ağustos 1990'da çıkartılan 661 sayılı karar ile Irak' yönelik genel ticaret yasağı konmuştur (Hürriyet, 2020a). Bu karara Enver Bozkurt şu itirazda bulunmuştur:

> *661 sayılı karar, sadece üye devletleri değil bütün devletlerin Irak ihracat ithalat ilişkilerini yasaklamaktadır. Halbuki 41. Maddeden, ambargonun sadece Birleşmiş Milletler üyesi devletlerce uygulanmasının istenebileceği anlamı çıkmaktadır. Burada Konsey, üye olmayan devletlere de bir yükümlülük getirmiştir (Bozkurt, 2007:100).*

Aslında bunun nedeni sorunun bölgesel değil küresel ölçekte olmasındandır. Kuveyt'e yapılan bir saldırı dünya petrol dengesini değiştirmekte bu da sorunu küresel hale getirmektedir. Nitekim alınan tüm kararlara rağmen Irak, Kuveyt'ten çekilmeyince BM tarafından 678 sayılı karar alınmıştır. Burada dikkat çeken nokta; Yemen'in bu karar hariç hepsinde çekimse oy kullanmış, bu kararda ise ret oyu kullanmış olmasıdır. Buradan da anlaşılıyor ki yapılan oylamalarda kullanılan oylar Eurovision Yarışması'nda olduğu gibi devletlerin birbirleriyle olan dostluk ve müttefiklikleriyle alakalıdır. Bu durum BM'ye olan güveni sarsmaktadır.

Ferdi meşru müdafaa hakkını Kuveyt'in kullanmadığını belirten Bozkurt, 7 Ağustos 1990'da Suudi Arabistan ile ABD arasında Irak'ın olası bir Suudi operasyonuna karşılık ABD'nin ülkesini savunmak için Arabistan'a gelmesi yönünde anlaşma yaptıklarını belirtir (Bozkurt, 2007:115). Böylelikle aslında ne BM'nin Irak'a müdahalesinin ne de Kore'ye müdahalesinin BM Antlaşması ile alakalı olmadığını, konunun petrol ve bölgesel mücadeleler uğruna hukukun alet edildiğini görmekteyiz. Halbuki, BM Antlaşması 2/4'ün ihlali sonucunda devletler bağımsız olarak 51. Maddeyi yürürlüğe sokarak ülkelerini savunabilmektedirler. Her ne kadar bunun şartını da BM belirlemiş olsa ve yapılan her faaliyetin raporunu istemiş olsa da devletlerin meşru müdafaa hakkı çerçevesinde topraklarını savunmaları meşrudur.

3.5. Meşru Müdafaa Hakkı

Kuvvet kullanma yasağının en büyük istisnası[11] olan meşru müdafaa hakkı Antlaşma'nın 51.maddesidir. Madde şu şekildedir:

"Bu Antlaşmanın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez." (İnhak, 2020)

Bu maddeye göre bir devletin kuvvet kullanımının meşru sayılabilmesi için "silahlı saldırı" altında olması gerekmektedir. Silahlı saldırı olarak ise BM'nin 1974 yılında yayınladığı "saldırının tanımı" yapılmış ve tanımın 3.maddesinde hangi fiillerin saldırı niteliği taşıdığı şu şekilde belirtilmiştir:

a- Bir Devletin silahlı kuvvetlerinin diğer bir devleti istila etmesi veya ona hücum etmesi veya ne kadar geçici olursa olsun, böyle bir istiladan veya hücumdan ileri gelen herhangi bir askeri işgal veya kuvvet yoluyla başka bir Devletin ülkesinin veya bir bölümünün ilhakı;

b- Bir devletin silahlı kuvvetlerinin, başka bir Devletin ülkesini bombardıman etmesi veya bir Devletin diğer bir devletin ülkesine karşı herhangi bir şekilde silah kullanması;

c- Bir Devletin liman veya kıyılarının diğer bir Devletin silahlı kuvvetleri tarafından abluka altına alınması;

d- Bir Devletin silahlı kuvvetleriyle başka bir Devletin kara, deniz veya hava kuvvetlerine veya deniz veya hava filolarına saldırması;

e- Bir Devletin başka bir Devlette sonuncusuyla yapılan bir anlaşmaya göre bulunan silahlı kuvvetlerinin o anlaşmada öngörülen hükümlere aykırı bir şekilde kullanılması veya bu silahlı kuvvetlerinin varlığının bu ülkede anlaşmanın sona ermesinden sonra da sürdürülmesi;

f- Ülkesini başka bir Devletin emrine veren bir Devletin, ülkesinin o Devlet tarafından üçüncü bir Devlete karşı saldırı amacıyla kullanılmasına izin vermesi;

g- Bir Devlet tarafından veya bir Devlet adına diğer bir devlete karşı yukarıda listesi verilen fiillere varan veya o ölçekte olan silahlı kuvvet fiillerini icra eden silahlı çetelerin, grupların, gayri nizami askerlerin veya paralı askerlerin gönderilmesi veya bu gibi fiillere önemli ölçüde karışılması (müdahil olunması)" (Gündüz, 2015:141-142).

Buradan da anlaşılacağı üzere saldırı silah kullanımının önemi vurgulanmış ancak silahın ne olduğu, nelerin silah sayıldığı konusu yoruma açık bırakılmıştır.

[11] Diğer istisnalar Antlaşma'nın 51, 53, 106, 107.maddeleri ile Güvenlik Konseyi ile alınan zorlayıcı tedbirlerdir ancak burada konu ile bağlantılı olmaması sebebiyle değinilmeyecektir.

Tanımın yapıldığı 1974 tarihini baz alacak olursak o günlerde kullanılan silahların konvansiyonel ve kitle imha olmaları sebebiyle bugün gelinen noktada siber alanda kullanılan silahların silah olarak sayılıp sayılamayacağı uzmanların yorumlamalarına bırakılmıştır. Bugün bu maddenin yorumlanmasında baz alınan 3 olay vardır. Bunlar; Caroline Olayı, Nikaragua Davası ve Osirak Reaktörü' nün Bombalanması Olayı 'dır.

3.5.1. Caroline Olayı

1837 yılında Kanada İsyanı sırasında meydana gelen (Gündüz, 2015:155) olayda hem Kanada hem de Kanada sınırına yakın ABD toprakları içerisinde örgütlenen isyancıların (Kedikli, 2005:29) bu sınır arasında bulunan Niagara nehri üzerinde bir ada olan Navy adasından İngiliz gemilerine saldırılarda bulunmuştur (Aydın, 2013:56). Bu saldırıları yaparken isyancılara destek veren Caroline isimli ABD gemisi İngilizler tarafından 29 Aralık gecesi bulunduğu Schlosser isimli limanda yakarak Nikaragua Şelalesi'nden aşağı atmıştır (Beyoğlu, 2018:100). Olayda iki ABD vatandaşı hayatını kaybetmiş (Beyoğlu, 2018:100) ve bir İngiliz tutuklanmıştır (Pirim, 2019:251). Olaydan sonra İngiltere Dışişleri Bakanı, İngiltere'nin meşru müdafaa ve kendini koruma hakkına dayanarak bu işlemi gerçekleştirdiğini söylemiştir (Kedikli, 2005:30). Bunun üzerine tarihe "Webster formulation" (Pirim, 2019:251) olarak geçen ve "ani, karşı konulmaz, başka bir araç seçimine ve düşünmeye imkân bırakmayan bir meşru müdafaa zaruretinin olduğunun" kanıtlanması (Taşdemir, 2006:80) ile ifade edilen bu formül Dışişleri Bakanı Daniel Webster tarafından kaleme alınan notada belirtilmiştir. Nota metni kısaca şu şekildedir:

"*Ani, karşı konulamaz, başka bir araç seçimine ve düşünmeye imkân bırakmayan bir meşru savunma zaruretini ispat etmek (Majesteleri' nin) Hükümeti'ne düşmektedir. Kanada yerel makamlarının, durumun vahametinin Amerikan topraklarına girmelerini gerektirecek olması dahilinde dahi makul olmayan ve aşırı olan bir şey yapmadıklarını ispatlamak da yine İngiliz hükümetine düşmektedir; zira meşru müdafaa zarureti ile haklı görülebilecek bir eylem, bu zaruret ile sınırlı olmalı ve kesinlikle bu kapsam dahilinde kalmalıdır. Caroline' in güvertesindeki kişiye ihtarda veya uyarıda bulunmanın mümkün olmadığı veya yararsız olduğu; gün ışığının beklenemeyeceği ispat edilmelidir: masum ile suçluyu ayırmanın mümkün olmayacağı; gemiye el koyma ve onu tutmanın yeterli olmayacağı, gemi limanda demirliyken, güvertesindeki silahsız kişiler uykudayken, gecenin karanlığında ona saldırmak, birkaçını öldürmek ve diğerlerini yaralamak, daha sonra akıntıya sürüklemek, onu yakmak ve gemide masum ile suçlunun bir arada olup olmayacağını veya canlı ile ölünün aynı yerde olup olmayacağını bilemeyecek kadar dikkatsiz davranmak ve insan hayatını korku ile dolduracak şekilde korkunç bir kadere sürüklemek için kaçınılmaz ve mevcut bir zaruretin olduğu da ispatlanmalıdır. Amerikan Hükümeti tüm bu şartların mevcut olduğuna inanmamaktadır…"* (Gündüz, 2015:155).

Bu notadan da anlaşıldığı üzere meşru müdafaa için kesin ve kabul edilebilir şartların sağlanması gerekmektedir. Ancak bu notada da belirtildiği üzere tüm ispat yükü meşru müdafaaya hakkı olduğunu iddia eden makama aittir. Siber alanda ise

kesin olsa dahi kabul edilebilirlik seviyesinde mutabakat sağlamada problemlerin yaşandığı bilinmektedir. Bunun dışında ispat yükünün tek bir devlete yani karşı tarafa ait olması adilane bir tavır olarak görülmesi pek mümkün görünmemektedir. Zira siber alan bir şeyleri ispat etmenin en zor olduğu alandır diğerlerine nazaran. Bunun sebebi alanın sanal bir ortam olması, saldırıyı yapanın izini kaybettirmesinin birçok yolu olması hatta tamamen anonim kimliklerle yapılabilmesi, saldırının izinin sürülebilmesini oldukça zorlaştırmaktadır. Böyle bir olayda ispat yükünün tek tarafa değil konsensüsle sağlanması gerekmektedir.

3.5.2. Nikaragua Davası

Bu dava 1962 yılında meydana gelen "Küba Krizi" (Sander, 2013:322) ile oldukça benzerdir. Nikaragua'da sağ tabanlı Somoza rejiminin solcu Sandinista devrimcileri tarafından yıkılması (Yılmaz ve Irk, 2015:156) sonucunda ABD, Küba'da gösterdiği tepkilerin benzerini burada da gösterdi. Anti-sosyalist gruplara silah ve para yardımı yapan ABD'nin yardımıyla Nikaragua'nın petrol tesislerine ve hava sahalarına saldırılar yapılması (Aydın, 2013:53) ve bu saldırıların başarısız olması sonrası Nikaragua Hükümeti Uluslararası Adalet Divanı'na (UAD) tazminat talebiyle başvurdu (Yılmaz ve Irk, 2015:156). Nikaragua, ABD'yi uluslararası teamüllere aykırı olduğunu düşündüğü suçlama iddialarına Gündüz şu şekilde yer vermektedir:

"*(1) Nikaragua'nın iç suları ve karasularına mayın dökmek, Nikaragua ticaret gemileriyle yabancı ticaret gemilerine zarar vermek ve Nikaragua'nın limanlarına, petrol tesislerine ve bir donanma üssüne saldırmak suretiyle kendisine karşı doğrudan güç kullanıldığını; (2) Sandinista hükümetini devirmek için savaşan Nikaragua gerillalarına yardım ettiğini ayrıca 1956 tarihli ABD-Nikaragua Dostluk, Ticaret ve Denizcilik Antlaşması'nı ihlal ettiğini ileri sürdü"* (Gündüz, 2015:156).

Bu dava ile ilgili alınan kararda kaynaklarda farklılıklar mevcuttur. Örneğin; Yılmaz ve Irk makalelerinde divan kararı ile ilgili şu satırlara yer vermektedir:

"*Nikaragua davasına ilişkin UAD kararına göre, devletin düzenli silahlı kuvvetlerin (ordu) gerçekleştirdiği sınır ötesi harekâtların yanı sıra, devlet tarafından bir başka devletin sınırına gönderilen ve benzeri ağırlıkta silahlı harekât gerçekleştiren düzensiz kuvvetlerin, grupların ve ücretli askerlerin eylemleri de "silahlı saldırı" olarak kabul edilmiş, sayılan bu durumlar karşısında devletin meşru müdafaa hakkı doğmuştur (IC),1986)"* (Yılmaz ve Irk, 2015:157).

Bunun dışında Gündüz ise kararı kısmi olarak aktardığı kitabında şu satırlara yer vermiştir:

"*195. Bireysel meşru müdafaa durumunda, bu hakkın kullanımı, ilgili devletin bir silahlı saldırının mağduru olmasına bağlıdır. Kolektif meşru müdafaaya başvurulması doğal olarak bu ihtiyacı ortadan kaldırmaz. Silahlı saldırı teşkil eden davranışların niteliği hakkında genel bir mutabakat oluşmuş gözükmektedir. Özellikle, silahlı bir saldırının sadece düzenli silahlı kuvvetlerin sınır ötesi harekâtını değil, ayrıca, "bir devletin aleyhine düzenli güçlerin ika edilebileceği ağırlıkta silahlı harekât ika eden silahlı grupların, düzensiz kuvvetlerin, ücretli askerlerin başka bir devlet tarafından veya onun adına gönderilmesini veya bu olaylara önemli ölçüde müdahale olunmasını" ihtiva ettiği*

genellikle kabul edilmektedir. 3314 (XXIX) sayılı Genel Kurul kararına ekli Saldırının Tanımının 3. maddesinin (g) paragrafında yer alan bu tarifin, uluslararası örf ve âdet hukukunu yansıttığı kabul edilebilir. Divan, örf ve âdet hukukundaki silahlı saldırı yasağının, bir devletin başka bir devletin ülkesine silahlı gruplar göndermesi olayına da uygulanabileceğini inkâr etmemektedir. Yeter ki böyle bir harekât, büyüklüğü ve etkileri itibariyle, düzenli silahlı güçler tarafından ika edildiği takdirde, sadece bir sınır olayı olarak değil, silahlı saldırı olarak nitelendirilebilsin. Ancak, Divan, "silahlı saldırı" kavramının sadece silahlı birliklerce ika edilen önemli büyüklüğe sahip eylemlerden ibaret olmadığı, asilere silah veya lojistik yahut başka tür destekler sağlamayı da kapsadığı yolundaki görüşü kabul etmemektedir. Bu tür yardımlar, tehdit ya da kuvvet kullanımı veya diğer devletlerin iç ya da dış işlerine müdahale olarak kabul edilebilir. Ayrıca, saldırıya uğradığı yolundaki görüşünü oluşturma ve beyan etmenin silahlı saldırının mağduru durumunda bulunan devlete düştüğü de aşikardır. Başka bir devlete durumu kendisini değerlendirmesi suretiyle kolektif meşru savunma yetkisini veren bir uluslararası teamül kuralı mevcut değildir." (Gündüz, 2015:157).

27 Haziran 1986 tarihli kararın 195. maddesini[12] doğrudan aktaran Gündüz'ün satırlarından da anlaşılacağı üzere başka bir devlete saldırı düzenlemek amacıyla "silah veya lojistik yahut başka tür destekler" sağlamasını silahlı saldırı olarak kabul etmemektedir. Paragrafta sözü edilen 3314 sayılı saldırının tanımının (g) maddesini hatırlayacak olursak "Bir Devlet tarafından veya bir Devlet adına diğer bir devlete karşı yukarıda listesi verilen fiillere varan veya o ölçekte olan silahlı kuvvet fiillerini icra eden silahlı çetelerin, grupların, gayri nizami askerlerin veya paralı askerlerin gönderilmesi veya bu gibi fiillere önemli ölçüde karışılması (müdahil olunması)" şeklindedir. Burada addedilen suç kabul edilmekle beraber Divan, kararında bunu "tehdit ya da kuvvet kullanımı veya diğer devletlerin iç ya da dış işlerine müdahale" olarak kabul etmektedir. Bunun yanı sıra Nikaragua Davası'ndan da hatırlanacağı üzere ispat yükü tamamen mağdur devletin yükü olarak görüldüğü tekrar edilmiştir. Oysa ki, saldırının tanımı açıktır ve yapılan bu eylemler tanıma göre "silahlı saldırı" olarak kabul edilmesi gereken bir hususdu. Bunun yanı sıra "büyüklüğü ve etkileri itibariyle, düzenli silahlı güçler tarafından ika edildiği takdirde" tanımı küçük ve düzensiz birliklerin düzenleyeceği saldırılar sonucunda onları destekleyen devletlerin sorumlu olmama tehlikesini beraberinde getirmektedir. Bunun yanı sıra yine aynı kararda ABD'nin mali yardımları "insani yardım" olarak görülmekte ve bunun uluslararası hukuka aykırı olmadığı beyan edilmektedir (Yılmaz ve Irk, 2015:157). ABD'nin 1979'da başlayan yardımları 1985 yılında yani karardan bir yıl öncesinde "kısıtladığının" beyan edildiği ve bunun dikkate alındığı da ayrıca karar metninin 242. paragrafında belirtilmiştir (ICJ,1986). Dava sonucunda ABD, tazminat ödemeye mahkûm edilmiş ancak Nikaragua'nın davadan vazgeçmesi sonucu dava düşmüştür (Sabah, 2020).

[12] Orijinal metin için bkz. https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (Erişim 25.05.2020)

Bu kararın belli başlı birkaç problemi doğurduğu aşikardır. Bunlardan ilk göze çarpanı "insani yardım" meselesidir. Türkiye'nin PKK ile mücadelesinde ABD'nin insani yardım adı altında PKK'nın uzantısı YPG'ye silah ve mühimmat gönderdiği hatta yalnızca ABD'nin değil birçok Avrupa ülkesinin bu yardımları gönderdiği bilinmektedir. Ancak Divanın verdiği kararda geçen bu insani yardım devletler arasındaki ilişkileri zedelemekte, müttefiklik gerekliliklerine uymamaktadır.

İkinci husus ise "pre-emptive" ve "preventive" olarak literatüre geçen ancak Türkçe olarak tam karşılıklarının bulunmadığı ve Taşdemir'in "vukuu muhakkak" ve "vukuu muhtemel" (Taşdemir, 2006:82) olarak çevirdiği 51. Maddenin geniş veya dar yorumlanması sonucu ortaya çıkan iki farklı görüştür. 20 Eylül 2002 yılında yani; Irak'a askerî harekât (20 Mart 2003) yapılmadan tam 6 ay önce dönemin ABD Başkanı George W. Bush tarafından yayınlanan ve kamuoyunda "Bush Doktrini" olarak geçen "Ulusal Güvenlik Stratejisi" isimli metinin temel dayanağı olan bu görüşün savunucularından biri Yoram Dinstein'dir. 1988 yılında yazdığı "War, Aggression and Self-Defence" kitabında bahsettiği üzere meşru müdafaanın kullanılması için ikna edici kanıtların olması halinde saldırıya geçilmese bile meşru müdafaa hakkının doğduğunu belirtmektedir (Dinstein' den aktaran Taşdemir, 2006:82). Bunun dışında vukuu muhtemel saldırı ise; gelecekte olabilecek herhangi bir saldırıyı, saldırganın böyle bir saldırıyı planladığı ya da başlatacak bir kapasiteye sahip olduğuna itimat gösterilecek bir neden olmasa bile, ortadan kaldırmak için kuvvet kullanılması (Ağır, 2016:85-86) olarak tanımlanmaktadır. Ancak böyle bir durumun ispatlanması neredeyse imkansızdır. Bunu bir örnekle açıklayacak olursak; diyelim ki karşıdan karşıya geçmek üzere ışıklarda bekleyen bir yaya olarak takım elbiseli, kravatlı, traşlı, dışarıdan bakıldığında toplumda yer edinmiş bir kişi imajı ortaya koyan biri ve belinde de ruhsatlı tabancası var. Bu kişiye "A" kişisi diyelim. Yolun karşı tarafında ise; A kişisi kadar bakımlı olmayan ve hatta belki de saçı sakalı birbirine karışmış, üzerine ziyadesiyle bol gelen bir takım elbise ve dışarıdan bakıldığında da iyi bir izlenim bırakmayan ancak onun da belinde ruhsatlı silahı olan bir kişi var. Bu kişiye de "B" kişisi diyelim. Rüzgârdan mütevellit B'nin bol gelen ceketi bir anlık havalanınca silahın kabzası gözükür ve B, nedeni bilinmeyen bir şekilde ani bir refleksle elini silahın kabzasını götürür. Bunu gören A, B'nin kendisini vuracağını düşünerek silahını çekip B'yi vurup orada öldürür. Peki şimdi ne olacak? A, henüz gerçekleşmemiş, ancak kendisinin deyimiyle "vukuu muhtemel" bir saldırıya karşı kendisini

savunduğunu iddia etmiş ve bunun meşru müdafaa olduğunu beyan etmiştir. Yapılan tahkikatta tanıkların ifadesi hiç şüphesiz A'yı doğrular niteliktedir. Zira A, "güvenilir" bir profil çizmekte iken ölen B kişisi "suça meyilli" bir görüntü sergilemektedir.

Burada da benzer bir durum söz konusudur. Gerek Nikaragua Davası gerekse birazdan bahsi geçecek olan Osirak Reaktörü 'nün Bombalanması olayı gerek bu ve buna benzer diğer davalarla da görüldüğü üzere görüntü olarak çizilen imaj suçun üstüne örtmede kullanılabilmektedir. Yalnızca uluslararası davalarda değil Türkiye'de işlenen kadın cinayetlerinde bile sanık sandalyesine oturan kişinin dış görünüşü, yargılamayı yapanların önünde olumlu bir imaj yakaladığından ötürü cezalarda indirme gidildiği, hatta beraat ettiği bile ne yazık ki birçok kez görülmüştür. Bu durumun uluslararası yansıması olan davalarda ise örneğin; Nikaragua Davası'nda sanık sandalyesinde olan ABD gerek uluslararası imajı gerekse nüfuzu bakımından adeta "sanık olamayacak" durumda görülmektedir. Oysaki, Nikaragua veya Irak veya İran profil olarak "potansiyel suçlu" olarak görülmekte bu da savunmalarını zorlaştırmaktadır. Zira Nikaragua'nın tazminat kazanması gerekirken davadan neden vazgeçtiği bilinmemekle beraber olası bir tazminat belki de ABD'nin uluslararası imajını sarsabilecekti. Ancak ABD'nin savunması ve Nikaragua'nın davadan vazgeçmesi Osirak Reaktörü'nün bombalanması için İsrail'e "yasal zemin" oluşturmuştur.

3.5.3 Osirak Reaktörü'nün Bombalanması

1981 yılında gerçekleştirilen saldırıda İsrail, Bağdat yakınlarında bulunan Osirak Nükleer Reaktörü'ne saldırı düzenlemiştir (Kedikli, 2005:63). Opera Operasyonu olarak tarihe geçen bu saldırıda İsrail, Irak'ın bu reaktörü kendilerini vuracak bir nükleer silah yapmak amacıyla inşa edildiğini iddia ederek bu saldırıyı gerçekleştirdi. Birleşmiş Milletler saldırıyı kınadı ve Irak'ın ülkelerinde nükleer gelişmeye hakkı olduğunu belirtti ve bunun yanı sıra İsrail'den Iraklıların zararlarının tazmin etmelerini istedi (Stanford, 2020). İsrail her ne kadar 51.maddeye dayanarak saldırıyı gerçekleştirdiğini söylese de BM nezdinde bu savunması bazı devletlerce kabul edilmemekle beraber, bazı devletlerce de kriterleri karşılamadığı kanaatini oluşturmuştur. Bunun dışında Richard Wilson reaktörün Fransız mühendis Yves Girard tarafından bomba yapmaya uygun olmayacak şekilde tasarlandığını ancak saldırı sonrasında bomba üzerinde çalışma yapmaya başlandığını belirtiyor (Theatlantic, 2020).

Bu üç olaydan da anlaşıldığı üzere; uluslararası hukukun uygulanması konusunda BM Antlaşması'nın imzalandığı tarih ile ilerleyen zamanlar arasındaki farklardan ötürü maddelerin -özellikle 2/4 ve 51. maddeler- farklı şekillerde yorumlanmasına bağlı olarak problemler yaşanmaktadır. Bu problemler uluslararası alanın anarşiye dönüşmesine neden olmaktadır. Bunun dışında hukuk sözü geçenlerin ve antlaşma metinlerini çıkarlarına uygun yorumlayanların tarafına kaymaya başlamıştır. Özellikle ABD ve İsrail'in BM Antlaşması'nı çıkarlarına uygun yorumlayabilmesi sonucunda devletlerin egemenlik haklarını bile ihlal edebileceğini göstermektedir. Antlaşma metninin muğlaklığı da buna zemin hazırlamaktadır. Gelişen teknoloji sonucu hayatın siber alana kaydığı şu dönemde bu anarşi giderek artmakta ve devletlerin denetlenebilirliğini zorlaştırmaktadır.

Yakın bir zamanda meydana gelen ve "Orchard Operasyonu" olarak bilinen olayda İsrail'in bu sefer de Suriye'deki El Kibar Tesisleri'ni vurması olayların siber alana taşındığı ilk olaylardan biridir. Siber güvenliğin ne kadar önemli olduğunun, en ufak bir dikkatsizliğin bile sonucu nerelere taşıyabileceğini ilk göstergeleri olan bu saldırı sonucunda uluslararası herhangi bir dava açılmamış hatta Suriyeli bir askeri sözcü olayla ilgili olarak "Hava savunma birimleri, herhangi bir insani veya maddi hasara neden olmaksızın ıssız alanlara bir miktar mühimmat bıraktıktan sonra onları terk etmeye zorladı" şeklinde beyanda bulunmuştur (Spiegel, 2020). Olayın nasıl vukuu bulduğunu ise Singer ve Friedman şu şekilde açıklamıştır:

"*2006'da Suriye Hükümeti'nden üst düzey bir yetkili Londra ziyareti esnasında dizüstü bilgisayarını otel odasında bıraktı. Dışarı çıktığında İsrail istihbarat örgütü Mossad'ın ajanları odasına girdi ve görüşmelerini izlemelerine izin veren bir Truva atını bilgisayarına yüklediler. Bu Suriyeliler için yeterince kötüydü.*

Yetkilinin dizüstü bilgisayarının hafızasında sakladığı resimleri de içeren dosyalar İsrailliler tarafından incelenmeye başlandığında, bir kişinin zayıf bir bilgisayar güvenliğinin daha ciddi sonuçlarının doğurduğu ortaya çıktı. Özellikle bir fotoğraf İsraillilerin dikkatini çekti. Mavi eşofmanlı bir Asyalı yanı başında bir Arap erkek ile Suriye çölünün ortasında duruyordu. Tehlikesiz olabilirdi ama Mossad daha sonra iki adamın kimliklerini Kuzey Kore nükleer programının liderlerinden biri olan Chon Chibu ve Suriye Atom Enerjisi Komisyonu Başkanı İbrahim Othman olarak tespit etti. İnşaat planları ve bölünebilir materyal üzerinde çalışmak için kullanılan bir çeşit borunun fotoğrafları gibi diğer belgelerler birleştirildiğinde İsrailliler dizüstü bilgisayarın bir atomik çalar saat olduğunu farkına vardı. Suriyeliler, Kuzey Kore'nin yardımıyla (Uluslararası Atom Enerjisi Kurumu'nun sonraki bir soruşturması İsrail'in şüphesini doğrulayacaktı) nükleer bir bombanın yapımında önemli bir adım olan plütonyum işlemek için El Kibar'da gizlice bir tesis inşa etmekteydi." (Singer ve Friedman, 2018:172-173).

Casusluk olarak atfedilecek bu operasyon bununla sınırlı kalması durumunda uluslararası hukuku ihlal etmediği yönünde yorumlara neden olabilirdi. Ancak saldırı

gerçekleştirilirken Suriye hava savunma sistemlerinin de hacklenmesi sonucunda İsrail uçaklarının radarlarda görülememesi egemenliğin doğrudan ihlalidir. Ancak, olayla ilgili Uluslararası Atom Enerjisi Kurumu dışında tahkikat yapan hiçbir kuruluşun olmaması nedeniyle konuyla alakalı net bir sonuca varılamamıştır.

Uluslararası hukukun mevcut düzeni yeterli gelemediği Antlaşma'nın imzalandığı tarihten itibaren kendini göstermektedir. O zamanlarda bile maddelerin açık ve net olmadığı, yoruma açık olduğu gözlemlenmiş ve bu durumda ihlal için arka kapıya neden olmuştur. Özellikle siber dünyanın bu kadar yaygınlaştığı şu zamanlarda yapılacak herhangi bir siber saldırının uluslararası hukukta karşılığının ne olacağı meçhuldür. Bu nedenle devletler bu tür mağduriyetlere karşı Waltz'un self-help sistemini kullanmak zorunda kalmıştır.

3.6. Bölüm Değerlendirmesi

Uluslararası hukuk, devletlerin kendi başlarına hareket etmelerini engelleyen, diğer devletlerin toprak bütünlüğünü korumayı hedefleyen bir organizasyondur. Devletler arasındaki herhangi bir anlaşmazlığı Waltz'un self-help kuramına bırakmak anarşiyi daha da körüklemek anlamına gelmektedir. Bu nedenle uluslararası hukuk gerek toplum nezdinde gerekse devletlerarası nezdinde ihtiyaç duyulan bir birimdir. Mevcut anarşinin etkilerini azaltmak ve siber dünyada var olan anarşinin reel dünyadaki anarşiyi körüklemesini ve yeni çatışmalara ve savaşlara sebebiyet vermesini engellemek amacıyla uluslararası hukuktaki bu açıklıkların giderilmesi gerekmektedir. Tüm bu anarşi ancak hukuk ile dizginlenebilir. Devlet öncesi dönemde olan anarşinin Waltz aksini iddia etmiş olsa da azalması hukuk sayesinde olmuştur. Yönetim şekli totaliter veya otoriter olan devletlerin kendi içlerinde yaşadıkları problem ve iktidarların haklına karşı uyguladıkları insani suçlar uluslararası hukukun gerekliliğini ve mevcudiyetine halel getirmez. Bu tezde uluslararası hukuka yer verilmesinin temel nedeni budur. Uluslararası hukuk olmadan siber dünyanın yalnızca uluslararası ilişkiler ve onun teorileri ışığında ele alınması sorunu anlamada yeterli olsa da çözüm konusunda bize bir şey sunmamaktadır.

4.SİBER GÜVENLİK

4.1. Giriş

Güvenlik, insanların temel önceliklerindendir. Bireyin veya devletin kendini güvende hissetmediği durumlarda başka bir işle meşgul olması düşünülemez. Antik çağlardan günümüze ise güvenlik algısında belirli değişimler gözlenmektedir. Can güvenliği en temel güvenlik sorunu olarak binlerce yıl zirvedeki yerini korurken günümüzde hukuk sayesinde bu güvenlik daha alt basamaklara kaymış ve yerini yenilerine bırakmıştır. Günümüzde ise en büyük sorunlardan biri siber güvenliktir. Giriş bölümünde de değinildiği üzere tüm bilgilerimizin ve özelimizin bulunduğu siber dünyada güvenliği sağlamak oldukça önemli hale gelmiştir. Bunun nedeni ise çalınmak için en çok uğraş verilen şeylerin başında kişisel bilgiler gelmektedir. Yaşam çalmaktan bilgi çalmaya evrilmiş olan günümüzde insanlar sahip oldukları bilgileri korumayı öncelik haline getirmiştir. Yalnızca bireyler değil siber dünyanın doğası gereği topluluklar ve devletler için de bilgi güvenliği öncelikli hale gelmiştir. Bu bölümde siber güvenliğin ne olduğu ve öneminin ne olduğu anlatılacaktır. Anarşinin, siber dünyaya yansıması ve uluslararası hukukun siber dünyaya ne kadar hâkim olduğu ve eksiklerinin neler olduğu anlatılacaktır. Tezin örnek olayı olan Stuxnet'in siber dünyada yaşanmış bir saldırı olduğu gerçeği doğrultusunda siber güvenliğin ne derece önemli olduğu okuyucunun bilgisine sunulacaktır.

4.2. Güvenlik Nedir?

Heywood güvenliği zarara karşı güvenli olma durumu, tehdit, sindirme ve şiddetten masun olma olarak tanımlar (Heywood, 2018:114). Birdişli ise, güvenliğin "yaşamı sürdürebilmek için gerekli olan tüm koşulları kapsayan çerçeve bir kavram" olduğunu belirtir ve Morgan ve Buzan'ın "sıhhat ya da statü gibi tanımlaması zor, analize gelmeyen" bir kavram olduğunu dolayısıyla güvenliği açıklama çabalarının ontolojiden başladığını belirtir ve kaygının olmadığı durum olarak açıklar (Birdişli, 2017: 25-26). Wolfers ise Lippman'ın "Bir ulus savaştan uzak kaldığı zamanlarda kendi temel değerlerini feda etmek zorunda kalmadığı müddetçe veya bir savaş halinde zafer kazanarak bu değerleri korumasını bildiği müddetçe güvenlidir." tanımına yer vererek bir ulusun güvenliğinin herhangi bir saldırı olasılığına karşı caydırıcılık kabiliyeti veya savaş halinde zafer kazanma kabiliyetine göre arttığını veya azaldığını ifade eder (Wolfers, 2017:46).

Güvenlik, insanlığın ilkel döneminden beri en önemli problemidir. Kendini güvende hissetme, Maslow'un ihtiyaçlar hiyerarşisinde fizyolojik ihtiyaçlardan sonra gelen ihtiyaçtır. İnsanın karnını doyurduktan sonra ilk işi sığınacak bir yer aramak ve geceyi hatta yaşamının ilerleyen dönemlerini orada geçirmeye elverişli bir yer bulmaktır. Daha da ötesi bulduğu yiyeceği herhangi bir yerde değil güvenli bir yerde yemeyi amaçlar. İlkel dönemde bu tür yerler dışarıdan saldırıya uğrama ihtimali nispeten daha düşük yerler olan ağaç kovukları veya ısınma konusunda daha elverişli olan mağaralardı. İlerleyen dönemlerde insanlar, ağaçlardan yaptıkları ahşap evleri bile yerden belli bir yükseğe inşa etmeye başladılar. Evlerin yerden yükseğe yapılmasının nedeni yılan, akrep vb. sürüngenlerin saldırılarından emin olma isteği yani güvenlik amaçlı idi.

Devletin inşası ile birlikte güvenlik artık devletin tekelinde toplanmış bir hal aldı. Devlet olarak tanımlanan bu organizasyon tüm sınırlar boyunca güvenliği bazı haklarını devraldığı vatandaşları adına sağlamaya başladı. Ancak güvenliği sağlamak için öncelikli olanın güçlü olmak olduğu görüldü. Zira güçsüz birinin kendini güvende hissetmesi pek mümkün değildi. Lippman'ın tanımladığı gibi savaştan uzak kalma ve olası savaş halinde ise zafer kazanabilmek için güçlü olmak gerekirdi. Peki güç nedir? Bu sorunun tıpkı güvenlik gibi üzerinde mutabakat sağlanmış tek bir tanımı yoktur. Nye ise gücü şu şekilde tanımlar:

> *"Güç, hava durumu gibidir. Herkes ona bağlıdır ve onun hakkında konuşur; fakat çok azı onu anlar. Tıpkı çiftçilerin meteorologların hava durumunu tahmin etmeye çalıştıkları gibi, siyasi liderler ve analistler de güç ilişkilerindeki değişiklikleri tanımlamaya e öngörmeye çalışırlar. Güç, aynı zamanda aşk gibidir: Yaşaması, tanımlanmasından ve ölçülmesinden daha kolaydır; fakat onun gerçekliğini azaltmaz. Sözlük anlamıyla güç, bir şeyi yapabilme kapasitedir. En genel anlamıyla, güç, birinin, istediği sonuçları elde edebilme becerisidir."* (Nye, 2020: 19-20).

Buradan da anlaşılacağı üzere güç ile güvenlik birbirleriyle yakından ilişkilidir. Klasik realizmde gücün güvenlik ile yakından ilişkisini Özdemir şu şekilde açıklıyor:

> "*Klasik realizm, politika bağlamında güç kavramını caydırıcılık yeteneği olarak yorumlamaktadır. Güvenlik ve gücün eşanlamlı olarak kullanılması ve gücün askeri güce daha fazla vurgu yapılarak bir amaç olarak ifade edilmesinin nedeni budur"* (Özdemir, 2008:127).

İngiliz Okulu temsilcilerinden Barry Buzan ise güvenlik kavramının "geleneksel olarak yan etki muamelesi gördüğünü güç ya da barıştan kaynaklanan ardıl bir devre olarak kabul edildiğini" (Buzan, 2017:167) belirterek, "1970'lerdeki ekonomik ve çevresel endişeler artana kadar güvenliğin belirli aktörlerin siyaset çıkarlarından öte farklı anlamlarda nadiren incelendiğini ve 80'lerin sonuna kadar ağır bir askeri vurguya sahip olduğunu" belirtmiştir (Buzan, 2015:27).

Güvenlik kavramının odağı olarak devletin gösterildiği bu görüş realistlere ait iken, özelikle 1980 ve sonrasında çevre, kadın hakları, çocuk hakları, bilgi edinme özgürlüğü vs. gibi konularda yaşanan gelişmeler sonucunda güvenlik, insan odaklı güvenlik olarak da ele alınmaya başlanmıştır. Bu odak noktası ise liberaller tarafından kullanılmaktadır. Bu konuda akla gelen ilk isim olan John Locke'a göre güvenliği Bagby şu şekilde aktarmaktadır:

> *"Locke'ın bir diğer farkı güvenlik konusunda Hobbes'un devlete yaptığı vurgudan farklı olarak insanların bir tiranın egemenliğinde yaşamaktansa hükümetin olmadığı doğal bir yönetimde (state of natüre) yaşamalarının daha güvenli olacağını söylemesidir. Locke'a göre insanlar kendilerini bir tehdit altında hissetmedikleri sürece doğal haklarından devlet adına vazgeçmeyeceklerdir ve güvenli olmak adına temel haklarından devlet adına vazgeçmelerindense kendi güvenliklerini sağlama özgürlüğüne sahip olmaları daha iyidir"* (Bagby' den aktaran Birdişli, 2017:72).

Devletlerin birbirleriyle olan ilişkilerinin zamanla artması neticesinde -ki bu ilişkiler genelde ticaret üzerinedir- ortaya çıkan anlaşmazlıkların nasıl çözüleceği konusunda temel ilke güçlü olanın bir diğerine istediğini yaptırması ile sonuçlanırdı. Realist tanımla uyuşan bu durum bir zaman sonra gereğinden fazla güçlenen bir devlete karşı, bu devletten muzdarip birden fazla devletin ittifak yoluyla bir araya gelerek gereğinden fazla güçlenen bu devlete karşı oluşturdukları bir sistem olan güç dengesi sistemi yüzyıllar boyu uluslararası sistemde hâkim pozisyonda idi. Zamanla sistem değişse de özünde gücün ve güçlü olmanın altında yatan temel neden güvenlik ve güvende olma isteğidir. Bugün gelinen noktada realistlerin ve liberallerin anlamada ve yol haritası çizmede yetersiz kaldığı bir güvenlik konusu ile karşı karşıyayız. Bu alan üzerinde yaşadığımız dünyanın dışında aynı zamanda içinde bir alan olan siber dünya ve bu dünyanın güvenliğinin sağlanması amacıyla ortaya çıkan siber güvenliktir.

Güvenlik, birçok teori tarafından farklı şekilde alınmaktadır. Bunlardan biri olan Kopenhag Okulu, güvenlik konusunu söz-edim yoluyla bir güvenlik meselesi haline getirmektedir (Baysal ve Lüleci 2015:63). Örneğin; bir iktidar olağanüstü tedbirler dizisi almak istediğinde söylem yoluyla bir güvenlik problemi yaratarak kendine geniş hareket alanı yaratmaktadır. Daha açık bir örnek vermek gerekirse; ABD, 11 Eylül saldırıları ile beraber söylem yoluyla bir güvenlik problemi yaratmış ve bunu meşrulaştırarak önce Afganistan'a ardından Irak'a askeri operasyonlar düzenlemiştir. Hatta bununla da kalmayarak İran'a da operasyon düzenleyeceğinin sinyallerini vererek nükleer tesislerini kapatmasını ve üretime son vermesi tehdidini birçok kez yinelemiştir. İnşacı güvenlik yaklaşımın temel taşlarından bir diğeri ise BM'dir. 1994

yılında yayınlanan raporda güvenlik insan odaklı ele alınmıştır (Birdişli, 2017:123). Bu rapora göre güvensizliğin kaynağının sosyal kaygılar olduğu belirtilmektedir (Birdişli, 2017:124).

İnşacı teori içerisinde incelenen bir başka güvenlik teorisi ise güvenlik topluluğu teorisidir. Karl Deutsch tarafından ortaya atılan bu kavrama göre; devletler modern demokratik hükümetler arasındaki etkileşimi ve iletişimi artırarak bir devletin başka bir devlet için tehdit oluşturmadığı bir güvenli toplum inşa edilebilir (Çelikpala, 2019:1). Mahkûmun İkilemi oyununda da benzer durum söz konusudur. Devletler arasında iletişim var olduğu sürece ortak bir yol bulmak mümkündür ve güven ancak bu şekilde inşa edilebilir.

Realizm ise güvenliği anarşinin üzerine inşa etmiştir. Uluslararası sistemin anarşik olduğunu bu nedenle her devletin kendi güvenliğini sağlamasını öngören realist güvenlik yaklaşımına göre güç, güvenlik için en önemli şeydir. Bu nedenler geçmişte ve günümüzde eli silah tutan herkesi asker olarak kabul etmiştir (Karabulut ve Değer, 2015:72).

Realizmin aksine liberalizm güvenlik ile güvenlik arasında denge oturtulması gerektiğini iddia eder. Buna göre devletler, bireysel özgürlüklere zarar vermeden yalnızca gerekli gördüğü taktirde belli ölçüde kısıtlayarak iç ve dış güvenliği sağlamalıdır (Uğuz, 2016:90).

Feminist teoride ise güvenliğin kendisi sorgulanmaktadır. Kimin için güvenlik sorusuna birey ve toplumun güvenliği (Demirtaş, 2019:2) yanıtını veren feminist teori, güvenliğin kim tarafından sağlandığı hususunda ise tüm literatürün ataerkil bir bakış açısıyla yazıldığını iddia ederek çatışmalarda kadınların erkeklerden daha olmasa bile, en az erkekler kadar etkilendiğini iddia eder (Baylıs, 2012:162).

Tezde ise eleştirel inşacı güvenlik teorisi desteklenmektedir. Zira siber güvenlik, daha çok söylem yoluyla oluşturulan bir güvenlik yöntemi olarak kullanılmaktadır. Her ne kadar siber güvenliğe gerçekten de ihtiyaç duyulsa da iktidar sahipleri şimdilik bu konuda kulağının üzerine yatsalar da günü geldiğinde veya kendi iktidarlarına yönelik bir tehdit gördüklerinde siber güvenlik konusunu toplumu şekillendirmek adına kullanmaktan çekinmemektedirler. Ülkemizde de ciddi eleştirilere maruz kalan sosyal medya yasa tasarısı buna örnektir. İktidar kanadına yönelik yapılan bu

eleştirinin temelinde sosyal medyada güvenliği sağlamaktan ziyade meşruiyetini zedeleyici haberlerin önüne geçmektir**.**

4.3. Siber Güvenlik

21.yy. ın ilk çeyreğini yaşadığımız bu günlerde dünya, küreselleşmenin de ötesine geçerek tüm iletişimin yeraltından geçen kablolarla sağlandığı bir yer haline gelmiştir. Bir yerden bir yere haber ulaştırmak için at sırtında günlerce yol gitmekten, birkaç "dokunma" ile dünyanın öbür ucuna haber yollayabilmek arasında üç yüzyıldan kısa bir süre var. Oldukça kısa sürede böylesi bir atılımın temelinde giderek artan iletişim ihtiyacı yatmaktadır. Devletlerin birbirleriyle olan ilişkilerini sıklaştırdığı ve hızlı kararlar alarak çabuk hareket etmeleri gerektiğinin anlaşıldığı savaşlar insanları yeni arayışlara itmiştir. 1835 yılında Samuel Morse tarafından bulunan Mors alfabesiyle haber taşımaya başlanan telgraf ile (Milliyet, 2020a) beraber haberleşme daha hızlı hale gelmiş ancak zamanla hızlı haberleşmenin daha hızlısına ihtiyaç hasıl olmuş ve 1876 yılında Graham Bell tarafından 1875 yılında yapılan araştırmalar neticesinde kabloların insan seslerini iletebilmesinin keşfedilmesi sonucunda bulunmuştur (Milliyet, 2020b). Dünya savaşları ile iletişim ihtiyacı had safhaya çıkmış ve 1962'den itibaren Savunma Bakanlığı projelerine dahil olan üniversiteler ve araştırma laboratuvarları arasında sağlıklı iletişim sağlamak üzere ARPANET kurulmuştur (Cavelty, 2017:63). Şu an hâlâ kullandığımız ağ sistemlerinin temeli olan ARPANET, (Elbahadır, 2019:12) başlangıçta oldukça kısıtlı gruplar tarafından kullanılmakta iken, zamanla tüm insanların hizmetine sunulmuştur. Her ne kadar kaynaklar internetin askeri kaynaklar tarafından icat edildiği konusunda mutabık olsa da Richard A. Clarke buna itiraz ederek şöyle diyor:

> *"Herkes interneti askeriyenin bir icadı zannediyor. Ama aslında bunu yapan 60'lı yıllarda MIT, Stanford ve Berkeley üniversitelerinde okumuş olan ve şimdi yaşlı insanlar olan hippie'ler. İlk internet dört bilgisayarın birbirine bağlanması ile oluşturuldu. Bunlar UCLA, Stanford, UC Santa Barbara ve Utah üniversitelerindeydi*." (Clarke ve Knake, 2010:47).

Bugün gelinen noktada ise bindiğimiz otomobilden evimizin sıcaklığına, banka hesaplarımıza erişimimizden sosyal medya hesaplarımıza erişime kadar hemen hemen her alanda siber alanı kullanmaktayız. Hâl böyle olunca günlük hayatımızdaki alışkanlıklarımız da değişmekte ve tüm toplum geri dönülemez biçimde teknolojiye bağımlı hale gelmektedir (Özkaya vd., 2019:31). Durum böyle olunca ortaya çıkan bu teknolojide güvenliğin nasıl sağlanacağı ile ilgili birtakım açmazlar meydana gelmektedir. Bunların başında ise siber güvenlik gelmektedir.

Siber güvenliğin birçok tanımı mevcuttur. En sade ve anlaşılır olanı ise Özkaya'nın şu tanımıdır: Siber güvenlik, kişisel veya kurumsal bilgi veya bilgi kaynaklarının yetkisiz erişim, saldırı, hırsızlık veya veriye zarar verme faaliyetlerine karşı korunması anlamına gelir (Özkaya vd., 2019:34). Buradan da anlaşılacağı üzere temel amaç sahip olunanları koruyabilmektir. Siber dünyada sahip olduklarımız reel dünyadakilerden biraz fazlasıdır. Özellikle sosyal medyanın hemen herkes tarafından kullanılmaya başlandığı şu günlerde tüm yaşantımız artık sanal aleme taşınmış durumdadır. Gittiğimiz yerlerde çekindiğimiz fotoğraflar, gezdiğimiz yerler, hatta kaybettiğimiz yakınlarımızı bile çevremizle sosyal medyadan paylaşır olduk. Bu tür paylaşımlar sanal dünyanın reel dünyaya bazı olumsuz etkileriyle sonuçlanabilmektedir. Örneğin; tatilde olduğumuzu gösteren fotoğraflar, birkaç yıl öncesine kadar çok popüler olan ve halen daha kullanılmakta olan "Swarm" adlı programla yer bildirimi yaparak aslında evde olmadığımızı da bir bakımdan beyan etmiş oluyoruz. Bu durum kişinin evini korunmasız hale getirmekte ve hırsızlar için ava dönüşmesine neden olmaktadır. Bunun dışında, örneğin; bir kişinin dayısıyla yaptığı paylaşım bile bazen başına dertler açabilmektedir. Zira kişinin dayısının soyadı aynı zamanda annesinin kızlık soyadıdır. Genellikle bankacılık işlemlerinde kullanılan anne kızlık soyadı bir anda kişinin arka kapı bırakmasına neden olmaktadır. Siber dünyada bu ve bunun gibi kişilerin yaşantılarını araştırarak onun hakkında olabildiğince veriye erişerek hayatına hükmedecek oranda bilgi sahibi olmaya çalışmaya sosyal mühendislik adı verilmektedir. Günümüzde en çok kullanılan yöntemlerden biri olan sosyal mühendislik sayesinde kişisel birçok verinin ele geçirilmesine, bilgisayar veya akıllı telefonlarının hacklenmesine neden olabilmektedir. Hack kelimesini Altınkaynak şu şekilde açıklamaktadır:

"*Hack kavramı medyada genellikle siber suçluların yaptıkları eylemler olarak tanımlanmaktadır. Bu tanım yanlış olup, toplumda da yanlış algıya yol açmıştır. Bir babaannenin yoğurt kabından saksı yapması da bir hack olayı iken; bilgisayar grafiklerinden karekök formülünü integer formunda hesaplayan hızlı bir algoritma geliştirme de hack olarak nitelendirilir. Siber güvenlik alanında ise bir açıklığı kullanmak olarak tanımlanmaktadır."* (Altınkaynak, 2018:1).

Tüm bunlar göz önüne alındığında ortaya çıkan sonuç, bilgi güvenliğini sağlamanın aslında ne kadar zor olduğudur. İnternetin olmadığı dönemlerde bizleri yalnızca komşularımız, akrabalarımız tanıyorken şu anda dünyanın öbür ucundaki herhangi birisi bile hakkımızda bilgi sahibi olabilmektedir. İşte burada güvenlik problemi ortaya çıkmaktadır. Çünkü küçük gruplar halinde yaşadığımız eski düzende bireyler birbirlerini tanıyor ve mahalle veya sokağa yabancı biri girdiğinde hemen fark

edilip göz ucuyla da olsa takip ediliyor ve olası bir mala veya cana zarar verme durumunda o küçük topluluk kendini savunabiliyordu. Ancak bugün, toplum yaşantımızın tamamıyla değişmesi, yaşadığımız alanın giderek büyümesi ve grupların giderek küçülmesi, ancak tam tersi olarak çevrenin sosyal medyada hiç olmadığı kadar büyümesi kişiyi açıkta bırakmakta ve bu açıklık onu güvensiz hale getirmektedir. Bireyler buradaki güvenliği sağlamak içinse çeşitli yollara başvurmaktadır. Bunun en temeli ve en yayın olanı ise şifrelemedir. Mail adreslerinin güçlü parolalarla korunması aynı şekilde sosyal medya hesaplarının kapalı konumda bulunması tıpkı evin perdelerini kapatmak gibi hesabın içerisini dışarıya kapatarak korumaya alınmaktadır. Ancak sanal dünya öyle bir yerdir ki dışarıdan bazı müdahalelerle evinizin perdesini açmak hatta içine sızarak kişiyi kapı dışarı ederek evini işgal etmek mümkündür. Olası böyle bir durumda ise nasıl eve hırsız girdiğinde polise başvuruluyor ve kanıt bulmak adına evde parmak izi taraması yapılıyor ise hacklenen yerlerde de aşağı yukarı aynı prosedür izlenmektedir. Ancak problem şu ki sanal dünyada doğası gereği parmak izi bulmak pek mümkün olmamaktadır. Bunun nedeni yaygın olarak kullanılan "vpn"dir. Vpn kullanmayı şu şekilde betimleyebiliriz: Diyelim ki evinize hırsız girdi ve altınlarınızı çalarak kayıplara karıştı. Polise yaptığınız ihbar sonucu eve gelip parmak izi, ayakkabı izi vb. izlerden yola çıkarak araştırma yapan yetkililer hırsızın Benin'in başkenti Novo Porta'da olduğunu tespit ediyor. İşin daha da ilginç yanı ise hırsızın aslıda Benin'in haritadaki yerini bile bilmediği çünkü doğma büyüme Helsinkili olduğunu öğreniyorlar. İşte vpn tam olarak bu anlama geliyor. Oturduğunuz yerden kullandığınız basit bir program sayesinde hiç olmadığınız bir yerde görünerek ulaşması günler sürecek yerlere belki de ulaşılamayacak bambaşka yerlere (vize çıkmazsa tabi) ulaşmayı sağlamayı ve ayak izinin takip edilmesini imkansıza yakın hale getirmeyi sağlar.

Teknolojinin insanların gözünü korkutmaması gerekir. Zira her ne kadar büyük tehlikelere gebe de olsa teknoloji günlük hayatımızı hiç olmadığı kadar kolaylaştırmaktadır. Pandemi dönemini yaşadığımız şu günlerde ülkemizde uygulanan kısıtlamalar nedeniyle fiziksel olarak yapmakta zorlanacağımız bazı işlerde oturduğumuz yerden halledebilir hale geldik. Örneğin; koronavirüs ile mücadele kapsamında trafik cezaları, motorlu taşıt vergisi, tapu harcı vb. gibi birçok ödemeler Gelir İdaresi Başkanlığı'nın yürüttüğü çalışma ile internet üzerinden kredi kartı ile ödenebilir hale geldi (Hürriyet, 2020b). Bunun dışında fabrikalarda her ne kadar

üretim bantlarında olmasa da home office çalışma olanağı getirildi. Bu sayede insanlar kendi sağlıklarını tehlikeye atmadan evlerinden işlerini halledebilir hale geldi. Ancak güvenlik her daim bir sorun olarak devam etmektedir. Her ne kadar Cavelty:

"*Toplam olaylar bazında sadece yüzde 3'ünün, durdurulması mümkün olmayan gelişmiş saldırılar olduğu düşünülmektedir. Saldırganların büyük çoğunluğu kötü savunma tedbirlerine sahip olan küçük ve orta büyüklükteki şirketleri hedef almaktadır. Bu tür olaylar medya ve hatta kolluk kuvvetlerinin dikkatini çekmemektedir."* (Cavelty, 2017:366).

Dese de bahsi geçen yüzde 3'lük kısmın geneli ne kadar etkilediğine değinmeyerek siber güvenliğin abartıldığını iddia etmektedir. Ancak çok yakın zamanda Twitter'a yapılan saldırıda yalnızca küçük ve orta ölçekli şirketlerin hedef alınmadığı artık çok daha büyük şirketlerin bile hedef haline geldiğini görmekteyiz. Burada dikkat edilmesi gereken bir diğer nokta ise saldırıları kimin yaptığıdır. Yılmaz'ın makalesinde iddia ettiği gibi; "Siber saldırı yöntemlerinin terör grupları tarafından kullanılmasının en önemli nedenlerinden biri saldırıyı düzenleyen kişilerin takip edilmesinin oldukça zor olmasıdır." (Yılmaz, 2020:68) bir durum söz konusu değildir. Zira böyle bir itham saldırıların amaç ve araç bakımından doğru şekilde değerlendirilmesinin önünde ciddi bir engel oluşturmaktadır. Clarke, bu tür tanımlamanın pireyi deve yapmak olduğunu belirterek şu açıklamaya yer verir:

"*İnanılan bir konu siber terör diye bir olgunu varlığı. "Siber terör", deve yapılan bir pire. O boya erişebilecek bir böcek yok; tamamen hayali. Develeşebilecek pireler dikkat dağıtıp konuyu yanlış yerlere çekmek için kullanılan aslında var olmayan öcüler.*

Birlikte kullanıldıkları zaman pire-deve olan "siber" ve "terör" sözcükleri yan yana getirilmemeli. Siber terör dediğinizde insanın aklına Usame Bin Ladin'in mağarasında oturup siber savaş yürütmesinin imajı geliyor. Şimdilik Usame'nin böyle bir şey yapma olasılığı yok. Ayrıca, büyük bir ihtimalle Bin Ladin mağarada değil, lüks bir villada oturuyordur.

İstihbarat kuruluşlarının elinde teröristlerin altyapıya yönelik siber savaş saldırıları yaptıklarına düşündürecek en ufak kanıt yok.

Günümüze dek, teröristler ne internete saldırdılar ne de fiziksel sistemlere saldırmak için interneti kullandılar. Elçilik, demiryolu otel gibi tesislere saldırılar düzenlerken, internet sadece haberleşme ortamı niyetine kullanıldı." (Clarke ve Knake, 2010:69).

Clarke' in de bahsettiği gibi terör grupları tarafından siber saldırı yapıldığı söylenerek konu siber teröre getirilerek asıl odaklanılması gereken yerden uzaklaşmaya neden olmaktadır. Ayrıca öyle olmuş olsa bile siber saldırı kullanılmasının nedeni takip edilmesinin oldukça zor olması değildir. Kaldı ki terör örgütleri çoğu zaman yapmadıkları saldırıları bile üstlenmektedir. Terör örgütlerinin gizli gizli saldırı yapmak gibi bir amacı yoktur. Saldırılarını yaptıktan sonra açıktan mesaj vererek isteklerini yaptırabilme adına bir koz olarak kullanırlar. Ayrıca hiçbir terör örgütü siber saldırı düzenleyebilecek kadar teknik donanıma sahip değildir. Ne alet edevat olarak ne de bilgi birikim olarak.

Peki siber güvenliği bu derece önemli kılan bu saldırılar kim tarafından ve nerelere yapılabilir? Sorusunun cevabı ise; herhangi bir kişi veya grup tarafından herhangi bir yere yapılabilirdir. Günümüzde siber dünyaya bu kadar bağımlı olan yalnızca bireyler değildir. Bireylere bu hizmetleri sağlayanlar da en az bireyler kadar açık hedeftir. Önceleri kişilerin kredi kartı bilgilerini çalmaya çalışan hackerlar artık kişileri bırakarak ana merkezlere yani bankalara saldırarak bir kişinin kart bilgilerini çalmaktansa o bankaya ait tüm müşterilerin bilgilerini çalmayı yeğlemektedir. Bir sistemin ana merkezine yapılan bir saldırı ile küçük küçük birçok saldırı yaparak -ki hepsinin başarılı olacağının garantisi yok zira birinden birinde yakalanma riski her zaman var- vakit kaybetmektense ana merkeze yapılacak doğrudan bir saldırı ile tüm merkez ele geçirilebilir.

Günümüzde tek bir merkezden hizmet dağıtımı birçok yerde kullanılmaktadır. Örneğin, barajlar, fabrikalar, nükleer tesisler, elektrik dağıtım tesisleri, su şebeke hatları vb. yerler SCADA (Supervisory Control and Data Acquisition) olarak adlandırılan ve "Merkezi Denetleme, Kontrol ve Veri Toplama" olarak çevrilen bir sistemle kontrol edilmekte ve PLC (Programmable Logic Controller) olarak adlandırılan ve "Programlanabilir Mantıksal Denetleyici" olarak çevrilen küçük bir makine ile tüm sistem çalıştırılmaktadır. Örneğin; bir şehirdeki sokak lambalarını akşam olduğunda yakmanız gerekiyor. Ancak kışın ve yazın havanın kararması farklı zamanlarda olduğu ve oldukça fazla sayıda sokak lambasını olduğu düşünüldüğünde bunu yapması gereken bir cihaza ihtiyaç duyulmaktadır. Diyelim ki kışın sokak lambalarının 17.00'da yazın ise 19.00'da yanmasını isteniyor. Yaz başlangıcı olarak 21 Haziran kış başlangıcı olarak ise 23 Eylül baz alınıyor. Bundan sonra tek yapılması gereken istenilen verileri PLC'lere doğru şekilde girmek. Artık sokaklar hava kardığında da aydınlık kalıyor. Tabi ki eğer birileri bunu sabote etmezse. İran'da ise Stuxnet adında bir virüs bu sabotajı gerçekleştirdi.

4.4. Stuxnet

2010 yılında bazı müşterilerin bilgisayarlarının kendiliğinden kapandığı şikâyeti üzerine yapılan incelemelerde Ralph Langner ve ekibinin yaptığı araştırma sonucunda fark edilen Stuxnet virüsü, siber dünyanın geleceğini etkileyecek güce sahip bir saldırı olarak tarihe geçti. Yayınladıkları raporda Trojan-Spy.0485 ve Malware-Cryptor.Win32.Inject.gen.2 olarak adlandırdıkları virüsleri antivirüs tabanına eklediklerini açıkladılar. Ancak Langner, laboratuvarında solucanı test etmeye

kalktığında çalışmadığını fark etti ve bunun belirli bir yere saldırmak amacıyla özel olarak hazırlanmış olabileceğini düşündü. Yaptığı araştırmalar sonucunda bulabildiği herhangi bir Windows bilgisayarlarına bulaşsa da asıl olarak Siemens marka denetleyicileri hedef aldığı ve bulduktan sonra hedeften emin olmak için model numaralarını, yapılandırma ayrıntılarını kontrol etmeyi ve hatta doğru program olup olmadığını kontrol etmek için kontrolörden program kodunu indirmeyi içeren karmaşık bir parmak izi sürecinden geçtiğini fark etti (Langner, 2011:49). Devam eden çalışma neticesinde bir nükleer santrale ve bunun da herhangi bir santral değil 984 adet santrifüjler dizisini işletmek için yapılandırılmış bir işletmenin peşinden gittiğini fark etti (Singer ve Friedman, 2018:159). Bu işletme ise İran'ın Natanz şehrinde kurulan nükleer tesisti. Virüsün nasıl bulaştığı konusunda ise kesin bir mutabakat sağlanamamakla beraber bir usb ile tesise sokulduğu tahmin ediliyordu. Zira nükleer santral olası bir siber saldırıya karşı internet ortamından arındırılmış hava boşluğuna sahip bir sistem üzerinde çalışmaktaydı. Ancak gelinen noktada internet ortamından arındırılan sistemlerin de siber saldırıya uğrayabileceği bu şekilde tecrübe edilmiş oldu.

Microsoft sistemli bilgisayarlarda "Grup İlkesi" gereği usb veya çıkarılabilir aygıtları engelleme imkânı mevcuttur. Okuma erişimini reddetme, yazma erişimini reddetme ve erişimi reddetme olarak üç farklı reddetme seçeneği mevcuttur. Kapalı devre sistemlere sahip bu tür sistemlerde koruma olarak bu tür reddetme seçenekleri kullanılmaktadır. Kaldı ki bugün herhangi bir makalenin bile kopyalanmasının istenilmemesi halinde web sitelerinde kopyala-yapıştır engellenebiliyorken bir nükleer santralde herhangi bir harici depolayıcının erişimini engellemek hiç de zor değildir. Ancak yapılan araştırmada kaynakların bu konuda bazı yerleri atladığını göstermektedir. Yukarıda da bahsedildiği üzere virüsün bir usb ile sisteme bulaştırıldığı iddiası mevcut. Ancak yayınların hemen hepsinde es geçilen bir nokta mevcut. Symantec'in 26 Şubat 2013 günü yayınlanan raporu. Bu rapora göre Stuxnet' in fark edildiği anki versiyonu Stuxnet 1.0 versiyonudur (Symantec, 2013:2). Bu versiyondan önce ise 1.0 kadar agresif olmayan 0.5 sürümü mevcut. Fark edilmesinin nedeni ise istenilen ölçüde olmadığı veya başarılı olamaması sonucunda güncellenen sürüm ile daha da agresif hale getirildiğidir. Stuxnet'in bir gaz boru hattı veya elektrik santrali gibi İran'da olması muhtemel belirli bir endüstriyel kontrol sistemini hedefleyen bir tehdit (Symantec, 2011:2) olduğunu belirten raporda toplamda 4 adet

yamanmamış Microsoft açığının kullanıldığı, sistemi sabote etmek için Siemens PLC'lerindeki kodun virüs tarafından değiştirildiği belirtiliyor (Symantec, 2011:2). Saldırının nasıl yapıldığına dair olası bir senaryo hazırlayan Symantec şu tahminde bulunmaktadır:

> *"Endüstriyel kontrol sistemleri (EKS), programlanabilir mantık denetleyicilerindeki (PLC'ler) kod gibi özel bir düzenek tarafından çalıştırılır. PLC'ler genellikle İnternet'e veya hatta dahili ağa bağlı olmayan Windows bilgisayarlardan programlanır. Ek olarak, endüstriyel kontrol sistemlerinin kendilerinin de internete bağlanması olası değildir.*
>
> *Öncelikle saldırganların keşif yapması gerekiyordu. Her PLC benzersiz bir şekilde yapılandırıldığından, saldırganlar önce EKS'nin şemalarına ihtiyaç duyacaktır. Bu tasarım belgeleri içeriden biri tarafından çalınmış olabilir veya Stuxnet'in veya diğer kötü amaçlı ikili dosyaların eski bir sürümü tarafından alınmış olabilir. Saldırganlar tesisteki bilgi işlem ortamının tasarım belgelerine ve potansiyel bilgisine sahip olduktan sonra, Stuxnet'in en son sürümünü geliştireceklerdi. Stuxnet'in her bir özelliği, belirli bir nedenle ve EKS'yi potansiyel olarak sabote etme nihai amacı için uygulandı. Saldırganların, kodlarını test etmek için PLC'ler, modüller ve çevre birimleri gibi gerekli ICS donanımını içerecek yansıtılmış bir ortam kurması gerekir. Ek olarak, kötü amaçlı ikili dosyaları, şüpheyi önlemek için dijital olarak imzalanması gereken sürücü dosyalarını içeriyordu. Saldırganlar bu görevi gerçekleştirmek için iki dijital sertifikayı ele geçirdi. Saldırganların dijital sertifikaları, iki şirketin tesislerine fiziksel olarak girmiş ve çalmış olabilecek birinden alması gerekirdi ki iki şirket fiziksel olarak birbirine oldukça yakın. Hedeflerine bulaştırmak için Stuxnet'in hedef ortama dahil edilmesi gerekir. Bu, tesise erişimi olan bir yüklenici veya içeriden biri gibi istekli veya bilmeyen bir üçüncü şahsa bulaşarak gerçekleşmiş olabilir. Orijinal enfeksiyon, çıkarılabilir sürücü tarafından içeri sokulmuş olabilir. Stuxnet, organizasyon içindeki bir bilgisayara bulaştıktan sonra, tipik Windows bilgisayarları olan ancak PLC'leri programlamak için kullanılan Field PG'lerini[13] araştırmak için yayılmaya başladı. Bu bilgisayarların çoğu ağa bağlı olmadığından, Stuxnet ilk olarak sıfır gün güvenlik açığı -iki yıllık bir güvenlik açığı- Step7 projelerine çıkarılabilir sürücüler yoluyla LAN üzerindeki diğer bilgisayarlara yayılmaya çalışacaktır. Stuxnet sonunda Step7'yi çalıştıran uygun bir bilgisayar bulduğunda, PLC'deki kodu değiştirecekti. Bu değişiklikler, muhtemelen Stuxnet'in yaratılmasına yatırılan büyük kaynaklar nedeniyle yüksek değerli bir hedef olarak kabul edilen sistemi sabote etti. Sorunu doğrulamaya çalışan kurbanlar, Stuxnet değişikliklerini gizlediği için herhangi bir hileli PLC kodu görmeyecektir. Kendi kendini çoğaltma yöntemlerini kullanma tercihleri, uygun bir Field PG'si bulmalarını sağlamak için gerekli olabilirken, aynı zamanda hedef kuruluşun dışındaki makinelere bulaşarak gözle görülür ikincil hasara neden oldu. Saldırganlar, amaçlanan hedefe etkin bir şekilde ulaşmak için ikincil hasarı bir gereklilik olarak değerlendirmiş olabilirler. Ayrıca saldırganlar, keşfedildikleri zaman büyük olasılıkla ilk saldırılarını tamamladılar."* (Symantec: 2011:3).

20 Temmuz 2010 yılında Stuxnet komut ve kontrol sistemlerine giden trafiği izlemek için bir sistem kuran Symantec 29 Eylül itibariyle 100.000 virüslü bilgisayar olduğunu görmüştür (Symantec, 2011:4). Bu bilgisayarların 60.000'den fazlasının ise İran'da olduğu ortaya çıkmıştır. Kurulum aşamasına gelindiğinde virüsün ilk olarak tehdidin uyumlu bir Windows sürümünde çalışıp çalışmadığını kontrol etmekten, bilgisayara halihazırda virüs bulaşıp bulaşmadığını kontrol etmekten, mevcut işlemin ayrıcalığını sisteme yükseltmekten, hangi antivirüs ürünlerinin kurulu olduğunu kontrol etmekten sorumlu olan bir .dll[14] dosyasının olduğu (Symantec, 2011:12) belirtilen raporda virüsün ne kadar özenle hazırlandığı gözler önüne seriliyor. Virüsün

[13] Field PC; Siemens için tasarlanmış ve PLC programlama amacıyla kullanılan laptop görünümlü cihaz.
[14] İçerisinde yazılımın işlevini yerine getirecek kod bulunan "dymanic-link library" adlı dosya türü.

yükleme işlemi tamamlandıktan sonra 80 numaralı bağlantı noktasındaki komut ve kontrol sunucusuyla bağlantı kuran Stuxnet virüsü saldırıya uğrattığı bilgisayarlar hakkında bazı temel bilgileri http aracılığıyla saldırgana gönderdiği ve bunun için www.mypremierfutbol.com ve www.todaysfutbol.com[15] adreslerinin kullanıldığını (Symantec, 2011:17) raporda görmekteyiz. Bir başka ayrıntı ise sürücü dosyalarından birindedir. Raporda şu şekilde belirtilmiştir:

"*Sürücü dosyasında proje yolu, b: \ myrtus \ src \ objfre_w2k_x86 \ i386 \ guava.pdb kaldırılmadı. Guava, mersin (mersin) familyası cinsindeki bitkilerdir. Dizenin önemli bir anlamı olamaz; ancak çeşitli yorumlar tartışılmıştır. Myrtus "MyRTUs" olabilir. RTU, uzak terminal ünitesi anlamına gelir ve bir PLC'ye benzer ve bazı ortamlarda PLC'lerin eşanlamlısı olarak kullanılır. Ek olarak, Wikipedia'ya göre, "Esther başlangıçta Hadassah olarak adlandırılıyordu. Hadassah, İbranice' de "mersin" anlamına gelir. " Esther, krala suikast düzenlenmesi planını öğrendi ve "Haman'ın kralına Pers İmparatorluğu'ndaki tüm Yahudileri katletme planını söyledi ... Yahudiler, yalnızca infaz müstakbellerini öldürmeye devam ettiler." Symantec okuyucuları herhangi bir atıf sonucuna varmaları konusunda uyarır. Saldırganlar, başka bir partiyi bulaştırma konusunda doğal arzuya sahip olurdu."* (Symantec, 2011:20).

İsrail'in suçlanması konusunda elde ufak da olsa bir şeyin olduğu bu komut yine de tam olarak bir kanıt sunmamakla beraber şüpheleri artırmıştır. Bir diğer şüphe ise virüsün içerisinde 4 Temmuz 2009 yılında otomatik olarak durdurmayı komut etmiş (Symantec, 2013:2) ve 24 Haziran 2012 yılında ise kendini imha etmeye programlandığı görülmüştür (Symantec, 2011:14). 4 Temmuz'da yayılmayı durdurmasının nedeni olarak yeni izinlerin alınması gerektiğini ve bir oyuncu değişikliğinin olacağını tahmin ediyor Symantec çalışanları. Bu değişiklik olarak ise Obama'nın seçilmesi gösteriliyor. Kodun oldukça büyük kaynaklara sahip olduğunu ve böyle bir kodun yazılması için ciddi emek harcanması gerektiğini belirten Symantec, bu kodun bir gencin yatak odasında yazabileceği bir kod olmadığını ve Stuxnet'in gerçek dünyadaki etkilerinin geçmişte tecrübe edilenlerin çok ötesinde olduğu belirtiliyor (Symantec, 2011:49-50).

New York Times yazarı David E. Sanger 2012'de yayınladığı bir makalede saldırının Bush döneminde başladığını ve adının "Olimpic Games" olduğunu iddia etmektedir (NYT, 2012).

Stuxnet, kim tarafından yazıldığı henüz kesin olmasa da İran'ın nükleer programını sekteye uğrattığı aşikâr. Yapılan saldırı sonucunda nükleer santralde bulunan santrifüjlerin dönüş hızlarında oynama yaparak (bazen çok hızlı bazen çok yavaş dönmesine neden olarak) santrifüjlerin patlamasına neden oldu. Santrifüjlerdeki

[15] Bu iki adrese de erişim antivirüs programları tarafından engellediğinden ötürü sağlanamamaktadır.

bu hız değişimleri ekranda görünmüyordu elbet ancak dönüş sırasında çıkardıkları sesten ötürü mühendisler bir şeylerin yanlış gittiğinin farkındaydı. Bazı santrifüjleri değiştirerek sorunu çözmeyi planlamalarına karşın yapılan her testten başarıyla geçen sistem bir süre sonra kendiliğinden hızlı dönmeye veya yavaş dönmeye başlıyordu. Hâl böyle olunca üretimde ciddi aksaklıklar meydana geliyordu. Ta ki 2010 yılının haziran ayına kadar. Siber saldırıların ortaya çok geç çıkması belki de hiç çıkmaması gibi durumlar söz konusudur. Stuxnet, dünyadaki birçok bilgisayara bulaştı ancak öyle akıllıca tasarladı ki hedeflenen dışında herhangi bir yere zararı olmadı. George Lucas konuyla alakalı şöyle diyor: "Eğer aynı anda tam olarak 984 Siemens santrifüjünden oluşan büyük bir seri işletmiyorsanız, bu solucandan korkmanıza gerek yoktur." (Singer ve Friedman, 2018:163).

Belki sıradan kullanıcılar için Stuxnet zararlı bir yazılım değildi ancak bu solucan işin boyutunun nerelere varabileceğini gösteriyordu. Kodun içerisine yazılan 24 Haziran 2012'de kendini imha etme yerine yazılacak herhangi başka bir komut örneğin; bulaştığı sistemi kapatması ya da başka tehlikelere yol açabilecek komutların olması durumunda nelerin olacağını kestirmek oldukça güç. Siber dünya; güvenliği bu derece az olan, tehlikesi aslında bu derecelere varabilen bir alandır. Günümüzde ise bu alanda herkes kendi güvenliğini kendi sağlamak mecburiyetinde kalmaktadır.

4.5. Bölüm Değerlendirmesi

Güvenliğin olmadığı yerde kaos hâkimdir. Zira güvenlik yoksa bireyler güvenliklerini sağlamak adına her türlü eylemden geri durmayacaklardır. Siber dünyada da güvenlik, kişilerin inisiyatifine bırakılmış durumdadır. Yukarıda da bahsedildiği üzere güvenlik ile ilgili her teorinin bir bakış açısı mevcuttur ancak konu siber güvenliğe gelindiğinde ise en kapsayıcı olanın konstrüktivizmden çıktığı görülmektedir. Stuxnet saldırısı daha önce hiç deneyimlenmemiş bir saldırı türüdür. Bu saldırı göstermektedir ki hava boşluklu sistemlere bile erişim sağlanabilmektedir. Bu durum bizleri harekete geçirmeye zorlamaktadır. Zira hava boşluklu sistemler bu zamana kadarki en güvenilir sistemlerdi. Sanal dünyanın varlığını bilmediği, göremediği ve öğrenemediği bu yüzden de saldıramadığı bu sistemlerin de artık erişilebilir hale gelmesi artık hiçbir bilginin güvende olmadığını bizlere kanıtlamıştır. Her ne kadar sanal güvenlik duvarları inşa edilse de sızma testleri uygulansa da en ufak bir hareket bile anbean kayıt altına alınsa da Stuxnet'te de görüldüğü üzere sistemler yanıltılabilirdir. Singer bunu şu şekilde açıklar:

Bir mermi asla nişancının ateş ettiği yerden farklı bir yöne doğru havada başkası tarafından yönlendirilemez. Ya da hiç kimse bir bombardıman uçağının pilotunun beynini havada yıkamamış ve sadakatini değiştirmemiştir. Fakat eğer robotik silah sistemleri üzerindeki bilgisayarlara ulaşılırsa, sahiplerinin niyet ettiklerinin tam tersini yapmaya "ikna" edilebilirler (Singer ve Friedman, 2018:178).

Stuxnet ise bu *ikna* edilebilirliğin en büyük örneğidir. Mühendisler, ekranlarında her şeyin normal olduğunu görmelerine rağmen, santrifüjlerdeki seslerden bile sistemde bir anormallik olduğunu anlayabildiler. Ancak bunu anlamak her zaman mümkün olmayabilir. Zira birçok sistem uzaktan kontrol edilmektedir. Eğer mühendisler santrifüjlerin sesini duyabilecek kadar yakında olmasaydı çok daha büyük felaketlere neden olabilirdi. Her ne kadar İran, saldırı sonrasında gerekli önlemleri aldığını ve bir daha böyle bir saldırıda başarılı olamayacaklarını iddia etse de bu pek mümkün görünmemektedir. Zira yalnızca bir kadının kalbine kullanıcı izni olmadan erişim sağlayamazsınız; onun dışındaki her yere erişebilir, her şeyi hackleyebilirsiniz.

SONUÇ

Günümüzü anlamak için onu iyi analiz etmek gerekir. İçinde yaşadığımız günümüz ise oldukça kompleks bir yapıdadır. Her şeyin iç içe geçtiği, birbirleriyle organik bağa sahip olduğu günümüzde bir şeyi anlamanın en iyi yolu; onu ilişkide bulunduğu şeylerle açıklamaktır. Bu tezde de yapılmaya çalışılan budur. Siber güvenlik anarşi ve uluslararası hukuk olmadan net olarak anlaşılabilecek ve üzerinde çözüm üretilebilecek bir alan değildir. Bunu yaparken de örnek olay olarak Stuxnet seçilmiştir. Stuxnet'i diğer saldırılardan ayıran ise saldırılan yer ve kodun kendisidir. Stuxnet, içerisinde dört tane zero-day[16] kodu bulundurmaktadır. Bir zero-day kodunun piyasa değerinin yüz bin Amerikan dolarının üzerinde olduğu gerçeği ışığında bir kişi veya grubun böyle türde bir saldırıyı gerçekleştirebilmesi muhtemel görünmemektedir. Oldukça profesyonelce hazırlanan içerik, yalnızca kodla değil içerisinde barındırdığı teknik bilgiyle de yazılması oldukça güç bir virüstür. Zira, bir yere saldırmanız için o yer hakkında bilgi sahibi olmanız gerekmektedir. Bir nükleer santrale saldırabilmeniz için ise nükleer santrallerin çalışma prensibini ve saldıracağınız yerdeki santralin içerisinde yer alan santrifüjler ve PLC'ler hakkında bilgi sahibi olmanız gerekmektedir. Bu da sıradan kişilerin elde edebileceği bir bilgi türü değildir. Aynı şekilde Stuxnet bize göstermiştir ki; böyle bir saldırı bir saatli bombaya bile dönüşebilmektedir. Virüsü inceleyen uzmanlar birkaç tarihe rastlamışlar ancak bu tarihin neye tekabül ettiğini bulmaları ise epey zamanlarını almıştır. Böyle bir durumun olacağını bilen saldırgan tarihi 24 Haziran 2012 tarihinde virüsün kendini tamamen imha etmesini değil de 2009 yılının herhangi bir gününde santrifüjlerin tamamının patlamasına neden olacak bir döngüyü birkaç satırlık yazıyla iliştirseydi ne kadar büyük bir felaketle karşı karlıya kalırdık bilinmez.

Siber güvenliğin, Waltz'un self-help kavramıyla sağlanabilecek bir güvenlik çeşidi olmadığı anlaşılmıştır. Bunun yanı sıra siber güvenliğin realizm veya liberalizm üzerinden değil de konstrüktivizm üzerinden değerlendirilmesinin temel nedeni; realizmin dünyayı devlet üzerinden, liberalizmin ise devlet ve uluslararası örgütler üzerinden değerlendirmesidir. Ancak siber dünya devletleri ve devletlerarası organizasyonlardan ziyade tüm insanları ilgilendiren bir konudur ve siber dünya reel

[16] "Sıfırıncı gün" olarak Türkçe' ye çevrilen bu kavram, daha önce görülmemiş bir açık anlamına gelmektedir. Öncesinde bilinmediği ve bu nedenle bir yamanın bulunmamasından ötürü sıfırıncı gün olarak adlandırılmaktadır.

dünyanın sahip olduğu tecrübelere sahip değildir. Bunun dışında konstrüktivizmin savunduğu argüman olan süreç kavramı siber dünyanın daha iyi anlaşılmasını sağlamaktadır.

Bu tezle beraber tüm dünyanın salahiyetini ilgilendiren bir güvenlik olan siber güvenliğin uluslararası hukuk nezdinde kesin bir çerçevesinin çizilmesi gerektiği anlaşılmıştır. Ancak BM Antlaşması'nın mevcut hali böyle bir düzenleme için yeterli değildir. Saldırı konusunda bile bir mutabakatın henüz sağlanamadığı siber saldırıların saldırı olarak kabul edilmesi gerekmektedir. Bunun yanı sıra sadece siber güvenliği içeren bir antlaşmaya ihtiyaç hasıl olduğu görülmüştür. Zira siber dünyada mevcut dünya ile tanımlanamayacak kavramlar ve olasılıklar mevcuttur. Yalnızca saldırı ve savunma bile başlı başına bir meseledir. Saldırıya karşı nasıl savunma yapılacağı ise tam bir muammadır. Grotius 'un öne sürdüğü orantılılık ve ayrımcılık ilkesini siber dünyada uygulamak görüldüğü kadar kolay değildir. Singer'in dediği gibi:

> *Orantılılık kanunu, sebep olduğunuz zarar ve yıkımın, özellikle istenmeyen hedeflere olan istenmeyen hasarların, çatışmayı başlatan zararı geçemeyeceğini belirtir. Eğer bir taraf sizin ineğinizi çaldıysa, siz haklı bir şekilde şehirlerine nükleer bomba atamazsınız. Ayrım kanunu, tarafların meşru hedefler ile hedef alınmaması gerekenleri (siviller ve yaralılar diyelim) ayırt etmesini ve sadece istenen, meşru hedeflere zarar verilmesi için her şeyi yapmalarını sağlar* (Singer ve Friedman, 2018:162).

Ancak Stuxnet'te de görüldüğü üzere saldırı, saldırılması gereken alanın oldukça dışına taşmış ve neredeyse tüm dünyaya yayılmıştır. Bu saldırı bize orantılılık ve ayrım kanununun siber dünyada uygulanmasının zorluğunu göstermektedir.

Buradan çıkartılacak bir başka şey ise siber dünyanın anarşik yapısıdır. Ancak bu anarşi, inşacı bir yaklaşımla ele alınmalıdır. Zira siber alanda herkes eşittir, herkesin bir ekranı vardır. Dolayısıyla her kişi ve kurum, saldırma ve saldırıya uğrama potansiyeline sahiptir. Anarşinin devletlerin ondan ne anladığı hususuna gelince burada siber güvenlik ile uluslararası hukuk arasında kurulmak istenen bağlantıyı aslında Wendt'in bu makalesi oluşturmaktadır. Zira İran'a yapılan bu saldırının arkasında ABD ve İsrail'in olduğunun düşünülmesinin ve Sanger'in makalesinde de bunu ısrarla söylemesinin nedeni ABD ve İsrail'in İran'ın nükleer enerji konusundaki tutumudur. Yalnızca bu iki devlet değil Almanya, Fransa ve İngiltere'nin geçenlerde yapmış olduğu E3 toplantısı sonucunda çıkan karar ve Dominic Raab'ın bu konuyla ilgili atmış olduğu twitte de belirttiği üzere İran asla nükleer silah geliştirmemelidir söylemidir. Halbuki bu üç ülke de -özellikle Fransa- ülkelerinde birçok nükleer reaktörü barındırmakta ve nükleer silaha sahip olmaktadırlar. Ancak konu İran' a geldiğinde -ki İran nükleer enerji üretmek amacıyla bu tesisi inşa ettiğini beyan etmiş

ve IAEA'nın kontrolünde bu işlemleri gerçekleştirmektedir- bu düşmanca tutumların arkasında İran'daki mevcut yönetim bulunmaktadır. Halbuki İran'a ilk reaktörü kuran da bir önceki bölümde de belirtildiği üzere ABD'dir. ABD, Sovyet yayılmacılığına karşılık bir partner olarak seçtiği İran'a ilk nükleer reaktörünü inşa etmiş ve gelecekte de sayılarının artacağının sinyallerini vermiştir. Ancak 1979 da gerçekleşen devrim ve bu devrim sonrasına ABD büyükelçiliğindeki çalışanların 444 gün boyunca rehin tutulması, Carter'ın iktidarının bu nedenle ciddi şekilde zayıflaması ve sonrasında Reagan döneminde ortaya çıkan İrangate skandalı ile beraber sorunun Ortadoğu sorunu olmaktan çıkara ABD'nin iç politika sorununa dönüşmesi sonucunda İran'a karşı tutumu ve 11 eylül sonrasında El Kaide ile olan mücadelesinde 30 yıldır iç politikaya zara veren tüm dış etkenleri bertaraf etmek adına 2002 de Bush'un İran, K.Kore ve Afganistan'ı şer ekseni ilan etmesi, devletlerin iç politikalarının uluslararası barışa ve düzene nasıl zarar verdiğinin bir kanıtı olmuştur. Bununla beraber BM 687,688 ve 1141 sayılı kararlarını gerekçe göstererek Irak'a askeri müdahalede bulunması akabinde gerçekleşen direniş sonucunda ikinci bir Vietnam'la karşılaşması Orta Asya'dan sonra Ortadoğu'da da mevut düzenin bozulmasına ve kaosa neden olmuştur. Askeri müdahale sonrasında yapılan incelemelerde sıklıkla dile getirilen ve müdahaleye en büyük gerekçe gösterilen kitle imha silahlarının bulunamaması uluslararası hukukun ve devletler-üstü bir karar mekanizmasına duyulan ihtiyacın ne denli olduğunu göstermiştir. Her ne kadar BM bu karar alıcı gibi görünse de güvenlik konseyinin 5 daimî üyesinden birinin çıkarlarına zarar verecek herhangi bir şeyin olma olasılığının ne kadar düşük olduğu alınan kararlardan görülmektedir. İşte bu anarşi bize devlet üstü bir karar ve yaptırım mekanizmasına duyulan ihtiyacı göstermektedir.

Siber dünyada ise böyle bir anarşinin sonuçlarının ne kadar yıkıcı olabileceği Stuxnet ile görülmektedir. Yazılan birkaç satırlık kodlarla bir nükleer santrale zarar vermek hatta istenirse Çernobil'den daha büyük bir patlamaya sebebiyet verebilmesinin mümkün olduğunu bizlere göstermiştir.

Uluslararası hukuk bugünlere gelene kadar çok uzun bir yol kat etmiştir. Bugün gelinen noktada kuralların pek çoğunun teamüllerden oluştuğu bilinmektedir. Yüzyıllarca süren ilişkiler sonucunda alınan kararlar ve yapılan uygulamalar neticesinde belirli bir ilerleme kaydedilmiş ve yapılan barış konferansları, dönemin ünlü hukukçuları ve filozoflarının görüşlerinin dile getirilmesi bu kuralların

uygulanmaya çalışılması ve işe yaradığının görülmesi sonucunda ilerleye ilerleye bugünlere gelmiştir. Hukukun temelini oluşturan şeyin aslına bakıldığında devlet öncesi yaşantının olduğu görülmektedir. Her ne kadar uluslararası hukukun başlangıcı olarak 1648 baz alınsa da devlet öncesi dönemlerde yapılan uygulamalar ilkel hukuku oluşturmaktadır. Hukuk zamanla evrilerek gelişim göstermiş ve bugüne gelmiştir. Bu gelişme sırasında birçok savaşlar yaşanmış, çok büyük katliamlar yaşanmış ve soykırımlara tanıklık edilmiştir. Ancak yaşanan her şey birer tecrübe olmuş ve bir daha yaşanmaması için çalışmalar yapılmıştır. 1. Dünya Savaşı sonrasında Wilson'un ısrarla kurulmasını istediği Milletler Cemiyeti'nin kurulması ancak pek bir işlevinin olmaması 2. Dünya Savaşı'nın engellenememesine neden olmuş ve bu savaşta yaşanan kıyım devlet-üstü bir organizasyona duyulan ihtiyacı göstermiştir. Her ne kadar BM savaş sonrası kurulmuş olsa da kuruluşunda üye olmak için getirilen kriterler Güvenlik Konseyi gibi bir merciinin oluşturulması ve işleyişi barışın sağlanmasının sürekli olamayacağını belli etmiş ve yaşanan bazı olaylar (Irak'a müdahale, Kırım'ın ilhakı, Gürcistan'a müdahale Kosova olayı, Ruanda vs.) bunu göstermiştir. Ancak siber dünya ilkel bir oluşum olarak ortaya çıkmış bir yapı değildir. Siber dünyayı kuran insanlar dönemin en eğitimli insanlarıdır ve inşa edilen bu dünyada bu tür tecrübelere yer yoktur. Her ne kadar iki dünya savaşı tecrübe edilmiş olsa da bir siber savaş bu iki dünya savaşından çok daha fazla zarar verebilir. Çünkü, günümüzde en temel ihtiyaçların bulunduğu yerler (elektrik, su, ısınma vs.) tamamıyla otomasyonla sağlanmaktadır. Bir ülkenin elektriğini kesmek için artık hava saldırıların ihtiyaç duyulmamaktadır. Bir ülkenin suya erişimini engellemek için kuşatmaya ihtiyaç duyulmamaktadır. Bunların yerine yapılacak bir siber saldırı bir ülkenin elektriği veya suya olan erişimini yok edebilir. Böyle bir durumda ise ne olacağı ve neler yapılması gerektiği konusunda ise kesin belirtilmiş bir prosedür, bir hukuk normu bulunmamaktadır. Çünkü böyle bir olay daha önce tecrübe edilmiş değildir. Tıpkı Çernobil'de olduğu gibi. Daha önce yaşanmamış ve yaşanması muhtemel olarak görülmemiş bir şey olan çekirdeğin açığa çıkması olayı Çernobil'de meydana gelmiş ve yerleşim yerinin, ülkenin hatta dünyanın kaderi bir profesörün eline bırakılmıştır. Belirli bir prosedürün olmaması sonucunda o anda alınabilecek en iyi kararlar alınmaya çalışılmış ve reaktörün üstü geçici olarak kapatılmıştır. Ancak geçen sürede radyasyon ciddi bir şekilde yayılmış ve Sovyetlerin olayı gizlemeye çalışmasında

rağmen Avrupa'nın çeşitli yerlerinde aktif olarak çalışan geiger sayaçlarının[17] verdiği alarmla ve yapılan çalışma ile böyle bir felaketin olduğu öğrenilmiştir. İran'da da aynı şey yaşanmış ve Cumhurbaşkanı Ahmedinejad'ın açıklamasında küçük bir zararın olduğu ancak bunun telafi edildiği belirtilmiştir. Her iki ülkenin de yaptığı bu açıklamanın temel nedeni iç politikadır. Ancak yaşanan böyle bir felaketin kamuoyundan gizlenmesi yalnızca o ülkeyi değil tüm dünyayı tehlikeye atmaktadır. Eski dönemlerde devletlerin bu tür girişimlerde bulunması anlaşılabilir bir durumdu. Düşman ülkelere karşı zayıf görünmemek ve işgal edilmemek adına kendini güçlü gösterme sadece devletlerin değil doğadaki tüm canlıların göstermiş olduğu bir reaksiyondur. Ancak günümüzde toprak fethetme olmadığı için devletlerin böyle bir endişelerinin olması tamamen değil ancak bazı yerlerde gereksizdir. Zira belirtildiği gibi günümüz dünyası bir siber dünyada devam etmekte ve bu dünyada her şey birbirine bağlıdır. Bu nedenle yaşanabilecek acı bir tecrübe yalnız orayla sınırlı kalmayabilir. Tıpkı Stuxnet'te olduğu gibi. Stuxnet'i fark edilebilir kılan şey bulaştığı bilgisayarların kendini kapatması olayıdır. Kullanıcıların bu şikâyeti üzerine yapılan incelemede ortaya çıkmıştır. Buradan da anlaşılacağı üzere devletler artık bu yöndeki davranışlarını da revize etmelidir.

Sonuç olarak siber dünyadaki anarşinin sonuçları ön görülemez ve yayılma kat sayısı reel dünyada yaşanan herhangi bir olaydan çok daha fazla olabileceği için devletlerarası ilişkilerde olduğu gibi bir evrim sürecinin olması beklenmemeli ve uluslararası hukukta gerekli önlemler alınmalıdır.

[17] Radyasyon düzeyini ölçmeye yarayan alet.

KAYNAKÇA

AA. (2020). *ABD-İran İlişkilerinin 67 Yıllık Tarihçesi* [Erişim: 14.08.2020, https://www.aa.com.tr/tr/dunya/abd-iran-iliskilerinin-67-yillik-tarihcesi/1693820]

Ağır, B. S. (2006). Bush Doktrini: Küresel Bir Hegomonik İstikrar Arayışı Mı? *Uluslararası ilişkiler Dergisi* 3(12), 71-100.

Altınkaynak, M. (2018). *Uygulamalı Siber Güvenlik ve Hacking,* Abaküs Yayınları, İstanbul.

Atar, E. (2020). *Bir Kararla Tarihi Yeniden Yazdılar.* [Erişim: 26.05.2020, https://www.sabah.com.tr/yasam/2011/09/09/bir-kararla-tarihi-yeniden-yazdilar]

Aydın, A. B. (2013). Uluslararası Hukukta Önleyici ve Öngörücü Meşru Müdafaa Hakkı, *Genç Hukukçular Hukuk Okumaları Birikimler 4, 51-64.*

Baylıs, J. (2012). *Uluslararası İlişkilerde Güvenlik Kavramı*, Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, Ursula Oswald Spring, Necati Polat (Der.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe,* İstanbul Bilgi Üniversitesi Yayınları, s.153-166.

Baysal, B. & Lüleci, Ç. (2015). Kopanhag Okulu ve Güvenlikleştirme Teorisi, *Güvenlik Stratejileri Dergisi* 11(22), 61-95.

Baysoy, E. (2015). Antik Dönemin Doğu Akdeniz Jeopolitiği. *Balkan Sosyal Bilimler Dergisi* 4(8), 13-21.

Beyoğlu, C. Ü. (2018). *Kuvvet Kullanma Yasağı Kapsamında Devletlerin Bireysel Meşru Müdafaa Hakkı.* Seçkin Yayıncılık.

Bidb (2020). *İnternetin Tarihçesi.* [Erişim: 06.02.2020, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi]

Birdişli, F. (2017). *Teori ve Pratikte Uluslararası Güvenlik: Kavram-Teori-Uygulama,* Seçkin Yayıncılık.

Bozkurt, E. (2007). *Uluslararası Hukukta Kuvvet Kullanımı*. Asil Yayın.

Buzan, B. (2015). *İnsanlar, Devletler & Korku,* (Çev.) Emre Çıtak, Uluslararası İlişkiler Kütüphanesi, İstanbul.

Buzan, B. (2017). *Barış, Güç ve Güvenlik: Uluslararası İlişkilerde Çatışan Kavramlar,* Esra Diri (Der.), Uluslararası İlişkilerde Anahtar Metinler, Der Yayınları, s.165-190.

Carnoy, M. (2015). *Devlet ve Siyaset Teorisi,* (Çev.) Simten Coşar, Aykut Örküp, Mete Pamir, Mehmet Yetiş, Dipnot Yayınları, Ankara.

Cavelty, M. D. (2017). *Siber Güvenlik,* Alan Collins (Ed.), Nasuh Uslu (Çev.), Çağdaş Güvenlik Çalışmaları, Uluslararası İlişkiler Kütüphanesi, s. 362-378.

Ceylan, S. G. (2004). Roma Hukukunun Günümüz Hukuk Düzenlerine Etkisi, *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 8(2), 0-0. Retrieved from https://dergipark.org.tr/tr/pub/ahbvuhfd/issue/48132/608803

Clarke, R. A. & Knake, R. K. (2010). *Siber Savaş*, (Çev.) Murat Erduran, T.C. İstanbul Kültür Üniversitesi Yayınevi, İstanbul.

Çelikpala, M. (2019). Güvenlik Topluluğu, *Güvenlik Yazıları Serisi,* No:43 Retrieved from https://trguvenlikportali.com/wp-content/uploads/2019/12/GuvenlikToplulugu_MitatCelikpala_v.1.pdf

Çifci, H. (2017). *Her Yönüyle Siber Savaş.*Tübitak Popüler Bilim Kitapları.

Demirtaş, B. (2019). Feminizm ve Güvenlik, *Güvenlik Yazıları Serisi,* No:3 Retrieved from https://trguvenlikportali.com/wp-content/uploads/2019/10/FeminizmGuvenlik_BirgulDemirtas_v.2.pdf

Digitalage (2020). *Teknoloji Tarihinden İlkler: İlk E-posta.* [Erişim: 06.02.2020, https://digitalage.com.tr/teknoloji-tarihinden-ilkler-ilk-e-posta/]

Ekren, A. (2017). 1979-1995 İran-ABD İlişkileri, *Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Dergisi*, 2(1), 146-155.

Elbahadır, H. (2019). *Hacking Interface.* Kodlab Yayınları.

Ersoy, E. (2014). Realizm, Ramazan GÖZEN (Der.), *Uluslararası İlişkiler Teorileri,* İletişim Yayınları, İstanbul, s. 159-187.

Follath, E. & Stark, H. (2020). *The Story of "Operation Orchard" How Israel Destroyed Syria's Al Kibar Nuclear Reactor.* [Erişim: 27.05.2020, https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html]

Gözen, R. (2014) *Giriş: Uluslararası İlişkiler, Teori ve Türkiye Tecrübesi,* Ramazan GÖZEN (Der.), Uluslararası İlişkiler Teorileri, İletişim Yayınları, İstanbul, s. 15-30.

Gözen, R. (2014) *İdealizm,* Ramazan GÖZEN (Der.), Uluslararası İlişkiler Teorileri, İletişim Yayınları, İstanbul, s. 67-119.

Grotius, H. (2011). *Savaş ve Barış Hukuk,* (Çev.) Seha L. Meray, Say Yayıncılık, İstanbul.

Gündüz, A. (2015). *Milletlerarası Hukuk.* Beta Basım.

Gzt (2020). *Beklenen Oldu. Peki, Sırada Ne Var?* [Erişim: 18.05.2020, https://www.gzt.com/mecra/beklenen-oldu-peki-sirada-ne-var-3356213]

Hasgüler, M. & Uludağ, M. B. (2012). *Devletlerarası ve Hükümetler Dışı Uluslararası Örgütler: Tarihçe-Organlar-Belgeler-Politikalar*. Alfa Yayınları.

Heywood, A. (2013). *Küresel Siyaset,* (Çev.) Nasuh Uslu & Haluk Özdemir, Adres Yayınları, Ankara.

Heywood, A. (2018). *Siyasetin ve Uluslararası İlişkilerin Temel Kavramları,* (Çev.) Fahri Bakırcı, BB101 Yayınları, Ankara.

Hobbes, T. (2018). *Leviathan,* (Çev.) Semih Lim, Yapı Kredi Yayınları, İstanbul.

Hook, S. W. & Spainer, J. (2014). *İkinci Dünya Savaşı'ndan Günümüze Amerikan Dış Politikası,* (Çev.) Özge Zihnioğlu Tanırlı, İnkilap Yayınevi, İstanbul.

Hürriyet (2020a). *BM'nin Irak Yaptırımları.* [Erişim: 26.05.2020, https://www.hurriyet.com.tr/gundem/bmnin-irak-yaptirimlari-103944]

Hürriyet (2020b). *Son Dakika... Kredi Kartıyla Vergi Ödeme Türleri Genişletildi.*[Erişim: 05.06.2020, https://www.hurriyet.com.tr/ekonomi/son-dakika-kredi-kartiyla-vergi-odeme-turleri-genisletildi-41481557]

International Court of Justice (ICJ). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) [Erişim: 26.05.2020, https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf]

İnsan Hakları Dairesi Başkanlığı (İNHAK). BM Antlaşması [Erişim:30.01.2020, https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf]

Jane, M. (2017). İran'ın Nükleer Politikasının Gelişimi ve Uygulanan Ambargo ve Yaptırımların Dış Politikasına Etkilerinin Analizi, *Bölgesel Araştırmalar Dergisi,* 1(2), 264-314.

Karabulut, A. & Değer, F. (2015). Uluslararası İlişkilerde Güvenlik Kavramı ve Realist Yaklaşım'a Genel Bakış, *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi* 2(2), 69-79.

Karakocalı, A. (2016). Roma Hukuku ve Uluslararası Hukuk, *Terazi Hukuk Dergisi* 11(115), 14-25.

Kaygusuz, Ö. (2014). Egemenlik ve Vestfalyan Düzen, Evren BALTA (Ed.), Küresel Siyassete Giriş: Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler, İletişim Yayınları, İstanbul, s.25-50.

Kaymaz, İ. Ş. (2007). Wilson Prensipleri ve Liberal Emperyalizm, *Atatürk Araştırma Merkezi Dergisi* 23(67-68-69), 145-174.

Kedikli, U. (2005), *BM Antlaşması'nda Meşru Müdafaa Hakkı.* (Yayınlanmamış Yüksek Lisans Tezi). Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Küçük, M. (2014). *Uluslararası İlişkilerde Sosyal İnşacılık*, Ramazan GÖZEN (Der.), Uluslararası İlişkiler Teorileri, İletişim Yayınları, İstanbul, s. 325-377.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon, *IEEE Security and Privacy: Building, Dependability, Reliability,and Trust The Science of Security*, 9(3), 49-51.

Mcdonald, G., Murchu, L. O., Doherty, S., Chien, E. (2013). Stuxnet 0.5: The Missing Link, *Symantec Security Response,* Versicon 1.0, 1-18.

Milliyet (2020a). *Mors Alfabesi.* [Erişim: 29.05.2020, http://blog.milliyet.com.tr/mors-alfabesi/Blog/?BlogNo=177472]

Milliyet (2020b). *Telefonu Kim Buldu? TelefonİIk Olarak Ne Zaman, Nasıl İcat Edilmiştir? Telefonun Tarihçesi* [Erişim: 29.05.2020, https://www.milliyet.com.tr/egitim/telefonu-kim-buldu-telefon-ilk-olarak-ne-zaman-nasil-icat-edilmistir-telefonun-tarihcesi-6211711]

Nicholas, F., Murchu, L. O., Chien, E. (2011). W32.Stuxnet Dossier, *Symantec Security Response,* Version 1.4, 1-69.

Nozick, R. (2015). *Anarşi, Devlet ve Ütopya,* (Çev.) Alişan Oktay, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

Nye, J. S., & Welch, D. A. (2015) *Küresel Çatışmayı ve İşbirliğini Anlamak* (Çev.) Renan Akman, Türkiye İş Bankası Kültür Yayınları, İstanbul.

Nye, Joseph S. (2020). *Yumuşak Güç,* (Çev.) Rayhan İnan-Aydın, BB101 Yayınları, Ankara.

Ongur, H. Ö. & Yavçan, B. (2014). *Uluslararası İlişkilerde Marksist Yaklaşımlar,* Ramazan GÖZEN (Der.), Uluslararası İlişkiler Teorileri, İletişim Yayınları, İstanbul, s. 257-289.

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

Özkaya, E., Sarıca, A. & Durmaz, Ş. (2019). *Siber Güvenlik: Saldırı & Savunma Stratejileri,* Buzdağı Yayınevi, Ankara.

Özpek, B. B. (2014). *Liberalizm ve Uluslararası İlişkiler,* Ramazan GÖZEN (Der.), Uluslararası İlişkiler Teorileri, İletişim Yayınları, İstanbul, s. 121-157.

Pirim, C. Z. (2019). Devletlere Atfedilmeyen Silahlı Saldırılara Karşı Meşru Müdafaa: Uluslararası Hukukta Sınır Ötesi Operasyonun Hukukî Zemini, *Türkiye Adalet Akademisi Dergisi* 0(40), 245-303.

Ponting, C. (2018). *Yeni Bir Bakış Açısıyla Dünya Tarihi,* (Çev.) Eşref Bengi Özbilen, Alfa Yayınları, İstanbul.

Roskin, M. G. & Berry, N. O. (2014). *Uluslararası İlişkiler: Uİ'nin Yeni Dünyası* (Çev.) Özlem Şimşek, Adres Yayınları, Ankara.

Sander, O. (2013). *Siyasi Tarih: 1918-1994*. İmge Kitabevi.

Sanger, D. E. (2012). *Obama Order Sped Up Wave Of Cyberattacks Against Iran.*[Erişim: 19.07.2020, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html]

Schmitt, M. N. (2017). *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations.* Cambridge University Press.

Singer, P. W. & Friedman, A. (2018). *Siber Güvenlik ve Siber Savaş: Herkesin Bilmesi Gerekenler,* (Çev.) Ali Atav, Buzdağı Yayınevi, Ankara.

Stanford (2020). *Operation Opera.* [Erişim: 28.05.2020, http://large.stanford.edu/courses/2016/ph241/sutter2/]

Sungur, N. (2020). *ABD'de Şer Ekseni Hazırlığı.* [Erişim: 28.05.2020, http://arsiv.ntv.com.tr/news/134221.asp]

Taşdemir, F. (2006). Uluslararası Anarşiye Giden Yol: Uluslararası Hukuk Açısından Önleyici Meşru Müdafaa Hakkı, *Uluslararası Hukuk ve Politika Dergisi* 2(5), 75-89.

Taylan, H. (2014), *Anarşizmin Felsefi Kökenleri.* (Yayınlanmamış Yüksek Lisans Tezi). Cumhuriyet Üniversitesi, Sosyal Bilimler Enstitüsü, Sivas.

The Atlantic (2020). *Letters To The Editor.* [Erişim: 04.06.2020, https://www.theatlantic.com/magazine/archive/2005/03/letters-to-the-editor/303727]

Türkoğlu, İ. & Seçilmiş, İ. E. (2006). Franz Oppenheimer'in Devlet Kuramı, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 14(1), 83-96.

Uğuz, A. (2016). Liberalizmde Güvenlik Kavramı ve Uluslararası Güvenliğe Getirilen Çözümler, Ümit G. & Eyüp Sami Y. (Ed.). *5. Lisansüstü Çalışmalar Kongresi Bildiriler Kitabı-2*s. 85-98.

Unıted Nation Documents (UNDOC). Definiton of Aggression [Erişim: 27.05.2020, https://undocs.org/en/A/RES/3314(XXIX)]

Uygun, O. (2019). *Devlet Teorisi.* Onikilevha Yayınları.

Waltz, Kenneth N. (2015). *Uluslararası Politika Teorisi,* (Çev.) Osman S. Binatlı, Phoenix Yayınevi, Ankara.

Wendt, A. (2013). Anarşi Devletler Ne Anlıyorsa Odur: Güç Politikalarının Sosyal İnşası, *Uluslararası İlişkiler Dergisi* 10(39), 3-43.

Wendt, A. (2016). *Uluslararası Siyasetin Sosyal Teorisi,* (Çev.) Helin Sarı Ertem & Suna Gülfer Ihlamur Öner, Küre Yayınları, İstanbul.

Wolfers, A. (2017). *Muğlak Bir Simge Olarak "Ulusal Güvenlik",*Esra Diri (Der.), Uluslararası İlişkilerde Anahtar Metinler, Der Yayınları, s.43-58.

Woodcock, G. (2014). *Anarşizm: Bir Düşünce ve Hareketin Tarihi,* (Çev.) Alev Türker, Kaos Yayınları, İstanbul.

Yalvaç, F. (2014) *Uluslararası İlişkilerde Teori Kavramı ve Temel Teorik Tartışmalar,* Ramazan GÖZEN (Der.), Uluslararası İlişkiler Teorileri, İletişim Yayınları, İstanbul, s. 31-65.

Yılmaz, B. A. (2020). Siber Terörizm ve Değişen İstihbarat Anlayışı, *Anadolu Strateji Dergisi* 2(1), 65-82.

Yılmaz, E. & Irk, O. (2015). Nikaragua Divan Kararları Işığında Kuvvet Kullanma ve Meşru Müdafaa Sorunu, *Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi* 13(2), 151-166.

ÖZGEÇMİŞ

Mesut Kesik; 1993 yılında Eskişehir'de dünyaya gelmiştir. İlk, orta ve lise öğrenimini Eskişehir'de tamamlamış ve lisans eğitimini de Dumlupınar Üniversitesi Siyaset Bilimi ve Uluslararası İlişkiler bölümünde 2016 yılında tamamlamıştır. 2017 yılında Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi ana bilim dalında yüksek lisans eğitimine başlamıştır. Yüksek lisans eğitimi sıranda Anadolu Üniversitesi Adalet Bölümü'nden mezun olmuştur.

Orcid: 0000-0003-3538-3198