KARADENİZ TEKNİK ÜNİVERSİTESİ*SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

ULUSLARARASI İLİŞKİLERİN KURAMSAL ÇERÇEVESİ VE SİBER GÜVENLİK KAVRAMININ ANALİZİ

YÜKSEK LİSANS TEZİ

Buğrahan EMİR

MAYIS-2020

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ*SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

ULUSLARARASI İLİŞKİLERİN KURAMSAL ÇERÇEVESİ VE SİBER GÜVENLİK KAVRAMININ ANALİZİ

YÜKSEK LİSANS TEZİ

Buğrahan EMİR

ORCID:0000-0003-4426-3278

Tez Danışmanı: Dr. Öğr. Üyesi Vahit GÜNTAY

MAYIS-2020

TRABZON

BİLDİRİM

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca KTÜ - Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzu'na uygun olarak hazırlanan bu Çalışmada yararlanılan kaynakların tümüne eksiksiz atıf yapıldığını, aksinin ortaya çıkması durumunda her tür yasal sonucu kabul edeceğimi beyan ederim.

Buğrahan EMİR
29.05.2020

ÖNSÖZ

Uluslararası İlişkiler bir disiplin olarak; hem teorik hem de olgusal açıdan tarihi süreçte yaşanan değişimlere uyum sağlamakta ve yol gösterici eğilimini devam ettirmektedir. Bu yaşanan değişimlerden biri de hiç kuşkusuz internetin yaygınlaşması ve olumlu yönlerinin yanı sıra olumsuz yönlerinin hem devletlerin hem de toplumların güvenliğine tehdit oluşturmaya başlamasıdır. Bu açıdan siber güvenlik çatısı altında inceleme olanağı bulunan siber saldırılar, siber terörizm, siber savaşlar yani bir bütün olarak siber olaylara yönelik ilgi de hem aktörler hem de araştırmacılar düzeyinde artmaktadır. Siber olaylar, konvansiyonel müdahale yöntemlerine göre belirli avantajları ve kolaylıkları barındırdığı için aktörler tarafından tercih edilmekte ve yeni bir müdahale biçimi olarak kullanılmaktadır. Çalışmada; siber saldırılar ve siber savaşların hangi açılardan Uluslararası İlişkiler disiplininin temel kavramlarını dönüştürdüğü ve aktörler tarafından tercih edildiği ortaya koyulmaya çalışılacaktır.

Bu çalışmanın karar aşamasından son halini almasına kadar geçen süreç içinde değerli bilgileri, yol gösterici ve içten tavrıyla çalışmaya ve şahsıma olan katkıları ayrıca göstermiş olduğu sabır sebebiyle danışman hocam Dr. Öğretim Üyesi Vahit GÜNTAY'a içten teşekkür ederim. Çalışmayla ilgili görüş ve önerilerini paylaşarak katkı sağlayan Doç. Dr. İsmail KÖSE ve Doç. Dr. Metin AKSOY'a teşekkürlerimi sunarım. Yoğun çalışma sürecim içerisinde göstermiş oldukları anlayış ve her koşulda yanımda olmaları sebebiyle babam Ali Kemal EMİR, annem Senem EMİR, kardeşim Kübra Nur E. TOPCU ve çalışmanın düzenlenmesinde yardımlarını esirgemeyen eşi Mehmet TOPCU'ya; ayrıca yüksek lisans sürecinde hayatıma dâhil olan Gülce TOPCU'ya teşekkür ederim. Yüksek lisans sürecimin ilk gününden son gününe kadar destekçim olan ve tecrübeleriyle yol gösteren Prof. Dr. Metin BERBER ve arkadaşlarım İlkay BOZ ile Berk ÇEVİK'e teşekkürü bir borç bilirim.

Mayıs, 2020 Buğrahan EMİR

İÇİNDEKİLER

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

ÖZET

Soğuk Savaş sonrası belirginleşen küresel terörizm, mikro milliyetçilik gibi yeni tehdit türlerinden biri de; kara, hava, deniz ve uzay harekât alanlarından sonra beşinci harekât alanı olarak nitelendirilen siber uzay üzerinden devlet ve toplum güvenliğine yönelik ortaya çıkan siber tehditler olmuştur. Dünya üzerinde internet kullanımının giderek yaygınlaşması ve internetin geçmiş dönemlerin geleneksel sınır algısını yok etmesi, bir bütün olarak internet ve ona bağlı elektrik, su, ulaşım, enerji gibi kritik altyapıları kapsayan siber alana gösterilen ilgide de belirgin artışlara sebep olmuştur. Bu süreçte devletler temel aktör olma konumlarını sürdürse de; devlet dışı örgütler, suç şebekeleri, çok uluslu şirketler gibi aktörlerin etkinlik kazanmasıyla Uluslararası İlişkiler disiplininde incelenen aktör algısında da değişimler yaşanmıştır.

Yeni aktörlerin interneti ve ilintili sistemleri kullanarak güvenliğe yönelik tehdit oluşturmasıyla siber güvenliği sağlayabilmek kamu ve özel sektör için elzem hale gelmiştir. Bu açıdan çalışmada, siber güvenliğe yönelik tehdit oluşturan siber suçlar, siber saldırılar, siber savaş ve siber terörizm gibi olgular açıklanarak ayırt edici yönleri ve etkin bir siber güvenlik oluşturmak için gerekenlerin ortaya konulması amaçlanmıştır. Ayrıca asimetrik özellik gösteren siber saldırılar ve siber savaşın, konvansiyonel saldırılar yerine ya da belirli durumlarda destek mahiyetinde yeni bir müdahale yöntemi olarak tercih edilebilirliği ölçülmeye çalışılmıştır. Bu açıdan konvansiyonel savaş yöntemleriyle siber savaşın özellikleri mukayeseli bir şekilde incelenmiş; örnek olaylar üzerinden de etki, kapsam, maliyet, atıf ve sorumluluk gibi çıktılarla siber savaşların tercih edilebilirliği sorgulanmıştır.

Siber uzayda hangi aktörün ne kadar bir siber gücü elinde bulundurduğunu tespit etmek saldırı-savunma dengesi açısından önem arz etmektedir. Devletlerin konvansiyonel kapasitelerini ölçebilmek gerçeğe yakın sonuçlar ortaya koyabiliyorken; siber kapasitelerini ölçebilmek farklı girdilerin hesaba katılması sebebiyle zor hale gelmektedir. Çalışmanın bir diğer amacı bu ölçümün gerçeğe en yakın şekilde yapılmasını sağlayabilmektir. Ayrıca siber güvenlik kavramının bir bütün olarak uluslararası ilişkiler disiplinini hangi açılardan dönüştürdüğünün klasik teoriler ve yaklaşımlar üzerinden ortaya konulması amaçlanmaktadır. Bu açıdan uluslararası ilişkiler disiplini içinde inceleme olanağı bulunan siber güvenlik kavramının benzeşen ve farklılaşan yönlerinin ortaya konulması amaçlanmaktadır.

Anahtar Kelimeler: Güvenlik, Kritik Altyapı, Siber Güvenlik, Siber Saldırı, Siber Savaş

ABSTRACT

One of the new threats which became evident after the Cold War such as global terrorism and micro nationalism has been cyber threats to the security of the state and society over cyber space, which is described as the fifth operation domain after land, air, sea and space operations domains. The widespread use of the internet in the world and the fact that the internet has destroyed the traditional border perception of the past have also caused significant increases in the interest shown in the cyber space, which includes the internet and critical infrastructures such as electricity, water, transportation, and energy. In this process, although the states continue being the main actors; actors such as non-governmental organizations, crime networks and multinational companies started standing out; thus perception of actors examined in the International Relations discipline have changed.

It became a must for the public and private sector to improve their cyber security skills as the mentioned actors caused new threats to security by using the internet and related systems. In this respect, the aim of this study is to explain the facts such as cybercrime, cyber attacks, cyber warfare and cyber terrorism, which pose a threat to cyber security, and to reveal its distinctive aspects and what it takes to create an effective cyber security. In addition, it is attempted to measure the preferability of cyber attacks and cyber warfare that show asymmetric features as a new intervention method instead of conventional attacks or to support them in certain situations. In this respect, the features of cyber warfare have been examined comparatively with conventional war methods; the preferability of cyber warfare has been questioned through outcomes such as impact, extent, cost, attribution and responsibility over case studies.

It is important to determine which actor possesses how much cyber power in cyber space, in terms of attack-defense balance. Measuring the conventional capacities of states has realistic results; measuring cyber capacities becomes difficult due to the different inputs taken into account. Another aim of the study is to ensure that this measurement is performed in the most realistic way. In addition, it is aimed to reveal how the concept of cyber security transforms the discipline of international relations as a whole through classical theories and approaches. In this respect, it is aimed to reveal the similar and differentiating aspects of the concept of cyber security, which can be examined within the discipline of international relations.

Keywords: Security, Critical Infrastructure, Cyber Security, Cyber Attack, Cyber Warfare

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GRAFİKLER LİSTESİ

Grafik Nr. **Grafik Adı** **Sayfa Nr.**

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AGİT	: Avrupa Güvenlik ve İşbirliği Teşkilatı
ARPA	: Advanced Research Projects Agency
ARPANET	: Advanced Research Projects Agency Network
BM	: Birleşmiş Milletler
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CCD COE	: Cooperative Cyber Defense Centre of Excellence
CDMA	: Cyber Defence Management Authority
CERN	: Conseil Européen pour la Recherche Nucléaire
CERT-EE	: Estonya Bilgisayar Acil Durum Müdahale Ekibi
CIA	: Central Intelligence Agency
COPRI	: Copenhagen Peace Research Institute
CSIS	: Center for Strategic International Studies
CSTB	: Computer Science and Telecommunications Board
Çev.	: Çevirmen
DDoS	: Distributed Denial of Service
Der.	: Derleyen
DoS	: Denial of Service
Ed.	: Editör
ENISA	: European Network and Information Security Agency
FBI	: Federal Bureau of Investigation
GRU	: Glavnoye Razvedyvatel'noye Upravleniye
IP	: İnternet Protokolü
IŞİD	: Irak Şam İslam Devleti
ITU	: International Telecommunication Union
KTÜ	: Karadeniz Teknik Üniversitesi
NASA	: National Aeronautics and Space Administration
NATO	: North Atlantic Treaty Organization
NCCT	: Network-Centric Collaborative Targeting
NSA	: National Security Agency
PLC	: Programmable Logic Controller
RBN	: Russian Business Network

SBU	: Security Service of Ukraine
SCADA	: Supervisory Control and Data Acquisition
SIPRI	: Stockholm International Peace Research Institute
ŞİÖ	: Şangay İşbirliği Örgütü
t.y.	: Tarih yok
USOM	: Ulusal Siber Olaylara Müdahale Ekibi
vd	: ve diğerleri
WWW	: World Wide Web

GİRİŞ

Uluslararası sistemin değişime ve dönüşüme uğradığı 1648 Westphalia Anlaşması'ndan sonra devletler aktör niteliği taşıyan en güçlü birimler olarak kabul edilmiştir. Devletlerin üstünde baskın hiçbir otoritenin olmadığı ve anarşik olarak nitelenen ortamda güvenliği sağlamanın devletin öncelikli amacı ve görevi haline geldiği düşünülmeye başlanmıştır. Ancak güvenlik kavramının özünün tartışmaya açık olması güvenlikle ilgili tanımların ve güvenliği sağlamaya dönük yaklaşımların çeşitlenmesine ve devletlerin de farklı yaklaşımlar benimsemesine yol açmıştır. Kimi ulus devletler güvenlik-özgürlük denkleminde ağırlığı özgürlük tarafına verirken; kimileri ise daha güvenlikçi bir yaklaşım benimseme yoluna gitmiştir.

Klasik anlamda ulusal ve uluslararası güvenliğe yapılan vurgu, Soğuk Savaş'ın bitişi ve ardından yaşanan küreselleşme sürecinin beraberinde getirdiği terörizm, milliyetçi çatışmalar, küresel ısınmanın yanı sıra internetin artan kullanımıyla birlikte siber olaylar gibi yeni tehditler sebebiyle dönüşüme uğramış ve bu tehditler büyük ölçüde ulus devletin kontrolü dışında meydana gelmeye başlamıştır. Özellikle internetin ve bilgisayar kullanımının dünya genelinde giderek yaygın hale gelmesi, beraberinde getirdiği birçok faydanın yanı sıra tehditlere maruz kalma riskini de arttırmıştır. Çünkü güvenlik-özgürlük denkleminde internet ve ona bağlı sistemler açısından ağırlık özgürlük kısmına hep daha yakın olmuş; internete erişimin belirli durumlar hariç tamamen engellenememesi belirleyici faktör olmuştur. Bu açıdan siber olayların aktif ve yeni bir tehdit şeklinde yer alması hem kapsayıcılık düzeyinin yüksek olması hem de sınırlanmasının zor olmasıyla doğrudan bağlantılı hale gelmiştir. Ayrıca devletlerin kritik altyapıları ve bilgi sistemleriyle siber alana artan entegrasyonu güvenlik açıklarını da aynı oranda arttırmış; problem alanını daha da genişletmiştir.

Özellikle 1990'lı yılların ortalarından itibaren hem terörizmin hem de kritik altyapıların korunmasının siber güvenlikle ilişkili olduğu fark edilince yeni gelişen bu alana gerek devletler gerek devlet dışı örgütler ve bireyler tarafından gösterilen ilgi de ivme kazanmıştır. Hatta bir dönem siber olaylar Amerika Birleşik Devletleri (ABD) tehdit listesinde en tepeye tırmanmış; siber terörizme, kitle imha silahları ve nükleer silahlar kadar hatta onlardan daha ciddi bir sorun gözüyle bakılmıştır. 2000'li yılların başından itibaren ise sınıflandırılmış bilginin değer kazanması ve teknolojinin gelişimiyle birlikte değerli bilgileri içeren ve yeni bir harekât sahası olarak görülen siber alana yönelik saldırılarda artış yaşanmıştır. Bu bağlamda etkin bir siber güvenlik sağlayabilmek gün geçtikçe gereklilik haline gelmiş aynı zamanda tehdit çeşitliliği sebebiyle giderek zorlaşmıştır.

Siber güvenliğe yönelik bir tehdit olarak ortaya çıkan ve kimi zaman hibrit savaş yöntemleri içerisinde operasyonel bağlamda tercih edilen siber savaşlar ya da onları savaş yapan saldırılar ise zaman içinde bireyler, örgütler ve devletler nezdinde ciddiye alınması gereken sonuçlar doğurmuştur. Kimilerine göre kullanılan saldırı yöntemleri ve ortaya çıkardıkları etki bakımından bir savaş kimliği atfedilmese de siber savaşlar gerçekleşmekte ve güvenliği tehdit etmektedir. Bu açıdan siber alanda gelişim gösteren ve kapasitelerini arttıran aktörler günümüzde bir adım öne geçecek gibi gözükmektedir.

Siber güvenlik çatısı altında inceleme olanağı bulunan siber savaşlar ve bağlantılı olarak siber saldırıların yıllar içinde artış göstermesi bunun nedenlerinin detaylı bir incelemesi gereğini doğurmuş ve bu yönde yapılan çalışmalar hız kazanmıştır. "Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi" isimli bu tez benzer bir çalışmanın ürünüdür ve bu nedenleri detaylı olarak ortaya koymayı; siber saldırılar ve aktörler arasındaki ilişkileri detaylı bir şekilde incelemeyi amaçlamaktadır.

Daha önce ayrı ayrı incelenen siber savaş ve siber saldırı örneklerinin bütüncül bir okuması yapıldığında siber uzaydan gelebilecek tehditlere ilişkin bir çerçeve ortaya koymak amaçlanmaktadır. Ayrıca devletlerin siber alana bağımlılıkları ve saldırı/savunma güçleri farklılık göstermekte bu nedenle doğru bir siber güç sıralaması ortaya koyabilmek önem taşımaktadır. Çalışmanın diğer bir amacı bu sıralamayı farklı girdilerle tespit ederek gerçeğe en yakın sonuçları ortaya koyabilmektir. Bu sonuçların ortaya koyulması siber alanda politikalar geliştirmeyi amaçlayan aktörler açısından önem taşımaktadır.

Bu açıdan çalışmanın araştırma soruları; ulusal ve uluslararası güveliği tehdit eden *siber savaşların, devletler özelinde konvansiyonel savaşlar yerine tercih edilebilir olup olmadığını belirlemeye odaklanmaktadır.* Siber uzayın kendine has yapısı güçlü/güçsüz devlet ayrımını belirsizleştirmekte; devletler için siber savaşları cazip hale getirmektedir. *Siber savaşlar, devletlerin giriştiği konvansiyonel savaşlarda destek işlevinde mi kullanılmakta yoksa devletler tarafından başlı başına bir müdahale yöntemi olarak mı tercih edilmektedir midir* sorusu ise çalışmanın diğer sorunsallarından birini oluşturmaktadır.

Yalnızca devletler değil; bireyler ve örgütler gibi devlet dışı aktörlere de hareket kolaylığı sağlayan siber uzayda bu aktörlerden devletlere ve toplumlara yönelebilecek siber saldırıların hangi özellikler açısından tercih edilebilir olduğunu belirlemek önemlidir. Çünkü Soğuk Savaş sonrası devletlerin ajandasında güvenliğe yönelik tehdit unsurlarına eklenen bireyler ve organize gruplar siber uzayın sağladığı anonimlik, giriş maliyetlerinin ucuzluğu gibi özellikler sayesinde etkilerini arttırabilmektedir. Bu açıdan çalışmanın bir diğer sorunsalı, *bu özellikleri tespit etmek ve gerçekleşmiş siber saldırı örnekleriyle tartışmaya tabi tutmaktır*.

Uluslararası İlişkiler disiplininde yeni bir boyut olan siber güvenlik ve ilintili olarak siber savaşlar ve saldırılara ilişkin klasik teorilerin ve güncel yaklaşımların belirli bir çerçeve etrafında yorumlanması önem taşımaktadır. Bu sayede teorik kalıplar siber güvenlik bağlamında yorumlanabilir ve farklı sonuçlara ulaşılabilir. Çalışmanın bir diğer sorunsalı ise, *teorilerin yorumlanması sonucu siber güvenliğin hangi açılardan uluslararası ilişkileri hem bir disiplin olarak hem de bir olgu olarak şekillendirdiğinin ve dönüştürdüğünün ortaya koyulmasıdır*.

Çalışmada eleştirel kaynak tarama yöntemiyle, açık kaynaklardan elde edilen bilimsel makaleler, kitaplar; Avrupa Birliği (AB), Kuzey Atlantik Antlaşması Örgütü (NATO) ve Birleşmiş Milletler (BM) gibi uluslararası örgütlerin, Symantec, Verisign, McAfee gibi şirketlerin ve Türkiye, ABD, Çin, Rusya gibi ülkelerin yayımladığı raporlar ve strateji belgeleri; yerli ve yabancı gazetelerin arşivlerinden elde edilen açık kaynaklardan yararlanılmıştır. Örnek olaylar ise 2007-2013 yılları arasında gerçekleşen, Rusya, ABD, Çin ve İsrail eksenli; ortaya çıkardığı etki ve siber güvenlik algısı üzerinde yarattığı değişimler baz alınarak seçilmiştir. Ayrıca bölümler arasındaki bilgiler birbiriyle bağlantılı özellik gösterecek şekilde aktarılmıştır. Örneğin önce siber saldırı yöntemleri ortaya koyulmuş; daha sonra bu yöntem kullanılarak gerçekleştirilen siber saldırılardan seçilen örnek olaylar verilmiştir.

Bu sorunsalların cevaplanması amacıyla çalışmanın birinci bölümünde, öncelikle siber alandaki kavramlara ilişkin temel bir çerçeve oluşturulacak ve *siber uzay, siber güvenlik* ve *siber tehdit* kavramlarının literatürdeki tanımlayıcı özellikleri ve ayırt edici yönleri ortaya koyulacaktır. Ardından sıkça birbirine karıştırılan *siber suç* ve *siber terörizm* kavramları incelenerek teknik özellikleri aktarılacaktır. Daha sonra *siber saldırı* kavramına açıklık getirilip farklı tür siber saldırıların ayırt edici yönleri ayrıca siber saldırılarda kullanılan *saldırı yöntemleri* ve *siber silahlar* tanımlanacak ve *siber silahların ekonomik etkilerine* de değinilerek bir çerçeve ortaya koymak amaçlanacaktır. Ayrıca genellikle birbirinin yerine kullanılan siber saldırı ve siber savaş kavramlarına ilişkin ayırt edici açıklamalar ortaya koyulacaktır. Son olarak *siber savaş* kavramı ele alınacak ve *caydırılık* konusu siber güvenlik bağlamında tartışılacaktır.

Araştırma sorularıyla bağlantılı olarak çalışmanın ikinci bölümünde, uluslararası ilişkiler teorileri olan *Realist ve Yapısal Realist Teori, Liberal ve Neoliberal Teori, Sosyal İnşacı Teori, Güvenlikleştirme* ve son olarak *Küreselleşme* kavramıyla siber alanın uluslararası ilişkiler içerisindeki kuramsal tartışması yapılacaktır. Siber güvenlik konusunun incelenebileceği kendine has bir teorisinin olmaması sebebiyle burada yapılan tartışmalar önem taşımaktadır. Uluslararası İlişkiler kuramlarının, siber güvenlik eksenli bir okumasının yapılması, kuramların siber uzayı açıklamada eksik kaldığı noktaların ortaya konulması açısından önem taşımaktadır.

Çalışmanın üçüncü ve son bölümünde ise öncelikle *siber savaş kapasitelerine* ilişkin genel bilgiler verilerek ülkelerin bu kapasitelerinin ölçümü ve sonuçları aktarılacaktır. Ayrıca siber alanda aktif olan ülkelerin kapasiteleri karşılaştırmalı şekilde analiz edilecek ve siber alana liderlik eden ülkelerin hangileri olduğu sorusuna yanıt bulmaya çalışılacaktır. İkinci olarak, Soğuk Savaş'ın ardından güvenliği tehdit eden, *Rusya kaynaklı olduğu iddia edilen dezenformasyon ve bilgi savaşının tezahürü olan ve hibrit savaş konseptinin bir ayağı olarak kullanılan siber saldırılar*; *Çin kaynaklı olduğu iddia edilen siber casusluk amaçlı siber saldırılar*; *ABD ve İsrail kaynaklı olduğu iddia edilen siber sabotaj casusluk girişimi amaçlı siber saldırılar* kullanılan yöntemler, ortaya çıkardığı etki ve sonuçları bakımından tarihsel bağlam içerisinde aktarılacaktır.

BİRİNCİ BÖLÜM

1. SİBER GÜVENLİK VE KAVRAMSAL ÇERÇEVE

1.1. Siber Alana İlişkin Kavramsal Çerçeve

Bilgi insanlık tarihi boyunca hep var olmuştur ve ihtiyaçlar bilgi birikimine göre şekillenmiştir. Tarihçiler de bilgiyi aktarırken ve tarih öncesi dönemleri adlandırırken, insanoğlunun hayatını devam ettirmek için icat ettiği aletlerin/araçların isimlerinden faydalanmıştır. Tarih öncesi devirlerin isimleri yeni madenlerin ve araçların ortaya çıkışıyla şekillenmiştir. Yazının bulunması İlkçağı başlatmış, Yeni Çağ olarak adlandırılan dönem ise İstanbul'un fethedilmesiyle başlamıştır. Son olarak Fransız İhtilali'nden bugüne kadar geçen süreyi betimlemek için Yakınçağ ifadesi kullanılmaktadır. 20. yüzyılın ortasından günümüze kadar geçen zamanı kapsayan ancak resmi olarak tanımlaması yapılmayan süreçle alakalı kullanılabilecek en doğru tanımlama ise insanoğlunun yaşamına yaptığı doğrudan etkiye bakıldığında Bilgi/İnternet Çağı şeklinde olabilir (Arıcak, 2015:13).

Çağa adını verdiğini iddia ettiğimiz dar kapsamıyla internetin, daha geniş kapsamıyla iletişim teknolojilerinin ortaya çıkışı ise Soğuk Savaş'ın iki cephesinden birini oluşturan Sovyetler Birliği'nin 4 Ocak 1957 yılında *Sputnik II* isimli uydusunu uzaya göndermesi sürecine kadar dayandırılabilir. Bu gelişmenin ardından ABD'nin bu alanda Sovyetler Birliği'yle mücadele edebilmesi adına Şubat 1958'de, *İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency, ARPA)* kurulmuştur (Darıcılı, 2017:4). 1962'de bilimsel çalışmalara katılan ARPA uzmanlarının ortak bir ağ kullanarak birlikte çalışmalarını sağlayabilmek için *İleri Araştırma Projeleri Ajansı Ağı (ARPANET)* kurulmuş ve böylece ilk ortak ağ ortaya çıkmıştır. Ancak belirtmek gerekir ki ARPANET askeri amaçlı bir ağdır. Çünkü ARPA mühendislerinin en önemli görevleri, Sovyetler Birliği'nin Soğuk Savaş süreci içinde ispatlamış olduğu teknolojik üstünlüğü ortadan kaldırmak ve fiziksel temelleri olan bir saldırı sonrası iletişimi sürdürebilmeyi sağlamaktır. Bu süreçten sonra ARPANET, İngiliz ticari ağı ve Fransız araştırma ağı ile birleşmiş ve ilk uluslararası ağ olarak niteleyebileceğimiz *Bilgisayar Ağlarının Uluslararası Ağı (International Network of Computer Networks*) kısıtlı bir kullanıcı çevresi için erişime açılmıştır (Bıçakçı, 2014:104-105).

1980'li yıllara geldiğimizde internet artık daha çok insan tarafından kullanılır duruma gelmiştir. 1989 yılında İngiliz bilim insanı olan Tim Berners Lee Avrupa Nükleer Araştırma

Merkezi'nde (CERN) çalışırken, *world wide web (www)* kavramını ortaya atmıştır. Esasen Web, dünyanın çeşitli yerlerindeki üniversite ve enstitülerde çalışan bilim insanlarının kesintisiz bilgi paylaşımı talebini karşılamak üzere tasarlanmış ve geliştirilmiştir. 1993 yılında CERN, www tasarımını kamusal alanla paylaşmıştır. Böylece CERN'deki ilk internet www projesinin kendisine ithaf edilerek kullanıcıların hayatına dâhil olması kararlaştırılmıştır (The Birth of the Web (t.y.), https://home.cern/science/computing/birth-web).

1.1.1. Siber Uzay Nedir?

Siber kelimesi köken olarak eski Yunanca *Kübernetes* sözcüğünden ortaya çıkartılmış ve temel olarak *sibernetik* kavramına dayandırılmıştır. Sibernetik kavramı ise *"teknolojik, biyolojik, sosyolojik ve ekonomik sistemlerde, kumanda uç iletişim sistemlerini incelemeye dayanan bir amaca doğru yönlendirilmiş etki bilimi"* şeklinde tanımlanabilir (Bayraktar, 2015:13). Sibernetik kavramı ilk olarak 1958 yılında sibernetik biliminin öncüsü olarak kabul edilen ve canlılar ile makineler arasındaki iletişimi inceleyen Louis Couffignal tarafından kullanılmıştır (Yılmaz, 2017:28).

Siber uzay ise, sanal yaşamlar ve toplulukların yaşadığı sanal alanlar olarak adlandırılabilir. Sebebi, yaşamların ve toplulukların gerçek toplumların sahip olduğu fiziksel gerçekliğe sahip olmamasından ileri gelmektedir (Jordan, 2003:1). Siber uzay kavramı ilk kez bilim kurgu yazarı William Gibson tarafından *Burning Chrome* isimli eserinde kullanılmıştır (Gibson, 1982:248). Gibson 1984 yılında kaleme aldığı ve bir bilgisayar korsanının Matrix ismindeki bir bilgisayar sistemi içindeki yaşadıklarını anlattığı *Neuromancer* romanında siber uzay kavramını daha da detaylandırma yoluna gitmiş ve siber uzayı; *"her ülkeden milyarlarca meşru kullanıcı tarafından, her ülkedeki matematiksel kavramlar öğretilen çocuklar tarafından deneyimlenen bir fikir, halüsinasyon. İnsan sistemindeki her bilgisayarın bankalarından soyutlanmış verilerin grafik gösterimi. Düşünülemez karmaşıklık"* şeklinde ifade etmiştir (Gibson, 1984:69). Esasında bu roman yalnızca siber uzay tanımlamasının yer alması açısından değil, ayrıca *sanal gerçeklik (virtual reality)*, *yapay zekâ (artificial intelligence)* ve *genetik mühendisliği (genetic engineering)* benzeri o dönem için çok yeni olan ancak geleceğe ışık tutan kavramların da işlendiği ilk eser olması açısından önem arz etmektedir (Keleştemur, 2015:133).

Farklı görüşler ışığında, Libicki ise siber uzaya ilişkin farklı bir tanımlama getirmiş ve siber uzayı *"kara, deniz, hava ve uzaydan bağımsız, iletişim altyapılarını kullanan sanal bir ortam"* olarak ifade etmiştir. Aynı zamanda karşıtlıkları barındırdığını da belirtmiştir. Siber uzayın kara, hava, deniz gibi diğer çekişme alanlarına benzediğini ancak diğerlerinden farklı olduğunu da eklemektedir (Libicki, 2009:11-12). Bu düşüncelerden hareketle daha geniş bir siber uzay tanımına ihtiyaç olduğu söylenebilir. Bu geniş tanımlardan biri, Andress ve Winterfeld (2011:20) tarafından *"Siber uzay, bilgisayarlar, bilgisayar donanımları (buna gömülü bilgisayar çiplerine sahip silah*

sistemleri de dâhildir), yazılım (hem özel sektör hem devlet tarafından geliştirilenler), protokoller, mobil cihazlar ve bu sistemin hareket etmesini sağlayan insanlar tarafından oluşur" şeklinde yapılmıştır.

Literatürde genel hatlarıyla farklı şekillerde tanımlanan siber uzaya ilişkin ülkemizde ise siber güvenlik stratejisinden sorumlu olan Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın getirdiği belirli tanımlamalar vardır. Türkiye'de 2016-2019 yılları arasını kapsayan Ulusal Siber Güvenlik Stratejisi'nde siber uzay, *"dünyanın her yerine ve dahi uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunlar arasındaki bağlantıyı sağlayan ağlardan oluşan veya bağımsız halde bulunan bilgi sistemlerinden oluşan sayısal ortam"* şeklinde tanımlanmıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi (t.y.), https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf). Daha eski tarihli Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda ise siber ortam başlığı altında tanımlanmış ve "*bağımsız halde bulunan bilgi sistemlerinden oluşan sayısal ortam"* kısmı tanımlamaya dâhil edilmemiştir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı (t.y.), https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf).

Çeşitli tanımlar ışığında söylenebilir ki siber uzay her şeyden önce bir bilgi ortamıdır. Oluşturulabilen, depolanabilen ve belki de en önemlisi paylaşılabilen dijitalleştirilmiş verilerden oluşmaktadır. Bu durum siber uzayın yalnızca fiziksel bir yer olmadığını ve bundan dolayı da herhangi bir fiziksel boyutta ölçümü karşılamayacağı anlamına gelmektedir. Ancak ifade etmek gerekir ki siber uzay tamamen sanal değildir. Fiziksel olarak veri depolayan bilgisayarları, bunun yanı sıra akışa izin veren sistemleri ve altyapıları içerir. Dijital dünya için sıklıkla internet tanımı kullanılırken, siber uzay eş zamanlı olarak bilgisayarı kullanan, arka planında yer alan insanları ve bu insanların bağlantılarının toplumu nasıl değiştirdiğini de içine almaktadır. Yani siber uzayın en önemli özelliklerinden birisi sistemlerinin ve teknolojilerinin insan üretimi olmasıdır (Singer ve Friedman, 2014:13-14). Son yıllarda hızla gelişen teknolojik yeniliklerle birlikte siber uzaydaki sistemler ve teknolojiler yalnızca insan üretimi olmaktan çıkmış, yapay zekâ, nesnelerin interneti[1] gibi yeni teknolojiler de siber uzayı oluşturan ögeler arasında yer almaya başlamıştır. Bu açıdan daha genel şekilde siber uzay, birbirlerine bağlı bilişim sistemlerinin hem insanlarla etkileştiği hem de bilişim sistemlerinin birbirleriyle etkileşim içinde olduğu fiziksel olmayan alanı ifade etmektedir (Bıçakçı, 2014:106).

Farklı tanımlar ışığında, her alanın doğrudan siber uzay/alan olarak ifade edilemeyeceği söylenebilir. Böyle bir ifadeyi ortaya koyabilmek için belirli özellikler tanımlamak gerekmektedir. Bu özelliklerden birincisi siber uzayın sahip olduğu katmanlardır. Dört önemli katmanın

[1] Nesnelerin İnterneti (Internet of Things: IoT) cihazların, farklı cihazlar ve platformlar ile internet aracılığıyla iletişim halinde olması olarak tanımlanmaktadır (Sağıroğlu ve Alkan., 2018:270).

varlığından bahsedilebilir. *Siber deneyime katılan insanlar* ilk katmanı oluşturmaktadır. Bu insanlar iletişim kuran, bilgiyle çalışan, karar veren ve planlayan ve bu çalışmalarıyla siber alanın doğasını dönüştüren insanlar olarak ifade edilebilir. Siber ortamda *depolanan, aktarılan ve dönüştürülen bilgiler* ikinci katmanı oluşturmaktadır. Bilginin yaratılması, yakalanması, depolanması ve işlenmesi deneyim için kilit bir önem taşımaktadır. *Mantıksal yapı taşları* üçüncü katmanı oluşturmaktadır. Mantıksal yapı, hizmetleri oluşturur ve siber uzayın platform yapısını destekler. Son olarak *mantıksal unsurları destekleyen fiziksel temeller* yer almaktadır (Clark, 2010:1-3).

Bu dört katman özelliğinin yanında siber uzay kendine has belirli karakteristik özelliklere de sahiptir. İlk olarak ifade edilmesi gereken konu *zamansallıktır*. Siber uzay geleneksel zamansallığı yakın anlılıkla değiştirir. İkinci olarak coğrafi ve fiziki konumun sınırlarını aşma olarak ifade edilebilecek olan *fiziksellik* gelmektedir. Üçüncü olarak *nüfuz etme* özelliği ön plana çıkmaktadır. Yani sınırları ve yetki alanlarını aşar. Dördüncü özellik ise *akıcılık* olarak ifade edilebilir. Akıcılık, sürekli değişkenlik ve yeniden yapılandırmayı ifade etmektedir. Beşinci özelliği *katılım* oluşturmaktadır. Siber uzay, politik ifade ve aktivizmin önündeki engelleri azaltmaktadır. Altıncı özellik olarak *atfetme* gelmektedir. Yani aktörlerin kimliklerini ve o olayla ilgili bağlantıları gizlemek. Son olarak ise *hesap verme zorunluluğu* karşımıza çıkmaktadır. Siber uzayda sorumluluk mekanizmaları kolayca atlanabilmektedir (Choucri, 2012:4). Yukarıda saydığımız özellikler gerek devletler gerek devlet dışı aktörler ve bireyler için siber uzayın artan önemini gözler önüne sermektedir.

Yukarıda sayılan özellikleri ve farklı tanımlamaları ile birlikte siber uzay olarak adlandırdığımız alan günlük yaşantımızın vazgeçilmez bir gerçeği haline gelmiştir. Doğası gereği hemen hemen her yerde bulunabilmesi, kapsamı ve geniş ölçeği nedeniyle, siber uzay yaşadığımız dünyanın temel bir gerçekliği halini almıştır. Gelişmiş dünyadaki hemen hemen herkes için ve gelişmekte olan dünyadaki birçokları için yeni bir gerçeklik yaratmıştır. Bu sebeple siber uzayın politik önemi görmezden gelinemez. Siber uzay, hükümetler, ordular, özel şirketler ve sivil ağlar tarafından yoğun bir şekilde tartışılmakta, sömürülmekte ve yeniden şekillendirilmektedir (Choucri, 2012:3-8).

Kara, hava, deniz ve uzayın ardından *beşinci muharebe alanı* (Güntay, 2018:101) olarak adlandırılan siber uzayın ne denli önemli olduğu da bu şekilde ifade edilebilir. Fiziksel dünyada yaşanan gelişmeler karşılığını siber uzayda bulabilirken; siber uzayda yaşanan gelişmeler de yankılanmalarını fiziksel dünyada bulabilir. Bu yüzden siber uzay ve fiziksel dünya gün geçtikçe birbirinden ayrılamaz bir hale gelmekte ve aktarılan çeşitli yaklaşımlar da siber uzayın yalnızca bilgisayar, internet gibi dijital varlıklara sahip olmadığını ve bunlardan çok daha fazlası olduğunu ortaya koymaktadır.

1.1.2. Siber Güvenlik Nedir?

Tarih boyunca insanın temel amaçlarından biri güvenliğini sağlamak olmuştur. Kimi zaman bu ihtiyacını bireysel olarak sağlamaya çalışmış, kimi zaman ise ittifaklar kurma yoluna gitmiştir. Bu ittifaklar bölgesel ve ulusal olabildiği gibi uluslararası ve hatta ulus üstü şekilde de olabilmiştir. Bu açıdan tarihin her döneminde insanın ve insanın kurmuş olduğu yapıların güvenliğini sağlamak birincil amaç olagelmiştir. Güvenlik denince kimin güvenliğinin sağlanacağı yani güvenliğin öznesi tarihin belirli dönemlerinde değişiklik göstermiştir. Bazen salt bireyin güvenliği kastedilirken; bazen devletin ve sistemin güvenliğinden bahsedilmiştir. Günümüzde, sağladığı fayda ve getirdiği tehlikelerle birlikte internetin ve siber uzayın güvenliği de öncelikli konulardan biri haline gelmiştir. Dünya nüfusunun yaklaşık 7 milyara ulaşması (Current World Population (t.y.), https://www.worldometers.info/world-population/?) ve bu nüfusun yaklaşık 5 milyarının (Global Social Media Users Pass 3.5 Billion (t.y.), https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion) internet kullanıcısı olması göz önüne alınırsa siber dünyanın güvenliğinin sağlanmasının önemi daha açık bir şekilde ortaya çıkmaktadır.

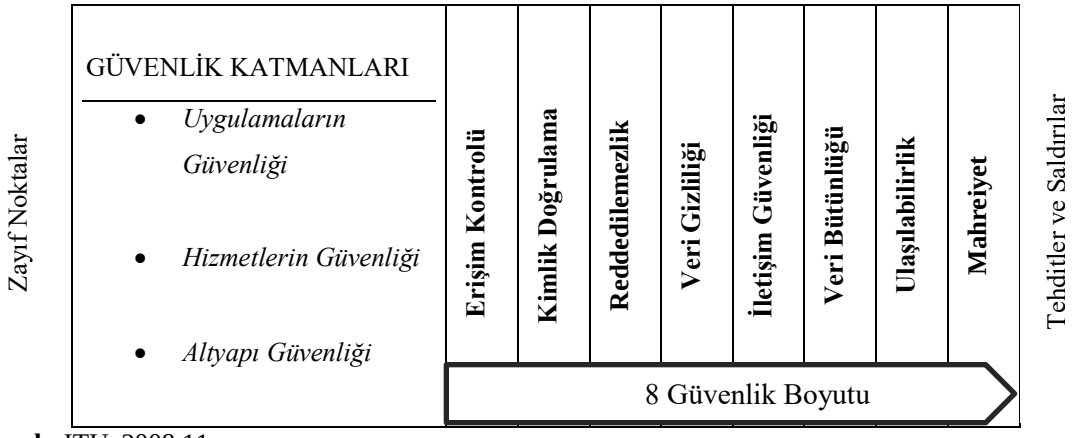
Güvenliği sağlamak için önce güvenliğin öznesi belirlenmelidir. Ancak karakteristik yapısından dolayı güvenliği sağlanacak olan öznenin belirlenmesinin zor olması *siber güvenlik* kavramının tanımlanmasına da yansımıştır. Siber uzay tanımında karşılaştığımız gibi siber güvenlik için de farklı tanımlamalar mevcuttur ve üzerinde uzlaşı sağlanmış bir tanımı bulunmamaktadır. Bu zorluk siber uzayın belirli sınırlarının olmaması bu sebepten neyin, kim tarafından korunacağının net olmamasından ileri gelmektedir. Ayrıca siber güvenlik kavramı, bilgi güvenliği ve bilgisayar güvenliği kavramlarıyla benzer anlamlarda kullanılabilmektedir. Benzerlik, bilgi güvenliğinin çoğunlukla kişisel ve kurumsal verilerin güvenliğiyle ilgili bir kavram olarak kullanılması ve bilgisayar güvenliğinin ise bilişim sistemlerinin tamamının güvenliği şeklinde kullanılmasından gelmektedir. Bu açıklamalar ışığında yapılan farklı tanımlar incelendiğinde, Uluslararası Telekomünikasyon Birliği'nin (ITU) tanımına göre, *siber güvenlik, veriler gibi varlıkların ve kritik kaynakların yetkisiz erişime, manipülasyona ve imha edilmesine karşı korunmasıyla ilgilidir* (ITU Global Security Agenda (GCA) A Framework for International Cooperation in Cybersecurity (t.y.) https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf).

Daha geniş bir tanımda ise, "*siber uzayda yer alan sistemlerin güvenliğini sağlamak (gizliliğinin, bütünlüğünün ve erişilebilirliğine zarar gelmemesi için uğraşmak) maksadıyla alınan tedbirler, bu amaca uygun olarak yürütülen faaliyetler, ortaya konan standartlar ve kurallar bütününe"* siber güvenlik denir. (Çifci, 2017:8). ABD eski başkanlarından Obama tarafından yapılan bir açıklama ise karar alıcıların siber güvenliğe bakış açısını yansıtmakta ve aslında siber güvenliğin ne düzeyde önemli olduğunu gözler önüne sermektedir. Obama açıklamasında siber güvenliğin, bir ülke için karşı karşıya bulunabileceği en ciddi ulusal güvenlik ve ekonomik tehdit olduğunu vurgulamıştır (Petangon'da bir ilk: Siber Savaş Birimi (24.05.2010),

https://www.cnnturk.com/2010/dunya/05/24/pentagonda.bir.ilk.siber.savas.birimi/577439.0/index.html).

Bu tanımlamalar ışığında siber güvenliğin, bilgi güvenliği ile doğrudan alakalı olduğu ifade edilebilir. O halde bilgi güvenliğini sağlayabilmek, siber güvenliği sağlamak açısından büyük bir anlam ifade etmektedir. Klasik anlamda bilgi güvenliği, bu durumda bilginin *gizliliği (confidentiality), bütünlüğü (integrity)* ve *erişilebilirliği (availability)* anlamına gelen ve C.I.A olarak kısaltılan kavramların sağlanmasıyla mümkün olabilmektedir. *Gizlilik*, bilgilerin yetkisiz kişilere açılmasının önlenmesi anlamına gelmektedir. Yetkili kişiler bu bilgilere erişim sağlayabilirken eş zamanlı olarak yetkisi olmayan kişilerin bu bilgilere erişimini engeller ve böylece koruma sağlamaktadır. Bilginin gizliliği, şifreleme (bilginin sır kullanılarak dönüştürülmesi), erişim kontrolü (bilmesi gereken kişilere ve/veya sistemlere sınırlı erişim sağlama), kimlik doğrulama ve yetkilendirme (bir kişi veya sistemin kaynaklara erişime izin verilip verilmediğinin belirlenmesi) yoluyla sağlanır. Bilgi güvenliğinin bir diğer yönünü oluşturan *bütünlükten* kasıt ise, bilginin yetkisiz kişiler tarafından değiştirilmesinin imkânsız hale getirilmesidir. Bütünlüğü sağlamanın yolları arasında yedekleme (bilgiyi belirli periyodlarla arşivleme), sağlama toplamı (bir dosyanın içeriğini sayısal bir değerle eşleştiren bir fonksiyonun hesaplanması) ve veri düzeltme yöntemleri (küçük değişiklikleri kolayca tespit edebilecek ve otomatik olarak düzeltebilecek veri saklama yöntemleri) kullanılabilir. Gizlilik ve bütünlüğün yanı sıra bilgi güvenliğine etki eden bir diğer önemli faktör yetkisi bulunan kişilerin zamanında erişebildiği ve değiştirebildiği özellik olan *erişilebilirliktir*. Bu da fiziksel korumalar (altyapı olarak inşa edilir ve fiziksel zorluk durumunda bile bilgiye erişimi mümkün kılar) ve hesaba dayalı (arıza durumunda yedek hizmet veren bilgisayar aygıtları) fazlalıklardır. Bilgi güvenliğinin sağlanması noktasında bu üç aşama büyük önem arz etmektedir (Goodrich ve Tamassia, 2014:3-8).

Şekil 1: Güvenlik Boyutlarını Güvenlik Katmanlarına Uygulama



Kaynak: ITU, 2008:11

Şekil 1, her güvenlik katmanında var olan güvenlik açıklarını azaltmak için güvenlik boyutlarının, güvenlik katmanlarına nasıl uygulandığını göstermektedir. Siber güvenlik, dışarıdan gelen tehditler ve saldırılar karşısında uygulamalar, hizmetler ve altyapılar gibi bir devlet için kritik öneme sahip olan varlıkların güvenliğinin sağlanmasını içermektedir. Sekiz güvenlik boyutunun hepsinin etkin olması varlıkların güvenliğinin sağlanması için elzemdir.

Siber güvenlik, ulusal ve uluslararası güvenliği tehdit ettiği için devlet güvenliğinde bir boyut olarak görülmektedir. Devletin kendisini ve kurumlarını tehditlere, casusluğa, sabotaj, suç ve sahtekarlığa, kimlik hırsızlığına ve diğer yıkıcı online işlemlere ve etkileşimlere karşı koruması siber güvenlik çatısı altında ifade edilebilir (Choucri, 2012:39). Devletlerin siber güvenliğe bakış açıları farklılık göstermektedir. Bu açıdan Tablo 1, bazı devletlerin siber güvenlik tanımlamaları arasındaki farklılıkları yansıtmaktadır.

Tablo 1: Devletlerin Siber Güvenlik Tanımlamaları

Ülkeler	**Siber Güvenlik Tanımlamaları**
Avusturalya	Ülkenin genel terörle mücadele çabalarının bir parçası
Avusturya	Esas olarak veri koruma konusu
Kanada	Acil duruma hazırlıklı olma çabasıdır
Finlandiya	Veri güvenliği konusu ve ekonomik öneme sahip bir konu
Fransa	Hem yüksek teknoloji ürünü bir suç konusu hem de bilgi toplumunun gelişimini engelleyen bir sorun
İtalya	Bilgi toplumunun ilerlemesinin bir parçası
Yeni Zelanda	Kritik altyapıların korunması

Kaynak: Cavelty, 2005:15-16

Devletler dışında uluslararası örgütler de küresel bir siber güvenlik kültürü oluşturma noktasında belirli adımlar atmışlardır. AB tarafından 2019 tarihinde yayımlanan *AB Siber Güvenlik Yasası* metninde ise farklı bir bakış açısı getirilerek siber güvenliğin yalnızca teknolojiyle ilgili olmadığı, aynı zamanda insan davranışının da eşit derece önemli olduğu vurgulanmıştır. Bu nedenle *siber hijyen* kavramı kullanılmış yani vatandaşlar, kurumlar ve işletmeler tarafından basit ve rutin önlemlerin düzenli olarak uygulanmasının siber tehditlerden kaynaklanan risklere maruz kalmayı en aza indirgeyeceği ifade edilmiştir (EU Cybersecurity Act., (2019), http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf). BM, 2002 yılında aldığı 57/239 sayılı kararı bu tarz bir siber güvenlik kültürü oluşturmayla ilgilidir ve tanımlayıcı unsur oluşturması açısından öncü metinlerden biridir. Bilgi teknolojisindeki hızlı gelişmelerin; hükümetlerin, işletmelerin, diğer kuruluşların ve bilgi sistemi ve ağları geliştiren, sahip olan, sağlayan, yöneten, hizmet veren ve kullanan bireysel kullanıcıların siber güvenliğe yaklaşma

şeklini değiştirmesi gerektiği vurgulanmış ve bu doğrultuda dokuz tanımlayıcı unsur oluşturulmuştur. Bu unsurlar şu şekildedir (Creation of a global culture of cybersecurity (31.01.2003), https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf):

> *(a) Farkındalık:* Katılımcılar bilgi sistemlerinin ve ağlarının güvenliğine olan ihtiyacın ve güvenliği arttırmak için neler yapabileceklerinin farkında olmalıdır;
>
> *(b) Sorumluluk:* Katılımcılar, bireysel olarak bilgi sistemlerinin ve ağlarının güvenliğinden sorumludur. Kendi politikalarını, uygulamalarını, prosedürlerini, önlemlerini düzenli olarak gözden geçirmeli ve içinde bulundukları ortama uygun olup olmadığını belirlemeli;
>
> *(c) Yanıt:* Katılımcılar, güvenlik olaylarının tespiti, müdahalesi ve bunların önlenmesi için iş birliği içinde ve zamanında hareket etmelidir. Tehditler ve güvenlik açıklarıyla ilgili bilgileri uygun şekilde paylaşmalı, hızlı ve etkili bir iş birliği için prosedürler uygulamalıdır.
>
> *(d) Etik:* Modern toplumlardaki ağların bilgi sistemlerinin yaygınlığı göz önüne alındığında, katılımcılar eylemlerinin ya da eylemsizliklerinin başkalarına zarar vereceğini kabul etmeli ve başkalarının meşru çıkarlarına saygı göstermeyi kabul etmelidir;
>
> *(e) Demokrasi:* Güvenlik, bilgi ve iletişimin gizliliği, serbest bilgi akışı, kişisel bilgilerin uygun şekilde korunması, düşünce ve fikir alış verişinde bulunma özgürlüğü gibi demokratik toplumlar tarafından tanınan değerlerle tutarlı bir şekilde uygulanmalıdır;
>
> *(f) Risk Değerlendirmeleri:* Tüm katılımcılar periyodik olarak risk değerlendirmeleri yapmalıdır. Bu risk değerlendirmeleri tehditleri ve zayıf noktaları kapsamalıdır.
>
> *(g) Güvenlik Tasarımı ve Uygulaması:* Katılımcılar, bilgi sistemlerinin ve ağlarının planlanmasında, tasarımında; işletim ve kullanımında güvenliği temel bir unsur olarak içermelidir;
>
> *(h) Güvenlik Yönetimi:* Tüm katılımcılar, diğer katılımcıların faaliyetlerinin tüm yönlerini kapsayan, dinamik olan risk değerlendirmesi için kapsamlı bir yaklaşım benimsemelidir;
>
> *(i) Yeniden Değerlendirme:* Katılımcılar, sürekli olarak bilgi sistemlerinin ve ağlarının güvenliğini gözden geçirmeli, yeniden değerlendirmeli, değişten tehditleri ve güvenlik açıklarını içeren güvenlik politikaları, uygulamaları, önlemleri ve prosedürlerinde uygun değişiklikleri yapmalıdır.

Daha önce de ifade edildiği gibi siber güvenlik toplumu ve bireyleri karmaşık ve agresif saldırılardan korumayı amaçlamaktadır. Önemli olan korumak istediklerimizin ve önceliklerimizin belirlenmesidir. Bu öncelik belirleme bazı soruların cevaplanmasını gerektirir: *(1) Sivilleri korumak için devlet ne ölçüde gereklidir? (2) Kritik altyapıları korumak için devlet ne ölçüde gereklidir? (3) Kamu ve özel sektörün denizaşırı varlıklarını korumak için devlet ne ölçüde gereklidir?* Bir sabah uyandığınızı ve hatalı bir işlem yüzünden banka hesabınızdaki bütün paranızın çekildiğini hayal edin. Bu devleti ilgilendiren bir durum mudur? Ya da siber saldırı tanımına uyar mı? En basit cevabın ulus devletin temel görevinin masum sivil nüfusu doğrudan zarar görmekten koruması olması gerekir. Siber güvenlik tanımının bu kadar karmaşık olmasının sebebi tam olarak bu noktada yatmaktadır. Çünkü bir siber saldırının mutlaka doğrudan devlete yönelik bir saldırı olması gerekmez. Dolayısıyla siber güvenliğin de sadece devleti ilgilendiren bir alan olduğunu düşünmek yanıltıcı olur. Banka hesabının çalınması ve maddi zarara uğramak doğrundan bireyi ilgilendiren ve ona yöneltilmiş bir saldırı olsa da devletin bu noktada uyarıcı ve bilgilendirici olması bireyin korunması açısından elzemdir (Guiora, 2017:17-19).

1.1.3. Siber Tehdit Nedir?

Tehdidi doğru tanımlayabilmek; o tehditle başa çıkabilmek için alınacak önlemler açısından hayati bir önem arz etmektedir. Bu açıdan bir *siber tehdidi* tanımlama çabası iki önemli sorunun cevabının verilmesini içermektedir: *(1) Saldırının arkasındaki kimdir? (2) Nasıl bir saldırı olmuştur?* Bu sorulara verilecek cevaplar siber tehdidin boyutunun ve niteliğinin belirtilmesi açısından kişilere ve kurumlara yardımcı olmaktadır. Benzer şekilde, Singer ve Friedman (2014:37-39) siber tehdit tanımlaması yaparken güvenlik açığı fikrini tehditten ayırabilmenin önemli olduğunu ifade etmektedir. Şöyle ki, kilidi açık bırakılmış bir kapı güvenlik açığı oluşturmaktadır ancak kimse içeri girmek istemiyorsa bunun bir tehdit oluşturduğunu söylemek tam anlamıyla doğru olmaz. Tersine şekilde bir güvenlik açığı ise birçok tehdide yol açabilmektedir. Açık kapı örneğindeki durumda bir terörist o kapıdan içeriye bir bomba sokabilir, rakipler internet yoluyla ticari sırları çalabilir, hırsızlar değerli malları çalabilir ya da yakıp yıkabilir. Bu sebepten tehditlerin ayırt edici yönü *aktör* ve *sonuçlarıdır*. Aktörün ayırt edici bir yön olmasının sebebi, aktörün belirlenebilmesinin bizi tehditler konusunda stratejik olarak düşünmeye yöneltmesinden ileri gelmektedir. Belirli durumlarda bir aktörün sadece rastgele saldırı amacı mı taşıdığı yoksa belirli bir hedefe yönelik saldırı amacı mı taşıdığı dahi önemli olmaktadır. Yani tehditler, potansiyel kötü aktörlerin ne yapmaya çalıştıklarını ve arkasındaki nedeni anlamaya çalışarak değerlendirilmelidir (Güntay, 2018: 92).

Tehdidi saptamaya yönelik genel açıklamalardan sonra siber tehditler, *"internete bağlanmayı mümkün hale getiren ve çevrim içi saldırılardan etkilenmeyi mümkün kılan araçların oluşturduğu unsurlar"* şeklinde tanımlanabilir (Güntay 2017:88). Daha özel olarak siber tehditlerin kullanım amacını ise, bilişim teknolojileri aracılığıyla, toplumların iç ve dış düzenlerini zayıflatma ya da topyekûn ortadan kaldırma istenci oluşturmaktadır (Güntay, 2018:92). Ayrıca siber tehditler (küresel) bilgi altyapısının kötü amaçlı olarak kullanılmasının bir sonucudur ve bundan dolayı teknolojik çevre özelliklerinin (hem şimdiki hem de gelecekteki) tehdit algısı üzerinde önemli bir etkisi bulunmaktadır (Cavelty, 2008:19). Siber tehditlere yönelik önemli bir başka nokta ise, teknik saldırıların yanı sıra günlük hayatta karşılaşılan dolandırıcılık, casusluk, fidyecilik gibi suçların siber uzay harekât sahası içerisinde (siber casusluk[2], siber fidyecilik[3], siber dolandırıcılık gibi) gerçekleşmesi halinin de siber tehditler kapsamında yer almasıdır (Keleştemur, 2015:316).

Siber tehditlerin ortaya çıkmasına zemin hazırlayan ve bu yolla siber savaşı da olanaklı hale getiren üç farklı boyutun varlığından söz edilebilir. Clarke ve Knake bu üç boyuttan ilkini

[2] Siber casusluk, devletlere, şirketlere, kurumlara, organizasyonlara ya da kişilere ait hassas nitelikteki bilgilerin siber uzay üzerinden belirli yöntemler kullanılarak ele geçirilmesi eylemidir (Yayla, 2013:196).

[3] Siber fidyecilik, siber saldırı çeşitleri arasında son dönemde popüler hale gelen bir yöntemdir. CryptoLocker isimli, kurbanlarına mail yolu üzerinden ulaşan ve naylon e-fatura gönderen ve bu yolla kurbanları zarara uğratan virüs siber fidyecilik açısından en güçlü silahlardan biridir (Keleştemur, 2015:316).

internetin kendi yapısından kaynaklanan mevcut eksiklikler, şeklinde açıklamıştır. Beş önemli eksikliğin birinci boyutun ortaya çıkmasına zemin hazırladığı söylenebilir. Bunlardan ilki adresleme sistemiyle ilgilidir. Adresleme sisteminin siber saldırıların hedefi olmasının sebebi, güvenliği yeterince düşünülmediği için tasarımından kaynaklanmaktadır. İkinci eksiklik olarak yönetişimin olmayışı gelmektedir. Teknik organların varlığına rağmen yetkili bir kurumun olmayışı, temelde interneti yöneten kimsenin olmadığını göstermektedir. Internet Corporation for Assigned Names and Numbers (ICANN), Internet Architecture Board, Internet Society gibi birçok sivil toplum ve devletlerarası kuruluşun varlığına rağmen yetkilerin tamamını tek başına elinde toplayan bir kurum bulunmamaktadır. İnternetin kendi yapısından kaynaklanan üçüncü eksiklik, açık ve şifresiz olarak sunulan işletim sistemlerinin varlığıdır. Google'ın bir sunucusu olan ve çoğu insanın kullandığı Gmail ücretsiz hizmet sunmakta ancak kişiler arası iletişimi de görebilmektedir. Kötü niyetli bir casus dinleyici gerekli programlara sahip olması halinde iki nokta arasındaki tüm trafiği dinleme imkânına sahip olmaktadır. Dördüncü eksiklik, zararlı yazılımların internet üzerinden kolayca dağılabilmesidir. Beşinci eksiklik ise, internetin çok geniş bir alana yayılan ve merkezi olmayan bir ağ olmasından kaynaklanmaktadır. Çünkü uzmanlar internete yönelik tasarımı yaparken güvenlikten ziyade merkezi kontrolü az olan bir yapı kurmaya çalışmışlardır (Çifci, 2017:300-301; Clarke ve Knake, 2010:45-46).

Clarke ve Knake tarafından açıklanan ikinci boyutu ise *yapısal (donanım ve yazılım) kaynaklı hatalar* oluşturmaktadır. Üç boyut içinde en önemlisi olarak nitelenebilecek olan boyut yapısal hatalar boyutudur. Bilgisayarlar üretim aşamasındayken ya da yeni bir programın yazılması esnasındayken bilerek ya da kaza sonucu belirli zafiyetler ve arka kapılar yerleştirilmesi olası bir durumdur. Bunun sonucunda da bu cihazlar ve yazılımlar siber saldırılarda gerek hedef ve gerekse silah olarak kullanılabilmektedir. Son boyutu ise, *değerli olan kritik sistemlere erişim imkanının online olarak artması* oluşturmaktadır. Siber tehditler su, elektrik, doğalgaz gibi devletler için kritik altyapıların giderek internete daha bağlı hale gelmesi sonucunda yalnızca bilgisayar sistemlerine verdikleri zararlar ölçüsünde değil; kritik altyapılara verdikleri zararlar ölçüsünde de asimetrik özellik gösteren bir saldırı şekli olarak kullanılabilmektedir (Aslay, 2017:25; Çifci, 2017:300-303; Clarke ve Knake, 2010:45-46).[4]

Aktarılan boyutlara ek olarak, siber uzayın kendine has yapısından kaynaklı tehdit değerlendirmesinin zor olması bir başka sorun olarak bireylerin ve devletlerin ajandasında yer almaktadır. Siber alandaki güvenlik açıklarının niteliği, onları değerlendirmeyi de oldukça zorlaştırmaktadır. Ayrıca siber silahlar, diğer silahlarla kıyaslandığında benzer fizik yasalarına bağlı değildir. Yeni ortaya çıkan kötücül yazılımların her bir parçası farklı tasarımları gereği farklı görevler üstlenebilmektedir. Diğer bir ifadeyle, fiziksel olmayan doğaları, tehdit değerlendirmesi

[4] Kritik altyapı kategorisi içinde yer alan elektrik şebekesini internete daha fazla bağımlı hale getiren ve ABD'de B. Obama tarafından ortaya konan akıllı şebeke projesi sağladığı faydaların yanında siber korsanların saldırı risklerine karşı bir savunmasızlığı da beraberinde getirmektedir (Clarke ve Knake, 2010:54).

görevini daha da zorlaştıracak şekilde ve sayılarda üretilip saklanabilecekleri anlamına gelmektedir. Potansiyel bir düşmanın eylem ve niyetlerini değerlendirme aşamasında, siber tehditlerin fiziksel olmayan doğası giderek önemli bir hale gelmektedir. Fiziksel dünyada sınırlarınıza kadar gelmiş bir düşman filosu tehdit ve kaynağı hakkında çok fazla kanıt sunabilirken; siber alanda tehdidin geldiğini fark edebilmek ve birçok devletin ve devlet dışı aktörün faaliyette bulunduğu bir ortamda düşmanı tam olarak belirleyebilmek giderek zor hale gelmektedir. Sonuç olarak siber tehditler, genç yaş grubundaki kişilerden, belirli ideolojiler etrafında hareket eden teröristlere ya da belirli çıkarlar ekseninde hareket eden devletlere kadar geniş bir yelpazeden gelebilmektedir. Siber tehditlerin özünde sahip olduğu merkezi olmayan yapısı ve sofistike olması sebebiyle tehdidin geldiği aktörün niyeti hakkında net bir görüşe sahip olmak zor hale gelmektedir. Teknolojinin beraberinde getirdiği kolaylıklar sayesinde dünyanın herhangi bir köşesindeki kötü niyetli bir kişi yeterli donanımla hem bireylere hem de devletlere yönelik siber tehdit oluşturabilir. Bu yönüyle siber tehditler aktörler için ciddiyetle üzerinde durulması gereken bir alan olarak göze çarpmaktadır (Kurnaz, 2016:64; Singer ve Friedman, 2014:148-150).

1.2. Siber Suç Kavramının İncelenmesi

Küreselleşme süreci sonrasında ortaya çıkan iletişim ve bilgi çağı kullanıcılara hız, işlem kolaylığı, belirli bir bölgeye bağlı iş üretim yükümlülüğünün ortadan kaldırılması, maliyetlerin nispeten azalması gibi yaşam koşullarını iyileştiren belirli kolaylıklar sağlarken bir yandan da dengeleri değiştirmiş ve bilgi çağının olumlu yönlerinden faydalanan insanları; çağın olumsuz etkilerinden biri olan *siber suç* ile tanıştırmıştır. Soğuk Savaş sonrası dönemde yeni güvenlik kaygılarının oluşmasına sebep olan siber suçlar ve siber saldırılar yaşadığımız ve gelecek yılların en önemli sorunu olacak gibi gözükmektedir (Özgöker ve Yılmaz, 2016:163).

Siber suçların saldırgan, saldırı, eylem ve suç konusu gibi geniş bir kapsam içermesi onun tanımının da net bir şekilde ortaya konulamamasına neden olmuştur. Siber suça ilişkin eski tanımlamalar siber suçu, *bilgisayar suçu, bilgisayarla ilgili suç* ya da *bilgisayarla işlenen suçlar* olarak ayırmıştır. Dijital teknolojinin yaygınlaşmasıyla birlikte, *yüksek teknoloji* veya *bilgi çağı suçu* gibi bazı yeni terimler tanımlamaya eklenmiştir. İnternetin yaygınlaşmasının beraberinde getirdiği yeni terimlerle birlikte *siber suç* ve *ağ suçu* olarak adlandırılmaya başlanmıştır. Ancak yine de yapılan bu tanımların siber suçun tüm anlamlarını tamamen kapsayamadığını belirtmek gerekmektedir. Çünkü bazı durumlarda ortada ağ ile ilişkilendirilebilecek bir şey yokken; bazı durumlarda da *yüksek teknolojili* ya da *elektronik suç* gibi terimler kullanmak suçun kesin olarak siber suç unsuru olduğunu belirtmek için çok geniş anlamlar içeren bir ifade olarak ortaya çıkabilmektedir. Bu bilgiler ışığında genel anlamda siber suç tanımı ise, *"yasadışı ya da belirli taraflarca yasa dışı olarak kabul edilen ve küresel elektronik ağlar aracılığıyla yapılabilecek bilgisayar tabanlı faaliyetler"* şeklinde yapılabilir (Gurjar, 2015:5; Thomas ve Loader, 2000:3).

Siber suçları doğru olarak tanımlayabilme çabası temelde onun fiziksel suçlardan ayrılan yönlerini de ortaya koymayı gerektirmektedir. Bu açıdan siber suçu fiziksel suçtan ayıran belirli karakteristik özellikler vardır. *Bilgisayar ağlarının anonimliği* ayrımlardan ilkini oluşturmaktadır. Bir kullanıcı ağ ortamında kimliğini kolayca gizleyebilir. Bu durum sadece bilgisayar suçlarını ve bilgisayar suçlularını tespit etme görevini zorlaştırmakla kalmaz aynı zamanda delil toplama görevini ve kanıtları izlemeyi de zor hale getirmektedir. Elde edilen veriler rutin olarak imha edildiğinden kanıtların kaybolması genellikle karşılaşılan bir sorundur. İkinci farklılığı *suçun değişen doğası* oluşturmaktadır. Fiziksel dünyada işlenen suçlar sanal alanda işlenen suçlardan farklılık göstermekte ve geleneksel suçlara uygulanan yasalar siber suçlar için tam anlamıyla geçerli olamamaktadır. Bir hırsızlık olayı için fiziksel alanda yeterli kanıtlar mevcutsa yasalar işleyebiliyorken, siber bir suç olan bilgi hırsızlığı için yeterli kanıt bulabilmek her zaman mümkün olamamakta ve yasalar işletilememektedir. Üçüncü farklılık ise *siber suçların sınırları aşan bir nitelik taşıması* olarak ifade edilebilmektedir. Siber suçların aynı anda birçok ülkede işlenebilir olması, ülkesel sınırlarının olmadığını ortaya koymaktadır. Bir web sitesinde yayımlanan zorla ele geçirilmiş, kötü niyetli ya da gizli kalması gereken materyallerin küresel olarak erişime açık olabilmesi hem siber suçların niteliğini göstermekte hem de siber suçlarla aktif mücadelenin zorluklarını ortaya koymaktadır. Son farklılığı ise *siber suçlarda kullanılan elektronik bilgilerin üretilmesi, depolanması, aktarılması ve silinmesinin hem daha kolay hem de daha ucuz olması oluşturmaktadır.* Veri hırsızlığının konusu olan bir materyal kolayca ve hızlı bir şekilde bir noktadan başka bir noktaya transfer olabilmekte ve siber suçun kendine has bu özellikleri nedeniyle kanun uygulayıcıların işlerini de zorlaştırabilmektedir (Karla, 2017:88-89).

Sahip olduğu karakteristik ve kolaylaştırıcı özelliklere karşı bireylerin ve devletlerin ortak bir tasnif oluşturma ve bu yolla suçlarla mücadele edebilmesi adına, siber suçlara ilişkin ulusal ve uluslararası alanda çeşitli düzenlemeler yapılmakta olup en kapsamlılarından birini Avrupa Konseyi tarafından hazırlanan *Siber Suç Sözleşmesi* oluşturmaktadır. Sözleşmenin ilgili ikinci bölümünde siber suçların tasnifi, bilgisayar sisteminin tamamına ya da bir kısmına yetki olmadan erişim anlamına gelen *yasadışı giriş*; sahip olma, temin etme, dağıtma yönlerinden tamamen yasaklanan *çocuk pornografisi*; *telif hakkı ve buna benzer yasadışı kopyalama ve çoğaltmayla alakalı suçlar*; internet ortamında verilerin değiştirilmesi, silinmesi ayrıca bilgisayar sisteminin işleyişine herhangi bir müdahale ve ekonomik yarar sağlama niyetiyle hileli ve dürüst olmayan müdahale anlamlarına gelen *bilgisayarla alakalı sahtecilik ve aldatma* şeklinde yapılmaktadır (Europe (2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561).

Benzer bir tasnif Wall (2001:3-7) tarafından yapılmış ve siber suç *amacına* ve *hedefine* göre alt bölümlere ayrılmıştır. Hackleme, silme, virüs bulaştırma yoluyla sınırları aşarak başkalarının sahip olduğu bilgilere zarar verme anlamına gelen *siber izinsiz girme* ilk siber suç kategorisini

oluşturmaktadır. Para ve mal çalmak, çevrimiçi kredi kartı sahtekârlığı ve fikri mülkiyet haklarının ihlali gibi *siber aldatmacalar ve hırsızlıklar* ikinci kategoriyi oluşturmaktadır. Müstehcenlik ve ahlakla ilgili yasaları ihlal eden *siber pornografi* üçüncü kategoriyi oluşturmaktadır. Son kategoriyi ise, gizlice takip etme ve nefret dolu konuşma yöntemleriyle yapılan ve kişinin başkalarına psikolojik zarar vermesi ya da psikolojik zararı teşvik edici şekilde yönlendirmesi bu yolla kişinin korunmasına ilişkin yasaları ihlal etmek anlamına gelen *siber şiddet* oluşturmaktadır. Tasniflemedeki ilk iki kategori mülkiyete karşı işlenen suçlar olarak ifade edilebilirken; üçüncüsü ahlaka karşı ve dördüncüsü ise kişiye karşı işlenmiş siber suçlar kategorisindedir (Yar, 2006:10-11).

Tanımı, kapsamı ve içeriği yukarıdaki şekilde ifade edilebilecek olan siber suçlarla mücadelenin zor ve pahalı olduğu unutulmamalıdır. Nitelikli ve yeterli personele ve personel için gerekli teknik altyapıya sahip olmak siber suçlara karşı mücadele etmenin temel koşullarından biridir. Ayrıca mücadele, yasalarla desteklenmeli, hukuk kuralları etkili bir şekilde uygulanmalı ve siber suçlar cezalandırılmalıdır. İnternetin sınırları aşan doğası sebebiyle hâlihazırda ve gelecekte oluşturulacak yasalar ve normlar da uluslararası bir nitelik taşımalı ve BM, AB gibi uluslararası örgütler nezdinde gerekli yasal düzenlemeler yapılmaya devam edilmelidir (Özgöker ve Yılmaz, 2016:166).

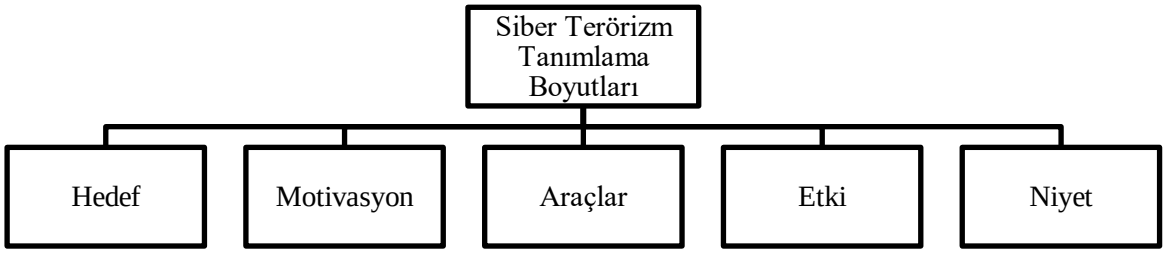
1.3. Siber Terörizm ve Özellikleri

Siber terörizm, gerek tanımı gerek kapsadığı alan itibariyle bir parça tartışmalı bir terim olarak göze çarpmaktadır. Tanımı konusunda üzerinde net bir uzlaşının sağlanamadığı terimin ilk kez kullanımı, 1980'lerde Kaliforniya'daki Güvenlik ve İstihbarat Enstitüsü'nden kıdemli bir araştırmacı olan Barry Collin tarafından yapıldığı düşünülmektedir. Collin, siber terörizm kavramını *"siber uzayın ve terörizmin bir noktada birleşmesi"* olarak basitçe tanımlamıştır. Bu tanıma istinaden 1980'lerin başında kavram, kullanıcıların gerçek zamanlı olarak bilgi alışverişinde bulunabilecekleri çevrim için bilgisayar ve ağ etkileşimlerini içeren fiziksel ve siber dünya tehditlerinin bir birleşimi olarak görülmüştür. Zamanla kapsamı genişleyen kavramla ilgili yapılan tanımlamalardan biri Lewis (2002:1) tarafından yapılmış ve *kritik altyapı* kavramına dikkat çekilerek siber terörizm*, "kritik ulusal altyapıları (enerji, ulaşım, haberleşme, finans gibi) işlemez hale getirmek, bir hükümeti ve sivil halkı zorlamak ve korkutmak için bilgisayar ağ araçlarının kullanılması"* şeklinde tanımlanmıştır. Ülkelerin ve kritik altyapıların giderek bilgisayar ağlarına daha bağımlı hale gelmesiyle ortaya çıkan güvenlik açıkları artmış ve düşman bir ülke ya da grup bu açıklardan yararlanır hale gelmiştir (Samuel vd., 2014:1083; Denning, 2001:281).

Siber terörizmi anlamaya yönelik farklı bir bakış açısında ise terörizmin bu çeşidinin, *"iç ve dış ağlar yoluyla siber uzaydan gelen ve farklı motivasyonlarla belirli bir hedefe yönelik gerçekleştirilen saldırı biçimi"* olduğuna dikkat çekilmiştir. Kuruluşun içinden ya da dışarıdan

gelebilecek olan saldırı kaynağının vurgulanması, iç ağlarda faaliyette bulunan siber teröristlerin ağa erişiminin daha kolay olması ve ortaya çıkardığı etki bakımından daha tehlikeli olduğundan dikkate değerdir (Mazari vd., 2016:2).

Şekil 2: Siber Terörizm Tanımlama Boyutları



Kaynak: Mazari vd., 2016:4

Siber terörizme ilişkin yapılan tanımlar ışığında analiz, Şekil 2'de gösterildiği gibi beş farklı boyutla tanımlanabilir. Bu tanımlarda *hedef* değişiklik göstermekte belirli durumlarda askeri kuvvetler, devletin siber ve fiziksel altyapıları olabilirken; belirli durumlarda da sosyal ve ulusal kimlikler, kritik ulusal altyapılar, özel sektör ve varlıkları hedef konumuna gelebilmektedir. Siber teröristleri eylem yapmaya iten *motivasyon* ise belirli durumlarda sosyal ve kültürel etmenler; belirli durumlarda da dini, politik inançları ve ideolojileri olabilmektedir. Siber terörizmin *etki* boyutu ise, bireye yönelik hizmetlerin tahrip edilmesi, bozulması, fiziksel-operasyonel ve bilgi altyapısına yönelik zararlar ve bireylere ve gruplara doğrudan zarar şeklinde ortaya çıkmaktadır. Son olarak *niyet* boyutu ise siyasi, sosyal, askeri ve ideolojik olarak avantaj kazanmak şeklinde ifade edilebilir.

Boyutları bu şekilde ortaya konulabilecek olan siber terörizmin örgütler için cazibeli hale gelmesinin de belirli sebepleri bulunmakta ve bu farklar temelde siber terörün klasik terörden farklılaşan yönlerini de ortaya çıkarmaktadır. İlk olarak *maliyet* faktörü ön plana çıkmaktadır. Klasik terör yöntemlerinde kullanılan bomba, silah gibi maliyeti yüksek araçlar yerine çipler, donanım/yazılımlar gibi daha az maliyet gerektiren ve erişimi daha kolay olan araçlar kullanılmaktadır. Bu açıdan bakıldığında siber terörizm çatısı altındaki saldırıların maliyet/fayda oranı oldukça yüksek gözükmektedir. İkinci olarak siber uzayın geneline hakim olan *anonomlik* özelliği ön plana çıkmaktadır. Siber uzayın kendine has yapısı aktörlere, klasik teröre kıyasla kimliklerini daha kolay gizleyebilme olanağı vermektedir. Belirli durumlarda siber teröristler, saldırının gerçekleştiği yerin çok uzağında bulunabilirler. Bu özellik sayesinde örgütler kendilerine katılacak kişileri hem daha kolay bulabilmekte hem de ikna etme konusunda daha güçlü hale gelmektedir. Üçüncü olarak *etki büyüklüğü* özelliği ortaya çıkmaktadır. Klasik terör yöntemleri kullanılarak gerçekleştirilen saldırılar bazı durumlarda etki alanı olarak saldırının gerçekleştirildiği bölge özelinde kalırken, siber terör yöntemleri kullanılarak gerçekleştirilen saldırılarda ise ulusal/uluslararası boyutlarda etkiler ortaya çıkabilmektedir. Dördüncü sırada *hedef çeşitliliği*

gelmektedir. Hedef olarak seçilebilecek noktaların fazlalığı ve bütün bu noktaları korumanın imkansiz olması siber terörizmi cazip hale getirmektedir. Çünkü teröristlerin, fazla sayıdaki hedef içinden zayıf ve savunulmayan birine saldırı düzenleme ihtimalleri daha fazladır (Güntay 2017:91; Polat, 2016:174-175; Doğrul vd., 2011:32-33).

Zaman içinde kritik altyapılara yönelik tehditlerin de spekturuma eklenmesiyle çehresi değişen ve genişleyen siber terörizm unsurlarının gerçekleşme aşamaları ise 1999 yılında ABD'de yapılan bir çalışmada ortaya konulduğu gibi üç şekilde olmaktadır. Siber terör saldırılarının birincisi *basit/yapılandırılmamış* olanlardır. Bu aşamada genellikle örgütün hedef çerçevesi tek sistem ya da ağlar gibi düşük yoğunlukta olmaktadır. Ayrıca örgüte ilişkin öğrenme ve komuta/kontrol yeteneği düşük düzeyde kalmakta, yapılan eylemden sağlanmak istenen fayda genellikle propaganda seviyesinde kalmaktadır. İkincisi birden fazla sistem ya da ağlara karşı girişilen sofistike saldırıları içeren *ileri düzeyde/yapılandırılmış* olanlardır. Bu aşamada örgüte ilişkin öğrenme ve komuta kontrol yeteneği orta düzeye çıkmıştır. Ayrıca bu aşamadaki saldırılarda hedeflenen ağa ya da sisteme hasar vermek ve değişikliğe uğratmak amaçlanmaktadır. Üçüncü aşama ise *karmaşık/koordinasyonlu* saldırıları içermektedir. Bu aşamada örgütün üstün zeka ve denetim gücüne sahip olması dikkate değerdir. Ayrıca hedefe yönelik analizlerin yapılandırılması bu aşamada çok ileri düzeye yükselmiştir. Karmaşık/koordinasyonlu saldırılara bir örnek olarak Körfez Savaşı döneminde ABD Savunma Bakanlığı Pentagon'a sızan bir grup Hollandalı hacker verilebilir. Hackerlar gizli dosyalara girmemiş olsalar bile sitenin içeriğinin değiştirilmesi o dönem için büyük bir yankı uyandırmış, Pentagon sızma işlemini Merkezi İstihbarat Teşkilatı'na (Central Intelligence Agency/ CIA) bizzat saldırıyı yapan kişinin telefon edip haber vermesi sonucunda öğrenmiştir. Bu ve benzeri örnekler siber terörizmin boyutlarını net bir şekilde ortaya koymaktadır (Polat, 2016:175-176).

Siber terörle alakalı üzerinde önemle durulması gereken bir başka noktayı ise sıkça biririyle karıştırılan ve birbiri yerine kullanılan teröristlerin siber ortamı kullanması ve siber terör farkı oluşturmaktadır. Terörist organizasyonların propaganda amacıyla siber ortamı kullanmaları, hayata geçirmeyi düşündükleri eylem planlarını siber ortam üzerinden koordine etmeleri gibi uygulamalar teröristlerin siber ortamı kullanmalarına örnek teşkil edebilecek uygulamalardır. Ancak siber terörizm olarak nitelenebilecek uygulamalarda, topluma, kurumlara ya da devlete yönelik ortada somut bir şiddet eylemi olmalı ya da en azından korku oluşturacak, toplumda infiale yol açacak biçimde hasara neden olunmalıdır. Siber uzay vasıtasıyla yaralanma ya da ölüme yol açan olaylar, su ve elektrik altyapısını, ulaşım ağını kesintiye ya da zarara uğratmaya yönelik girişimler siber terörizm şeklinde nitelenebilecek olan örneklerdir (Çifci, 2017:9)

1.4. Siber Saldırılar ve Özellikleri

Bilgisayar ve internet kullanımının dünyada giderek daha yaygın hale gelmeye başlaması kullanıcılarına belirli kolaylıklar sağlarken beraberinde belirli tehditler de getirmektedir. Bunların ilkleri arasında, kurumların ve devletlerin *siber saldırılara* maruz kalması yer almaktadır. Siber güvenlikle ilişkili diğer kavramlar gibi siber saldırının da üzerinde tam olarak uzlaşı sağlanan bir tanımı mevcut değildir. Mevcut olan çeşitli tanımlama çabalarından genel kabul gören birine göre siber saldırı, *"düşman bilgisayar sistemlerini, ağlarını ayrıca bir bütün olarak bu sistemlerin ve ağların kapsamında bulunan bilgi ve programları değiştirmek, bozmak, aldatmak veya yok etmek için yapılan kısa ve uzun süreler boyunca gerçekleştirilebilen kasıtlı eylem ve işlemlerin kullanımını"* ifade etmektedir. Bir siber saldırı, rakip sistemlerin veya ağların rakip için daha kullanışsız hale gelmesine ve güvenilmez olmasına neden olduğu için önem arz etmektedir (Lin, 2010:63).

Hükümetlerin ve uluslararası örgütlerin, siber saldırıların yol açtığı tehdidin kapsamını anlamak için giriştiği tanımlama çabalarının dikkat çeken iki örneğinden biri ABD'ye; diğeri ise Şangay İşbirliği Örgütü'ne (ŞİÖ) aittir. ABD'de Birleşik Devletler Siber Komutanlığı kurulduktan hemen sonra, 2011 yılında komutanlığın siber operasyonlarda kullanılmak üzere yayımladığı sözlükte siber saldırıları tanımını *"bilgisayarın ve bilgisayarla ilgili ağların ya da sistemlerin kullanımı vasıtasıyla hedef unsurun kritik siber sistemlerini, mal varlığını, fonksiyonlarını bozma ya da tahrip etme amaçlı düşmanca hareket"* şeklinde yapılmıştır. Burada önemli nokta siber saldırıların amaçlanan etkilerinin hedeflenen bilgisayar sistemleri veya verileriyle sınırlı olmak zorunda olmamasıdır. Yani bu tanıma göre kritik alt yapılara yapılan saldırılar da siber saldırı kategorisinde değerlendirilmektedir. Bu tanımlamanın temel bir özelliği siber saldırıları, kritik siber sistemlere zarar vermesi düşünülen düşmanca eylemlerle sınırlandırmasıdır (Hathaway vd., 2012:824; Cartwright, 2011:5).

ŞİÖ, ABD Siber Komutanlığı'ndan farklı olarak siber saldırılara ilişkin geniş anlamda araç tabanlı bir yaklaşım benimsemiştir. Örgüt, muhtemel teknolojilerin (yeni bilgi ve iletişim teknolojileri) kullanımıyla ortaya çıkabilecek tehditleri ve hem sivil hem de askeri alanlarda uluslararası güvenlik ve istikrarın sağlanmasına yönelik olmayan amaçlar için kullanılan araçlarla ilgili endişelerini dile getirmektedir (Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 2008: 202). Ayrıca ŞİÖ, bilgi güvenliğine yönelik bilgi savaşını[5] da tanımlamaya ekleyerek, sosyal ve politik, sosyal ve ekonomik sistemlerin yanı sıra diğer devletlerin manevi,

[5] ŞİÖ tarafından bilgi savaşı, *"toplumu ve devleti istikrarsızlaştırmanın, kritik ve diğer yapılara zarar vermenin yanı sıra, bir devleti karşı tarafın çıkarları doğrultusunda karar almaya zorlamak için kitlesel psikolojik beyin yıkamanın da kullanılması"* olarak tanımlar (Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, 2008:2020).

ahlaki ve kültürel alanlarına yönelik zararlı bilgi girişini, *bilgi güvenliğine yönelik tehditler* olarak nitelendirmektedir. Bu niteleme, ŞİÖ'nün siber saldırı tanımını siyasi istikrarı baltalamak için siber teknoloji kullanımını içeren geniş bir tabanda ele alması açısından önemlidir (Hathaway, 2012:825).

Bir siber saldırının gerçekten ne olduğunu tanımlamak için öncelikle onun geleneksel saldırılardan ayrılan yönleri ortaya konulmalıdır. Genel olarak siber saldırılar çok hızlı bir şekilde gerçekleşmekte ve bazen saldırıya uğrayan taraf henüz ne olup bittiğini anlamayamadan saldırıya maruz kalmaktadır. Nerdeyse ışık hızında gerçekleşen siber saldırılarda kinetik silahlar yerine dijital araçlar kullanılmaktadır. Kullanılan araçlar önem arz etmektedir çünkü bu yolla siber saldırılar, geleneksel saldırıların olağan fiziği ile kısıtlanamaz hale gelmektedir. Fiziki sınırlardan bağımsız hale gelmesi aynı anda birden fazla yerde gerçekleşebileceğini ortaya koymaktadır yani aynı siber saldırı aynı anda birden fazla hedefi vurabilir konumdadır (Singer ve Friedman, 2014:68-69; Todd, 2009:68-69).

Bunun yanı sıra bazı siber saldırıların sonuçları, kitle imha silahları içeren saldırıların sebep olduğu yıkımla benzerlik gösterebilir.[6] İlaveten geleneksel saldırıların maliyetine kıyasla siber saldırıların maliyeti çok daha düşük kalmaktadır. Ayrıca, siber uzayın kendine has karakterini oluşturan atfetmenin zorluğu siber saldırıların arka planını (arkasındaki aktörü) ortaya çıkarmayı zorlaştırmakta ve saldırının kaza sonucu mu yoksa isteyerek mi yapıldığı noktasında karar vermeyi daha zor hale getirmektedir. Siber saldırıların, geleneksel saldırı yöntemlerinden farklılık gösterdiği son noktayı ise hedef unsuru oluşturmaktadır. Siber saldırılarda öncelikle amaç bir bilgisayarı ve içindeki bilgileri hedef almaktır. Saldırının sonuçları fiziksel hasar durumu ortaya çıkarsa da, hasar ilk olarak dijital alemdeki bir olaydan meydana gelmektedir. (Singer ve Friedman, 2014:68-69; Todd, 2009:68-69).

Siber ve geleneksel saldırı yöntemleri arasındaki bu farklar ışığında siber saldırı konusunda daha genel bir tanım ortaya koyma çabalarını karşılayan dört genel özellik olduğu ifade edilebilir. Bu özelliklerden ilki *"bir siber saldırı bir bilgisayar ağının işlevlerini siyasal veya ulusal güvenlik amacıyla baltlamak için yapılan herhangi bir eylemden oluşmaktadır"* şeklinde açıklanabilir. İkinci olarak *"bu terim, eylemin aktif olarak yürütülmesi gerektiğini ifade etmektedir: saldırı veya aktif savunma"*. Aktif savunma, saldırı yapan bilgisayar sistemlerine saldırmak ve mevcut siber saldırıları durdurmak için tasarlanmış elektronik karşı önlemleri içermektedir. Belirtmek gerekir ki hükümetlerin hem aktif hem de pasif savunmaları kullanması muhtemeldir ve ikisi birlikte çalışacak şekilde tasarlanmıştır. Üçüncü özellik saldırının yöntemi ve amacını da içeren *"bir siber*

[6] Modern toplumların altyapısı bir siber saldırı esnasında kolayca hedef haline gelebilecek teknolojiye ya da verilere dayandığından bu tür bir altyapının devre dışı bırakılması ya da verilerin manipüle edilmesi bir topluma ciddi zararlar verebilir. Örneğin, hava kontrol sistemlerine müdahale etmek ya da baraj kapak kontrol sistemlerine erişim sağlamak ciddi sonuçlar doğurabilir (Todd, 2009:68).

saldırı hackleme, mantık bombaları, kesme vb. yollarla gerçekleştirilebilir ancak bir bilgisayar ağının işlevini baltalamayı veya bozmayı hedefliyor olması gerekir" şeklinde ifade edilebilir. Son özellik ise siyasal ya da ulusal güvenlik ekseninde amaca yöneliktir ve *" siyasi ya da ulusal güvenlik amacı, siber saldırıyı basit bir suçtan ayırmaktadır[7]"* şeklinde ifade edilebilir. Eylemin tanımının diğer tüm unsurları yerine getirildiği durumlarda bir aktörün siber alanda gerçekleştirdiği herhangi bir agresif eylem, ulusal güvenliği etkilediği için bir siber saldırıdır. Bu durum devlet dışı bir aktör tarafından gerçekleştirilirse de aynı durum geçerli olmakta ve işlenen siber suç, siber saldırı kategorisine koyulmaktadır (Hathaway vd., 2012:824-830).

1.4.1. Gizliliği (Confidentiality) Tehlikeye Atan Siber Saldırılar

Gizlilik saldırıları, sistemler ve kullanıcılara dair verileri toplamak ve faaliyetleri izlemek için bilgisayar ağlarına giriş yapma çabalarını kapsamaktadır. Gizliliği tehlikeye atan siber saldırıların değer ölçümünü yapabilmek, hem ele geçirilen bilgilere hem de bu bilgilere erişmek için verilen çabanın boyutuna bağlı olmaktadır. Kredi kartı hırsızlığı ve jet savaş uçağının tasarımını ele geçirmeye çalışan bir ajanı düşündüğümüzde ikisi de gizliliğe yönelik saldırı kapsamına girmektedir. Ancak finansal dolandırıcılığa nazaran casusluğun sonuçları açık bir farklılık göstermektedir. Bu tür saldırılar sonucu ortaya çıkan asıl zorluk, bilginin büyük miktarda ve organize bir şekilde çalındığı durumlarda gün yüzüne çıkmaktadır (Singer ve Friedman, 2014:70).

2013 yılında gerçekleşen ve ABD silah sistemlerine ait hassas bilgilerin Çinli siber korsanlar tarafından çalınıldığının düşünüldüğü ve Pentagon tarafından hazırlanan raporla hırsızlık sonucu silah tasarımlarına ulaşıldığının ve bu tasarımların Çin'in silah sistemlerinin gelişimini hızlandırmak için kullanılabileceği konusunda uyarılarda bulunulduğu olay, gizliliği tehlikeye atan siber saldırılara örnek olarak verilebilir (Nakashima, 2013).

1.4.2. Bütünlüğü (Integrity) Tehlikeye Atan Siber Saldırılar

Bütünlük saldırıları, gizlilikten farklı olarak içeriden bilgi çıkarmak yerine bilgiyi değiştirmek için sisteme girmeyi kapsamaktadır. Bu girişler, sanal dünyada bulunan verileri ve fiziksel dünyada verilere göre hareket eden insanları ve bu verilere dayanan sistemleri manipüle etme işlevini yerine getirmektedir. Bu saldırı türü genellikle, kullanıcının algısında veya durumsal bilincinde değişiklik ortaya çıkarmaya, bunun yanı sıra, bilgi sistemleri aracılığıyla yönlendirilen veya işletilen fiziksel cihazların ve işlemlerin sabote edilmesine ya da bozulmasına neden olur. Bu çeşit bütünlük saldırılarının farkedilmesinin zor olması dolayısıyla gizlilikle hareket ettiği söylenebilir. Çünkü bilgisayar sistemlerine neler olduğunu anlama noktasında güven duyulmakta

[7] İnternet dolandırıcılığı, kimlik hırsızlığı, fikri mülkiyet haklarının gasp edilmesi gibi siyasi ya da ulusal güvenlik amacıyla gerçekleştirilmeyen suçlar, siber saldırının bu son unsuruna uymadığı için siber saldırı değil; siber suç kategorisi altında incelenmektedir (Hathaway vd., 2012:830).

bu yüzden sistem hata vermediği sürece bu tür saldırıların farkedilmesi zorlaşmaktadır (Singer ve Friedman, 2014:71).

Bütünlük saldırılarının hedefleri ve sonuçları değişkenlik göstermektedir. Burada etki kavramı önemli hale gelmektedir. Çünkü amaçlanan etki, bir devlet kurumunun kamuya açık web sitesini değiştirmek olabileceği gibi bir ülkenin resmi kararlarını uygulama yeteneğine zarar verme, kendini savunma ya da devletin halkına hizmet sağlamasını (elektirik, gaz, petrol dağıtımı, sağlık sistemleri gibi) engelleme gibi stratejik olarak büyük nitelikte zararlar olabilir. Bu açıdan değiştirilen veriler, gerçekleştirilen bütünlük saldırısının önemini belirleyen şeylerdir. 2012 yılında Suudi Arabistan'ın petrol firması Aramco'nun yaklaşık otuz bin bilgisayarına yönelik gerçekleştirilen siber saldırıda bulaştırılan virüs, bilgisayarlardaki dosyaları silmiş yerlerine ise yanmış Amerikan Bayrağı koymuştur. Bilginin bütünlüğüne yönelik yapılan *Shamoon* isimli bu siber saldırıyı İranlı siber korsanlar üstlenmiştir. Bu saldırının ortaya koyduğu sonuç hedefin büyük olmasının, etkinin de büyük olduğu sonucunu doğurduğudur (Çifci, 2017:197; Singer ve Friedman, 2014:71).

Bütünlüğe yönelik saldırılara bir başka örnek ise, 1999 yılında Kosova'daki savaş esnasında gerçekleşmiş, NATO hava savaşı planlayıcıları Sırbistan ordusuna ait merkezi hava savunma komuta ağına gerçek dışı hedefler ve mesajlar yerleştirmek için bir çeşit siber saldırı tasarlamışlardır. Ancak planlamada bir yanlışlık olması durumunda böyle bir siber saldırı sonucu sivil hedeflerin risk altına girebileceği, Sırp hava savunma ağınının askeri uçaklarla sivil ve ticari uçakları karıştırabileceği bu noktada da evler, hastaneler, okullar gibi sivil yapıların bombalanabileceği düşüncesiyle NATO bu siber saldırıyı başlatmamış ve geri adım atmıştır (Kelsey, 2008:1434-1435).

1.4.3. Erişilebilirliği (Availability) Tehlikeye Atan Siber Saldırılar

Erişilebilirliği tehlikeye atan siber saldırılar, aynı anda birçok sunucudan yoğun bir giriş talep ederek bir ağa erişimi engellemek, hizmet reddine ya da fiziksel ve sanal işlemleri durdurmak için ağı çevrimdışı hale getirmeye çalışan saldırılardır. Bu tür saldırıların etkisini değerlendirmede önemli bir nokta, siber güvenlik uzmanı Dmitri Alperovitch'in de belirttiği gibi, *ölçek* ve *etki* büyüklüklerinin hesaplanmasından geçmektedir. Örneğin, online bir oyun sitesine hizmet reddi yoluyla yapılan yarım saatlik bir saldırı sitede aktif olan oyuncular için büyük gibi gözükebilir. Ancak bu saldırının etkisi, bir ülkenin kritik altyapısının bazı bölümlerini etkileyen ve uzun süreler boyunca gerçekleşen bir hizmet reddi saldırısına kıyasla daha az stratejik ve caydırılması noktasında daha az dikkate değerdir (Singer ve Friedman, 2014:70).

Erişilebilirliği tehlikeye atan saldırılara bir örnek, 2009 yılında gerçekleşen ABD ve Güney Kore'deki bir dizi hükümet ve ticari web sitesinin hizmet reddi saldırılarıyla devre dışı bırakılması

verilebilir. Güney Kore bu saldırılar sonucunda Kuzey Kore'yi suçlasa da ABD olaya daha temkinli yaklaşmıştır. Saldırının kaynağı konusunda bir netlik ortaya konulamasa da bu saldırı, erişilebilirliğe yönelik saldırılarla ilgili kolektif bir sorunu ortaya koyması açısından önemlidir. Saldırılarda kullanılan botnetler, dünyanın dört bir tarafından suçsuz kullanıcıları ve bilgisayarları dahil ederek saldırgan ya da saldırganların etrafından bir anonimlik ağı oluşturmakta ve bu sayede saldırının kaynağına ilişkin kesin bir atıf yapılamamaktadır (Hathaway vd., 2012:838).

1.5. Sık Kullanılan Siber Silahlar ve Saldırı Yöntemleri

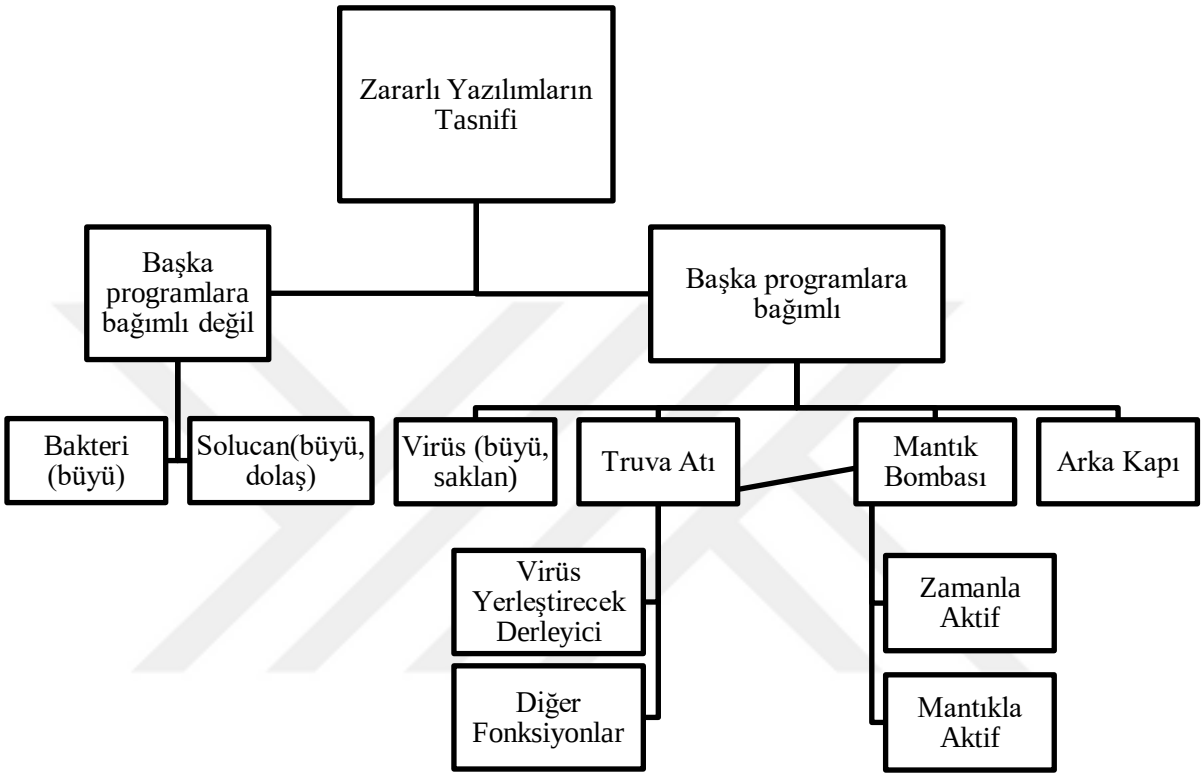
Siber saldırılar farklı yöntemlerde ve türlerde ortaya çıkabilmektedir. Bir bilgisayardan, başka bir ağa, bilgisayara ya da sisteme yönlendirilen saldırılar temelde üç türe ayrılabilir. Bu ayrım, *sözdizimsel (syntactic), anlamsal (semantic), karıştırılmış (blended)* saldırıları içermektedir. Sözdizimsel saldırılar, bilgisayarın işletim sistemine ve/veya işlevlerini kontrol eden yazılım düzeyine yönlendirilen saldırılardır. Son yıllarda yaşanan saldırıların çoğu bu kategoridedir ve solucanlar, virüsler, truva atları ve hizmet reddi saldırılarının kullanımı sözdizimsel saldırı kategorisindedir. Anlamsal saldırılar, sözdizimsel saldırılardan farklı olarak işletim sistemini değil; bir kullanıcının eriştiği verinin doğruluğuna olan güvenini hedef alır. Anlamsal saldırılar, verilerin kullanıcıların bilgisi olmadan değiştirilmesi şeklinde gelişir ve yukarıda bahsettiğimiz bilginin bütünlüğünü tehlikeye atan saldırı türüne örnek olmaktadır. Karıştırılmış saldırılar, sözdizimsel ve anlamsal saldırıların birleştirilmesi yoluyla yapılır (Brenner ve Goodman, 2002:27).

Genel hatlarıyla bu şekilde ifade edilebilecek olan siber saldırıları yöntemlerinden sonra konuyu daha özele, siber silahlara indirdiğimizde ise öncelikle siber silahların geçmiş silahlanma yarışından ayrılan yönleri karşımıza çıkmaktadır. 21. yüzyıl siber silahlanmasını geçmişteki silahlanma yarışlarından temelde ayrı kılan nokta, silahlanmanın sadece devletlere özgü bir oyun olmamasından ileri gelmektedir. Siber uzayın kendine has yapısını hem pozitif hem de negatife çevirebilecek olan keskin ölçek, hem devlet hem de devlet dışı özel aktörlerin hareket sahası olarak kullanılabilmesinden kaynaklanmaktadır. Çünkü siber uzay küçük gruplara büyük etkiler doğurma şansı tanımaktadır. Ayrıca bu küçük grupların yalnızca güçleri değil; silahlanma kontrol uzmanları tarafından çoğalma olarak adlandırılan, paylaşabilme yetenekleri de ayrımın bir başka keskin ucunu oluşturmaktadır. Savaş uçakları ya da atom bombası yapımından farklı olarak, siber uzayda faaliyet gösteren bireyler ve gruplar siber silahlarla ilgili yeni yeneteklerin nasıl ortaya çıkabileceği konusunda, çok basit yöntemlerle, binlerce kişiye bilgi verebilirler. Örneğin uzman grubu tarafından yoğun çalışmalar sonucu ortaya çıkarılan Stuxnet virüsünün yayılmasından birkaç hafta sonra Mısırlı bir blogger yeni siber silaha ilişkin nasıl yapılır rehberi yayımlamıştır (Singer ve Friedman, 2014:157-158).

21. yüzyılda sık kullanılan siber silahlar ve saldırı yöntemlerini incelediğimizde ise karşımıza solucan, virüs, truva atı, mantık bombası, tuş kaydedici, rootkit, köle bilgisayarlar gibi zararlı

yazılımlar ve sistemleri etkilemeye yönelik hizmet dışı bırakma saldırıları ve sosyal mühendislik yöntemleri gibi sözdizimsel saldırı örnekleri çıkmaktadır. Çifci (2017:168) zararlı yazılımları başka programlara bağlı olup olmamasına göre ayırmış ve Şekil 3'te bu ayrım gösterilmiştir.

Şekil 3: Zararlı Yazılımların Tasnifi



Kaynak: Çifci, 2017:168

1.5.1. Solucan

İngilizce *worm* olarak ifade edilen ve başka programlardan bağımsız olarak çalışabilen bilgisayar solucanı, kendi kopyalarını bilgisayardan bilgisayara yayarak gelişim gösteren bir tür kötü amaçlı yazılımdır. Bilgisayar solucanlarının en önemli özelliği kendilerini insan etkileşimi olmadan kopyalayabiliyor oluşudur. Yazılım açıkları ya da maillere ve anlık iletilere ekli olarak bulaşabilen bu kötü amaçlı yazılım türü kurulduktan sonra kullanıcıya fark ettirmeden işe koyulur ve sistem üzerinde açıklık oluşturarak veri çalmak, arka kapı oluşturmak gibi birçok faaliyette bulunabilir (What is a computer worm, and how does it work? (t.y.), https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html). Bulaştığı süreçten itibaren ağlarda ve sistem üzerinde kısmi yavaşlamaya sebep olan solucanlar, çok kısa süre içinde çok fazla sayıda bilgisayara bulaşabilir. İnternet yoluyla dolaşıma giren ve bilinen en büyük hasara neden olan solucan *Morris Internet Worm*'dur. Ayrıca gerçekleştiğinde büyük yankı uyandıran

Stuxnet, *Duqu*, *Conficker*, *Slammer* gibi etkili solucan örnekleri de vardır (Çifci, 2017:169; Keleştemur, 2015:227).

1.5.2. Virüs

Bilgisayar virüsleri kendi başlarına çoğalabilen ancak çoğalmadan önce bir bilgisayara ya da dosyaya kendilerini bağlayabilecek bir programa ihtiyaç duyan zararlı yazılım türlerindendir. Solucanlardan temel farkı bu noktada yatmaktadır. Genellikle bilgisayardaki verileri değiştirerek ya da silerek siber saldırılarda etkili olurlar (Dashora, 2011:246). Virüslerin tehlike boyutu, onu oluşturan kişinin niyetine ve yaratıcılığına bağlı olarak değişebilmektedir. Virüslerden bazıları yalnızca propaganda ya da kişisel tatmin amacıyla ortaya çıkarılırken bazıları ise bilgisayarı hatta bir bütün olarak sistemleri kullanışsız duruma getirmektedir (Keleştemur, 2015:222).

1.5.3. Truva Atı (Trojan Horse)

Truva atı, yararlı bir programla birlikte sisteme giren ancak eş zamanlı olarak sistemde zarar meydana getirmeyi amaçlayan zararlı yazılım türlerindendir. Truva atı da tıpkı virüsler gibi başka programlara bağımlı yazılımlardandır. Virüslerden farkı ise, bilgisayarlar arası kendisini kopyalama özelliğinin bulunmamasıdır (Çifci, 2017:171). Bir truva atı kurmanın en yaygın şekli e-posta yoluyla gerçekleştirilmekte ve ekli dosya sayesinde sisteme bulaşmaktadır (Dashora, 2011:247).

1.5.4. Mantık Bombası (Logic Bomb)

Zararlı yazılımların bu türü diğer türlerden farklı olarak zamanının belli olduğu ve belirli koşullar (tetikleyici olay olarak bilinir) gerçekleştiğinde otomatik olarak devreye giren uygulamalardandır. Mantık bombası, sinsi bir şekilde çalıştırılacağı günü bekleyebilir. Kuluçka olarak tabir edilen bu bekleyişi nedeniyle, Rus istihbarat servisleri tarafından yoğun olarak kullanılan *kuluçka ajan* şekline benzediği ifade edilebilir (Keleştemur, 2015:228).

1.5.5. Arka Kapı (Backdoor/Trapdoor)

Yalnızca siber saldırganın bildiği arka kapılar, klasik kimlik kontrol sistemleri dışına çıkılarak ve rutin incelemelerle bulunamayacak biçimde hedef sisteme yalnızca saldırgan tarafından bilinen noktalardan ulaşmayı sağlayan yöntemler ve girişler bütünü olarak ifade edilebilir (Çifci, 2017:172). Arka kapılar bazen, sisteme tekrar erişebilmek için tasarımcı tarafından konulan ancak üzerinden zaman geçtikten sonra unutulan açıklıklar şeklinde de karşımıza çıkmaktadır. Arka kapılar ile ilgili yaygın bir iddia Microsoft'un gelişim sürecinde, Amerikan

Ulusal Güvenlik Ajansı'nın (NSA) yardım ettiği buna karşılık ise NSA'in geliştirilen tüm işletim sistemlerine bir arka kapı eklediği şeklindedir (Bıçakçı, 2014:109).

1.5.6. Tuş Kaydedici (Keylogger)

Tuş kaydediciler, siber istihbaratçılar tarafından da sıkça kullanılan, klavyedeki tuş vuruşlarını izleyen ve bu vuruşları anlamlı bir bütün halinde kaydederek ağ üzerinden saldırgana ileten bir zararlı yazılımdır. Genellikle şifreleri yakalama amacı taşıdığı söylenebilir (Keleştemur, 2015:224; Sommer ve Brown, 2011:25). Klavyeler, bilgisayar bileşenleri içinde en sık kullanılan ara yüzlerden biri olduğu için tuş kaydedicilerin kullanıcı hakkında bu yolla bilgi toplaması da sık başvurulan yollardan biri haline gelmiştir. Donanım ve yazılıma bağlı olarak iki gruba ayrılsa da baskın olan form yazılıma bağlı kaydedicilerdir. Yazılıma bağlı olanların ucuz ve kolay kullanılıyor oluşu tercih edilme sebebini de arttırmakta ve çoğunlukla izleme amacıyla kullanılmaktadır. Donanıma bağlı olanlar genellikle donanımla ilgili bileşenlerine bağlıdır. Yani ana karta gizlice yerleşmiş olabilir ve tespit edilmesi dahi zaman zaman zor hale gelmektedir (Tuli ve Sahu, 2013:107; Damodaram ve Valarmathi, 2010:620).

1.5.7. Rootkit

Kök kullanıcı takımı olarak Türkçeleştirilen rootkitler esasen, Çifci'nin (2017:173) aktardığı şekliyle bilgisayarın arka planında faaliyetini sürdüren işlemleri; dosyalara ve sisteme ait bilgileri işletim sisteminden gizleyerek etkisiz halde gözükmesini sağlayan programlardır. Genel olarak, işletim sistemleri içerisinde çekirdek seviyesinde çalıştıkları için ortaya çıkarmak ve sistemi tamamen temizlemek zor hale gelmektedir. Teknolojinin ilerlemesiyle birlikte günümüzde kullanım alanı ve amacı, sistemde bulunan başka zararlı yazılımların kolayca çalışabilmelerini sağlamak haline gelmiştir (Keleştemur, 2015:226).

1.5.8. Köle Bilgisayarlar (Botnet)

Köle bilgisayarlar, bilgisayarların yüklenen bir yazılım aracılığıyla uzaktan kontrol edilebilmesi ve bu yolla siber saldırganın hedeflediği sonuçlara ulaşabilmesini sağlayan ve uzaktan erişim nedeniyle sahibinin bilgisi dışında işlemler gerçekleştiren bu nedenle de zombi olarak adlandırılan bilgisayarlar ortaya çıkaran bir sistemdir (Ünver vd., 2011:24). Köle bilgisayarların günümüzde en tehlikeli ağ tabanlı saldırı türlerinden biri haline gelmesinin en temel sebebi, hem açık etki bırakan hem de zekice kurgulanmış saldırılar için çok büyük ve koordineli ana bilgisayar gruplarının kullanılmasını içermesidir. Bu büyük bilgisayar grupları zombilere ya da botlara dönüştükten sonra, uzaktan kontrol edilebilecek biçimde birleştirilir. Böylece tek bir komut ve kontrol altına giren botlar topluluğu botnetleri oluşturur. Bu açıdan bir köle bilgisayar saldırısının

değeri, siber saldırganın kontrol ettiği çok sayıda (genellikle onlarca, yüzlerce ve bazı durumlarda milyonlarca) bilgisayarla ölçülmektedir (Owens vd., 2009:92; Strayer vd., 2008:1).

Köle bilgisayarların etkisinin dikkat çekici bir örneği, Afrika kıtasında devlet bilgisayarları da dahil olmak üzere tüm bilgisayarlarda %80 oranında zararlı yazılım olduğunun tahmin ediliyor olması ve bu durumun bir salgının siber eşdeğeri olarak görülmesi şeklindedir. Bir milyon köle bilgisayarın çok uluslu şirketlerin sistemlerini, on milyon köle bilgisayara sahip bir sistemin (Conficker gibi) büyük bir Batı devletinin sistemini felç edebileceği düşünülünce, köle bilgisayarların yarattığı tehdit daha net anlaşılmaktadır. Ancak köle bilgisayar sisteminin izlerinin takip edilmesi ve saldırganın tespitinin zorluğu ve genellikle tespit edilenlerin suçsuz köle bilgisayar kullanıcılarıdan oluşuyor olması ülkelerin hukuk sistemlerini ve kolluk kuvvetlerini zor durumda bırakmaktadır. Ayrıca köle bilgisayar sahiplerinin kontrolü altında bulunan bu etki gücü büyük ağı ticari yollarla kiraladıkları da gözlemlenmektedir. Bu durum da kolluk kuvvetlerinin görevini zorlaştıran bir başka unsur olarak dikkate değerdir (Bıçakçı, 2014:123-124; Carr, 2012:13).

1.5.9. Hizmet Dışı Bırakma (Denial of Service) / Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service)

Bir hizmet dışı bırakma saldırısı (DoS), kullanıcıların ulaşmak istediği kaynakları kullanmasını önlemek için yapılmakta olup basit bir tanımlamayla saldırganın hedeflediği sistemin rutin işleyişini bozmak/zarar vermek amacıyla yaptığı saldırı türlerindendir. Bir siber saldırgan, vermek istediği zararın daha büyük olması durumunda Dağıtık Hizmet Dışı Bırakma (DDoS) saldırıları da yapabilmekte, temelde hizmet dışı bırakma saldırılarından farkını ise tek bir merkeze yönelik saldırıların birden fazla noktadan geliyor olması oluşturmaktadır. Hizmet reddi saldırıları üç farklı şekilde yapılabilir: *(1) Bir ağa taşma girişiminde bulunularak meşru ağ trafiği önlenebilir*, daha açık bir ifadeyle, bir tünele aynı anda binlerce arabanın girmeye çalışması gibi düşünülebilir. *(2) İki makine arasındaki bağlantılar bozulmaya çalışılır böylece bir hizmete erişim engellenmiş olur* ve *(3) belirli bir bireyin, belirli bir hizmete erişimi engellenmeye çalışılır* (Keleştemur, 2015:292-296; Lau vd., 2000:2275).

Çok sık başvurulan bir yöntem olan DDoS saldırılarına Türkiye'de birçok kez maruz kalmış, son örneği ise 27 Ekim 2019 tarihinde gerçekleşmiş ve bankacılık[8], haberleşme[9] sektörü ve ayrıca

[8] Saldırılara maruz kalan bankacılık şirketlerinden biri olan GarantiBBVA sosyal medya hesabından özür metni paylaşılmıştır: *"Dijital hizmetlerimize yönelik yoğun internet trafiği nedeniyle dijital kanallarımızda erişim sıkıntısı yaşamaktayız. İnternet servis sağlayıcılarımızla beraber sorunu gidermek için çalışıyoruz. Müşterilerimizin yaşadığı mağduriyet için özür dileriz."*

[9] Saldırıya maruz kalan haberleşme şirketlerinden biri olan Türk Telekom yazılı açıklamada bulunmuştur: *"Ülkemizin en büyük siber güvenlik merkezine sahip olan şirketimizin aldığı önlemlerle yurt içi ve yurt dışı internet trafiği herhangi bir olumsuzluğa meydan vermeksizin normal seyrinde devam etmektedir."*

birkaç büyük şirket hedef alınmıştır. Bilgi Teknolojileri ve İletişim Kurumu (BTK) çatısı altında faaliyet gösteren Ulusal Siber Olaylara Müdahale Ekibi (USOM) gerekli önlemleri almaya çalışsa da yıl içinde gerçekleşen saldırıların toplam maliyetinin 2 trilyon dolara ulaştığı tahmin edilmektedir (Türkiye'ye yönelik siber saldırılar bertaraf edildi (2019), https://www.trthaber.com/haber/turkiye/turkiyeye-yonelik-siber-saldirilar-bertaraf-edildi-437841.html).

1.5.10. Sosyal Mühendislik

Güvenlik sistemlerinde en zayıf bileşen olarak insanların değerlendirilmesi, aynı zamanda en zayıf bileşenin istismar edilmesi aracılığıyla veri elde edilmesinin de yolunu açmaktadır. Sosyal mühendislik böyle bir durumda devreye girmekte ve *"insanları aldatmak, dışarı bilgi vermelerini sağlamak ya da bir eylemde bulunmalarını olanaklı kılmak için manipüle etmek"* anlamına gelmektedir (Mann, 2008:11). Sosyal mühendislik kavramı, bilgi teknolojileri ve sistemleri açısından bireylerin, hedefli bir organizasyon hakkında diğer bireylerden bilgi edinebileceği sosyal-psikolojik bir süreç olarak görülmektedir. Belirtmek gereki ki, sosyal mühendisler bilgisayar korsanları değil; bilgisayar korsanlarının işini kolaylaştıran ya da bilgiye ulaşmayı mümkün kılan kişilerdir. Sosyal mühendisin amacı, kuruluşa dair bilgilere ya da bilgi sistemlerine fiziksel ya da dijital yollarla erişim sağlamaktır. Kullanılan teknikler açısından basit izinsiz girişler olabileceği gibi, daha yüksek teknolojilerin kullanımını da içermektedir. Sosyal mühendis, sisteme erişim sağladıktan sonra verilerin çıkarılması, bozulması ya da silinmesi için bilgisayar korsanlarının sisteme giriş sağlamasına izin verebilir (Thornburgh, 2004:134).

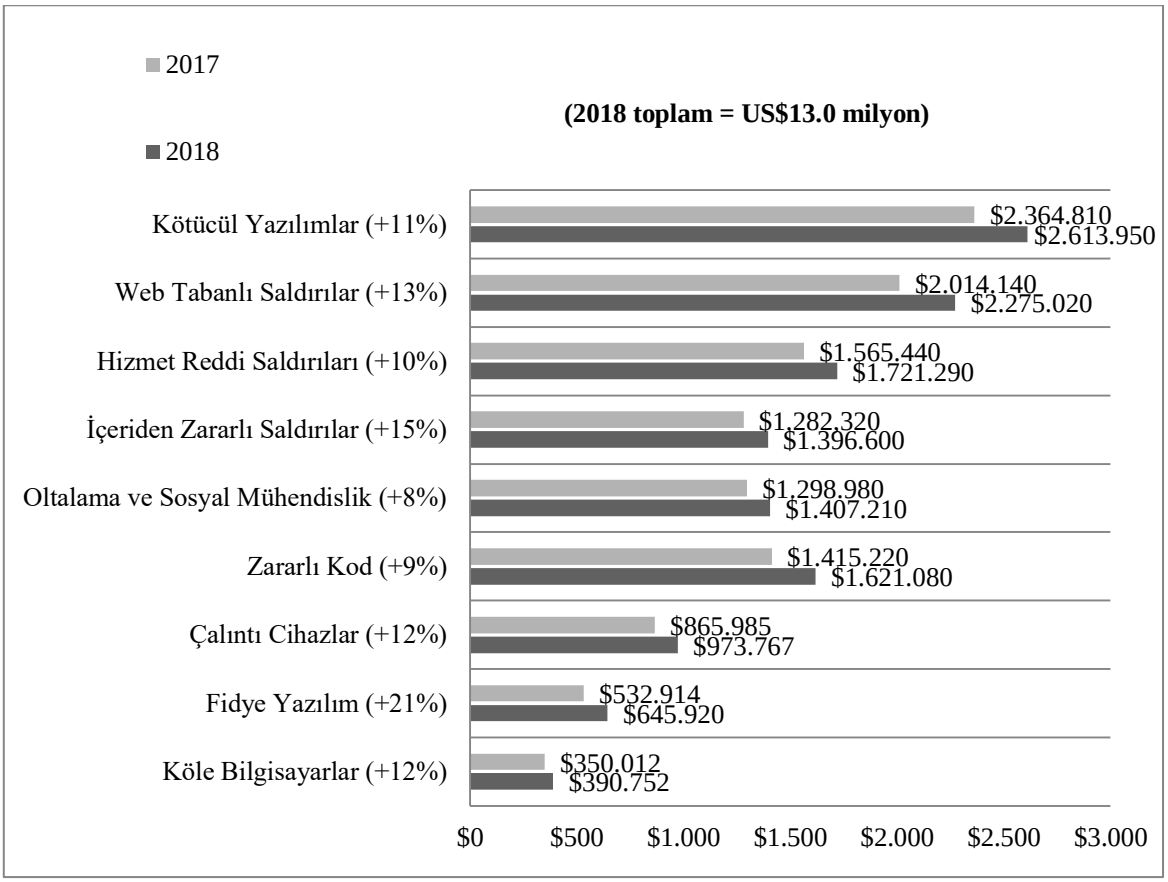
Sosyal mühendisler, veri elde etmenin dışında internet (sosyal medya) yoluyla manipülasyonda bulunma amaçlı faaliyetler de gösterebilmektedir. Burada manipüle edilmesi amaçlanan hedef kitle genellikle ülkelerin istihbarat servisleri tarafından tespit edilmiş kişilerden oluşmaktadır. Sosyal mühendisler, hedef kişilerin eylemlerini, hareket planlarını öğrenerek olası bir tehdidin uzak tutulmasını sağlamaktadır (Keleştemur, 2015:213). Ayrıca sosyal mühendisler, sosyal paylaşım siteleri üzerinden, kişiler hakkında tek başına bir anlam ifade etmeyen ve herkesin ulaşabildiği bilgileri analiz yoluyla birleştirerek önem derecesi yüksek bir bilgi bütünü ortaya çıkarmaktadır (Bayraktar, 2014:138).

1.6. Siber Silahların Ekonomik Etkileri

Siber saldırı yöntemleri ve kullanılan siber silahlar sonucu oluşan zararın ekonomik etkisi de yıldan yıla artış göstermektedir. Grafik 1, siber suçlar sonucu karşılaşılan zararların artmakta olduğunu ve 2017-2018 yılları içinde en pahalı siber saldırı türü olarak kötücül yazılımlar ve web tabanlı saldırıların ön plana çıktığını göstermektedir. Ayrıca, içeriden gerçekleşen zararlı saldırılar (+15%) ve fidye yazılımlarla gerçekleştirilen saldırıların (+21%) bir önceki yıla göre en yüksek

artış gösteren alanlar olması dikkat çeken bir başka noktayı oluşturmaktadır. İçeriden zararlı saldırıların etkisinin büyük olmasının sebebi, siber saldırganın etki etmek istediği alana hakimiyetinin yüksek derecede olmasından kaynaklanıyor gibi gözükmektedir.

Grafik 1: Saldırı Türüne Göre Yıllık Ortalama Siber Suç Maliyeti[10]



Kaynak: Bissell vd., 2019:17-18

1.7. Siber Savaş Kavramı

Diğer siber aksiyonlar gibi siber savaş hakkında da herkesin üzerinde uzlaşabildiği net bir tanımlama bulunmamakta hatta siber savaşların gerçekten bir savaş olup olmadığı noktasında da bir belirsizlik hüküm sürmekte ve konuyla alakalı literatürde farklı görüşler bulunmaktadır. Kavramla alakalı Carr (2012:2) tarafından yapılan ve Sun Tzu'dan esintiler taşıyan bir tanımlamada siber savaş, *"savaşmadan savaşma sanatı ve bilimi; kanını dökmeden bir rakibi yenmek"* şeklinde yapılmıştır. Farklı bir tanımlamada ise siber savaş, bilgi kavramı ekseninde tanımlanmış ve *"bilgi ile ilgili askeri operasyonlar yürütmek ve yürütmek için hazırlık yapmak"* şeklinde kullanılmıştır. Bu tanım, düşmanınızın sizinle ilgili bilgi sahibi olmasını engellerken bir yandan da düşman hakkında herşeyi öğrenmeye çalışmak, yani bilginin kullanılmasını referans göstermektedir

[10] Grafikteki veriler 11 ülkede ve 16 sektörde yapılan araştırmaları birleştirmektedir.

(Arquilla ve Ronfeldt, 1997:30). Siber savaşın bilgi savaşı temelli açıklanmaya çalışılması, kavramın serpilmeye başladığı 1990'lı yılların başında iki terimin birbirinin yerine kullanılmasına dayanmaktadır. Ancak günümüzde birbirinin yerine kullanma kabul edilmemekte; bilgi savaşı daha kapsamlı bir şekilde siber savaşı da kapsayan bir kavram olarak ifade edilmektedir (Yayla, 2013:185).

Siber savaş tanımlarından en popüler olanı ise, ABD Başkanı Bush'a siber güvenlik konusunda danışmanlık yapmış olan R. Clarke'a attir ve siber savaşı *"bir devletin, başka bir devletin bilgisayarlar sistemine ya da ağlarına zarar verme ya da kesinti yaratma nedeniyle sızma eylemi"* şeklinde tanımlamıştır (Clarke ve Knake, 2010:8). Clarke'a ait tanımlamada öne çıkan, savaşın iki devlet arasında gerçekleşmesi şartı ve girişilen eylemin kesinti ya da zarara neden olma koşulu gerçekleşen olayların siber savaş kategorisi içinde incelemeye alınması noktasında yardımcı olmaktadır (Çifci, 2017:7). Singer ve Friedman (2014:121) da benzer bir niteleme ortaya koyarak, nerede gerçekleştiğine bakılmaksızın (kara, hava, deniz, uzay ya da siber uzay) savaşın suçtan ayrılmasını sağlayan siyasi bir amacı ve şekli olduğunu ayrıca daima bir şiddet unsuru içerdiğini ileri sürmektedirler.

Siber savaşın tanımının yanı sıra kinetik etki oluşturma gerekliliği de bir başka tartışmalı durumu oluşturmaktadır. Liff (2012: 404-405) bu konuda araçları kinetik olmayan bilgisayar ağı işlemleri için siber savaş tanımının kesinlikle kapsayıcı ve geçerli olduğunu ifade etmektedir. Ayrıca, siber savaşı, doğrudan politik ve askeri hedeflere sahip bilgisayar ağı saldırını (bu saldırılar zorlayıcı bir niyetle ve/veya bazı stratejik ve kaba kuvvetlerin sona ermesinin bir aracı olarak yapılır) ve bilgisayar ağı savunmasını içerecek şekilde kavramsallaştırmıştır. Bu açıdan siber savaş, medyada sık sık bu kapsamda dile getirilen, eğlence için hack yapmak, kar kaynaklı siber suç ya da siber casusluk faaliyetlerini kapsamamaktadır. McGraw (2013:112) ise siber savaşın fiziksel dünyada, askeri uzmanlarca kinetik bir etki olarak adlandırılan bir sonucu gerektirdiğini ifade etmektedir. Yani düşman bir ülkenin komuta konrol sistemine kötü amaçlı yazılımlar bulaştırmak böylece kontrolü ele geçirerek düşmanın dronelarının yanlış yere saldırmalarını sağlamak bir siber savaş eylemi olarak sayılmalıdır. Çünkü araçlar sanal olsa da etki fiziksel olmuştur.

Tanım ve etki boyutlarının yanı sıra siber savaş kavramının, gerçek bir savaş hüviyeti taşıyıp taşımadığıyla da alakalı çeşitli görüşlerin olması onun, klasik savaş yöntemlerinden farklılaşan karakterini de ortaya koymayı gerektirmektedir. Örneğin, siber savaşlar geleneksel egemenlik nosyonları ve onları düzenlemek amacıyla geliştirilen ahlaki ve yasal doktrinler üzerinde büyük bir baskı oluşturmakta ve siber uzayın sınırları ortadan kaldıran yapısı nedeniyle klasik egemenlik nosyonunu ve devlet sınırlarını dağıtmış gibi gözükmektedir. Ayrım ilkesinin korunabilmesi gittikçe zor hale gelmekte ve siber savaşlarda askeri ve sivil nüfus arasındaki ayrım giderek belirsizleşmektedir. Aktarılan açıklamalar siber savaşın, savaş alanına ait olduğunu iddia edenleri destekler niteliktedir. Ancak siber savaşların, gerçek bir savaş hüviyeti taşımadığını iddia edenler

ise onun yalnızca ekonomik bir zarara ve sınırlı bir hasara neden olduğunu bu yüzden savaş alanına ait olmadığını savunurlar (Finkelstein ve Govern, 2015:xv-xvi). Bu açıdan savaş ve siber savaş arasındaki ayrımı/ayrımları ortaya koyabilmek önem taşımaktadır.

Tablo 2: Konvansiyonel Savaş-Siber Savaş Özelliklerinin Kıyaslanması

Konvansiyonel Savaşın Özellikleri	**Siber Savaşın Özellikleri**
Konvansiyonel savaşlar, savaş beyanıyla başlamaktadır.	Herhangi bir savaş beyanı bulunmamaktadır.
Konvansiyonel savaşlar, genellikle barış anlaşmalarıyla biter.	Herhangi bir barış anlaşmasıyla bitmez.
Savaş, şiddetin bir biçimidir.	Siber saldırılar bir şiddet eylemidir ancak savaş olmasını gerektirmez.
Savaşlar, siyasi grupları içeren örgütlü, kanlı, büyük çaplı bir çatışmadır. Bu sebepten toplu bir eylemdir.	Büyük çaplı bir çatışma olasılığı mümkündür. Siyasi grupların dahiliyeti ve örgütlü olması da mümkündür bu sebepten siber savaşlar da toplu bir eylemdir ancak bilinen kanlı bir siber savaş örneği yoktur.
Egemen devletler arası askeri çatışma şeklinde gerçekleşir.	Siber savaşın kendisi bir savaş olabilmesi için konvansiyonel savaş çerçevesinin bir parçası olmalıdır.
Savaşan devletlere uygulanan savaş yasaları, yani hukuk kurallar vardır.	Uygulanacak yasalarla ilgili bir belirsizlik vardır.
Toplu şiddetin aşırı türdeki bir tezahürüdür.	Siber savaş iki toplum arasında bir şiddet eylemi olabilir. Aşırılık siber savaşın doğasıyla daha az ilgilidir.

Kaynak: Ventre, 2011:215-216

Farklı bir ayrım ise Çifci, (2017:23) ve Keleştemur, (2015:164-165) tarafından ortaya konmuş ve saldırının *kaynağına, hızına, etkisine, maliyetine, saldırı belirtilerine, hasarın tespitine* ve *kullanılan silahlara* yönelik olarak yedi kriterle klasik savaş ve siber savaş arasındaki ayrım açıklanmaya çalışılmıştır. Bu ayrım siber savaşın, klasik savaşlara göre tercih edilebilir yönlerini ortaya koyması açısından önemlidir. Örneğin siber savaşların maliyet yönünden geleneksel savaş yöntemlerinden ucuz olması ya da oluşturduğu etki yönünden saldırıya uğrayan alanla sınırlı kalmaması devletler tarafından bu alana gösterilen ilginin artmasının da sebeplerindendir.

Tablo 3: Klasik Savaş ve Siber Savaş Arasındaki Farklar

Değişkenler	Klasik Savaş	Siber Savaş
Saldırının Kaynağı Yönünden	Saldırının kaynağını saptamak görece kolaydır.	Saldırının kaynağını belirlemek genellikle çok zordur.
Hızı Yönünden	Savaşta kullanılan enstrümanların (uçak, füze vb.) hızıyla doğru orantılıdır.	Kullanılan internet altyapısının hızındadır.
Etkisi Yönünden	Fiziksel alanda büyük etki doğurmaktadır.	Kritik altyapılar örneğinde olduğu gibi fiziksel etki de yaratabilir. Ancak çoğunlukla bilgi ve iletişim sistemleri üzerinde etkilidir.
Maliyeti Yönünden	Etki aracı olarak kullanılan silahlara ve sistemlerin maliyetine doğrudan bağlıdır ve genellikle oldukça pahalıdır.	Bilgi ve iletişim sistemlerin ucuzluğu sebebiyle genellikle ucuzdur.
Saldırı Belirtisi Yönünden	Saldırının farkına varılması ihtimali çok daha yüksektir.	Saldırının farkına bazen çok geç, bazen de saldırı bittikten sonra varılabilir.
Hasar Tespiti Yönünden	Saldırının etkileri fiziksel olarak görülebildiğinden (insan kaybı, binaların yıkılması vs.) hasar tespiti nispeten daha kolaydır.	Fiziksel bir etkisi (örneğin kritik altyapılara yönelik) olmadığı sürece hasar tespiti yapmak nispeten daha zordur.
Kullanılan Silahlar Yönünden	Fiziksel yıkım etkisi yüksek (tank, bomba, uçak, füze vb.) araçlar kullanılır.	Bilgisayarlar, yazılımlar, çipler gibi araçlar kullanılır.

Kaynak: Çifci, 2017:23; Keleştemur, 2015:164-165

Sonuç olarak siber savaşlar (ya da onu savaş yapan saldırılar)[11] silahlı çatışma alanında radikal dönüşüme sebep olmuş; *mekan* , *zaman* ve belki de en önemlisi *ispat* kavramını kökünden zayıflatarak saldırgan ve hedef arasındaki ilişkiyi asimetrik hale getirmiştir. Örnek olarak konvansiyonel savaş koşullarında kritik önem taşıyan ve veri kümesi işlevi gören *mekansal boyut*, siber saldırı esnasında bir noktadan anında başka bir noktanın vurulabilmesi sayesinde aşınmaya uğramıştır. Mekan kavramının önemini yitirmesi hedefin *tepki verme süresini* ortadan kaldırır

[11] Sıkça birbirinin yerine kullanılan siber savaş ve siber saldırı temelde etki ve bağlam yönünden farklılaşmaktadır. Siber savaşların etkisinin silahlı çatışmayla eşdeğer olması ya da silahlı çatışma bağlamında ortaya çıkması gerekir. Bilgisayar ağının işlevini zayıflatmak ve siyasi ya da ulusal güvenlik amacı ikisinde de ortaktır (Hathaway vd., 2012:833).

çünkü hedefin saldırının merkezine dair kesinlik oluşturmasının önüne geçer. Diğer taraftan ispat kavramının aşınmaya uğraması, *dijital dünyada her şeyin çarpıtılabilir olmasıyla* alakalıdır. İspat kavramının aşınmaya uğramasıyla birlikte saldırıya cevap verme ya da meşru müdafa yapma gibi fikirler de geçerliliğini kaybetmektedir. Bu sayede hedefin operasyonel kapasitesini işlemez hale getirmek amaçlanmaktadır (Filiol, 2011:249-251).

1.7.1. Operasyonel Siber Savaş

Operasyonel siber savaş, Libicki (2009:139-140) tarafından *"askeri hedeflere ve askeri kaynaklı sivil hedeflere yönelik, savaş zamanı gerçekleştirilen siber savaşlar"* şeklinde tanımlanmıştır. Operasyonel siber savaşlar bir ülkenin askeri kapasitesi içinde doğrudan belirleyici bir etken olmasa da doğru zamanda ve dikkatli bir biçimde kullanılırsa önemli bir güç çarpanı olabilmektedir. Burada dikkat edilmesi gereken nokta, operasyonel siber savaşın başlı başına bir savaşı kazanamayacak ancak destek unsuru[12] olarak işlev görebilecek bir bileşen olduğudur. Siber savaşların destek mahiyetinde kullanılmasının doğurduğu etki saldırıya uğrayan devletin altyapısının siber ortama ne kadar bağlı olduğuyla doğrudan alakalıdır. Eğer rakibinizin herhangi bir siber altyapısı yoksa operasyonel yöntemler kullanışsız hale gelmektedir (Çifci, 2017:20).

1.7.2. Stratejik Siber Savaş

Stratejik siber savaş, Libicki, (2009:117) tarafından *"bir devlete ve o devletin toplumuna yönelik gerçekleştirilen, öncelikli olarak ama sadece hedef kitlenin davranışını değiştirmek için yapılmayan bir siber saldırı stratejik siber savaş olurdu"* şeklinde tanımlanmıştır. Saldırılar devletlerden gelebileceği gibi devlet dışı aktörlerden[13] de gelebilmektedir. Eğer saldırılar devlet dışı bir aktörden geliyorsa, saldırıya uğrayan açısından, karşı vuruş yapabileceği bir hedef bulması çok zor hale gelmektedir. Stratejik siber savaşlarda başka bir önemli nokta saldıran ve saldırıya uğrayan arasında başka bir aktif savaş durumunun yaşanmadığının varsayılmasıdır. Bu varsayım, stratejik ve operasyonel siber savaşlar arasındaki farkı da oluşturmakta; siber savaş destek mahiyetinde kullanılıyorsa stratejik siber savaş kapsamının dışında kalmaktadır.

1.8. Siber Güvenlik ve Caydırıcılık Kavramı

Caydırıcılık kavramı, *"bir tarafın başka bir tarafı bir eylem planından kaçınmaya ikna etmesi için tehditlerin kullanımı"* olarak ifade edilebilir. Tehdidin caydırıcılığı, hedefin üstlenmek zorunda kalacağı maliyetler ve kayıplar sebebiyle hedeflenen eylemi gerçekleştirmeme kararına

[12] Hava savaşının 20. Yüzyılın çoğunda gösterdiği destek işlevine benzer bir işlev göstermektedir (Libicki, 2009:158).

[13] Bu noktada ifade etmek gerekir ki, siber savaşın stratejik olarak kullanımı devlet dışı bir aktör olarak bireyin kapasitesini çokça aşan bir durumdur. Ayrıca siber çatışmaların kinetik çatışmalara yaklaştığı noktada siber çatışmaların stratejik olması büyük bir rol oynamaktadır (Akyeşilmen, 2018:250).

ikna edebildiği ölçüde başarılıdır (Huth, 1999:26). Başka bir tanım ise caydırıcılığın, *"bir tarafın kendine avantaj sağlayacak ancak diğer tarafa zarar verecek şekilde davranmasını engellemekle ilgili olduğunu"* vurgulamış ve caydırıcılığın saldırgan bir aktörün, diğer aktörün savunması tarafından caydırılması yani eyleminin sonuçsuz bırakılması ve bir tarafın, diğer tarafı misilleme korkusundan dolayı kısıtlaması özelliklerine vurgu yapılmıştır (Bendiek ve Metzger, 2015:555).

Bu bilgiler ışığında siber savaşa yönelik caydırma stratejileri de genellikle Soğuk Savaş teorileriyle mukayese edilmesi ekseninde analiz edilmektedir (Lupovici, 2011:51). Bu durumun temel sebebi, siber uzayda savunmanın zor ve maliyetli olması aynı zamanda yanlış anlaşılmanın ve tespite ilişkin netliğin her zaman olamamasından kaynaklanmakta; ayrıca bu eksende incelenme yapılması, nükleer caydırıcılık benzeri siber caydırıcılığın oluşturulması ve uygulanmasının mümkün olup olmadığının belirlenmesinin önemli olmasından kaynaklanmaktadır (Güntay, 2017:91). ABD Dışişleri Eski Bakanı John Kerry tarafından yabancı hackerların, *modern zamanların nükleer silahları* (Smith, 2013) olarak lanse edilmesi ya da 2010 yılında ABD İstihbarat Direktörü Mike McConnel'in Washington Post'a verdiği demeçte belirttiği (Lan ve Xin, 2010:1) *"1950'li yıllara dünyanın geri döndüğü ve o zaman nükleer silahların yayılmasını engellemek için başvurulan yöntemlere şimdi siber tehditleri engellemek için başvurulması gerektiği"* fikri bir bakışı yansıtmakta aynı zamanda siber caydırıcılığın uygulanabilir olup olmadığının da belirlenmesinin önemini ortaya koymaktadır.

Caydırıcılık (nükleer, kriminal/hukuki, siber) birçok farklı biçimde ele alınmaktadır. Bu açıdan formlar tekil, tekrarlı, simetrik ve asimetrik yapıda olabilmektedir. Tablo 4, bu ayrımı ortaya koymakta ve farklı türler arasındaki ilişkiyi yansıtmaktadır. *Nükleer* caydırıcılığın tekil ve simetrik özellik taşıması etkilerinin çok şiddetli olması ve bu sebepten kullanmaya cesaret edilmesi noktasında tereddütlerin bulunmasından ileri gelmektedir. *Kriminal (hukuki)* caydırıcılığın tekrarlı ve asimetrik olması ise, suç işleyenlerin çoğunun tekrar suç işleme niteliği göstermesinden ileri gelmektedir. *Siber* caydırıcılığın tekrarlı özellik göstermesi noktasında ise dikkate değer bir durum vardır. Çünkü uygulanan siber misilleme eylemlerinin hiçbiri bir devleti tamamen ortadan kaldırıcı özellik göstermez, hükümetin değişmesine ya da silahsızlanmaya sebep olmaz. Bir devlet saldırabilir, misillemeyle yüzleşebilir sonra tekrar saldırmak için fırsat kollayabilir. Simetrik özellik taşıması ise benzerler arasında ortaya çıkmasından ileri gelmektedir (Libicki, 2009:30-31).

Tablo 4: Farklı Caydırıcılık Türlerinin Özellikleri

Caydırıcılık	Tekil	Tekrarlı	Simetrik	Asimetrik
Nükleer	X		X	
Kriminal (Hukuki)		X		X
Siber		X	X	

Kaynak: Libicki, 2009:30-31

Siber caydırıcılık, diğer tüm caydırıcılıklara benzer şekilde ve daha önce belirttiğimiz gibi, aktörün saldırgan davranmamaya karar vermesi durumunda başarılı hale gelmektedir. Aktörün bu kararı vermesinde, siber saldırganlık maliyetlerinin faydalarından daha ağır basmasının sağlanması ve siber uzayda kısıtlamanın faydalarının maliyetten daha ağır basmasının sağlanması koşulları etkili olmaktadır. Karar vericilerin bilgi eksikliği ve karar alırken birçok içsel faktörü hesaba katması nedeniyle başarılı bir siber caydırıcılık için düzenli bir caydırıcı mesaj alışverişi şeklinde sürekli diyalog[14] ilk koşul olarak ön plana çıkmaktadır (Goodman, 2010:107-108). Bu noktada karşılaşılan bir zorluk ise siber uzayda faaliyet gösteren aktörlerin çeşitliliği ve fazlalığıdır. Bu çeşitlilik, caydırıcı mesajın kime ve nasıl iletileceğinin net olmadığı bir alan ortaya çıkarmaktadır. Çünkü bazı durumlarda aktörler, yalnızca sanal alemde anonim kalanlar değil, reel dünyada bilinen fiziksel bir adresi bile olmayanlar olabilir (Lupovici, 2011:53).

Başarılı bir siber caydırıcılık için ikinci kilit nokta, aynı zamanda siber caydırıcılığı farklı ve zor kılan noktalardan biri, *kime* karşı caydırıcılık ve misilleme yapılacağının tespit edilmesinin gerekliliği ve zor oluşudur. Bu noktada kim sorusunun cevabı kimlikle ilgili olduğu kadar bağlamla[15] da ilgilidir (Singer ve Friedman, 2014:145-146). Bir siber saldırı esnasında, saldırının kaynağının tespit edilememesi karşı hasara sebebiyet verecek misilleme önlemi alma yeteneğini de kısıtlar. Bu açıdan misilleme tehdidinin gerçekliği hem ulusal hem de uluslararası kamuoyu tarafından sınanır hale gelir (Lupovici, 2011:52). Ayrıca kime karşı caydırıcılık ve misillemede bulunulacağının tespit edilmesinin yanında, devletler caydırıcılık ve misilleme için karşı koyabilecek araçlara ve istekliliğe de sahip olmalıdır. İstekliliğe sahip olması siber caydırıcılığı, konvansiyonel caydırıcılığa yaklaştıran bir unsurdur (Goodman, 2010:109).

Başarılı bir siber caydırıcılık için üçüncü kilit noktayı oluşturan unsur devletlerin kapasiteleriyle yakından ilgilidir. Güçlü bir siber saldırı sonucunda devletlerin karşılık verme kapasitelerinin tamamen devre dışı kalmaması gerekmektedir (Goodman, 2010:109). Ancak siber uzayda bu koşul belirli ihtilaflar barındırmaktadır. Soğuk Savaş caydırıcılığında ikinci vuruş yeteneğine/kapasitesine[16] sahip olmak ve karşı tarafın *hayatta kalabilir* olduğunun bilincinde olmak caydırıcılık sağlamıştır. Çünkü ilk vuruş sonucu karşı tarafın askeri kapasitesini tamamen kaybetmeyeceği ve bu sayede caydırıcılık sağlanacağı düşünülmüştür. Bu açıdan *hayatta kalma* nispeten belirgin olmuştur. Ancak siber çağda, yapılan bir siber saldırı sonucu *hayatta kalan* bir

[14] Soğuk Savaş esnasında, Küba Füze Krizi sonrası ABD ve Sovyetler Birliği liderleri arasında hem kriz hem de kriz dışı anlarda doğrudan haberleşme amacıyla kurulan kırmızı telefon hattına benzer bir kanal oluşturulabilir.

[15] Bağlamla kastedilen şudur ki NATO'nun partneri olan Estonya'ya yönelik saldırıların, Moskova merkezli değil de Tahran merkezli olması Bush yönetimi açısından farklı tepkilerin verilmesi sonucunu doğurabilirdi. (Singer ve Friedman, 2014:146). Bu durum aynı zamanda birinci bölümde bahsedilen sosyal inşacı teorideki kimlik algısıyla da yakından alakalıdır.

[16] İkinci vuruş yeteneği Wohlstetter (1958) tarafından ortaya konmuş, bir ilk vuruş sonucunda gelen saldırıyı karşılama ve hala düşmana yıkıcı bir misilleme yapma yeteneğinin olmasını ifade etmek için kullanılmıştır (Freedman, 1986:753).

karşı gücün nasıl görüneceği belirsiz gözükmektedir (Singer ve Friedman, 2014:147). Bir siber savaş sonucu uygulanacak ikinci vuruş kapasitesinin aracı olarak diplomatik aksiyonların mı yoksa çatışma çözümüne yönelik aksiyonların mı hayata geçirileceği netlik kazandırılması gereken bir husus olarak gözükmektedir (Güntay, 2017:99).

Misilleme aracı olarak kullanılacak yöntemlerin seçiminin zorluğuna dair somut bir örnek, 2015 yılında ABD'de gerçekleşmiş ve Personel Yönetimi Ofisi veri tabanlarından 20 milyondan fazla Amerikan vatandaşının verilerinin çalındığı iddiası üzerine Obama yönetimi Çin'e misilleme yapılması gerektiğini belirlemiştir. ABD'li yetkililerin yaptığı çok sayıda gizli toplantıdan sonra içinde sembolik yaptırımlardan çok daha ciddi aksiyonlara (diplomatik protestolardan ABD'deki bilinen Çin uyruklu ajanların sınır dışı edilmesine kadar) geniş bir yelpaze belirlenmiş ancak misillemenin uygulanmasının iki ülke arasındaki bilgisayar korsanlığı çatışmalarını daha da arttıracağından korku duyulmuştur. Ayrıca Beyaz Saray, yapılacak misillemenin orantılı olması durumunda bile dezavantajlarının, avantajlarından ağır bastığını; Çin'de Amerikan firmalarında iş yapan bireyler üzerinde olumsuz etkileri olacağını deklare etmiştir. Cezai yaptırım uygulanmasından ise ABD istihbaratı tarafından Çin bilgisayar sistemlerine, yaklaşan saldırılar konusunda uyarılarda bulunmak için yerleştirilmiş birçok çipin de açığa çıkması dâhil, istihbarat operasyonları sonucu yerleştirilmiş yazılımların açığa çıkabileceği endişesi sebebiyle sıcak bakılmamıştır (Sanger, 2015).

Sonuç olarak siber casusluk olarak ele alınabilecek bu olay göstermektedir ki pratikte caydırıcılık kuramının siber alana uygulanması belirli sorunları barındırmakta ve geliştirilmesi gereken bir alan olarak görülmektedir. Çünkü Knake ve Clarke (2010:99) tarafından ifade edildiği gibi, caydırıcılık sağlayabilmek için olmazsa olmazlardan biri kilit ağlar için etkili savunma sistemleri geliştirebilmektir. Bunun sağlanamaması halinde nükleer savaşlar açısından güçlü bir set ortaya koyan caydırıcılık kuramı, siber savaşların önüne geçme açısından etkisiz hale gelmektedir.

İKİNCİ BÖLÜM

2. ULUSLARARASI İLİŞKİLERDE KURAMSAL YAKLAŞIMLAR VE SİBER GÜVENLİK

2.1. Realist/Yapısal Realist Teori ve Siber Güvenlik

Siber güvenliğin fiziksel dünyada anlamını bulması ve belirli bir çerçeveye oturtulup incelenebilmesi teoriler aracılığıyla mümkün hale gelmektedir. Bu açıdan Realist/Yapısal Realist teorinin temel argümanlarının 1900'lerin sonunda gelişmeye başlayan bir alan olan siber güvenlik bağlamında tartışılması, teorilerin eksiklik ve güncellenmesi gereken noktalarını ayrıca günümüz şartlarında geçerliliği sorgulanır hale gelen bazı argümanlarını net bir şekilde ortaya koyabilmek açısından önem arz etmektedir. Bu gerekliliği gerçekleştirmek, eksikliği ve benzeşen noktaları ortaya koyabilmek adına bu bölümde önce Realist/Yapısal Realist teorinin entelektüel geçmişi ve temel görüşleri aktarılacak ardından bu teorilerin siber güvenlik alanı içinde kazandığı anlam ve boyut karşılaştırmalı olarak tartışılacaktır.

2.1.1. Realist ve Yapısal Realist Teorinin Temel Görüşleri

Realist teorinin entelektüel geçmişini Antik Çağ'da M.Ö. 417-400 yılları arasında yaşamış olan Thucydides'e ve Sparta ile Atina arasında yirmi sekiz yıl süren savaşın yirmi bir yılını ele aldığı çalışması *Peleponez Savaşı Tarihi*'ne kadar götürmek mümkündür. Ardından, 1462-1527 yılları arasında 16. yüzyıl İtalya'sında yaşamış olan siyaset felsefecisi Niccolo Machiavelli, *Prens* adlı eserini kaleme alarak realist yaklaşımın örneklerini vermeye devam etmiştir. 1588-1679 yılları arasında yaşamış İngiliz siyaset felsefecisi Thomas Hobbes, siyaset alanında kabul edilen ilk teori olan *Leviathan* isimli eseriyle realist teorinin arkasındaki fikir gücünü oluşturmuşlardır. 1780-1831 yılları arasında yaşayan ve Napolyon Savaşlarında görev alan bir Prusyalı general olan Carl von Clausewitz tamamlamaya ömrünün yetmediği ancak daha sonra kendi el yazılarının karısı tarafından yayımlanmasıyla realist okullarda temel bir kaynak olarak kalan *Savaşta* adlı eseriyle teorinin gelişmesine katkı sağlayan bir başka isim olmuştur. Ardından, uluslararası ilişkiler alanında bir klasik olarak kabul edilen ve iki savaş arası dönemi (1919-1939) yansıttığı eseri *Yirmi Yıl Krizi* ile realistlerin entelektüel öncüsü ve İngiliz Okulu'nun atası olarak anılan ve 1892-1982 yılları arasında yaşayan Edward H. Carr ortaya koyduğu görüşlerle realist teorinin serpilmesini sağlamıştır. Realist teorinin entelektüel birikime katkı yapan bir başka isim ise 1904-1980 yılları arasında yaşayan ve en etkili Uluslararası İlişkiler kuramcılarından biri olarak bilinen Hans J. Morgenthau, 1948 yılında yayımladığı *Uluslararasında Politika* adlı kitabıyla politik realizmin temel ilkelerini ortaya koymuştur. Bütüncül bir uluslararası ilişkiler yaklaşımı benimsemesi

sebebiyle birçok yönden örnek teşkil etmiş ve realizmi kurumsallaştırmıştır (Viotti ve Kauppi, 2012: 42-52).

Realizmin tarihi geçmişini şekillendiren isimlerin ve eserlerin ardından temel varsayımları incelendiğinde *devletlerin meşru ve merkezi bir üst otoritenin olmadığı anarşik dünyada temel ve en önemli aktör olarak varsayıldığını görmekteyiz.* Devlet, kendisini aşılamaz ve sert bir kabukla çevrelemeye çalışan bölgesel bir varlıktır. Şirketler (bölgesel, çok uluslu), insan hakları örgütleri, BM, AB ve NATO gibi ulus aşırı organizasyonlar üyelerinden ayrı bir egemenliği ve varlığı olmadığı gerekçesiyle aktör olarak kabul edilmezler. Realistler açısından uluslararası ilişkiler ve uluslararası politika başat aktör olan devletlerarasındaki mücadele süreci olarak nitelenmektedir. Güç, kelime haznesindeki anahtar kavramdır ve ihtilafları çözmenin bir aracı olarak kullanılmaktadır. Bu bağlamda Uluslararası İlişkiler, özellikle dünya politikasını şekillendirdikleri (Soğuk Savaş sırasında ABD ve Sovyet Rusya tarafından tanık olunan) ve en maliyetli savaşlarda (Birinci ve İkinci Dünya Savaşları) yer aldıkları için başta büyük güçler olmak üzere bu birimler arasındaki etkileşimleri inceleme işidir. Ayrıca realistler uluslararası ilişkileri, listenin başında ulusal güvenlik kaygıları olan hiyerarşi sorunları açısından görmektedirler. Realist teori, uluslararası istikrarın başarısını, sürdürülmesini veya bunun nasıl bozulduğunu inceleme eğilimindedir (Arı, 2013:140; Viotti ve Kauppi, 2012:39; Knutsen, 1992:235).

Bunun yanı sıra realistler *devleti üniter bir aktör olarak görürler*. Bu görüş, realistlerin devleti sert bir kabuk ya da mat bir kara kutu ile çevrelenmiş olarak görmelerinden ileri gelmekte ve devlete tek bir birim gözüyle bakılmaktadır. Aslında realist düşünceyle ilişkilendirilen ortak bir varsayım, devlet içindeki siyasi farklılıkların nihayetinde otoriter olarak çözüldüğü ve hükümetin bir bütün olarak devletle ilgili tek bir sesle konuşabileceği yaklaşımıdır. Realistler açısından devlet, herhangi bir zaman diliminde, herhangi bir konuda tek bir politikaya sahip olduğu düşünülen üniter (bütüncül) bir aktördür. İfade edilen görüşün istisnaları olmakla beraber bu istisnalar aslında aktarılan kuralı kanıtlayan ve destekleyen istisnalar olarak ifade edilebilir (Viotti ve Kauppi, 2012:39).

Realistler, ileri bir varsayımda bulunarak devleti rasyonel (amaçlayıcı) bir aktör olarak kabul ederler. Devletler, güvensizlik ve kusurlu bilgi koşulları altında çalışan üniter rasyonel aktörlerdir. Rasyonel bir dış politika karar alma süreci hedeflerin beyan edilmesi, devlete sunulan mevcut imkânlar açısından uygulanabilir tüm alternatiflerin dikkate alınması, bu hedeflere ulaşmanın, incelenen çeşitli alternatifler sayesinde, göreceli olma olasılığı ve bunlara ilişkin her türlü alternatifle birlikte fayda ve maliyetleri içerecektir. Bu rasyonel sürecin ardından devletlerin karar vericileri faydayı maksimize eden (faydayı maksimize etmek ya da maliyeti en aza indirmek) ya da en azından kabul edilebilir bir sonuç ortaya çıkartan olasılığı seçerler. Güç politikalarının mantığı, devlet adamlarının üç şey yapmasını gerektirir: *değişen güç dağılımını gözlemlemek, bu dağılımın oluşturduğu tehditler açısından kendi çıkarlarını ve hayatta kalmasını değerlendirmek* ve *açıklarını*

minimize etmek ve fırsatlarını maksimize etmek ve bunu, kaynakları ve seçeneklerinin sınırları dâhilinde yapmak. Bu şekilde hareket etmeyen karar vericiler hem kendilerinin hem de devletin yok edilmesi ile karşı karşıyadırlar. Aktarılan sebeplerden ötürü rasyonellik bir insan özelliği değil, anarşik bir siyasi sistem içindeki davranışsal olarak tasarlanmış bir aktör niteliği olarak görülmektedir (Viotti ve Kauppi, 2012:40; Buzan, 1996: 54-55).

Realistler, devletin karşı karşıya olduğu sorunlar hiyerarşisi içinde ulusal ya da uluslararası güvenliğin listenin başında olduğunu varsayarlar. Askeri ve bununla bağlantılı siyasi meseleler, dünya siyasetine hükmetmektedir. Bu bakış açısından dolayı Realistler için, devletin varlığının devamını ilgilendiren ulusal güvenlik sorunları önceliklidir ve *yüksek politika* yani güvenlik ve prestijin en üst düzeye çıkarılması, olarak görülürler. Genellikle daha önemsiz görülen ekonomik, sosyal, ticari, mali meseleler ise *düşük politika* yani sağlık ve refahın üst düzeye çıkarılması, olarak nitelendirilebilir (Viotti ve Kauppi, 2012: 40, Morse, 1971:383).

Realizm, tüm biçimlerinde insan koşullarının uluslararası düzeyde sürekliliğini vurgulamaktadır. Realistler, bu sürekliliğin kaynağını, devletlerin politik inşasında yansıtıldığı gibi insan doğasının kalıcılığında bulma eğilimindedirler. Thomas Hobbes'un görüşleri, realizmin insanın doğasına ilişkin görüşlerinin çerçevesinin çizilmesinde önem arz etmektedir. Hobbes, *Leviathan* isimli eserinde insan doğasıyla ilgili üç önemli varsayımda bulunur: *Erkekler eşittir (cinsiyetlendirilmiş dil standart on yedinci yüzyıl kullanımını yansıtmaktadır), anarşik bir ortamda etkileşime girerler* ve *rekabet, çekingenlik ve zafer tarafından harekete geçirilirler.* Bu koşulların birleşimi, *herkesin herkese karşı savaşına* yol açmaktadır (Donnelly, 2005: 32). Hobbes'un da ortaya koyduğu gibi realist düşünürler, insan doğasını olumsuz şekilde ele almaktadırlar. İnsanı ilişkilerinde kötü, çıkarcı, egoist ve hırslı şekilde tasvir etmişlerdir. Bireylerin ilişkilerinde gücü ön plana alması ve güce dayalı bir çıkar benimsemesi gibi devletlerinde peşinde oldukları şey güç ve çıkarlarını en üst noktaya taşımaktır. Devletlerin sürekli güç ve çıkar peşinde koştuğu bir ortamda da savaş ve çatışma olağan hale gelmekte, kapasitesini arttırma istenciyle hareket eden devletler sahip oldukları ölçüsünde rakiplerini hâkimiyetleri altına almak istemektedirler (Arı, 2013:138; Buzan, 1996:50; Shimko, 1992:286;).

Son olarak klasik realizm konusu içinde ifade edilmesi gereken bir diğer konu, realizmin kurumsallaşmasında büyük katkısı olan Hans J. Morgenthau'nun *Politics Among Nations (Uluslararasında Politika)* isimli çalışmasında açıkladığı siyasal gerçekçiliğin altı ilkesidir. Bu ilkelerden birincisi *politikanın, genel mahiyette, toplum gibi kökleri insan doğasında olan objektif yasalarca yönetildiğine inanılmasıdır.* Toplumu geliştirmek için öncelikle toplumun içinde yaşadığı yasaları anlamak gerektiğini ifade eder ve yasaların işleyişinin bizim tercihlerimizden etkilenmediğini vurgular. Ayrıca Morgenthau'ya göre, bir dış politika sorununda kendimizi devlet adamının yerine koymalı, aynı koşullar altında biz olsak ne yapar, hangi alternatifi seçerdik şeklinde sorular sormalıyız. İkincisi, *siyasal gerçeklik olgusunun başlangıç noktasını, güç*

yönünden tanımlanan çıkar kavramı oluşturmaktadır. Morgenthau, devlet adamının da güç olarak tanımlanan çıkar kavramına göre düşündüğünü ve hareket ettiğini; tarihteki olayların bu varsayımın delillerini taşıdığını ifade etmektedir. Üçüncüsü, *Realizm, çıkar kavramının politikanın özü olduğunu ve evrensel olarak geçerli nesnel bir kategori olduğunu varsayar.* Dördüncüsü, *siyasal gerçekçilik, siyasal eylemin ahlaki öneminin farkındadır.* Realizm, devletlerin eylemlerine evrensel ahlak ilkelerinin aynen uygulanamayacağını ve zaman ve mekânın somut koşullarından damıtılmaları gerektiğini ifade eder. Beşincisi, s*iyasal gerçeklik, belli bir devletin eylemlerini evreni yöneten ahlaki yasalarla belirlemeyi reddeder.* Altıncısı, *siyasal gerçekliği diğer düşünce okullarından ayıran şey gerçeğin kendisidir.* Siyasal gerçeklik, entelektüel olarak, tıpkı ekonomist, hukukçu ya da ahlakçıların yaptığı gibi siyasal alanın özerkliğini korur. Güç olarak tanımlanan çıkar kavramı üzerinden incelenirse, belirli bir politika hakkında ekonomist bunun toplum refahı üzerindeki etkisini; hukukçu yasal kurallara uygun olup olmadığını; ahlakçı ise moral ilkelere uygunluğunu sorgular. Siyasal gerçekçi ise bu politikanın devletin gücü üzerindeki etkisini sorarak siyasi eylemleri siyasi kıstaslarla değerlendirir. Yukarıda ifade edilenler realizmin güç, güvenlik, çıkar gibi kavramlara bakış açısını net bir biçimde ortaya koymaktadır (Arı; 2013:153-156; Morgenthau, 1997: 4-13).

Sonuç olarak net bir çıkarım yapmak adına realizmin varsayımlarını üç noktada toplamak istersek ilk olarak ulus devletlerin veya karar vericilerin uluslararası ilişkileri anlamada temel aktörler olduğunu ifade edebiliriz. İkinci olarak ulusal politika konusu ve uluslararası politika konusu arasında keskin bir ayrım vardır ve üçüncü olarak ise uluslararası ilişkilerin güç ve barış mücadelesi olduğunu söyleyebiliriz. Bu mücadelenin nasıl ve neden gerçekleştiğini anlamak ve onu düzenlemenin yollarını önermek disiplinin amacıdır (Vasquez, 2004:37).

2.1.1.1. Klasik Realizmden Yapısal (Neorealizm) Realizme

Çoğu realist, içerdiği görüşlerde *neo* ön ekini hak edecek hiçbir şey olmadığını düşündüğü için neorealizm terimi bir parça tartışmalı bir terim haline gelmiştir. Bununla birlikte çoğu gözlemci bu iddiayla aynı fikirde değildir, realizmde birçok şeyin değiştiğini ve neorealizmin bu değişikliği belirtmenin bir yolu olduğunu ifade eder (Brown ve Ainley, 2005:41). Realist teorinin sorgulanmaya ve eleştirilmeye başlanması 1970'lerin sonuna doğru neorealist teorinin ortaya çıkmasına zemin hazırlamıştır. Kenneth Waltz tarafından 1979 yılında yayımlanan kitabı *Theory of International Politics (Uluslararası Politikanın Teorisi)*, daha önce klasik realist teorilerde önemli bir yer tutan devletlere odaklanma yerine dikkatleri uluslararası çevreye yöneltmiş ve böylece realist teorinin dönüşümünü sağlamıştır. Waltz, değişik siyasal sistemlere ve çelişen ideolojilere rağmen neden devletlerin benzer davranışlar sergilediklerini açıklamaya çalışmıştır. Problemi, neorealizme göre, sistemik kısıtlamaların devletler ve dış politika davranışları arasında yer aldığını varsayarak çözmüştür. Yapı kavramı bu noktada devreye girmektedir. Uluslararası yapı kavramı,

benzer koşullar altındaki devletlerin kendi içsel farklılıklarına rağmen benzer davranışlar geliştirmelerinin sebebini oluşturmaktadır (Glaser, 2017:17; Arı, 2013:157; Linklater, 1995:242).

Uluslararası sistemler âdem-i merkeziyetçi ve anarşik yapıdadır. Ulusal yapılar ve uluslararası yapılar arasındaki çeşitlilikler, sistemlerden her birinin birimlerinin amaçlarını tanımlama ve bu amaçlara ulaşma yöntemlerine dair araçlar geliştirme şekillerine yansımaktadır. Waltz'a göre uluslararası sistemin yapısı, iç siyasal sistemlerin yapısından *sistemin düzen ilkesi, birimlerin karakteri* ve *kabiliyetlerin dağılımı* yönünden ayrılmaktadır. İç siyasal sistemlerde örgütlenme ilkesi hiyerarşi olmasına rağmen uluslararası sistemin işleyiş prensibi açısından ana ilke anarşidir. Hiyerarşik yapıdaki ulusal sistemde birimler farklılaşır, emir ve itaat ilişkileri vardır ve bireyler karmaşık bir sosyal iş bölümü içinde uzmanlaşmakta özgürdürler. Farklılaşmış birimler birbirlerine uzmanlıkları ilerledikçe daha yakından bağımlı hale gelir. Aksine anarşik sistemlerde ast-üst ilişkisi söz konusu değildir, bu noktada temel birimlerin fonksiyonlarında benzerlikler bulunmaktadır. Hiyerarşik düzenler içerisindeki bireyler işlevsel olarak aynı, eşit olmayan yeteneklerle donatılırlar oysa anarşik sistemdeki devletler tamamen aynı işlevleri yerine getirmek (hayatta kalmak) için eşit olmayan yeteneklerle donatılmışlardır (Linklater, 1995:244; Waltz, 1979:88-104).

Waltz'un devletlerin davranışlarına yön verdiğini ileri sürdüğü uluslararası sistemin anarşik olması demek uluslararası sistemi kontrol edecek merkezi bir kontrol mekanizmasının, üst erkin, olmayışı anlamına gelmektedir (Waltz, 1979:88). Devletlerin bu anarşik sistem içerisinde temel motivasyonu varlıklarını devam ettirmeleridir. Devletlerin amacı, diğerlerinin sahip olduğunu almak değil, kendi sahip oldukları mevcutları korumak olduğu için bu motivasyon zararsız bir motivasyon olarak ifade edilebilir (Glaser, 2017:17). Waltz'a göre anarşik bir ortamda kendi başının çaresine bakma (self-help) temel bir eylem prensibi haline gelmektedir. Çünkü diğer devletler potansiyel bir tehdit oluşturmaktadır ve sistemin anarşik yapısı nedeniyle saldırıya uğramaları durumunda bunu tersine çevirecek üst bir otorite de bulunmamaktadır. Burada da güç dengesi devreye girmekte ve statükonun devamlılığını sağlamaktadır. Çünkü devletler, diğer devletlerin güç kazanmadığından emin olmak isterler (Mearsheimer, 2013:80; Waltz, 1979,111).

Son olarak yapısal realistler arasında, devletin ne ölçüde bir gücü kontrol etmeyi hedeflemesi gerektiği konusunda uzlaşmazlık bulunmaktadır. Saldırgan realistler, devletlerin her zaman daha fazla güç elde etmek için fırsatlar aramaları gerektiğini ve mümkün olduğunda bunu yapmaları gerektiğini ifade etmektedir. Saldırgan realistlere göre, devletler mutlaka güçlerini maksimize etmelidir ve nihai hedefleri hegemonya olmalıdır, çünkü devletin hayatta kalmasını garantilemenin tek yolu olarak bunu görmektedirler. Çünkü devletler, birbirlerini gerçek ya da en azından potansiyel olarak düşman gibi gördükleri rekabetçi bir dünyada yaşarlar ve bundan dolayı birbirleri pahasına da olsa güç kazanmaya çalışırlar. Buna karşılık savunmacı realistler ise herhangi bir devletin çok güçlenmesi durumunda dengelemenin gerçekleşeceğini savunurlar. Bir devletin çok

güçlenmesi durumunda diğer büyük güçler ordularını oluşturarak, onlara karşı yükselen devleti dengelemek isteyecek ve hatta onu yok edecek bir koalisyon kuracaklardır (Mearsheimer, 2001:52; 2013:80-81).

2.1.2. Realist ve Yapısal Realist Teorinin Siber Güvenlik ile Tartışılması

Realist ve Yapısal Realist teori açısından anarşik bir uluslararası sistemde devletlerin temel analiz birimi olarak alınmakta ve devlet bütüncül ve yekpare bir aktör olarak görülmektedir (Viotti ve Kauppi, 2012:39). Ancak devlet dışı aktörlerin analiz birimi olarak kabul edilmemesi realist teori ile siber uzay güvenliğini açıklamaya çalışırken eksik kalınan kısımdır. Çünkü siber uzayda gerçekleşen bir siber saldırı ya da savaşta belirli durumlarda savaşan ya da saldırıya uğrayan ülkelere dahi mensup olmayan bireyler internet üzerinden gerçekleşen saldırılara katılabilmekte ve devlet güvenliği ile ilgili endişelere yön verebilmektedir. Gelişmiş devletlerin hala, diğer aktörlere nazaran, daha fazla ekonomik kaynağa sahip olduğu ve teknolojik kaynağı yönetme gücünün bulunduğu inkâr edilemez bir gerçektir. Fakat yeterli bilgi ve donanıma sahip bireyler, şirketler, devlet dışı örgütler geniş çapta saldırılar başlatabilmekte ve devletlerin ulusal güvenlik politikalarını etkileyebilmektedir. Bunun en önemli örneklerinden biri, *Moonlight Maze (Ay Işığı Labirenti)* adı verilen ve bir grup bilgisayar korsanının karmaşık araçlar kullanarak içlerinde National Aeronautics and Space Administration (NASA), Pentagon, özel üniversiteler, araştırma laboratuvarları ve diğer devlet kurumlarının da olduğu geniş bir sisteme yaptığı saldırıdır. Bu saldırı sonucunda yüzlerce gizli doküman, şifre, hassas materyal ve hatta Pentagon'un savaş planlama sistemi ile ilgili bilgileri çalındığı iddia edilmiştir (Adams, 2001:98-99). Bu saldırı göstermektedir ki siber uzay içerisinde devletlerin ve devlet dışı birimlerin yer aldığı yeni bir savaş alanı haline gelmiştir ve siber uzay güvenliğini yalnızca devlet boyutunda incelemek eksiklikleri de beraberinde getirmektedir.

Bunun yanı sıra yapısal realizmin uluslararası sistemde birincil aktör olarak devletlere veya büyük güçlere odaklanma eğilimi siber uzayda kimin büyük güç olduğunun tanımlanmasının zor olması sebebiyle de çelişkiye uğramaktadır. Ekonomik ve askeri olarak zayıf devletler bile kendi siber kapasitelerine sahiptir. Bunun anlamı bu devletlerin siber uzayda zayıf olmadıklarıdır. Fiziksel dünyada bir devletin gücünü doğru bir şekilde ölçmek mümkünken, siber uzayda bu ölçüm net bir şekilde yapılamamaktadır. ABD ekonomik ve askeri olarak güçlü bir devlet olmasına karşın sık sık siber saldırılara maruz kalabilmekte ve zarar görmektedir. Dolayısıyla yapısal realizm, siber uluslararası sistemlerde gücün yapılandırılmasını yeterince açıklayamamaktadır (Isnarti, 2016:157).

Realist teori açısından ele alınan konular arasında yüksek politika ve alçak politika ayrımı yapılmaktadır (Viotti ve Kauppi, 2012: 40, Morse, 1971:383). Yakın bir zamana kadar siber uzay, özellikle uluslararası ilişkiler bağlamında realist teori açısından düşük politika konusu yani ikincil derecede önemli bir konu olarak görülmüştür. Ancak son yıllarda internetin özünü oluşturan siber

alan, yüksek politika alanını oluşturan ulusal güvenlik hususları, hükümetler için kritik olan karar sistemleri ve kritik altyapılar gibi alanları etkileyerek düşük politikadan yüksek politika konumuna gelmiştir. Bu durumun en temel örneklerinden biri kendini kar amacı gütmeyen bir medya kuruluşu olarak lanse eden Wikileaks'in, 2010 yılında yüzbinlerce hassas ABD devlet belgesini yayımlamasıdır. Bu yayımlamanın siber uzaydan yapılması ve devlet güvenliğini tehlikeye sokması aslında siber uzayın ulusal güvenliğin önemli bir parçası olduğunu ve artık düşük politika konusu olarak ele alınmasının tehlikelerini ortaya çıkartmış, devlet karar vericilerini bu yeni gelişen tehdit karşısında önlemler almaya itmiştir (Choucri ve Clark, 2013:21-24).

Realist teorinin varsayımlarının siber uzay boyutunda değerlendirilmesinde eksik kalınan bir başka nokta insan doğasına ilişkin realist teorinin varsayımlarıdır. Daha önce de ifade edildiği gibi, Realist teorinin insan doğasına ilişkin görüşleri olumsuz bir çerçevededir. İnsan doğasına yönelik bu olumsuz görüş siber uzaya da belirli açılardan uymaktadır. Siber uzayda faaliyette bulunan kötü amaçlı bilgisayar korsanlarının varlığı realizmin ortaya attığı insan doğasına yönelik görüşlere belirli açılardan uyuyor gibi gözükse de içinde çelişkiler barındırmaktadır. Çünkü sadece kötü amaçlı kişiler değil; iyi bir amaç uğruna hareket eden ve bilgisini bu yönde kullanan insanlar da siber uzayın paydaşları arasında yer almaktadır (Tarhan, 2017:12). Hatta literatürde bu kişileri tanımlamak için *beyaz şapkalı hacker* tabiri kullanılmaktadır. Beyaz şapkalı hackerlar, siber uzayda suç işleyen kişilerin kullandığı araçlara ve yöntemlere en az onlar kadar hâkim olan ancak bu becerilerini savunma amaçlı kullanan ve bünyesinde bulunduğu kurum/kuruluş için maruz kalınan siber saldırılardan ya hiç ya da en az zararla ayrılmasını sağlayan kişilerdir (Çifci, 2017:265). Bu kişiler firmaların yayımladığı yazılımların açıklarını tespit edip firmalara bildirerek de faaliyet gösterebilmektedir.

Realist teori ve alt alanları için en önemli konulardan biri de anarşi olgusudur. Daha önce açıkladığımız gibi anarşi olgusu, sistemi kontrol eden bir üst erkin olmayışı anlamına gelmektedir (Waltz, 1979:88). Siber uzay için de anarşik nitelendirmesi yapılabilir. Çünkü benzer şekilde siber uzayı da yöneten bir üst erk yoktur. Ancak devletler, ulusal güvenliklerini riske attığı gerekçesiyle belirli internet sitelerine erişim engeli getirebilmekte ve bu yolla bir üst erk tavrı sergileyebilmektedirler. Bunun yanı sıra siber uzayda, devletler güvenlik ikilemi benzeri bir sorunla da karşı karşıya kalmaktadır. Toplumlar ve devletler, bilgi teknolojileriyle alakalı olarak daha güvenilir hale gelmeye çalıştıkça eş zamanlı olarak siber saldırılara karşı da savunmasız hale gelmektedir (Eriksson ve Giacomello, 2006:226). Bu fikrin özünü bir devletin, ulusal sistemlerini internete ne kadar bağımlı hale getirirse muhtemel saldırılardan da o kadar fazla etkilenebilir düşüncesi oluşturmaktadır. Bu durumun en açık örneğini 2007 yılında maruz kaldığı saldırılarda büyük zarara uğrayan Estonya oluşturmaktadır. Estonya'da hem devlet hem özel sektör sistemleri internete büyük oranda bağlıdır ve internet ortamından yoğun bir şekilde faydalanmaktadır. Bu özelliğinden dolayı *e-stonya* şeklinde de nitelendirildiği olmuştur (Çifci, 2017:184). İnternet ortamını bu derece yoğun bir faaliyet alanı olarak kullanması aynı zamanda saldırılardan da yoğun

bir şekilde etkilenmesi sonucunu doğurmuştur. Bu açıdan da realizmin özünde bulunan güvenlik ikilemi kavramıyla benzerlik kurulabilecek şekilde siber uzayda da çok fazla bağımlılık maruz kalınan bir saldırıdan çok fazla etkilenme sonucu doğurmakta ve yansımalarını bulabilmektedir.

Savunmacı ve saldırgan realist teori açısından siber uzay incelendiğinde, saldırgan realistlerin iddia ettiği gibi devletler birbirlerine zarar verme kapasitelerine sahip olduğunda, her bir saldırıya karşı devletin mümkün olduğu kadar güvenli olabilmesi için mümkün olduğunca fazla güce sahip olması görüşü ve bu bağlamda nisbi gücün maksimuma çıkarılması gerektiği ifadesi siber uzay için tam olarak doğru olmamaktadır (Snyder, 2002:151). Siber uzayda meydana gelen bir siber savaşa devletlerin dâhil olması, kinetik bir savaşa dâhil olmaktan daha kolay olabilmektedir. Çünkü siber savaşlar, kinetik savaşlardan daha ucuzdur. Siber savaşa dâhil olan bir devletin tanklar, füzeler, modern savaşçılar gibi araçlara sahip olmasına gerek yoktur. Bu nedenle zayıf bir ekonomisi ve askeri gücü olan bir devlet bile siber savaşlarda varlık gösterebilir. Çünkü yeterli teknik ve bilgi donanımına sahip, bilgisayar kullanabilen ve ağa bağlı herhangi bir kişi siber saldırı başlatabilir. Devletin ekonomik ve askeri gücü ikinci planda kalmaktadır ve siber uzayın bu özelliği sayesinde aktörlerin kimliği de gizli kalabilmektedir. Bu gizlilik siber bir saldırının kaynağı ülke hakkında bilgi vermemekte, nisbi gücünü ölçmeyi zorlaştırmaktadır. Sonuçta askeri ve ekonomik olarak çok gelişmemiş devletler dahi siber bir güç olabilir (Isnarti, 2016:154).

2.2. Liberal/Neoliberal Teori ve Siber Güvenlik

Siber güvenliğin fiziksel dünyada anlamını bulması ve belirli bir çerçeveye oturtulup incelenebilmesi teoriler aracılığıyla mümkün hale gelmektedir. Bu açıdan Liberal/Neoliberal teorinin temel argümanlarının 1900'lerin sonunda gelişmeye başlayan bir alan olan siber güvenlik bağlamında tartışılması, teorilerin eksiklik ve güncellenmesi gereken noktalarını ayrıca günümüz şartlarında geçerliliği sorgulanır hale gelen bazı argümanlarını net bir şekilde ortaya koyabilmek açısından önem arz etmektedir. Bu gerekliliği gerçekleştirmek, eksikliği ve benzeşen noktaları ortaya koyabilmek adına bu bölümde önce Liberal/Neoliberal teorinin entelektüel geçmişi ve temel görüşleri aktarılacak ardından bu teorilerin siber güvenlik alanı içinde kazandığı anlam ve boyut karşılaştırmalı olarak tartışılacaktır.

2.2.1. Liberal ve Neoliberal Teorinin Temel Görüşleri

Liberal teori, geçmişi Aydınlanma Dönemi'nde İngiltere'den John Lock, Almanya'dan Immanuel Kant ve ortaya koyduğu *Ebedi Barış* eserine, İskoçya'dan Adam Smith, Fransa'dan Montesquieu'ye ve ortaya koyduğu *Yasaların Ruhu* eserine kadar uzanabilecek olan uluslararası ilişkiler içindeki en etkili ve büyük teorilerden biridir. Liberal teori, modern sanayi toplumlarının şekli üzerinde derin bir etkiye sahiptir. Eşitlik, özgürlük, rasyonellik, mülkiyet gibi kavramlar klasik liberal düşüncenin sacayaklarını oluşturmaktadır (Arı, 2013:293; Burchill, 2005:55).

Liberal teorinin yaklaşımlarını dört önemli başlık altına inceleyebiliriz. *Maddi ve sosyal malların tüm vatandaşlar arasında eşit dağıtılması anlamına gelmeyen fırsat eşitliği* 19. yüzyıl liberalizminin ilk temel taşını oluşturmaktadır. İkincisi, *insanın doğal ihtiyaçlarını ve isteklerini rasyonel bir şekilde yerine getirebilecek kapasiteye sahip olduğu iyimser bir bakış açısıdır.* İnsan, kendisini çevreleyen fiziksel gerçekliği anlama ve üstesinden gelme becerisine sahiptir. İnsana kendi yaşam planına göre mutluluğu özgürce arama hakkını gerçekleştirme fırsatı verilmelidir. Çünkü insan kendini geliştirme ve kendine güvenme kapasitesine sahiptir. Liberalizmin temel taahhüdü, en iyi toplumun rasyonel bireye en büyük özgürlüğü sağlayan toplum olduğudur. Liberaller için sosyal politikanın uygun amacı, bireyin özgürlüğünü ve özerkliğini en üst düzeye çıkarmaktır. Bireyin özel amaçlarına ulaşma özgürlüğüne olan bu talep, 19. yüzyıl liberalizminin üçüncü köşe taşını oluşturmaktadır. Liberalizmin dördüncü ve son temel taşını *özel mülkiyet* oluşturmaktadır. Özel mülkiyet yoluyla insan özel amaçlar arayabilir ve böylece kişiselliğinin ve mutluluğunun farkına varabilir. Çalışmak kişiyi teşvik eder, bu yolla birey sadece kendini zenginleştirmez aynı zamanda toplumu da zenginleştirir (Knutsen ve Torbjorn, 1992:133-134). Tarihi özelliklerini bu şekilde ortaya koyduğumuz liberal düşüncenin uluslararası ilişkiler temelli yaklaşımlarını da ortaya koymak bu noktada önem taşımaktadır.

Uluslararası ilişkilerde liberal imge, sadece devletleri değil aynı zamanda uluslararası ve hükümet dışı örgütler, sivil toplum örgütleri ve bunları birbirine bağlayan ve çoğu zaman da kesişen ağlardan oluşmaktadır. Beş temel varsayım uluslararası ilişkilerde liberalizmi şekillendirmektedir. Bunlardan birincisi, *devletlerin yanı sıra devlet dışı uluslararası aktörler de dünya siyasetinde önemli varlıklardır.* Belirli konularda uluslararası kuruluşlar kendi başlarına aktör olabilmektedirler. Bunun yanı sıra bazen bireyler; genellikle ise çok uluslu şirketler, çevre güvenliğine dönük çalışan sivil toplum kuruluşları ve insan hakları kuruluşları dünya siyasetine etki edecek derecede önemli rol oynayabilmektedir. Bu tarz farklı paydaşların dünya siyasetini nasıl, ne ölçüde ve hangi koşulların yönlendirmesi altında etkilediğini açıklamak, liberaller için esas mücadeleyi oluşturmaktadır (Viotti ve Kauppi, 2012:129).

Varsayımlardan ikincisi, *birçok liberal hem devletler hem de devlet dışı aktörler arasındaki ekonomik veya diğer karşılıklı bağımlılık ya da birbirine bağlılık biçimlerinin devlet davranışları üzerinde ılımlı etkiye sahip olduğunu ifade etmektedir.* Egemenlik dışı aktörlerin ortaya çıkması ve hızlı bir şekilde genişlemesi ve küresel sivil toplum kavramının oluşmaya başlaması ortak strateji ve hedeflere yönelik ulus ötesi ağların büyümesi sayesinde olmaktadır. Bu büyüme her zaman iyi yüzünü göstermemekte, bazen de terör ve suç örgütleri karanlık yüzlerini gösterebilmekte; devletleri ve halkları çeşitli tehditlerle karşı karşıya bırakabilmektedir. Üçüncü olarak Liberal uluslararası ilişkiler düşüncesi, *uluslararası politikanın gündemini çok çeşitli olarak görmekte ve buna uygun ele almaktadır.* Uluslararası politikanın gündeminin yalnızca askeri güvenlik meseleleri tarafından belirlendiği fikri liberallerce reddedilmektedir. Ayrıca ekonomik sosyal ve çevresel konuların da çok önemli olduğunu belirterek, yüksek ve alçak politika arasındaki ayrımın

da yanlış çizildiğini ifade etmektedirler. Realist teori için alçak politika olarak görülen bu konular, bazen diğer askeri güvenlik meselelerinden daha belirgin güvenlik konuları olarak görülebilirler. Dördüncü varsayım, *anarşi ve yeteneklerin dağılımının devlet davranışına etkisiyle yukardan aşağı bir görüş benimseyen yapısal realistlerin aksine çoğu liberal, devlet-toplum ve birey düzeyinde faktörlerin uluslararası ilişkileri ve sonuçlarını nasıl etkilediğini inceleyen içten dışa bir bakış açısı benimsemiştir.* Demokratik barış teorisi, karar verme süreçleri ya da algı ve küçük grup davranışlarıyla ilgili yapılan çalışmalar bu duruma örnek olarak verilebilir. Son olarak *temel görev, barışın olmadığı koşullarda uluslararası işbirliğinin hangi koşullar altında gerçekleşebileceğini keşfetmek olmaktadır.* Uluslararası kuruluşların rolü, örneğin, bölgesel entegrasyon ve karşılıklı bağımlılık çalışmalarında önemli bir noktadır. Bu açıdan görev, yalnızca tanımlama yapmak değil bunun ötesine geçerek açıklama elde etmek olmaktadır (Viotti ve Kauppi, 2012:130).

Liberal literatürde Rousseau, Kant, Schumpeter ve Doyle'a kadar uzanan ortak bir görüş birliği, savaşların militarist ve demokratik olmayan devletler tarafından kendi çıkarlarını korumak için çıkartıldığı yönündedir. Savaşlar, güçlerini ve servetlerini bölgesel yayılmalarla gerçekleştirme eğiliminde olan bir *savaşçı sınıf* tarafından tasarlanmıştır. Demokratik süreçler ve kurumların varlığı yönetici elitlerin savaş düşüncesini kırabilir ve böylece şiddete eğilim azalabilir. Bu açıdan da liberal demokrasiler çatışmak için bir dayanak bulamaz ve çatışmaya ilgi göstermezler. Bu noktada *demokratik barış teorisi* ortaya çıkmaktadır. Devletlerarasındaki savaşın ortadan kalkma ihtimali, liberal düşünceye göre, liberal-demokratik hükümetlerin yayılması ile mümkün olabilir. Ancak bu düşüncenin varlığı, demokratik devletlerin demokratik olmayan devletlerle savaşmaya daha az eğilimli olduğu anlamına gelmemektedir. Ortadoğu ve Orta Asya'da yaşananlar göz önüne alındığında demokrasilerin otoriter devletlerle savaşmak için hala bir iştahının olduğunu söylemek yanlış olmaz (Burchill, 2005:58-60).

2.2.2. Liberal ve Neoliberal Teorilerin Siber Güvenlik ile Tartışılması

Demokratik devletlerarasında fiziksel dünyada savaşın yaşanmaması gibi siber alanda da birbirlerine saldırmaları nadir görülen bir durumdur. Demokratik devletler tarafından yapılan siber saldırıların çoğu Çin, Rusya ve Irak gibi farklı bir ideolojiye karşı yapılmış ve kinetik savaş stratejisinin bir parçası olarak kullanılmıştır. Bunun yanı sıra demokratik ülkeler arasında siber suç, hacktivizm ve siber casusluk olayları gerçekleşmektedir. Mayıs 2015'te gerçekleşen, bir Avusturalyalının ABD ordusunu ve Microsoft'u hackleyerek helikopter simülasyonu yazılımı ve yeni oyun konsolu ile ilgili bilgileri çalması her ikisi de demokratik olan ülkeler arasında da bu tarz olayların yaşanabildiğini açıkça göstermektedir (Isnarti, 2016:158).

Öte yandan daha önce de ifade edildiği gibi liberaller devletlerin dünya siyasetinde merkezi bir aktör olduğu düşüncesiyle aynı fikirdeler ancak realist düşünürlerin aksine devletlerin hiçbir şekilde uluslararası ilişkilerde önemli roller üstlenen tek aktör olmadığını iddia etmektedirler.

Aslında uluslararası politika alanında son yıllardaki en büyük değişikliklerden biri kayda değer bir sermayeye sahip ulus ötesi şirketler, hükümetleri devirme gücüne haiz sosyal hareketler, karar alıcılar üzerinde etkili olan baskı grupları, geniş bir tabana yayılan siyasi parti ağları, göçmenler ve terörist gruplar olarak sayabileceğimiz yeni aktörlerin ortaya çıkması olmuştur. Bu nedenle liberalizm, siber uzayda yeni çevrim içi grupların ortaya çıkmasına, yeni görsel ve işitsel bilgi iletişim teknoloji türleri aracılığıyla sohbet odalarında ve bloglarda faaliyette bulunanlara farkındalık gösterme potansiyeline sahiptir (Eriksson ve Giacomello, 2006:230).

Farkındalık gösterme potansiyelinin yanı sıra siber alanın hızla büyümesi dünya siyasetinde önemli ve hızla gelişen bir bağlamı yansıtmaktadır. Düşük giriş fiyatı, anonimlik ve kırılganlıktaki asimetriler, daha küçük aktörlerin siber alanda sert ve yumuşak güç kullanma kapasitesine sahip olması dünya siyasetinin geleneksel alanından daha fazla kapasiteye sahip oldukları anlamına gelir. Devletler dünya sahnesinde baskın aktörleri olmaya devam edeceklerdir ama tıpkı liberallerin ileri sürdüğü görüşlerde olduğu gibi sahneyi çok daha kalabalık ve kontrol etmesi zor bulacaklardır. Küresel bilgi çağında devletler için en temel sorunlardan biri en güçlü devletlerin bile kontrolü dışında çok fazla şeyin yaşanmasıdır. Birçok gözlemci tarafından ileri sürüldüğü gibi bilgi devrimi bürokratik hiyerarşileri düzleştirecek ve yerlerini ağ örgütleriyle değiştirecektir. Artan sayıda devlet işlevini özel piyasalar ve kar amacı gütmeyen kuruluşlar üstlenecek ve yerine getirecektir. Devletler, insan yaşamı için çok daha az merkezi olacak, insanlar birden fazla gönüllü sözleşmeyle yaşayacak ve bir fare tıklamasıyla topluluklara girip çıkabileceklerdir (Nye, 2010:1).

İnternetin ortaya çıkışı, yalnızca mevcut devlet dışı örgütler için değil aynı zamanda yeni ortaya çıkan çevrim içi gruplar için de gerçek zamanlı küresel iletişimi mümkün kılmıştır. Bunun açık bir şekilde hem olumlu hem de olumsuz etkileri olabilir. Entegrasyon, iş birliği ve özgürlük kolaylaşırken aynı zamanda terörizm, ulus ötesi suçlar ve devletin istikrarsızlaştırılması da kolaylaşabilir. Bilgi devriminden sonra gelen entegrasyon, karşılıklı bağımlılık ve iş birliğine en açık örnek telekom sektöründe ortaya çıkmıştır. Ordu, sivil telekom ağlarını her zaman bir dereceye kadar kullanmıştır ancak şu anda askeri iletişimin büyük çoğunluğu sivil ağlar aracılığıyla iletilmektedir ve ordu gerçekten de bu ağlara bağımlı hale gelmiştir. Bilgisayar ağları sert askeri gücün gelişimine dahil olmuş ancak eş zamanlı olarak yumuşak gücün dayanak noktasını oluşturmuştur (Eriksson ve Giacomello, 2006:232).

Liberaller, devletin tek başına siber güvenliği sağlayamayacağına inanmakta ve siber güvenliğin sağlanabilmesi için uluslararası devlet/özel sektör iş birliğinin varlığını gerekli görmektedirler. Ancak bunun yanı sıra bugüne kadar siber güvenlik, siber saldırı veya siber savaş konusunda çok taraflı ve kapsamlı bir uzlaşı ya da işbirliğinin olmaması ve bu çabaların genellikle NATO, AB gibi uluslarüstü örgütler nezdinde yürümesi bir eksikliği ortaya koyuyor gibi gözükmektedir. Çünkü liberaller de, yapısalcı realistler gibi uluslararası işbirliğinin önünde bazı engellerin olduğunu kabul ediyorlar. Bir devletin, başka bir devletin yetenekleri ve niyetleri

hakkındaki bilgisinin eksik olması ve bunun sonucu olarak imzacısı olunan bir uluslararası anlaşmaya rağmen diğer devletin hile yapacağını düşünmesi işbirliğine engel olan nedenlerden biri olarak gösterilebilir. Uluslararası işbirliği konusundaki liberal iyimserliğe rağmen uluslararası kurumların ve yapılan anlaşmaların siber güvenlik ve siber savaşla etkin bir şekilde ilgilenip ilgilenmeyeceğinden emin olamamaktayız. Ayrıca liberalizmin eksik kaldığı bir başka nokta ise, liberal normların ve kurumların bu alanda nasıl etkili bir şekilde çalışacağı hakkında yeterli bilgi ve tartışma sunmaması olarak gösterilebilir (Isnarti, 2016:158-159).

Son olarak, siber uzayın gelişmesiyle beraber neoliberal teoride de belirgin güncellemeler olmuştur. Joseph S. Nye'ın yumuşak güç tanımlamasının yanında siber güç de kavram olarak tanımlanmış ve kullanılmaya başlamıştır. Nye tarafından *"baskı ya da ödeme yapma yerine çekiciliğin kullanılması"* olarak ifade edilen yumuşak güç, bir ülkenin kültürünün, siyasi ideallerinin ve vaadettiği politikalarının çekiciliğinden ortaya çıkmaktadır (Nye, 2004:x). Siber güç ise *"diğer operasyonel ortamlardaki ve güç araçlarındaki avantajları oluşturmak ve olayları etkilemek için siber uzayı kullanma yeteneği"* şeklinde tanımlanmıştır. Siber güç, tercih edilen sonuçları üretmek için hem siber uzay içinde hem de siber uzay dışında kullanılabilmektedir (Nye, 2010:4). Bu şekilde liberal ve neoliberal teori siber uzay güvenliğine yönelik açıklamalar getirmeye çalışmıştır.

2.3. Sosyal İnşacı Teori ve Siber Güvenlik

Siber güvenliğin fiziksel dünyada anlamını bulması ve belirli bir çerçeveye oturtulup incelenebilmesi teoriler aracılığıyla mümkün hale gelmektedir. Bu açıdan Sosyal İnşacı teorinin temel argümanlarının 1900'lerin sonunda gelişmeye başlayan bir alan olan siber güvenlik bağlamında tartışılması, teorilerin eksiklik ve güncellenmesi gereken noktalarını ayrıca günümüz şartlarında geçerliliği sorgulanır hale gelen bazı argümanlarını net bir şekilde ortaya koyabilmek açısından önem arz etmektedir. Bu gerekliliği gerçekleştirmek, eksikliği ve benzeşen noktaları ortaya koyabilmek adına bu bölümde önce Sosyal İnşacı teorinin entelektüel geçmişi ve temel görüşleri aktarılacak ardından bu teorilerin siber güvenlik alanı içinde kazandığı anlam ve boyut karşılaştırmalı olarak tartışılacaktır.

2.3.1. Sosyal İnşacı Teorinin Temel Görüşleri

Bazı yazarlar tarafından bir uluslararası politika teorisi olarak görülmeyen İnşacılık, 1980'lerin başında realizmin ve liberalizmin inşacı bir eleştirisi olarak başlamış çarpıcı bir şekilde güçlü bir araştırma programına ve çeşitli yaklaşımlarla sürdürülen deneysel araştırmalarda önemli bir güç haline gelmiştir. İnşacılık, uluslararası ilişkiler içerisinde bir orta yol ya da köprü olarak konumlandırılabilir. Bu açıdan her türlü sosyal ilişkileri incelemenin bir yolu olarak ifade edilebilir. Uluslararası ilişkiler disiplini içerisinde inşacılık terimini ilk kez kullanan Nicholas Onuf olmuştur.

Ardından gelen Friedrich Kratochwil ve Alexander Wendt ise terime atıfta bulunarak gelişmesinde büyük katkı yapmışlardır. 1989 yılında yayımlanan *World of Our Making: Rules and Rule in Social Theory and International Relations* isimli eseriyle Onuf, inşacı düşünceyi ortaya koymuş ardından gelen Wendt ise 1992 yılında yayımladığı *Anarchy is What States Make of it: the social construction of power politics* isimli eseriyle inşacılığın uluslarası ilişkiler içerisinde önem atfedilen bir teori olmasını mümkün kılmıştır. İnşacılık, insanların ne yaptığı, neden toplumların farklı olduğu yada dünyanın nasıl değiştiği hakkında genel açıklamalar önermez bunun yerine ilgisiz görülen meseleler hakkında teorileştirmeyi mümkün kılar. İnşacı düşüncenin temelinde insanoğlunun sosyal varlıklar olduğu ve sosyal ilişkilerimiz olmadan bizi insan yapan şeyin eksik olduğu düşüncesi yatmaktadır. Diğer bir ifadeyle sosyal ilişkiler insanları oldukları kişi haline getirir ya da inşa eder. İnşacı düşünce, insanların toplumu şekillendirdiğini; toplumun da insanları şekillendirdiği ve bunun iki yönlü bir süreç olduğu düşüncesini ileri sürmektedir. İnsanların ve toplumların birbirini inşa sürecini karşılıklı olarak ve sürekli yapan şey ise sosyal kurallardır. İnsanlara ne yapmaları gerektiğini söyleyen ifadeler olan kuralları insanların mutlaka bilmesi gerekmez. Çünkü bir kuralın ne anlama geldiği bilinmiyorsa bile insanların pratikteki davranışlarına bakarak çıkarsama yapmak mümkündür. Ayrıca kurallar bir toplumdaki aktif katılımcıların kim olduğuna dair bilgi de vermektedir. İnsanın sosyal bir varlık olmasını sağlayan çevresiyle ve doğayla etkileşim içinde olmasıdır. Aynı zamanda sosyal inşacılar, uluslararası ilişkilerde aktörlerin yaptıkları şeylerin, sahip oldukları çıkarların ve faaliyet gösterdikleri yapıların objektif veya maddi şartlardan ziyade sosyal normlar ve fikirler tarafından tanımlandığını ileri sürmektedirler (Viotti ve Kauppi, 2012:278; Zehfuss, 2004: 10-11; Barkin, 2003:326; Wendt, 1999:193; Onuf, 1998: 58-59).

Sosyal inşacılığın ontolojik önermelerini üç genel başlık altında toplamak mümkündür. Birincisi, *yapıların sosyal ve politik aktörlerin -bunlar birey ve devlet olabilir- davranışlarını şekillendirdiği ve normatif veya fikirsel yapıların maddi yapılar kadar önemli olduğu* varsayımıdır. Bu varsayım, fikirlerin ayrıcalıklı bir konumda bulunması ve temel alınması gerektiğinin ifadesini yanıstmaktadır. Wendt, sosyal yapıların üç unsurunu ileri sürmüştür. İlki *paylaşılan bilgidir*. Sosyal yapılar kısmen paylaşılan anlayışlar, beklentiler veya bilgi ile tanımlanabilir. Bunlar ister çatışma ister işbirliği halinde olsun aktörleri ve ilişkilerinin doğasını oluşturmaktadır. Örneğin güvenlik ikilemi devletlerin güvensizlik içinde oldukları ve birbirlerinin niyetleri hakkında en kötüsünü varsaydıkları ve bunun sonucu olarak kendi kendine yardım (self-help) düşüncesiyle hareket ettikleri ve bu anlayış toplamından oluşan sosyal bir yapıdır. Ancak güvenlik toplulukları ise devletlerin anlaşmazlıkları savaşsız çözdükleri ve birbirine güvendikleri ortak bilgilerden oluşan farklı bir sosyal yapıyı oluşturmaktadır. İkinci sırada silahlar yada ekonomik varlıkların dahil olduğu *maddi kaynaklar* yer alır. İnşacılar maddi kaynakların paylaşılan bilginin yapısı yoluyla anlam kazandığını iddia etmektedirler. Yani örneğin ABD için müttefiklik ilişkisi içinde olduğu İngiltere'nin sahip olduğu beş nükleer silah başlığı, Kuzey Kore'nin sahip olduğu bir nükleer silah başlığından daha az tehlikeli gözükmekte çünkü ABD'nin bu iki ülkeye dış politika açısından

bakışı farklılık oluşturmaktadır. Son olarak sosyal yapılar yalnızca aktörlerin düşüncelerinde yada maddi yapılarda değil *uygulamalarda* da bulunmaktadır. Yani sosyal yapı sadece süreç içerisinde vardır. Örneğin Soğuk Savaş, kırk yıldan fazla bir süre boyunca büyük güç ilişkilerine yön veren ortak bir bilgi yapısı olmuş ancak aktörler bir kez bu temelde hareket etmeyi bırakmışlar ve sona ermiştir (Agius, 2017:88; Reus-Smit, 2005: 196; Wendt, 1995: 73-74).

Ayrıca sosyal inşacılar, maddi gerçekliğin (bilgisayarlar ve kabloları gibi) yanı sıra sosyal gerçekliğin (kimlik, çıkar, norm gibi) olduğunu ve ikisini birbirinden ayırt etmenin anlamlı olduğunu savunurlar. Yani sosyal gerçeklik, maddi gerçeklikten farklı olarak, sosyal olarak inşa edilir ve her zaman değişime açık bir özellik taşımaktadır. Bu nedenle çıkarlar ve kimlikler gibi sosyal gerçekliklerin hiçbir zaman durağan olarak görülemeyeceğini ifade ederler. Sosyal inşacılığın ikinci ontolojik önermesi *kimliklerin çıkarları ve dolayısıyla eylemleri oluşturmasından dolayı maddi olmayan yapıların aktörlerin kimliklerini nasıl şartlandırdığının anlaşılmasının önemli olduğunu savunurlar.* İnşacı düşünce mensupları, aktörlerin çıkarlarını geliştirme yöntemlerini anlayabilmenin çok çeşitli uluslararası politik olguyu açıklamak için çok önemli olduğunu savunmaktadırlar. Çıkar oluşumunu anlamak için de bireylerin yada devletlerin sosyal kimlikleri üzerine yoğunlaşmaktadırlar. Bu yüzden çıkarların temeli olarak kimliği görürler ve sosyal bağlamdan bağımsız olarak yanlarında taşıdıkları çıkar portföyü olmadığını ileri sürerler. Aktörler bunun yerine durumları tanımlama sürecinde çıkarlarını tanımlarlar. Sosyal inşacılığın üçüncü normatif önermesi *yapı ve bu yapıyı yapanların karşılıklı olarak oluşturulduğu* fikridir. Aktörlerin kimliklerini ve çıkarlarını normatif ve fikirsel yapılar iyi bir şekilde oluşturur. Ancak daha önce bahsettiğimiz gibi aktörlerin uygulamaları olmasaydı bu yapıların da mevcut olamayacağını ileri sürerler (Eriksson ve Giacomello, 2006:233; Reus-Smit, 2005:197; Wendt, 1992:398).

2.3.2. Sosyal İnşacı Teorinin Siber Güvenlik ile Tartışılması

İnşacı bir bakış açısı ile siber güvenliği ve dolayısıyla güvenliği tehdit eden siber savaşı anlamak için siber savaşın sosyal olarak nasıl inşa edildiğini anlamak gerekmektedir. Teknolojideki hızlı gelişmeler siber alanın da genişlemesine yol açmış böylece siber alan hem birey hem de devlet güvenliğini tehdit eder hale gelmiştir. Dahası, siber savaş ve siber uzay güvenlik kavramını genişletmiştir. Siber uzay güvenliği, inşacı teori bakış açısıyla analiz edilirken dikkat edilmesi gereken ilk nokta üzerinde önemle durulan kimliğin oluşumudur. Siber savaşlarda düşman olarak tanımlanan unsurlar genellikle siber saldırganlardır. Fakat saldırı bir düşmandan değil de benzer kimliğe sahip bir aktörden geldiğinde siber casusluk olarak isimlendirilmekte ve farklı bir kimlik atfedilmektedir. Bunun yanı sıra kimliklerin ve çıkarların yanlış algılanışı tıpkı fiziksel dünyada olduğu gibi siber dünyada da savaşların nedeni olabilmektedir. Devletlerin birbiriyle konuşacak, normlarını paylaşacak ve farklı kimliklere saygı duyacak olması siber savaşların gerçekleşme ihtimalini de azaltabilmektedir (Isnarti, 2016:161). Benzer şekilde siber uzayda faaliyet gösteren

devlet dışı örgütler, sivil toplum kuruluşları gibi farklı oluşumların da birbirlerini konumlandırdıkları noktalar önem taşımaktadır. 2015 yılında meydana gelen ve Anonymous isimli hacker grubunun üstlendiği Türkiye'deki *.tr* uzantılı web sitelerine yapılan saldırıda hacker grubu Türk devletinin Irak ve Şam İslam Devleti (IŞİD) terör örgütüne sözde destek verdiğini ileri sürmüştür. Herhangi bir belge ya da somut kanıta dayanmayan bu iddialar atfedilen kimlik algısını yansıtmaktadır. Hacker grubu, Türk devletine bir anlam yüklemiş ve bu anlam da tıpkı inşacıların ifade ettiği gibi onların davranışlarını yönlendirmiştir (Anonymous Türkiye'ye Savaş Açtı (2015), https://www.cnnturk.com/dunya/anonymous-turkiyeye-savas-acti).

Kimlik olgusunun yanı sıra dilin, siber uzay güvenliğine etkisini gösterme noktasında inşacı analiz yol gösterici olabilir. Siber güvenliğin soyut ve teknik olarak karmaşık dünyası gerçek ya da çevrimdışı dünyada tanıdık olan şeylerle analojiler kurarak anlamlı hale getirilebilir. Gerçek dünyada var olan bal petekleri, böcekler, solucanlar, virüsler benzetme yoluyla siber uzayda da kullanılabilmektedir. Virüsler nasıl insan vücuduna girdiğinde insanları hasta ediyorsa bilgisayar sistemine girdiklerinde de sistemin işleyişinde aksaklıklara neden olabilmekte hatta devre dışı bırakabilmektedir. Bu yüzden fiziksel dünya ve siber dünya arasında benzetme yoluyla bir tanımlama yapılmıştır. Sık sık *bilgi savaşı* ya da *elektronik Pearl Harbour* kavramlarının kullanılması içeriğinde özel bir anlam da taşımaktadır. Bu özel anlam doğası gereği dijital olan, bununla birlikte, geleneksel savaşla karşılaştırılan fiziksel sonuçlara sahip olunduğunu ifade etmektedir. İnşacı analiz, bu tür söylemlerin önemini ortaya koyarak katkıda bulunabilir. Siber uzay güvenliği üzerine inşacı analizin bir diğer katkısı, siyasi söylem ve kamuoyunu manipüle etmek için sembollerin kötüye kullanılması olarak tanımlanan ve en bilinen kullanımı Murray Edelman'ın çalışmalarında özünü bulan *sembolik politika* kavramına dayanmaktadır. Sembolik politikanın kayda değer bir uygulaması düşmanın bayrağının yakılmasından daha az düşmanca ancak yine de buna benzer olan web sitelerinin ara yüzlerinin değiştirilmesidir (Eriksson ve Giacomello, 2006:235).

2017 yılında isimleri *Cyber-Warrior Akıncılar* olan bir grup Türk hacker, Balfour Deklarasyonu'nun 100. yılı dolayısıyla *Times of Israel* haber ajansının web sitesine saldırı düzenlemiştir. Şekil 4 bu saldırı sonucu değiştirilen ara yüzü göstermektedir. Times of Israel sitesinin ara yüzüne Türk bayrağı ve kendi amblemlerini koyan grup bu yolla sembolik politikanın bir örneğini gerçekleştirmiş ve yayımladıkları metin ile düşman olarak gördükleri gruba karşı düşüncelerini ifade etmiştir. Ayrıca bu yolla karşıt grubu psikolojik olarak etkileme amacı gütmüşlerdir. Sosyal inşacı teorinin siber uzay güvenliğine yönelik görüşleri bu şekilde ortaya konulabilir.

Şekil 4: Times of Israel Sitesinin Ara Yüzüne Yerleştirilen Görüntü

Kaynak: (Türk Hackerlardan İsrail'e Siber Saldırı (02.11.2017), https://www.aa.com.tr/tr/dunya/turk-hackerlardan-israile-siber-saldiri/955178)

2.4. Güvenlikleştirme ve Siber Güvenlik

Siber güvenliğin fiziksel dünyada anlamını bulması ve belirli bir çerçeveye oturtulup incelenebilmesi teoriler aracılığıyla mümkün hale gelmektedir. Bu açıdan Güvenlikleştirmenin temel argümanlarının 1900'lerin sonunda gelişmeye başlayan bir alan olan siber güvenlik bağlamında tartışılması, teorilerin eksiklik ve güncellenmesi gereken noktalarını ayrıca günümüz şartlarında geçerliliği sorgulanır hale gelen bazı argümanlarını net bir şekilde ortaya koyabilmek açısından önem arz etmektedir. Bu gerekliliği gerçekleştirmek, eksikliği ve benzeşen noktaları ortaya koyabilmek adına bu bölümde önce Güvenlikleştirmenin entelektüel geçmişi ve temel görüşleri aktarılacak ardından bu teorilerin siber güvenlik alanı içinde kazandığı anlam ve boyut karşılaştırmalı olarak tartışılacaktır.

2.4.1. Güvenlikleştirmenin Temel Tartışması

Önde gelen yazıları Barry Buzan, Ole Waever, Jaap de Wilde gibi yazarlarca ortaya konan ve Kopenhag merkezli Çatışma ve Barış Araştırmaları Enstitüsü'nde (COPRI) ortaya çıkan Kopenhag Okulu ekolü geliştirmiş olduğu güvenlikleştirme ve güvenlik dışılaştırma düşünceleriyle güvenlik üzerine yeni bir bakış açısı getirmeye çalışmıştır. Askeri güvenlik sektörü dışında dört farklı sektör daha belirlemiş olması Kopenhag Okulu'nun ortaya koyduğu en dikkat çekici yeniliklerden biri

olarak ifade edilebilir. Beş genel güvenlik sektörü askeri güvenlik sektörü yanı sıra *çevresel, ekonomik, toplumsal* ve *siyasi* güvenlik alanlarından oluşmaktadır (Emmers, 2017:131-132). Sektörler, belli etkileşim türlerini tanımlarlar. Bu açıdan askeri sektör baskı ile ilişkilendirilirken, siyasi sektör ise otorite ve tanınma ile ilişkili hale getirilmiştir. Çevresel sektör insan ilişkileri ve gezegenin biyosferi ile ilişkilendirilirken toplumsal sektör ise kolektif kimlikle ilişkilendirilmiştir. Son olarak ekonomik sektör ise ticaret, üretim ve finans ile ilişkilendirilmiştir (Buzan vd., 1998:7).

Güvenlikleştirme yaklaşımının temelleri 1995 yılında Ole Waever tarafından yayımlanan *Securitization and Desecuritization* isimli makalede ortaya konulmuş bu süreçten sonra 1998 yılında Barry Buzan, Ole Waever ve Jaap de Wilde gibi önde gelen Kopenhag Okulu temsilcileri tarafından yayımlanan *Security: A New Framework for Analysis* isimli çalışmada geniş bir çerçevede incelenerek güvenlik çalışmaları altında yerini almıştır. Güvenlik, siyaseti oyunun bilinen kurallarının ötesine taşıyan ve konuyu özel bir tür politika olarak ya da politika üstü şeklinde çerçeveleyen bir harekettir. Siyasallaşmanın daha ileri bir versiyonunu ise güvenlikleştirme oluşturmaktadır. Teoride, herhangi bir sorun siyasal alanın konusu dışından (nonpoliticized); siyasal alana doğru (politicized) oradan da güvenlik (securitized) alanının konusu olmaya doğru geniş bir tayfta yer alabilir. Devletin bu sorunla ilgilenmemesi ve kamusal tartışmalarda yer almaması sorunun siyasal alanın dışında olduğunun göstergesidir. Sorun, toplumsal tartışmanın bir parçası olup, devletin karar vermesini ve kaynak tahsisini hatta daha nadir şekilde toplumsal yönetişim biçimini gerektiriyorsa siyasi alanın dışından siyasi alanın merkezine kaydığını söylemek mümkündür. Son olarak eğer sorun acil durum önlemleri gerektiriyor ve siyasi işlemlerin normal sınırları dışındaki eylemler haklı gösterilmeye çalışılıyorsa siyasi alandan güvenlikleştirme alanına doğru kaydığı söylenebilir. Güvenlikleştirme, bir konunun devletin güvenlik gündemine sokulması sonrası o konuya karar alıcıların öncelik vermesi gerekliliği doğurduğu için önemlidir (Buzan vd., 1998:23-24; Booth, 1997:111).

Siyasi alanın dışından siyasa alana ve oradan da güvenlik alanına uzanan tayfta güvenlik ile ilgili konuların yerleşimi mevcut şartlarla uyumlu bir şekilde yapılmakta ve belirli koşullar altında herhangi bir konu belirli bir aşamada sonlanabilmektedir. Daha net ifade edersek, İran, Suudi Arabistan gibi bazı devletler dini konuları politikleştirmeyi tercih ederken; Hollanda, Belçika gibi bazı devletler ise bunu tercih etmeyeceklerdir. Tercih eden devletler bu konuları güvenlik kısmına dâhil ederken tercih etmeyenler ise siyaset dışı bırakacak böylece farklı ülkelerde aynı konular tayfın farklı bir ucunda kalacaktır. Sorunların siyasi alanın sınırları içerisinde politikleşmeden kalması yani güvenlik alanına yükselmemesi ideal olduğu düşünülen durumdur. Ayrıca belirli bir süre sonra karar alıcılar sorunlara dikkat çekmeyi bırakırsa sorun tayfın siyasi alanın konusu dışında olan bölümüne doğru kayar ve depolitize hale gelir (Miş, 2011: 349; Buzan vd., 1998:24).

Başarılı bir güvenlikleştirme eyleminin belirli anahtar kavramları bulunmaktadır. Bu kavramlardan birincisini, varlığına yönelik bir tehdit olduğu varsayılan ve hayatta kalma talebinde

bulunan *referans nesnesi* oluşturmaktadır. Devlet egemenliği ve ulusal kimliğin tehdit altında olduğu iddiası için, çoğu zaman, güçlü bir hamle gerekli görülmektedir. Mikro, makro ve orta düzeyde incelenen referans nesneleri, güvenlikleştirme için büyük önem taşımaktadır. Mikro düzey bireyler, küçük gruplar gibi girdilerden oluşmaktadır. Ancak mikro düzeydeki aktörlerin meseleleri güvenlikleştirebilecek meşruiyete sahip olmaları çok ender görülmektedir. Küresel barış ya da tüm insanlık gibi konular makro düzeyde referans nesnesi olabilecek konulardır. Ancak makro düzeyde de başarılı bir güvenlikleştirme yapmak zor gözükmektedir. Güvenlikleştirmenin daha kolay yapılabildiği orta düzey ise referans nesnelerinin en verimlilerinin bulunduğu alandır. İkincisini, referans nesnesinin varlığına yönelik bir tehdit olduğunu ileri süren *güvenlikleştirici aktörler* oluşturmaktadır. Güvenlikleştirici aktör ve referans nesnesi arasındaki ayrım daima net bir şekilde ortaya koyulmamıştır. Genellikle devlet hem referans nesnesi hem de güvenlikleştirici aktör olarak görülebilmektedir. Ayrım, daha geniş bir güvenlik konseptinde açıkça gerekli hale gelmektedir. En zor ayrımın referans nesnesi ve güvenlikleştirici aktörler arasında olması bu ayrımın biraz tartışılmasını da beraberinde getirmektedir. Söz edimi yoluyla güvenlikleştirmeyi gerçekleştiren aktörler (kişi, grup ya da elitler) güvenlikleştirici aktör kategorisi içinde sayılmaktadır. Ayrımın tartışmalı olması sebebiyle güvenlikleştirmeyi gerçekleştiren doğru aktörün seçimi araştırmacıya kalmaktadır. Üçüncü sırada başarılı bir güvenlikleştirme eylemi için ikna edilmeleri elzem olan *hedef/alımlayıcı kitle* gelmektedir. Her ne kadar nüfusun tamamı ya da vatandaşlar hedef kitle olarak düşünülse de aslında siyasi sistem ve konunun niteliğine göre bu durum değişebilmektedir. Son olarak güvenlikleştirme sürecine doğrudan dâhil olmayan bunun yanında sektörün dinamiklerini derinden etkileme kapasitesine sahip olan ve sektörde merkezi konumda bulunan *işlevsel aktörler* gelmektedir. Referans nesnesi ya da referans nesnesi adına güvenlik çağrısı yapan aktör olmayan işlevsel aktörler, güvenlik alanındaki kararları önemli ölçüde etkileyebilmektedir (Baysal ve Lüleci, 2011:77-81; Waever, 2003:11-12; Buzan vd., 1998:35-36).

Anahtar kavramların ardından güvenlikleştirme sürecinin analizinde dikkat edilmesi gereken noktalardan biri, güvenlikleştirici aktörün bir konuyu referans nesnesinin varlığına yönelik tehdit olarak kurgulamasının ve bununla alakalı olağanüstü önlemler talep etmesinin doğrudan bir güvenlikleştirme eylemi yaratmadığıdır. Eğer hedef/alımlayıcı kitle söz edimi (speech act) aracılığıyla bunu böyle kabul ederse, yani ikna edilirse, başarılı bir güvenlikleştirmeden söz edilebilir. Aksi durumda başarılı bir güvenlikleştirmeden değil; bir güvenlikleştirme hamlesinden söz edilebilir. Çünkü güvenlikleştirici aktörün, referans nesnesinin varlığına yönelik tehdide karşılık alacağı olağanüstü önlemleri hedef/alımlayıcı kitleye kabul ettirmesi bu önlemleri alabilmesi için hayati önem arz etmektedir. O halde başarılı bir güvenlikleştirme eyleminin olmazsa olmazı, hedef/alımlayıcı kitlenin tehdit konusunda ikna edilmesini sağlayan başarılı konuşma eylemi (söylemsel boyut) ve bunun yanı sıra güvenlikleştirici aktörün tanımladığı tehdide karşı ivedi tedbirler alması (söylemsel olmayan boyut) aşamalarını içermektedir (Emmers, 2017:136; Buzan vd., 1998:25).

Güvenlikleştirme eylemi içerisinde güvenlikleştirici aktörler, hedef/alımlayıcı kitleyi konuşma eylemi yoluyla referans nesnesinin varlığına yönelik bir tehdit konusunda ikna etse bile bazı durumlarda olağanüstü önlemler almayı tercih etmeyebilirler. Yani güvenlikleştirici aktörler, siyasi süreçler içinde bir çözüm bulma amacı da taşıyabilirler. Ancak şunu da belirtmek gerekir ki varoluşsal tehdide yönelik siyasi süreçler içerisinde çözüm bulma kararı, sorunun daha az tehdit edici olduğu anlamına gelmemektedir. Sorun hala bir güvenlik sorunudur. Çünkü aktör tarafından ileri sürülen tehdit, hedef/alımlayıcı kitle tarafından kabul edilmiştir. Ayrıca daha önce de bahsettiğimiz gibi bir şeyin güvenlik sorunu olup olmadığını belirleyen şey aktör ve hedef/alımlayıcı kitle arasındaki bu etkileşimdir. Burada ifade edilen sadece, karar alıcının siyasal sistem yoluyla bir çözüm bulmayı tercih etmiş olabileceğidir. Siyasal sistem yoluyla bir çözüm bulunduğunda bir acil durum önlemi kabul etmek verimsiz hale gelecektir (Collins, 2005:572-573).

Aktarılanlar ışığında başarılı bir güvenlikleştirme eylemi için üç aşamalı bir sürecin varlığından söz edilebilir (Akgül-Açıkmeşe, 2011:61):

Birinci aşama: Bir meselenin varlığa yönelik yaşamsal bir tehdit olarak addedilmesi gerekir. Bir meselenin güvenlik sorunu haline gelmesi, elitlerin meseleyi güvenlik sorunu olarak sunmalarıyla ilgilidir. Meselenin içeriğiyle ilgili bir kısıtlama bulunmamakta, değişken yelpazedeki birçok sorun güvenlik sorunu olarak ilan edilebilmektedir.

İkinci aşama: Karar alıcılar ve diğer aktörler tarafından sunulan ve tehlike arz ettiği ileri sürülen tehdit için olağan siyasi süreçler dışına çıkılarak olağandışı önlemler alınması gerektiği ileri sürülmelidir. Yaşamsal tehdidin belirlenmesi alınacak olağandışı önlemlere meşruiyet kazandırma noktasında işe yaramaktadır. Meşruiyetin sağlanmasıyla beraber yaşamsal tehditle mücadele etmek amacıyla askerlik ya da vergi gibi özel ve olağanüstü çeşitli yetkiler kullanılabilir hale gelecektir.

Üçüncü aşama: Hedef/alımlayıcı kitlenin ikna edilmesinden oluşmaktadır. Bu kitle, yaşamsal tehditle mücadele amacıyla ortaya konan olağanüstü tedbirleri kabul etmelidir. Başka bir ifadeyle elitler, yaşamsal tehdidi -söz edimi yoluyla- olağanüstü tedbirlerin alınmasının gerekliliği noktasında ilgili kitleyi ikna etmek için ileri sürecektir ve kitle de yaşamsal tehdidin doğasına ilişkin ileri sürülenlere ikna olacaktır. İkna edilememesi durumunda daha önce de ifade edildiği gibi başarılı bir güvenlikleştirme hareketinden söz edilememektedir.

Başarılı güvenlikleştirme sürecinin yanı sıra güvenlikleştirme süreçleri, tıpkı İkinci Dünya Savaşı sonrasında Batıda var olan Sovyet/komünist tehdidi gibi başarılı ve uzun bir süreci kapsayan şekilde olabilir. ABD'nin Irak'a yönelik hedef gösterme girişimi ve dünya kamuoyunu sınırlı bir şekilde ikna etmesi gibi kısıtlı bir başarı sağlayabilir ya da Vietnam Savaşı'nda gördüğümüz ABD'nin kamuoyu desteğini kaybetmesi gibi başarısız hale gelebilmektedir. Ayrıca son yıllarda artan sayıda çalışmaya kaynaklık eden ve ilgi çekici hale gelen kimlik ve göç, çevre ve enerji,

küresel sağlık, din, siber güvenlik[17] gibi önemli konular güvenlikleştirme teorisi içinde de daha fazla incelenir hale gelmiş ve toplumsal ve siyasi olayları anlamada rehber niteliğinde kullanılır olmuştur. Hem araştırılan konular açısından hem de araştırmacıların konumu açısından Avrupa temelli güçlü bir vurgu ile karakterize edilen güvenlikleştirme literatürü ise göç ve iklim değişikliği gibi çoğunlukla Avrupa güvenlik meseleleri olarak görülen konuların aynı şekilde Avusturalya ve ABD'de de önceliğe alınması literatüre katkıyı genişletmiştir. Son olarak siber güvenlik, terörizm ve devletlerarası çatışmalar da dâhil olmak üzere gittikçe artan sayıdaki sorunlara verimli bir yaklaşım olanağı sunması sadece Avrupa'dan değil, Kuzey Amerika ve Asya Pasifik'ten de çok sayıda araştırmacıyı bu konuyla ilgilenir hale getirmiştir (Balzacq vd., 2016:507; Buzan, 2008: 108).

2.4.2. Güvenlikleştirmenin Siber Güvenlik ile Tartışılması

Güvenlikleştirmeye yapılan ilk katkılarda siber uzayın önemi tam olarak fark edilememiştir. Bununla birlikte, ilk zamanlardaki çalışmalardan sonra siber güvenlik ve güvenlikleştirme daha geniş teorik gelişmelere yol açtığı için yapılan çalışmalar artarak devam etmiştir. Güvenlikleştirme konusu içinde siber güvenliğin önemi bu alanla ilgili iki önemli ve birbiriyle ilişkili eğilimden kaynaklanmaktadır. Birincisi giderek daha fazla siber uzay temelli verilere, sistemlere ve teknolojiye bağımlı hale gelen bireyler, şirketler, toplumlar ve devletlerin varlığıdır. Bu tarz farklı aktörlere, çeşitli tehditleri tanımlarken yeni güvenlikleştirme hamleleri geliştirmek için verimli bir zemin sunmaktadır. İkinci olarak, Soğuk Savaş'ın bitişinden bu yana güvenlik uzmanları ve bürokrasiler arasında süregelen yeni tehdit ve risk arayışlarına siber uzayla meşgul olmak tam olarak uymaktadır (Balzacq vd., 2016:515).

Güvenlikleştirme içerisinde siber uzaya dönük incelemelerin artmasından sonra yapılan çalışmalarda çerçevelendirme yaklaşımının öne çıktığı görülmektedir. Çerçeveleme önemlidir çünkü bir siber olayı, *siber suç* ya da *bilgi savaşı* olarak nitelendirmek yaptığı çağrışımlar ve alınacak karşı önlemler için önemlidir. Siber suç çerçevelendirmesi yapmak olayı polisle ilgili ve daha basit bir yaklaşım haline getirirken, bilgi savaşı olarak çerçevelendirmek daha geniş olarak kolluk kuvvetlerinin kullanılmasını hatta ordunun rolünü meşrulaştırmaktadır. Bu açıdan aynı sorunu karakterize etmek amacıyla kullandığımız farklı kelimeler ve semboller olayın nasıl anlaşıldığına ve cevap olarak hangi eylemlerin verileceğine dair gereklilik noktasında büyük önem taşımaktadır. Çerçeve, eksik tanımlanmış, biçimsiz ve problemli bir durumun anlam kazanabileceği ve etkilenebileceği bir perspektiftir. Çerçeveleme yaklaşımı içinde yaşadığımız karmaşık dünyayı anlamlandırmak için kullanılan yöntemlerden biridir ve daima bir şekilde yorumlanan şeyleri daha ciddiye almak anlamına gelmektedir. Çerçeveleme yaklaşımı belirli bir alanın sosyal anlamı

[17] Güvenlikleştirme teorisinin çerçevesinin çizildiği ilk dönemlerde siber güvenlikle alakalı sorunlar devletlerin varlığına yaşamsal bir tehdit olarak algılanmamıştır. Çünkü siber güvenliğin, devletlerin karşı karşıya kaldığı başka güvenlik problemleri üzerinde basamaklama (cascading) etkisinin olmadığını ileri sürülmüştür (Buzan vd., 1998:25).

üzerindeki sembolik çekişme olarak görülmektedir. Ayrıca burada anlam aynı zamanda ne yapılması gerektiğini de ima etmektedir (Bendrath vd., 2007:59; Rein ve Schön, 1993: 146).

O halde çerçeveleme teorisi, dilbilimsel etkileşim çalışmalarına dayanır ve anlamların ve ortak varsayımların herhangi bir konunun yorumlanmasını hangi açılardan biçimlendirdiğine işaret etmektedir (Oliver ve Johnston, 2000:37). Çerçeveler, söylemsel hegemonya mücadelesinde kullanılan esas araçlardan biri haline gelmektedir. Tehdit çerçevelemesi durumunda, bir şey belirli bir tehdit olarak kategorize edilir. Ardından aktörler dünyayı, oluşturulan kategorilere göre görmeye başlarsa çerçeveleme pratik sonuçlar doğurur. Çerçeveler üç ana soruyu ele almaktadır: *(1) Çerçeveler sosyal eylemi nasıl etkilemektedir? (2) Hangi çerçeveler hangi sebeplerle özellikle başarılıdır? (3) Çerçeveler nasıl değiştirilebilir?* İkinci soruyla bağlantılı olarak ortaya konulabilecek üç adet çerçeve bulunmaktadır. *Tanısal (diagnostic) çerçeve*, bir problemi açıkca tanımlar; *belirti (prognostic) çerçeve,* çözüm önerileri ve bu çözüm önerilerine ulaşmak için izlenecek stratejiler, taktikler ve hedefler önermekle ilgilidir. *Motivasyonel çerçeve*, nedenin arkasındaki kuvvetleri toplamak ya da bir eylem çağrısında bulunmak şeklinde ifade edilebilir (Cavelty, 2008:30).

Tablo 5: Siber Tehditlerle Alakalı Tehdit Çerçevelemesinin Anahtar Kelimeleri

Siber Tehditler İçin:	
Bilgisayar (-temelli) saldırılar	Siber Güvenlik Açığı
Bilgisayara izinsiz giriş	Siber Savaş
Kritik Bilgi Altyapıları	Elektronik Pearl Harbour
Kritik Altyapılar	Bilgi Savaşı
Siber Saldırılar	Ulusal Güvenlik (bilgi güvenliği vb. ile bağlantılı olarak)
Siber Güvenlik	Bilgi Altyapısının Güvenlik Açığı
Siber Terörizm	Siber Tehditler

Kaynak: Cavelty, 2008:38

Çerçeve yaklaşımıyla ilgili bu genel açıklamalardan sonra Tablo 5, siber uzayın güvenlikleştirilmesinde kullanılan kavramları yansıtmaktadır. Bu anahtar kavramlar, bir metin içindeki tehdit çerçevelerini saptamak ve bir konuyu konuşma eylemi yoluyla güvenlikleştirmek ya da daha genel olarak bir siber-tehdit çerçeveleme eylemi geliştirmek için kullanılan kelime listesidir. Oluşturulan bu kavramlar, rahatsız edici bir olay tarafından başlatılmış inanç ya da kaynaklardaki değişime uygun olarak bir araya getirilirler. Başarılı tehdit çerçevelerinin özellikleriyle ilgili birkaç çıkarım yapılabilir. Bir tehdit çerçevesindeki tehdit konusu ne kadar genişse, tehdit çerçevesinin başarılı olması muhtemeldir; ayrıca referans nesnesinin toplumsal

refaha ilgisi ne kadar yüksek ve ne kadar yerelse tehdit çerçevesinin başarılı olma ihtimali de o kadar fazladır. Son olarak motivasyonel çerçevedeki motivasyon çağrısı ne kadar acilse, tehdit çerçevesinin başarılı olma ihtimali de o kadar fazladır (Cavelty, 2008:40).

Aktarılan teorik bilgiler ışığında siber uzayın güvenlikleştirilmesi süreci analiz edildiğinde Nissenbaum (2005:67) siber güvenliğe yönelik üç tehdit kategorisi geliştirmiştir. İlk tehdit kategorisi, bire-bir ve çok sayıda etkileşimli iletişimin yanı sıra bire-çok yayın iletişimi için son derece etkili bir araç olarak hizmet eden *yeni ortamın* (kastedilen internettir) geniş kapsamlı gücünden ortaya çıkmaktadır. Daha net bir ifadeyle, örneğin, 11 Eylül 2001 saldırılarından önce bile medya, ağın tehlikeli potansiyeli konusundaki hükümet endişelerine dikkat çekiyordu. ABD'de USA Today tarafından yayımlanan bir makalede hükümet yetkililerinin El Kaide terör örgütünün steganografi[18] yöntemini kullandığından şüphelenildiğini ifade etmiştir. Bu yöntem ile terör örgütü, spor chat odaları, pornografik bültenler gibi web siteleri üzerinden gizli bilgileri örgüt üyelerine iletmektedir. İlave olarak, terörist grupların interneti planlar hazırlamak, fon toplamak, propaganda yapmak ve güvenli bir şekilde iletişim kurmak için kullandığı Ağustos 2001'de Temsilciler Meclisi'den önceki ifadesinde Leslie G. Wiser tarafından ifade edilmiş ve siber uzayın güvenlikleştirilmesine yönelik konuşma eylemi yapılmıştır (Nissenbaum, 2005:67).

Nissenbaum tarafından ikinci ve üçücü tehdit kategorileri *felaket getiren siber saldırılar* ve *kritik altyapıya yönelik zayıflatıcı saldırılar* olarak ifade edilmiştir. Bu kategorilerin konuşma eylemi yoluyla güvenlikleştirilme denemelerine bir örnek, dönemin ticaret bakanı Bill Daley tarafından yapılan bir açıklamada yansımasını bulmuştur. Daley açıklamasında, giderek bilgi teknolojilerine daha bağımlı bir ekonomiye sahip olduklarını ve e-dünyaya öncülük etmenin ABD için çok önemli olduğunu belirtmiştir. Ancak bilişim teknolojilerine daha fazla bağımlı hale gelmenin yeni ve farklı tehditlere de aynı oranda maruz kalmak olduğunu ifade etmiştir. "*Korunmaya çalıştığımız en büyük tehdit nedir? Hackerlar ve vandalizm mi? Yoksa yerli ve yabancı terör mü?"* şeklinde gelen sorulara ise bunların hepsinin tehdit oluşturduğunu söylerek yanıt vermiştir. Genç bir hackerdan; endüstriyel casusluğa, sahtekarlığa ve hırsızlığa kadar uzanan geniş bir skala olduğunu ifade etmiş ve en sonunda kritik altyapılarına karşı bilgi savaşı başlatacak bir ülke olduğunu belirtmiştir. Açıklamalardan anlaşılan internetin kendisinin devlete yönelik kapsamlı bir saldırı için potansiyel bir savaş alanı olarak resmedildiğidir (Nissenbaum, 2005:67-68).

ABD özelindeki bu açıklamalardan sonra daha geriye gittiğimizde ise siber güvenliğin güvenlikleştirici bir konsept olarak tarihinin bilgisayarların yaygınlaşması ve bilişim disipliniyle başladığını görmekteyiz. 1991 yılında yayımlanan Computer Science and Telecommunications

[18] Steganografi, gizli mesajların tespit edilmesini önleyen şekillerde bilgiyi gizleme sanatı olarak ifade edilmektedir. Yunancadan üretilen kavram, "örtülü yazı" anlamına gelir (Johnson ve Jajodia, 1998:26).

Boards (CSTB) raporunda güvenlik, *"sistemin istenmeyen şekilde açığa vurulmasına, değişitirilmesine ve tahrip edilmesine karşı koruma*" şeklinde açıklanmıştır. Ayrıca siber güvenliğe yönelik tehditler yalnızca amaçlı bireyler/gruplardan değil; sistemik hatalardan da kaynaklanmaktadır. Daha açık bir ifadeyle, kasıtlı tehditlere ek olarak siber alanda çalışan bilgi sistemleri herhangi bir aktörün müdahalesi olmadan kendileri ya da içinde bulundukları fiziksel ve toplumsal ortamlar için istenmeyen tehlikeli durumlar oluşturan öngörülemeyen eylemlere neden olmaktadır. Bu ek siber uzay tehlikelerine karşı korunmaya *siber uzay güvenliği* denilmekte ve tam bir koruma için bireyler, iş dünyası, hükümet yani bir bütün olarak toplum kapsamlı bir siber uzay güvenliği yaklaşmını benimsemelidir (Hansen ve Nissenbaum, 2009:1160; Anderson ve Hundley, 1997:232).

Bu açıklamalar ışığında siber güvenlik, bilgisayar güvenliğine ilave güvenlikleştirme olarak görülebilir. 1991 CSTB raporunda geleceğin teröristinin klavyeyle bir bombadan daha fazla zarar verebileceği ve kayda değer bir güvenlik seferberliği içinde olmamız gerektiği ifade edilmiştir. Raporda geçen *"... şimdiye kadar büyük bir saldırı başlatılmadı ancak eylem yapılmazsa ciddi olayların yakın gelecekte gerçekleşeceğini, dolayısıyla yakın gelecekte şansımızın tükeceneğine inanmak için bir neden olduğunu savunmak güvenlikleştirme söyleminin kilit unsurlarından biri"* ifadesi raporun yayımlandığı 1991 yılından geleceği görür gibidir (Hansen ve Nissenbaum 2009:1161). Çünkü 2007 yılında gerçekleşen Estonya siber saldırısı, 2008 Gürcistan-Rusya Savaşı ve 2010 Stuxnet saldırısı siber uzaydan gelebilecek saldırıların devletler için ne derece yıkıcı olduğunu ve siber uzayın güvenlikleştirilmesinin gerekliliğini ortaya koymuştur.

Son olarak Hansen ve Nissenbaum'un ortaya koyduğu, güvenlikleştirme teorisi içerisinde Buzan ve çalışma arkadaşları tarafından kavramsallaştırılan beş farklı güvenlik sektöründen ayrı olarak yeni bir *siber güvenlik sektörü* tanımlaması yapma gerekliliği görülmektedir. Siber güvenlik sektörü, kamu-özel sektör sorumluluğunda ve hükümet otoritesi altında birleşik bir alan olarak görülmektedir. Bunun yanı sıra siber güvenlik sektörüne özgü üç güvenlik yöntemi de oluşturulmuştur. *Hiper güvenlikleştirme,* tehditleri aşırı derecede büyütülerek güvenlikleştirilmesini yansıtmaktadır. Söylem geri dönüşümsüzlüğü vurgulamaktadır. Yani dijital bir sistem hasara uğradığında ya da tam olarak ortadan kalktığında asla eski haline dönüştürülemeyeceği ifade edilmektedir. *Günlük güvenlik uygulamaları,* ağ güvenliği konusunda ortaya çıkabilecek felaket senaryolarının öğelerini günlük yaşamdan bilindik deneyimlerle ilişkilendirerek hiper güvenlikleştirme senaryolarını daha makul hale getirir. Son olarak *teknikleştirme,* siber güvenlikleştirmelerin meşrulaştırılmasında kritik rol oynar. Ayrıca hiper güvenlikleştirmelerin desteklenmesinde ve kamuoyu ile günlük güvenlik uygulamalarının önemi hakkında konuşmakta da büyük rolleri vardır. Siber güvenlik sektörünü diğer sektörlerden ayıran şey, referans nesnelerinin ulusal ve rejim/devlet güvenliğiyle bağlantılı olmasıdır (Balzacq, 2016: 517; Hansen ve Nissenbaum, 2009:1162-1168). Sonuçta siber uzayın güvenlikleştirilip güvenlikleştirilmeme kararı, karar alıcılara aittir. Ancak somut olaylar ışığında söylenebilir ki bireyler, örgütler ve

devletler gibi farklı aktörler için asimetrik yapısı nedeniyle siber uzay çeşitli faydaları barındırmakta ancak aynı zamanda belirli riskler de getirmektedir. Bu açıdan devlet güvenliğiyle bağlantılı olarak siber güvenliğin sağlanması noktasında gün geçtikçe daha somut adımların atılacağı söylenebilmektedir.

2.5. Küreselleşme Olgusu ve Siber Güvenlik

Siber güvenliğin fiziksel dünyada anlamını bulması ve belirli bir çerçeveye oturtulup incelenebilmesi teoriler aracılığıyla mümkün hale gelmektedir. Bu açıdan küreselleşme olgusunun temel argümanlarının 1900'lerin sonunda gelişmeye başlayan bir alan olan siber güvenlik bağlamında tartışılması, teorilerin eksiklik ve güncellenmesi gereken noktalarını ayrıca günümüz şartlarında geçerliliği sorgulanır hale gelen bazı argümanlarını net bir şekilde ortaya koyabilmek açısından önem arz etmektedir. Bu gerekliliği gerçekleştirmek, eksikliği ve benzeşen noktaları ortaya koyabilmek adına bu bölümde önce küreselleşme olgusunun entelektüel geçmişi ve temel görüşleri aktarılacak ardından bu teorilerin siber güvenlik alanı içinde kazandığı anlam ve boyut karşılaştırmalı olarak tartışılacaktır.

2.5.1. Küreselleşme Olgusunun Temel Tartışması

Küreselleşme kavramı, Batı Bloku karşısında Doğu Bloku'nun yıkılması ve Soğuk Savaş'ın bitişiyle birlikte 1990'lı yıllarda hız ve anlam kazanarak hayatımıza girmiştir. Farklı tanımları yapılan kavrama ilişkin, Giddens (1990:64) tarafından yapılan bir tanımda küreselleşme, *"dünya çapında sosyal ilişkilerin yoğunlaşması yoluyla, yerel olayların kilometrelerce uzakta meydana gelen olaylar tarafından şekillenmesi"* şeklinde ifade edilmiştir (Dumanlı Kürkçü, 2013:3). Başka bir tanımda ise küreselleşme, *uluslar-medeniyetler-politik topluluklar üçgeni arasındaki sistemik bağımlılıkların genişleme ve derinleşme sürecini tarihi açıdan yansıtan bir kavramdır*. Temelde, en eski medeniyetlere ve aralarındaki ilişkilerin tarihine kadar uzanmaktadır. Yani, eski uygarlıklar arasındaki ara sıra gerçekleşen karşılaşmalara kadar geri götürülebilecek aşamalı bir tarihsel süreç olarak anlaşılmalıdır. Bir başka tanımda ise küreselleşmenin ekonomik yönüne vurgu yapılmış ve *mal, hizmetler ve uluslararası sermaye akımlarında artan sınır ötesi işlem hacmi ve ayrıca teknolojinin daha hızlı ve yaygın boyutlandırması yoluyla dünya çapındaki ülkelerin artan ekonomik karşılıklı bağımlılığı* şeklinde bir tanım getirilmiştir. (Held ve McGrew, 2003:51; Wolf jr., 2000:2-3).

Farklı tanımlar ışığında küreselleşmenin net bir tanımının yapılamadığı ve tarihi süreci ifade eden bir kavram olduğu söylenebilir. Bunun yanı sıra küreselleşmenin farklı boyutları mevcuttur. Bu farklı boyutlar içerisinde en önemli vurgu ekonomik boyuta yapılmaktadır ancak yapılan ileri çalışmaların sosyolojik boyutu vurguladığını söylemek de yanlış olmayacaktır. Bu boyutlardan *ekonomik boyut,* insan yaşamındaki doğrudan ve gözle görülür etkileri nedeniyle küreselleşmede

başlıca etken unsur haline gelmiştir ve kavram olarak da ülkeler arasındaki artan ekonomik karşılıklı bağımlılık sürecini ifade etmektedir. Küreselleşmenin ekonomik boyutu, mal ve hizmetlerde artan sınır ötesi ticaret miktarını, uluslararası sermaye akışının artan hacmini ve iş gücündeki artan akışı yansıtmaktadır (Koçer, 2004:106; Fischer, 2003:3).

Diğer bir boyutu ise *siyasal boyut* oluşturmaktadır. Küreselleşmenin siyasi boyutu, gelecekte ulus devletin varlığını sürdürüp sürdüremeyeceği ve küreselleşmenin modern siyasi toplumun doğasına dönük soruşturması temelindeki tartışmalarla şekillenmektedir. Mesafeleri ortadan kaldıran ve artık bir çeşit siyasi kaynak olarak görülmekten çıkartan küreselleşme, gelişmiş iletişim araçlarını teşvik etmiştir. Bu yolla devletler tarafından kontrol edilmesi daha zor hale gelen alanlarda, sınırlar ötesi akışı destekleyen bireyler arasında doğrudan ilişkiler kurulması sağlanmıştır. Böylece 1990'lar sonrası ortaya çıkan küresel düzen, bölgesel olmaktan çıkmış ve fiziksel sınırların gittikçe ortadan kalkmasıyla ya da en azından böyle olacağı düşüncesiyle, dünya *küresel bir köy*[19] haline gelmiştir. Ayrıca küreselleşmenin siyasal yansıması sonucunda her birey potansiyel bir aktör haline gelmiş, devletlerin uluslararası sistemdeki aktör nitelikleri tartışmaya açılmıştır. Küreselleşme, vatandaşların klasik anlamdaki aidiyetlerini yıprattığı ve otorite üzerindeki siyasi sistem tekelini reddettiği için bireyin sahip olduğu kimlikleri de çoğaltmaktadır. Din veya etnik kökene dayalı kimlik temelli taahhütler ve uluslarüstü katılım, devletin güç ve egemenliğini yansıtma kapasitesine meydan okumakta ve siyaset, realizm tarafından ima edilen hiyerarşik pozisyonunu kaybetmektedir (Badie, 2001:255; Held ve McGrew, 1998:219).

Küreselleşmenin diğer bir boyutunu ise *sosyo kültürel boyut* oluşturmaktadır. Toplumların giderek birbirine daha benzer hale gelmeye başlaması sosyo kültürel boyutun bir yansımasıdır. Çünkü teknolojinin küreselleşmesiyle birlikte ucuz ve anlık bilgi toplumlar arasında hızla yayılmaya başlamış ve bu yayılım beraberinde baskın ülkelerin kültürel değerlerinin de yayılmasını getirmiştir. Benzer markalar kullanmak, benzer giyim stilleri benimsemek ve son aşamada benzer yaşam tarzlarına sahip olmak sosyo kültürel boyutun yansımalarını göstermektedir.

Küreselleşme kavramı, etkilediği farklı boyutların yanı sıra güvenlik kavramının da özünde belirli değişikliklere sebep olmuştur. Çünkü bireylere ve devletlere yönelik tehdidin içeriği ve şekli değişikliğe uğramıştır. Geçmişte tehdit olarak kabul edilen bazı unsurlar bu özelliğini yitirirken; daha önce tehdit olarak kabul edilmeyen bazı yeni unsurlar da hayatımıza girmiştir. Çevre sorunları, bölgesel milliyetçilikler, salgın hastalıklar, etnik kökenli çatışmalar, kapsamı genişleyen terörizm, uyuşturucu, silah ve özellikle savaşlarla bağlantılı insan kaçakçılığı yeni ve üzerinde önemle durulması gereken uluslararası güvenlik sorunları olarak devletlerin ajandasında yer almaya başlamıştır. Bu tehditlere paralel olarak devletlerin, özel sektörün ve bireylerin karşı karşıya kaldığı

[19] Küresel Köy kavramı ilk kez "Marshall McLuhan" tarafından *Understanding Media: The Extentions of Man* isimli kitabında kullanılmış ve tanımlanmıştır.

bir başka yeni tehdit türünü ise siber tehditler oluşturmaktadır. Küreselleşmenin beraberinde getirdiği teknolojik ilerleme sayesinde devletler ve bireyler daha çok siber alana bağlı hale gelmiş ve dünyanın çoğu bölgesinde bir dijitalleşme gerçekleşmiştir. Önceleri devletler siber güvenliğe yeteri kadar önem göstermese de zaman geçtikçe ve tehditlerin boyutu değiştikçe devletler, özel sektör ve bireyler gerek ulusal gerek uluslararası yapılanmaların da yardımıyla bu alandaki tehditleri bertaraf etmeye çalışmışlardır (Yılmaz, 2017:24; Koçer, 2004:110).

2.5.2. Küreselleşme Olgusunun Siber Güvenlik ile Tartışılması

Küreselleşmeyle birlikte devletlerin güvenliğini etkileyen çevre dinamik değişimlere uğramıştır. Güvenlik eğilimleri ve dış faktörlerin artan birbirine bağlılığı nedeniyle çevrenin öngörülebilirliği gittikçe azalmaktadır. Yeni tür tehditlerin hem kaynakları hem de taşıyıcıları devletlerin yanı sıra devlet dışı örgütlerden gelmekte ve bu tehditler uluslarüstü bir nitelik kazanmaktadır. İç ve dış güvenlik tehditleri arasındaki farklar belirsiz hale gelmekte ve güvenlik ortamının dengesi küresel ve bölgesel düzeyde ortaya çıkan yeni aktörlerin hedeflerinden etkilenmektedir (Podhorec, 2012:19).

Bu yeni çevrede, küreselleşmenin beraberinde getirdiği teknolojik yeniliklerin ortaya çıkardığı siber tehditler ve siber terörizm olgusuyla birlikte devletlerin güvenliği sağlamaya dönük farklı güvenlik yaklaşımları benimsemesi de kaçınılmaz hale gelmektedir. Bu güvenlik yaklaşımlarının başlıcaları arasında da *siber güvenlik* yer almaktadır. Çünkü siber terörizm ve saldırılar asimetrik bir nitelik taşımakta ve net bir tanımının yapılamaması kategorileştirilmesini de zorlaştırmaktadır. Siber terörizm, bilinmez kalmak isteyen, zarar verme potansiyelini arttımak isteyen ve psikolojik etki ve medya çekiciliğine önem veren *modern zaman teröristleri* için cazip bir konumda bulunmaktadır. Siber teröristler, bilgi iletişim araçlarını kullanarak ülkelerin enerji, ulaşım, taşımacılık gibi kritik altyapılarını hedef alan, bu altyapılara zarar vermek veya tamamen kullanışsız hale getirmek isteyen kişileri kapsamaktadır. Yaptıkları eylemler de siber terörizm olarak ifade edilmektedir (Weimann, 2005:130-131).

Ayrıca internetin varlığından sadece siber alemde faaliyet gösteren teröristler değil; fiziksel dünyada faaliyette bulunan teröristler de faydalanmakta ve geniş kitlelere ulaşabilmek ve kendilerine fon sağlamak için bir platform olarak interneti kullanmaktadırlar. İnternette teröristler; geleneksel televizyon ve yazılı medyadan farklı olarak, mesajları üstünde daha fazla doğrudan kontrol sağlayabilmektedirler. Terörist örgütlerin internet siteleri daha kapsamlı arka plan bilgilerine izin vermekte, taraftarlarını harekete geçme noktasında daha hızlı motive edebilmekte ve genellikle hedeflerine ulaşmak için şiddet kullandıklarını gizlemelerini sağlayabilmektedir. Yani internete bağlı her makine potansiyel bir matbaaya, bir yayın istasyonuna dönüşmektedir. 21. yüzyılda teröristler, *internete sahip olmanın* bu faydasından yoğun bir şekilde yararlanmaktadır. Geçmişte şiddet eylemleriyle iletişim kuran (örneğin önemli kişileri kaçırıp toplumun ilgisini o

yöne toplama) ve bu eylemleri ideolojik gerekçelerini ortaya koymak için bir fırsat olarak gören teröristler, internetin yaygınlaşmasıyla birlikte medya tarafından değiştirilmeyen ve sansüre uğramayan bilgileri paylaşabilmektedir (Anderson, 2003:25).

Küreselleşmenin beraberinde getirdiği değişen tehditlerin (özelde siber tehditler) niteliğine uygun olarak uluslararası örgütler ve kurumlar da aldığı kararlarda belirli güncellemeler yapmıştır. *Avrupa Konseyi tarafından Siber Suç Sözleşmesi*[20] hazırlanmış ve bir ilk özelliği göstererek siber suçlara ilişkin imzalanan uluslararası metin olmuştur (Önok, 2013:1241). Güvenlik temelli ittifaklar incelendiğinde, ilk örnek olarak 1994 yılında yaşanan Rus-Çeçen Savaşı'nda Çeçenlerin, ölü Rus askeri fotoğraflarını internete yüklemesiyle artık internetin sadece iletişim amaçlı kullanılan bir ortam olmadığını, aynı zamanda korunması gerektiğinin farkına varan NATO 1990'lı yılların sonlarına doğru ise üyelerini siber saldırılar konusunda uyarmaya başlamıştır. Fakat üyelerini uyaran NATO siber saldırı gerçeğiyle, dağılma süreci yaşayan Yugoslavya'daki Sırp hedeflere yönelik düzenlediği saldırılar sebebiyle, daha erken yüzleşmek zorunda kalmıştır. Bu süreçten sonra 1999 yılında hazırladığı dokümanla NATO, her ne kadar siber tehditlere nispeten daha az değinilse de, siber güvenlik alanındaki ilk adımını atmıştır (Bıçakçı, 2014:117-118; Darıcılı, 2016:413). BM açısından ise ilk çalışmalar 1980'li yıllardan itibaren başlatılmış, siber suçlara yönelik belirli çözümler ortaya konulmaya çalışılmıştır. Bu açıdan *45/121 (1990) sayılı, BM Genel Kurulu tarafından alınan karar* (United Nations, (1990), https://undocs.org/en/A/RES/45/121) bilgisayar destekli suçlarla alakalıdır ve o tarihten itibaren alınan kararlarda da siber suçlara yönelik vurgu yapılmış ve üye devletlerin siber güvenliği sağlanmaya çalışılmıştır (Önok, 2013:1239).

Sonuç olarak internetin ve bilgi iletişim araçlarının küreselleşmesi hem devletleri hem de uluslararası örgütleri güvenlik algısı bağlamında belirli değişiklikler yapmaya ve yeni tehditlerle yüzleşmeye zorlamış; bununla birlikte artık klasik anlamda sınırların etrafına yüksek duvarlar örmenin eskisi kadar avantaj sağlamadığını ortaya çıkarmıştır. Bireyler, devletler, devlet dışı örgütler ve diğer aktörler nezdinde ulaşılmak istenen bilgiler için sanal ortamlar bulunmaz bir fırsat yaratmaktadır. Ağlar yoluyla, başkalarının sahip olduğu kritik bilgilere sahip olmak günümüzde güvenliğin ve bağımsız olmanın kilit noktalarından biri haline gelmiştir (Özdemirci ve Torunlar, 2018:82). Bu sebepten de siber güvenliği sağlayabilmek bireyler ve devletler için büyük önem arz etmektedir. Singer ve Friedman'ın (2014:162) ifade ettiği gibi, *diğer savaşlardan farklı olarak, siber savaşların sonu gelmeyecek; çünkü imternet, orta sınıfın gelişimi için hayati olan endüstrilerin sürekli küreselleşmesiyle birlikte korunacak yeni savaş alanları yaratacaktır*.

[20] Bahsi geçen sözleşme, 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilip; 1Temmuz 2004 tarihinde Budapeşte'de üyelerin imzasına sunulara yürürlüğe girmiştir.

ÜÇÜNCÜ BÖLÜM

3. SOĞUK SAVAŞ SONRASI YENİ BİR ÇATIŞMA BİÇİMİ OLARAK SİBER SAVAŞLAR

3.1. Ülkelerin Siber Savaş Kabiliyetlerinin Ölçülmesi

Soğuk Savaş sonrası süreçte devletler askeri kapasitelerini çeşitlendirme ve geliştirme noktasında siber uzayın sağladığı faydaları yeni bir fırsat penceresi olarak görmüş, bu doğrultuda başta ABD, Çin Halk Cumhuriyeti, Rusya Federasyonu olmak üzere Kuzey Kore, İsrail, Almanya, İran gibi birçok ülke siber alanda saldırı ve savunma kapasitesine sahip olmayı amaçlamıştır (Darıcılı, 2019:14). Devletlerin siber alanda sahip olduğu saldırı ve savunma kabiliyetlerini değerlendirebilmek ise kabul edilebilirliği olan bir siber savaş kabiliyeti[21] listesi oluşturabilmek adına önem arz etmektedir. Ülkelerin siber uzaydaki savaş kabiliyetlerini değerlendirebilmek, siber silahların ve saldırı yöntemlerinin klasik silahlar ve saldırı yöntemlerine kıyasla belirli farklar taşıması ayrıca daha az somut veriler içermesi sebebiyle zor hale gelmekte ve incelenen farklı kaynaklar farklı sonuçlar ortaya koymaktadır. Askeri harcama bakımından üst sıralarda yer alan devletlerin aynı zamanda siber alana en çok yatırım yapan ayrıca bu alanda kabiliyetlerini geliştirmeye çalışan devletler olması ortak bir yön olarak dikkat çekicidir (Çifci, 2017:30).

Yüksek askeri harcamalar gerçekleştiren devletlerin, siber alanda da harcamalarını arttırarak kabiliyetlerini geliştirmeye çalıştığı düşüncesi genelde kabul görüyor olsa da siber savaş gücü potansiyeli geliştirme noktasında belirli istisnaları bulunmaktadır. Örneğin, Stockholm Barış Araştırmaları Enstitüsü (SIPRI) tarafından yayımlanan askeri harcamalara yönelik rapor (Military expenditure by country, in constant (2017) US$ m., 1988-2018, 2019) dikkate alındığında Japonya yaklaşık 46 milyar dolarlık askeri harcamasıyla altıncı sırada yer almakta ve ön plana çıkan ülkelerden biri konumunda bulunmaktadır. Ancak Dennesen (2011:36) tarafından ortaya konan ve siber alanda aktif ülkeleri dört gruba ayıran başka bir raporda ise siber savaş kabiliyeti bakımından Japonya dördüncü grup ülkeler arasında yer almakta siber güvenlik politikası ve savunma kabiliyetine sınırlı kaynak ayıran ülke konumunda bulunmaktadır.

Yukarıdaki örnekte görüldüğü gibi siber savaş kabiliyeti geliştirmek ve siber alanda güçlü olabilmek devletlerin bunu tercih etmesiyle doğrudan ilişkilidir. Ülkelerin siber savaş kabiliyetlerinin ölçülmesi noktasında belirleyici bir faktör olarak ön plana çıkan ve siber alandaki saldırı ve savunma kapasitelerini geliştirmek isteyen devletler tarafından oluşturulan *siber*

[21] Devletlerin siber uzaydaki saldırı ve savunma kabiliyetlerinin, "siber savaş kabiliyeti" olarak tek çatı altında toplanmasının temel sebebi kabiliyet belirlenirken ortaya çıkan bir ikilemden ötürüdür. Şöyle ki, siber savaş kabiliyetini arttırıcı bir katkı yapan örneğin bilgi ve iletişim altyapısının siber alana entegrasyonu, altyapının eş zamanlı olarak siber saldırılarda hedef konumunda olması ve savunulması gereken bir alan olarak belirlenmesi sebebiyle hem savunma hem saldırı faktörleri içinde değerlendirilmiş bu sebepten siber savaş kabiliyeti ana başlığı altında tek bir inceleme yapılmıştır.

ordular[22] ölçümde kilit bir nokta olarak yer almaktadır. ABD, Çin Halk Cumhuriyeti, Hindistan, Rusya Federasyonu, İngiltere, Fransa, İsrail gibi önde gelen ülkelerin yanı sıra; AB ve NATO gibi örgütler de siber kabiliyetlerini geliştirebilmek adına bünyesinde siber birimler bulundurmaktadır. Siber ordular, siber politika ve siber stratejinin geliştirilmesine ilişkin stratejik yön oluşturulmasına yardımcı olarak bir ulus devlete değer ve güç katmaktadır. Ulusal kritik altyapıları etkili bir şekilde koruma, ulusal siber tehdit analizlerini yürütme ve bunlara katkıda bulunma yeteneğine sahip olan siber ordular; siber tehditlere ve siber silahlara hızlı bir tepki verebilecek, olası siber saldırılar için tehdit portföyü geliştirecek ve siber karşı saldırı oluşturulmasında etkin bir noktada bulunacaklardır. Aktarılan sebeplerden ötürü siber savaş kabiliyeti oluşturmak isteyen devletler açısından siber ordular kurmak günümüz dünyasında elzem hale gelmiştir (Aschmann vd., 2015:21).

Ülkelerin sahip olduğu siber savaş kapasitelerine ilişkin referans noktası oluşturan farklı bir özellik ise ülke içindeki kaynaklardan, başka ülkelere ve bölgelere yönelen siber saldırı trafiğinin yoğunluğudur. Radu (2019) tarafından aktarılan ve Center for Strategic & International Studies (CSIS,) isimli düşünce kuruluşunun 2006-2019 yıllarını kapsayan ve siber casusluk ve siber savaşlara ilişkin siber olayların listesinin oluşturulduğu raporda (CSIS (t.y.), https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3G1QKa), Rusya Federasyonu ve Çin Halk Cumhuriyeti'nin 2006'dan beri en büyük tehdit kaynağı ülkeler olduğu ortaya konulmuştur. Sadece 2018 yılının Aralık ayında bile Çin Halk Cumhuriyeti ile ilgili dört büyük olay bildirilirken; Rusya Federasyonu için ise üç olay bildirilmiştir.

Yine aynı rapora göre, 2006'dan 2018 yılına kadar Çin Halk Cumhuriyeti, her biri bir milyon dolardan fazla kayba neden olan, 108 siber olaya karışmıştır. Avrupa'daki iletişimi tehlikeye atmak, on iki ülkede siber casusluk faaliyeti gerçekleştirmek ve ABD'de faaliyet gösteren büyük bir otel zincirinin milyonlarca müşterisinin bilgilerini çalmak gibi suçların kaynağı olarak görülen Çin Halk Cumhuriyeti devleti; aynı zamanda Batı'daki siber saldırıların en büyük devlet sponsorlarından biri olarak görülmektedir. Yine aynı rapora göre Rusya Federasyonu ise bu süreçte, aralarında NATO operasyonlarını, Ukrayna Hükümetini, Estonya ve Gürcistan internet altyapısını siber saldırılar yoluyla etkisiz hale getirmek gibi olayların bulunduğu 98 büyük siber olaydan sorumlu tutulmuştur (Radu, 2019).

Rapor içerisinde, Rusya Federasyonu ve Çin Halk Cumhuriyeti'nin ardından İran 44 olayla üçüncü sırada gelmektedir. 38 olayla Kuzey Kore dördüncü sırada; 16 önemli siber olayla Hindistan ise beşinci sırada yer almaktadır. ABD ise yalnızca dokuz olayda siber saldırılarının

[22] Askeri bir siber ordu, siber beceriler hakkında geniş bir anlayışa sahip, askeri ve stratejik altyapıları savunabilen ve siber saldırılar başlatabilen, son derece yetenekli bir bilgi teknolojisi grubu olan siber savaşçılardan oluşur (Aschmann vd., 2015:21).

kaynağı olarak görülmüş ve suçlu bulunmuştur. ABD'nin siber saldırı trafiğinde son sıralarda bulunması savaş kabiliyetinin düşük olduğu sonucunu ortaya çıkarmamaktadır. Çünkü siber uzayda ABD, etkin caydırıcılık ve maliyeti arttırma yoluyla gücünü ortaya koymaya çalışmaktadır. Bu yolla kanun gücünün uygulanabilirliğini arttırmak, etkin cezalandırma yoluna gitmek, etkili siber operasyonlar yürütmek ve uygulanabilir önlemlerin sonuçsuz kalması halinde askeri güç kullanmak gibi tedbirler ortaya koymaktadır (Korhan, 2017:89-90). Son olarak raporda dikkat çekilen yalnızca Japonya ve Avustralya'nın son iki yıl içerisinde gerçekleşen siber saldırılarda, saldırı kaynağı olmaması noktası ise yukarıda bahsettiğimiz ve askeri harcamalarda üst sıralarda yer alan Japonya'nın siber savaş kapasitesinin neden düşük olduğu ortaya koyduğumuz savımızı kanıtlar niteliktedir.

Sonuç olarak dünya genelindeki ülkeler olası bir fiziksel savaş için askeri kapasitelerini, silah sistemlerini, personel yeteneklerini geliştirmek için çaba gösteriyor, pahalı ve büyük tatbikatlar yapıyor ve bütçeden büyük kaynaklar ayırıyorken; kendine has özellikleri sebebiyle çok hızlı cereyan edebilen siber savaşlara yönelik kabiliyetlerini geliştirmekten geri duracağını düşünmek çok mantıklı gözükmemektedir. Bu sebepten olası bir fiziksel savaşta destek mahiyetinde de kullanılabilen ve büyük etkiler doğuran siber savaşlara yönelik devletlerin kabiliyetlerini ölçmek önem arz etmektedir.

3.1.1. Ülkelerin Siber Savaş Kabiliyetleri Nasıl Ölçülür?

Ülkelere ait savaş kapasiteleri ölçümü yapılırken, sahip oldukları askeri birliklerin sayısı, ordunun eğitim düzeyi, savunma sanayiye yaptıkları yatırımlar, geliştirdikleri silah sistemleri ve *bir ülkenin amaçlı eylemler yoluyla stratejik hedefleri izleme kapasitesi* olarak tanımlanan ve nüfus, coğrafya, teknoloji, ekonomi, politika gibi farklı doğal ve sosyal etkenlerle ölçülen milli güç unsurları hesaba katılmaktadır (Çifci, 2017:28; Ünal ve Yarman, 2014:279). Ülkelere ait siber savaş kapasitesi ölçülürken ise farklı metotlar kullanılmış; en bilinen hesaplamalardan biri ise Clarke ve Knake, (2010:74) tarafından yapılmış olup yalnızca başka ülkelere saldırı kapasitesi ekseninde inceleme yapılmamış aynı zamanda *savunma*[23] ve *bağımlılık*[24] boyutu analize dahil edilmiştir. Tablo 6, siber saldırı, siber bağımlılık ve siber savunma yetenekleri ayrı ayrı puanlandırılmış olup seçili ülkelerin siber bağımlılığı azaldıkça aldıkları puanların arttığı ifade edilmiştir.

[23] Savunma, *"bir ülkenin bir saldırı sırasında karşı tarafı durdurma çabası"* olarak ifade edilmektedir.

[24] Bağımlılık, *"bir ülkenin saldırıya açık sistemlere ve ağlara duyduğu gereksinimin ölçüsü"* olarak ifade edilmektedir.

Tablo 6: Siber Savaş Gücü Ölçüm Sonuçları

ÜLKE	Siber Saldırı	Siber Bağımlılık	Siber Savunma	Toplam
ABD	8	2	1	11
Rusya	7	5	4	16
Çin	5	4	6	15
İran	4	5	3	12
Kuzey Kore	2	9	7	18

Kaynak: Clarke ve Knake, 2010:75

Tablo 6 incelendiğinde, siber bağımlılığın yüksekliğinin siber savunmanın etkinliğini önemli ölçüde etkilediği görülmüştür. Yani siber bağımlılığı en düşük ülke olan Kuzey Kore, siber bağımlılığı en yüksek ülke olan ABD'ye göre siber savunmasını daha kolay yapacak gibi gözükmektedir. Ayrıca siber saldırı gücü en düşük ülke olmasına rağmen toplam puanlamada en üst basamakta yer almakta ve yüksek bir siber savaş kabiliyetine sahip gibi gözükmektedir. ABD en yüksek siber saldırı gücü puanına sahip olmasına rağmen bağımlılığı sebebiyle siber savunması da düşük hale gelmekte bu yüzden toplam puanlamada siber savaş kabiliyeti açısından diğer ülkelerin gerisinde kalmaktadır. Bu durum aynı zamanda bir *siber savaş açığı* yaratmaktadır. Yani daha düşük bütçelere sahip ülkeler siber alandaki olaylarda etkili olabilmekte ve örneğin ABD'ye bir saldırı düzenlendiğinde yaratılan etki yüksek olabilmekte aynı zamanda saldıran ülke güçlü bir siber savunma kapasitesine sahipse karşı saldırıdan en az hasarla kurtulma şansına sahip gibi gözükmektedir (Clarke ve Knake, 2010:75).

Dikkat çeken başka bir detay ise, İran'ın orta dereceli bir siber bağımlılığı olmasına rağmen siber savunmasının düşük olmasıdır. Bunun sebebinin ise 2010 yılında maruz kaldığı Stuxnet saldırısı olduğu söylenebilir. Siber bağımlılığı düşürmek günümüzde sistemlerin siber ortama giderek bağımlı hale gelmesi sebebiyle zor gözükmektedir. Yapılması gereken toplam puanı ve dolayısıyla kabiliyeti yükseltmek adına siber saldırı gücünü daha etkin boyutlara taşımak olacaktır (Clarke ve Knake, 2010:75).

Ülkelerin siber savaş kabiliyetlerine ilişkin farklı bir ölçüm, Billo ve Chang, (2004:22) tarafından siber savaş kabiliyetinin konu alanları belirlenerek yapılmıştır. Devlet ve özel sektörün Tablo 7'de belirtilen kabiliyetlerinin toplamı yüksek olan ülkeler, yüksek siber savaş kabiliyetine sahip ülkeler olarak konumlandırılmaktadır. Yani bir ülkenin, örneğin devlet kaynaklı bir girdi olan aktif savaş birimlerine sahip olması ülkenin siber savaş kapasitesini arttırmaktadır. ABD Siber Komutanı Keith Alexander tarafından yapılan bir açıklamada *Cybercom* çatısı altında 13 adet saldırıya yönelik ekibin oluşturulacağı ifade edilmiştir (Pellerin, 2013). Çin Halk Cumhuriyeti ise 30 siber savaşçıdan oluşan ve Mavi Ordu ismini taşıyan siber ordusunun varlığını kabul etmiştir

(Çin'in gizli "süper ordu"su ortaya çıktı (2011), http://www.milliyet.com.tr/dunya/cinin-gizli-super-ordusu-ortaya-cikti-1395440).

Tablo 7: Siber Savaş Kabiliyetinin Konu Alanları

Kamu	Özel Sektör
Aktif Siber Savaş Birimleri	Bilgisayar bilimi/mühendisliği için geliştirilmiş eğitim sistemi-akademi
Mevcut Siber Savaş Doktrini	Kamunun ağa erişim imkânı
Bilgisayar Olaylarına Acil Durum Müdahale Ekipleri	Bilgisayar Güvenliği Programları
Siber suç önleme/soruşturma ekipleri	Teknolojik olarak gelişmiş ülkelerde eğitim gören yabancı öğrenciler
Siber programlara sahip, devlet tarafından işletilen akademik kurumlar	Devlet destekli bilgisayar korsanları
Devlet destekli bilgi teknolojileri (BT) projeleri	Donanım üretme yetenekleri
İstihbarat Servis Yetenekleri	Yüksek hızlı erişim
Askeri Komuta ve Kontrol, İletişim, Bilgisayar, İstihbarat (C4I) bilgi savaşı yeteneği	Bilgi teknolojileri iletişimi, altyapısı ve güvenlik firmaları
Askeri istihbarat birimleri	Uydu ve telefon bağlantıları sayısı
Askeri birliklerin yetenekleri	Bilgi teknolojilerinin genel durumu ve entegrasyonu
Bilgi teknolojilerinin genel kullanımı	Denetleyici Kontrol ve Veri Toplama Sistemi'ni (Supervisory Control and Data Acquisition/ SCADA) de içeren süreç kontrol sistemleri
Devletlerarası bilgi teknolojileri girişimleri	Yazılım geliştirme yetenekleri
	Bilgi Teknolojileri sektöründe aktif olan / Bilgi Teknolojileri kullanan ulus ötesi şirketler

Kaynak: Billo ve Chang, 2004:22

3.1.2. Ülkelerin Siber Savaş Kabiliyetlerinin Karşılaştırmalı Analizi

Ülkelerin siber savaş kabiliyetleri Dennesen (2013:32-35) tarafından analiz edilmiş ve ülkeler siber kabiliyetleri açısından dört gruba ayrılmıştır. Birinci grupta ABD, Çin ve Rusya yer almaktadır. Bu gruptaki ülkelerin temel özelliği, siber güvenlik ve siber savunma açısından gelişim

sağlamaya yönelik çalışmalara ve uluslararası politikalara yön veren ülkeler olarak ön plana çıkmalarıdır. Siber savunma açısından en büyük desteği sağlayan bu ülkeler aynı zamanda siber güvenlik politikası ve siber savunma gelişimine adanmış en büyük varlıklara ve insan kaynaklarına sahiptir. Kapasite ve aktivite olarak ise bu ülkeler konvansiyonel savunma alanında siber yeteneklerden yararlanmakta; diğer birçok ülkeye karşı geniş kapsamlı, uzun süreli, karmaşık saldırı ve savunma faaliyeti yürütmektedir.

Aynı çalışmada (Dennesen, 2013:32) ikinci grup ülkeler ise İngiltere, Fransa ve İsrail olarak belirlenmiştir. İkinci grup ülkelerin temel özelliği, birinci gruptakileri yakından takip etmeleri ancak daha az insan kaynağına ve altyapıya sahip olmaları şeklinde ifade edilebilir. Kapasite ve aktivite bakımından ise, saldırı ve savunma operasyonlarının karmaşıklığı açısından birinci gruptaki ülkelere benzerlik göstermekte ancak ölçek olarak daha dar ve gerçekleştirdikleri büyük operasyonların sayısı da daha az olmaktadır.

Üçüncü grubu ise Hindistan, Güney Kore, Tayvan, Almanya ve Türkiye oluşturmaktadır. Bu ülkeler, siber savunma yeteneklerine ve siber güvenlik politikalarına önemli miktarda kaynak ayıran ancak bu alanda lider vasfı taşımayan konumda bulunmaktadırlar. Üçüncü grup ülkeler, birçok şekilde birinci gruptaki ülkelerin uygulamalarını taklit etmektedirler. Kapasite ve aktivite bakımından ise bu gruptaki ülkeler kapsamlı ve sürekli savunma faaliyeti yürütmekte ancak genellikle çok daha az hedefe karşı daha az saldırgan aktivite yürütmektedirler (Dennesen, 2013:35).

Çalışmada son olarak dördüncü grubu oluşturan ülkeler ise İsveç, Avustralya, Japonya, İran, Pakistan, Hollanda, Finlandiya'dır. Aktarılan ülkeler siber güvenlik politikasına ve savunma yeteneklerine sınırlı kaynak adamış ülkelerdir. Kapasite ve aktivite bakımından ise güçlü ama eksik savunma faaliyetine ve sınırlı saldırı faaliyetine sahiptirler. Bu ülkeler iç kaynaklarını korumaya odaklanmışlardır (Dennesen, 2013:35).

G20 ülkelerinin, 2011 yılı ve daha önceki dönem verilerini temel alarak, ekonomilerindeki bilgi teknolojilerinden yararlanırken siber saldırılara karşı koyma yeteneklerini karşılaştıran Siber Güç Endeksi (Economist Intelligence Unit, 2011)[25] de siber savaş kabiliyetlerine ilişkin ülkeler hakkında bilgiler vermektedir. Endeks hangi ülkelerin dijital çağda iyi bir performans gösterdiğini; hangilerinin ise dijital çağda henüz siber güçten yararlanamadığını ölçmeyi amaçlamakta ve yapılan inceleme göstermektedir ki, Birleşik Krallık, ABD, Avustralya, Almanya ve Kanada gibi gelişmiş batı ülkeleri dijital alana liderlik etmektedir.

[25] Raporda ülkeler, 4 ağırlıklı özelliğe göre birleştirilen 39 gösterge (2007-2011 yılları arasını kapsayan) baz alınarak sıralanmıştır. 1) Yasal ve Düzenleyici Çerçeve, 2) Ekonomik ve Sosyal Bağlam, 3) Teknoloji Altyapısı ve 4) Endüstri Uygulaması ağırlıklı özellikleri oluşturmaktadır.

Tablo 8: Siber Güç Endeksi

Ülkeler	Yasal ve Düzenleyici Çerçeve[26]	Ekonomik ve Sosyal Bağlam[27]	Teknoloji Altyapısı[28]	Endüstri Uygulaması[29]	Genel Siber Güç Sıralaması
Almanya	99.3 (1.)	64.2 (1.)	58 (6.)	60.6 (5.)	68.2 (4.)
ABD	97.3 (2.)	52.9 (7.)	62.3 (3.)	75.3 (2.)	75.4 (2.)
Arjantin	52.7 (13.)	33.8 (13.)	28.5 (12)	25.5 (17.)	35.4 (12.)
Avustralya	89.4 (6.)	60.2 (3.)	66.5 (1.)	66.6 (3.)	71 (3.)
Birleşik Krallık	97.3 (2.)	56 (5.)	61.4 (5.)	89.1 (1.)	76.8 (1.)
Brezilya	57.5 (11.)	31.1 (14.)	35.9 (10.)	29.3 (11.)	38.6 (10.)
Çin	27.4 (18.)	50.9 (8.)	33.3 (11.)	27.3 (14.)	34.6 (13.)
Endonezya	32.6 (17.)	23.8 (18)	9.3 (18.)	26.3 (16.)	23.5 (19.)
Fransa	90.6 (4.)	48.2 (9.)	55 (7.)	52 (7.)	61.8 (6.)
Güney Afrika	58.6 (10.)	24.5 (16.)	7.5 (19.)	26.9 (15.)	30.2 (16.)
Güney Kore	63.8 (9.)	54.1 (6.)	63.5 (2.)	57.7 (6.)	59.7 (7.)
Hindistan	49.8 (14.)	20.4 (19.)	19 (16.)	22.2 (19.)	28.3 (17.)
İtalya	73.8 (8.)	34.3 (12)	47.9 (8.)	41 (8.)	49.5 (9.)
Japonya	90.5 (5.)	61.2 (2.)	45.7 (9.)	38 (9.)	59.3 (8.)
Kanada	83.9 (7.)	58.8 (4.)	61.5 (4.)	61.1 (4.)	66.6 (5.)
Meksika	55.6 (12.)	35.5 (11.)	24.1 (14.)	28.1 (13.)	36.3 (11.)
Rusya	36.4 (16.)	39.3 (10.)	25 (13.)	25.5 (17.)	31.7 (14.)
Suudi Arabistan	27.2 (19.)	25.8 (15.)	20.6 (15.)	28.5 (12.)	25.7 (18.)
Türkiye	49.2 (15)	24 (17.)	15.9 (17.)	29.9 (10.)	30.4 (15.)

Kaynak: Economist Intelligence Unit, 2011:4-6

[26] Genel endekste %26.3 ağırlıklıdır. Bu kategori beş göstergede ölçülmüştür: 1) Hükümetin siber gelişime bağlılığı, 2) Siber koruma politikaları, 3) Siber sansür (veya eksiklik), 4) Politik etkinlik, 5) Fikri mülkiyetin korunması

[27] Genel endekste %25 ağırlıklıdır. Bu kategori dört göstergede ölçülmüştür: 1) Eğitim seviyesi, 2) Teknik beceriler, 3) Ticaret açıklığı, 4) İş çevresindeki inovasyonun derecesi

[28] Genel endekste %26.3 ağırlıklıdır. Bu kategori beş göstergede ölçülmüştür: 1) Bilgi ve iletişim teknolojisine erişim, 2) Bilgi ve iletişim teknolojilerinin niteliği, 3) Bilgi ve iletişim teknolojisinin finansal anlamda karşılanabilirliği, 4) Bilgi teknolojisine yapılan harcama, 5) Güvenli sunucu sayısı

[29] Genel endekste %22.5 ağırlıklıdır. Bu kategori beş göstergede ölçülmüştür: 1) Akıllı şebekeler, 2) E-sağlık, 3) E-ticaret, 4) Akıllı ulaşım, 5) E-devlet

3.2. Siber Savaş Kabiliyetleri Bağlamında Siber Saldırı Örnekleri

3.2.1. Estonya Saldırıları

Estonya, başkenti Tallinn'de, 26-27 Nisan 2007 tarihlerinde, çoğunlukla etnik Rus kökenli[30] gençlik grupları tarafından başlatılan ve iki gece boyunca yoğun bir şekilde devam eden sokak ayaklanmalarına ardından siber ortama taşınan, büyük yankı uyandıran ve yaklaşık üç hafta boyunca devam eden siber saldırılara tanık olmuştur. Olayların temeli, Estonya'nın Nisan 2007 tarihinde NATO; Mayıs 2004 tarihinde de AB üyesi olmasına kadar götürülebilir. Bu gelişmeler Rusya tarafından, Estonya'nın Batı'nın kurum ve yapılarının tam teşekküllü bir üyesi olarak siyasi yörüngesini kalıcı olarak terk ettiğinin işareti şeklinde algılanmıştır. Bu gelişmelerin ardından Estonya Devleti, Sovyet geçmişinin kalıntılarını ve izlerini ülkeden silmek istemiş; Tallinn'de bulunan ve yıkılması ya da yer değiştirilmesi gerektiğini savunanlar arasında tartışmalara neden olan, bronz Kızıl Ordu askeri şeklindeki anıtın kaldırılarak askeri mezarlığa taşınması da olayların fitilini ateşlemiştir. Anıt, İkinci Dünya Savaşı sırasında Nazilerle savaşırken ölen Rus askerlerini temsil etmekte olup, Estonya'nın bağımsızlığını kazanmasının ardından ise Sovyet işgalini ve baskısını temsil ettiği düşünüldüğü için Estonyalılar tarafından öfke ve provokasyon kaynağı olarak görülmüştür (Valeriano ve Maness, 2015:142-143; Rid, 2012:11; Bıçakçı, 2012:215).

Olayların gelişimine daha yakından bakıldığında, 26 Nisan akşamı anıtın kaldırılmasına karşı çıkan yaklaşık bin kişilik bir grup anıt alanında toplanmaya başlamıştır. Önceleri sakin bir protesto şeklinde başlayan eylem, ilerleyen saatlerde polise karşı şiddete, Tallinn merkezinde ve ülkenin kuzeydoğusundaki Jõhvi şehrinde geniş çaplı yağma ve tahribata dönüşerek boyut atlamıştır. Bu olaylar sonucu polis 1300 kişiyi tutuklamış; ayaklanmalarda yaklaşık yüz kişi yaralanmış ve bir kişi hayatını kaybetmiştir. Sokak ayaklanmalarının neden olduğu maddi kaybın yaklaşık 4.5 milyon Euro olduğu tahmin edilmektedir. Bu süreçten sonra hükümet hızlı bir karar vererek, 27 Nisan gecesi heykeli önce belirsiz bir yere ardından 30 Nisan'da da askeri mezarlığa götürmüştür (Tikk vd., 2010:16).

Ani bir şekilde ortaya çıkan sokak isyanlarına *online ayaklanmalar*[31] da eşlik etmiş ve 27 Nisan'da gece geç saatlerde Estonya'ya yönelik siber saldırılar böylece başlamıştır. Faz 1 olarak ifade edilebilecek olan bu süreç saldırganların ping taşkınları ve basit hizmet reddi saldırıları gibi oldukça düşük teknolojili yöntemler kullanmaları şeklinde gerçekleşmiştir. 30 Nisan'a kadarki bu süreçten sonra DDoS saldırılarının etkisini arttırmak için botnetler kullanılmaya ve kolektif

[30] 2020 Mart ayı itibariyle 1.317.800 kişinin yaşadığı Estonya'da, %25,2 oranında Rus etnik nüfusu bulunmaktadır (Ülke Künyesi (t.y.), http://www.mfa.gov.tr/estonya-kunyesi.tr.mfa).

[31] Belirtmek gerekir ki bu süreçten sonra yaşananlar için örneğin The New York Times *"siber uzaydaki ilk gerçek savaş"* tabirini kullanmıştır. Estonya Savunma Bakanı ise bu durumu bir ulusal güvenlik meselesi şeklinde nitelendirmiştir (Landler ve Markoff, 2007). Estonya Siber Güvenlik Koordinasyon Komitesi Başkanı ise daha ileri giderek yaşananları "bir tür terörizm" olarak ifade etmiştir (Blomfield, 2007).

saldırıların zamanlaması giderek daha fazla koordine hale gelmeye başlamıştır (Rid, 2012:11). Saldırıların boyut ve yöntem değiştirmesinde, internete yüklenen ve Estonya'nın elektronik alt yapısına karşı kullanılabilecek olan DDoS ve aksatma saldırılarının nasıl yapılacağını gösteren yayınların payı büyüktür. Bu yayınlardan ilham alan ve yönlendirilen Rusya kaynaklı binlerce kullanıcı eş zamanlı olarak Estonya'nın bilgisayar sistemlerine yüklenmiştir. Saldırılar genel olarak DoS, web site tahrifatı ve gereksiz e-mail gönderme şeklinde gerçekleşmiştir (Shakarian vd., 2013:16).

Esasen Estonya'ya yönelik saldırılar yeni ya da karşı konulamaz olmamıştır ancak bilgi sistemlerine yönelik halkın güveninin ve kullanımının yüksek oluşu saldırıların önemli bir tehdit oluşturmasına neden olmuştur. Bu noktada 2001 yılında kullanıma giren *X-Road* veri değişim katmanı programının etkisi büyüktür. Bu program aracılığıyla Estonya'daki devlet-özel kurumlar ve bireyler birbirine bağlanmakta, farklı kurumlara ait veri tabanları arası bağlantı gerçekleştirilmekte ve standart bir kimlik doğrulama hizmeti verilmektedir (Kalja, 2002:47). Bu program, E-devlet şeklinde nitelenen uygulamaların en gelişmiş örneklerinden biri konumunda bulunmaktadır. Hatta öyle ki, Estonya'da yapılan 2005 yerel seçimleri internet üzerinden yapılmıştır. Ayrıca internet bankacılığı (e-banking) işlemleri de yoğun olarak kullanıldığı için siber saldırının etki boyutu artmıştır. Dikkat çekici başka bir nokta ise ilk saldırılar esnasında Estonya'daki siyasi parti, başkan ve başbakan kısacası hükümetle ilgili siteler, medya şirketleri ve iletişim firmaları hazırlıksız yakalandıkları için büyük zarar alırken; Hansabank ve SEB gibi önde gelen iki banka bu saldırılara hazırlıklı oldukları için ilk dalga saldırıları daha az hasarla atlatmışlardır (Bıçakçı, 2012:214-215; Barletta, 2008:481).

Bu süreçten sonra gelişen ve Tablo 9'da Faz 2 olarak ifade edilen, dört dalga halinde gerçekleşen ve 30 Nisan-18 Mayıs arasını kapsayan ana saldırılarda ilave birkaç devlet sitesine[32] ve günlük gazeteye daha saldırı düzenlenmiştir. Örneğin Başbakan Andrus Ansip'in mensubu olduğu siyasi partinin web sitesinde kendisine Hitler bıyığı eklenmiş bir resim yayımlanmıştır. 30 Nisan günü Estonya hükümeti *.ru* ile biten tüm Web adreslerini filtreleyerek Rusya üzerinden gelen yoğun internet trafiğini engellemeye başlamıştır. Ertesi gün siber saldırılar doğrudan Estonya İnternet Servis Sağlayıcıları'nı (Estonian Internet Service Providers-ISPs) hedef almaya başlamıştır. Bu süreçten sonra hükümet, Estonya Bilgisayar Acil Durum Müdahale Ekibi (CERT-EE), bankalardan ve çeşitli devlet kurumlarından uzmanlar ve kolluk kuvvetleri de dâhil olmak üzere farklı kesimlerle bir dizi toplantı gerçekleştirmiştir (Barletta, 2008:482; Finn, 2007).

[32] Etkilenen siteler arasında Başbakanlık (peaminister.ee), Ekonomik İşler ve İletişim Bakanlığı (mkm.ee), İçişleri Bakanlığı (sisemin.gov.ee), Dışişleri Bakanlığı (vm .ee) ve Estonya Parlamentosu (riigikogu.ee) bulunmaktadır (Schmidt, 2013:5).

Tablo 9: Estonya 2. Faz Saldırı Dalgaları

1.Dalga (4 Mayıs)	DDoS saldırıları web sitelerine ve DNS'lere karşı devam ederken; Botnet kullanımında büyük bir artış gözlemlendi. Siber saldırganlar, izlerini çeşitli yollarla gizlemeye çalıştı: küresel botnetler kullanmak, saldırılarını diğer ülkelerdeki (NATO ülkeleri dâhil) proxy sunucuları aracılığıyla yönlendirmek, Internet Protokol (IP) adreslerini taklit etmek.
2.Dalga (9-11 Mayıs)	9 Mayıs Rusya'da Zafer Bayramı olarak kutlandığı için yeni bir saldırı dalgası bekleniyordu. Beklendiği gibi 9 Mayıs'ta saldırılar yaklaşık %150 artarak iki gün boyunca devam edip, sonrasında kesildi. 9 Mayıs'taki saldırılar yüzünden aynı anda 58 site hizmet veremez duruma geldi. Bu saldırı dalgası çoğunlukla devletin (resmi iletişim kanalları dâhil) web sitelerini hedef aldı. Faz 1'deki saldırıları az hasarla atlatan bankalarda Faz 2'deki saldırılardan daha çok etkilendi. Örneğin ülkenin en büyük ticari bankası Hansabank 9 Mayıs'ta bir buçuk; 10 Mayıs'ta iki saat boyunca işlem göremez hale geldi.
3.Dalga (15 Mayıs)	Devlet kurumlarının web sitelerine yönelik güçlü DDoS saldırıları (yaklaşık 85 bin köle bilgisayardan) 15 Mayıs gece yarısına kadar sürdü. Ancak ağ kapasiteleri zaten arttırılmış olduğundan, artan trafik miktarı önemli bir sorun yaratmadı. Ancak en büyük ikinci ticari banka olan SEB'in internet sitesi yaklaşık bir buçuk saat boyunca hizmet veremez duruma geldi.
4. Dalga (18 Mayıs)	Devlet kurumlarının web sitelerine yönelik yeni DDoS saldırıları ortaya çıktı, bankalar bu tarihten sonra bile kesinti yaşamaya devam ettiler.

Kaynak: Tikk vd., 2010:19-20

Saldırılarla başa çıkmak için gerçekleştirilen bu toplantılar sonucu verilen ilk teknik yanıt, sunucuların bant genişliğini kademeli olarak arttırmak (daha fazla veri trafiği işleme kapasitesine izin vermek) ve kötü niyetli trafiği filtrelemek olmuştur. Saldırının tepe noktasına ulaştığı 9 Mayıs'a kadar ağların bant genişliği kapasitesi, normal kapasitenin dört katına (2 Gbps'ten 8 Gbps'e) çıkarılmıştır. Ayrıca güvenlik yamaları ve duvarları, saldırı algılama sistemleri, erişim engelleme ve birden çok sunucu ve/veya bağlantı kullanılması gibi farklı teknik önlemler de alınmıştır (Tikk vd., 2010:24). Ancak dağıtılmış hizmet reddi saldırısının, saldıran bilgisayarların sayısız olması ve IP adreslerinin değiştirilebilir/taklit edilebilir olması nedeniyle saldırıya verilecek yanıtların etkinliğinin de sınırlı kalmıştır (Shakarian vd., 2013:18).

Estonya'ya yönelik siber saldırılara karşı alınan önlemlerin uluslararası düzeyde olumlu olarak görülebilecek katkılarından biri Estonya CERT'in, başta Almanya (CERTBund), Finlandiya (CERT-FI) ve Slovenya (SI-CERT) olmak üzere Avrupa'daki diğer CERT'lerle iletişime geçerek işbirliği halinde hareket etmesi olmuştur. Bu kolektif uzmanlık sayesinde saldırının doğası ve saldırı trafiğini oluşturan sistemlerle ilgili genel bir tablo ortaya konabilmiş ve etkin müdahale şansı ortaya çıkmıştır (Schmidt, 2013:13; Shakarian vd., 2013:19). Ayrıca uluslararası destek adına NATO ve AB sürekli olarak bilgilendirilmiştir. Ayrıca kendi sınırlarından yönelen saldırıları sınırlandırmak için birçok ülke uluslararası işbirliği teklifinde bulunmuştur. Yanı sıra NATO ve ABD'den gözlemciler olayları incelemek, tavsiyede ve yardımda bulunmak amacıyla Estonya'ya ziyaretler gerçekleştirmiş; ABD'den bazı kurumlar saldırı kaynaklarını tespit etme ve etkisizleştirme konusunda yardımcı olmuşlardır (Tikk vd., 2010:24).

NATO ve AB özelinde yaşanan gelişmeler de uluslararası düzeyde olumlu görülebilecek katkılardan bir diğerini oluşturmaktadır. 2006 yılında, başta terörizm önceliğiyle oluşturulan güvenlik belgesine siber güvenlik konusu da ilave edilmiştir. 2008 Bükreş Zirvesi ise siber güvenliğin ana başlık olarak ele alınması ve hazırlanan *Sonuç Bildirgesi'nde* ilk kez yer alması açısından önem ifa etmektedir. Bu sürecin ardından yaşanan iki önemli gelişme NATO'nun somut adımlar ortaya koyma iradesini göstermiştir. Bu açıdan Brüksel merkezli bir NATO Siber Savunma Yönetim Otoritesi (Cyber Defense Management Authority/CDMA) kurulmuş; daha sonra hareket kabiliyetini geliştirmeyi amaçlayan NATO tarafından siber saldırılara hedef olan Estonya/Tallinn merkezli Siber Savunma İşbirliği Mükemmeliyet Merkezi (Cooperative Cyber Defense Centre of Excellence/CCD COE) kurulmuştur (Bıçakçı, 2012:217-218). Ayrıca bir Alman yetkili NATO 5. maddesinin kapsadığı güvenlik garantisinin siber alana da yayılması gerektiğini ifade etmiştir. AB cephesinde ise, Kasım 2010'da *İç Güvenlik Stratejisi* yayımlanmıştır. Bu strateji belgesiyle birlikte siber güvenlik tehditlerine entegre yanıtlar ortaya konulmasının ve Avrupa Ağ ve Bilgi Güvenliği Ajansının (European Network and Information Security Agency/ENISA) görevlerinin daha önce sınırlı olan analitik rolünün ötesinde önemli ölçüde genişletilmesinin gerekliliği ortaya konulmuştur. Estonya'ya yönelik saldırılara gösterilen bu çok taraflı yanıtlar, devletlerin ya da devlet dışı aktörlerin internetin bir silah olarak kullanılarak tehdit oluşturulmasına seyirci kalamayacaklarını ve yaşananlardan kendilerini ayrı tutamayacaklarını idrak etmeleri açısından önem göstermektedir (Herzog, 2011:55).

Estonya'nın DDoS saldırılarına aldığı önlemleri takiben saldırılar azalarak son bulmuştur. 2007 yılında Estonya'da yaşananlarla ilgili önemli bir nokta, saldırıların arkasında kimin olduğunun belirsiz kalması olmuştur. Estonya Savunma Bakanı'nın Kremlin'i işaret etmesi gibi münferit nitelemeler olmuş fakat ne NATO ne de Avrupa Komisyonu'ndan uzmanlar herhangi bir kanıt bulamamıştır (Rid, 2012:12). Saldırılardan yaklaşık iki yıl sonra Konstantin Goloskokov isminde, *Nashi* olarak bilinen Kremlin yanlısı bir genç grubun lideri saldırının kendisi ve diğer

grup üyeleri tarafından yapıldığını iddia etmiştir. Mart 2009'da ise Duma milletvekili Sergei Markov, saldırıların sivil toplumdan gelen bir tepkinin parçası olarak gerçekleştirildiğini söylemiştir. Goloskokov ve Markov tarafından iddia edilenler saldırının bir kısmıyla eşleşse de olayların arkasındaki isim/isimler tespit edilememiştir (Shakarian vd., 2013:19; Tikk vd., 2010:24).

Sonuç olarak Estonya'ya yönelik siber saldırılardan çıkarılabilecek derslerin başında siber olaylar ile geleneksel uluslararası rekabet dinamikleri arasındaki bağlantının boyutu gelmektedir. Olaylara müdahalesi resmi olarak kanıtlanmasa da Rusya'nın, siber kapasitesi yüksek ancak siber taktik kullanımı sınırlı bir devlet olması da göz önüne alındığında, özellikle eski Sovyet bölgesinde bir tehdit algıladığında siber saldırıları önemli bir anahtar olarak kullanabileceği görülmektedir (Maness ve Valeriano, 2015:148). Ayrıca Estonya'da yaşananların normal bir siber suçtan farklı ve fazlası olduğu dikkate alındığında ceza hukukunun kapsamının genişlemesi gerektiği (siber saldırıların sıklığının artması ve bu tür saldırıların artan internet erişimi ve kullanımı nedeniyle daha tehlikeli hale gelmesi sebebiyle cezaların arttırılması gibi) ve ortak bir siber güvenlik stratejisinin benimsenmesinin önemi ortaya çıkmıştır. Yaşananların endişe verici gerçekliği, içinde bulunduğumuz bilgi çağında, bilgisayar meraklılarının artık ulus devletlerin egemenliğini ve refahını, çoğu zaman kendi konforlarını bozmadan tehdit edebileceğidir (Herzog, 2011:54; Tikk vd., 2010:28-29).

3.2.2. Gürcistan Savaşı

Sovyetler Birliği'nin yıkılmasının ardından bağımsızlığını yeniden kazanan Gürcistan, Sovyet ardılı diğer komşularından bazılarının aksine uzun bir tarihe ve güçlü bir ulusal bilince sahip olması noktasında öne çıkmaktadır. 1990'lı yılların başından itibaren Batı ile entegrasyon arayışına giren Gürcistan; 2003 yılından sonra Gül Devrimi ortaya çıktıktan ve dönemin devlet başkanı Eduard Shevardnadze devrildikten sonra entegrasyon çabalarını güçlendirmiştir. Yeni seçilen devlet başkanı Mihail Saakashvili, batı kurumlarıyla ve ayrıca Güney Osetya ve Abhazya gibi ayrılıkçı Gürcü eyaletleriyle bütünleşme çabalarına hız vermiştir. Ancak bütün bu girişimler, Rusya tarafında 2008 yılında savaşa varacak derecede güçlü bir tepki yaratmıştır (Kozlowski, 2013:238).

Yaşananlar mikro ölçekte incelendiğinde savaşa varan bu çözümsüzlüğün coğrafi ve yasal arka planını tanımlayan ve temellendiren iki sorunun varlığından söz edilebilir. Bunlar Gürcü kuvvetleri ve Güney Osetya arasında artan gerilimin varlığı ve 1992 yılında başlayan, bölgedeki barış gücünün hukuki statüsünün geliştirilmesidir. Gürcistan'ın; Türkiye ve Azerbaycan ile olan stratejik sınırları, kilit altyapı yolları ve Karadeniz'e erişimi gibi sahip olduğu coğrafi artıları sebebiyle Rus ilgisi bu ülkeye karşı yüksek olmuştur. Gürcü milliyetçiliğinin arttığı o yıllarda rejimin etnik azınlıklara sergilediği ayrımcı davranışlar sebebiyle Ağustos 1990'da Güney Osetya bağımsızlığını ilan etmiş, Aralık 1990'da seçimleri kazanan Zviad Gamsakhurdia'nın koalisyonu

iktidara gelerek Güney Osetya'nın özerk bir yer olarak statüsünü kaldırmıştır. Artan bu gerilim sonucu Ocak 1991'de Gürcistan güçleri Güney Osetya'nın başkenti Tskhinvali'ye girmiş, bir tarafta Gürcü devlet güçleri, diğer taraftan Güney Osetya ayrılıkçı güçleri ve bir tarafta da Kuzey Osetya'nın (fiilen Rus toprağı olduğu için Rusya) dâhil olduğu bir iç savaş ortaya çıkmıştır. Haziran 1992'de Gürcistan devlet başkanı Eduard Shevardnadze ve Rusya devlet başkanı Boris Yeltsin bir araya gelerek ateşkes imzalamış ve Haziran 1992 tarihinde *Gürcistan-Osetya Çatışmasının Çözümüne İlişkin Soçi Anlaşması* imzalanmıştır. Bu anlaşmayla birlikte ateşkes ilan edilmiş, milis güçler dağıtılmış ve iki tarafı birbirinden ayıran bir koridor oluşturulmuştur (Thomas, 2009:36-37).

Sayısız barış çabasına ve ateşkese rağmen bölgedeki gerilim düşmemiş, istikrar sağlamak için 1992 yılında Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) bünyesinde bir barış koruma gücü oluşturulmuş; bu gücün yönetiminde yaşanan problemler de yukarıda bahsedilen çözümsüzlüğün temelini oluşturan ikinci sorunun varlığına yol açmıştır. Barış koruma gücü, Rus komutanın liderliğinde Rus, Gürcü ve Güney Osetya birliklerinden oluşturulmuştur. Zaman geçtikçe Rusya'nın tarafsızlığının Güney Osetya lehine bozulmaya başladığı görüşü yayılmış ayrıca Güney Osetya ve Gürcü barış koruma birliklerinin sayıları azalırken Rus birliklerin sayıları aynı kalmıştır. Birkaç yıl barış koruma gücü olayları kontrol altında tutabilmişse de zaman geçtikçe tansiyon yükselmiş ve ayrılıkçı güçlerin provokasyonları artmıştır. Nihayetinde 7 Ağustos 2008'de kırılma noktasına ulaşan olaylar sonucu Gürcü kuvvetleri ayrılıkçı güçlere sürpriz bir saldırı başlatmış ve Güney Osetya'yı işgal etmiştir. Rusya Federasyonu ise *yurtdışındaki Rus vatandaşlarını koruma* konusundaki ulusal yükümlülüklere atıfta bulunarak 8 Ağustos'ta Gürcistan'a yanıt vermiş, yanı sıra siber savaşçılarını da denkleme dâhil etmiş ve böylece 8.8.2008 savaşı başlamıştır (Tikk vd., 2010:67-68; Thomas, 2009:38).

21. yüzyılda unutulmuş gibi görünen klasik devletin devlete karşı savaşının hatırlatıcısı olan bu olayda, orduların savaş alanındaki davranışları geçmişi hatırlatsa da bir yönü tam anlamıyla bir yeniliği yansıtmıştır. Bu yenilik savaşın artık yalnızca karada, havada, denizde, uzayda değil; siber uzayda da gerçekleşebileceğidir (Kozlowski, 2013:238). Tablo 10'da görüldüğü gibi siber saldırılar sıcak çatışmanın başlamasından günler önce gözlemlenmeye başlamış; 8 Ağustos'ta ise Rusya'nın konvansiyonel müdahalesiyle eş zamanlı şekilde zirve noktasına ulaşmıştır. Aynı zamanda siber saldırılar Rid (2012:13) tarafından ifade edildiği gibi, konvansiyonel bir operasyonla eş zamanlı olarak gerçekleştirilen ilk siber saldırı olma özelliği taşımaktadır. Gürcistan'a yönelen siber saldırılar genel itibariyle Devlet Başkanlığı, Dışişleri Bakanlığı ve Gürcistan Ulusal Bankası gibi ülkenin önde gelen kamu web sitelerinin tahrif edilmesi, devlet bağlantılı web sitelerinin yanı sıra medya, özel sektör gibi farklı alanlara yönelik DDoS saldırıları ve siber saldırganların sayılarını ve

etki alanlarını arttırmak için çeşitli Rus forumlarında (StopGeorgia.ru[33] gibi) kötü amaçlı yazılım yayımlaması aşamalarından oluşmuştur.

Tablo 10: Gürcistan Savaşı'nda Siber Saldırı Zaman Çizelgesi

19/07/2008	Gürcistan Devlet Başkanı Mihail Saakashvili'nin web sitesi (president.gov.ge) DDoS saldırısı sebebiyle 24 saatten fazla kullanılamaz duruma gelmiştir.
8/08/2008	8 Ağustos'ta birden fazla komut ve kontrol sunucusu Gürcistan web sitelerine (Gürcistan Başkanı, Merkezi Hükümet, Dışişleri ve Savunma Bakanlıklarının ana sayfaları gibi) ve Gürcistan'ın davasına sempati duyan (Georgia Online, News.ge gibi haber siteleri web sitelerine) siber saldırı düzenlenmiştir. 9 Ağustos'ta Gürcistan'ın en büyük ticari bankası olan TBC saldırıya uğramıştır.
10/08/2008	İçinde Gürcistan Parlamentosu ve bazı sivil toplum kuruluşlarının da bulunduğu *.ge.* uzantılı web sitelerine yönelik yeni saldırılar düzenlenmiştir. Saldırıların yöneldiği IP adresinin Türkiye kaynaklı olduğu ortaya konulmuştur.
11/08/2008	Saakashvili'nin web sitesi yeniden erişime açık hale getirilmiştir. Ancak, Saakashvili'yi Hitler olarak tasvir eden görüntüler yayımlanarak site tahrif edilmeye devam edilmiştir. Ayrıca Merkezi Hükümet, Dışişleri ve Savunma Bakanlıklarının ana sayfaları bu süreçte çevrimdışı kalmaya devam etmiştir. Gürcistan Dışişleri Google'ın sunucusu *blogspot.com* aracılığıyla bir basın açıklaması yayımlamıştır.[34] Gürcistan'ın en büyük İngilizce haber sitesi *Civil.ge* de blog üzerinden yayım yapmaya devam etmiştir.
12/08/2008	12 Ağustos itibariyle *.ge* uzantılı sitelere yönelen botnet saldırılarının çoğu azalmaya başlamış ve saldırı modeli de değişmiştir. 13 Ağustos'ta ise çok sayıda Rus kaynaklı internet servis sağlayıcısından gelen ve Gürcistan Hükümeti web sitelerini hedefleyen hata mesajları bildirilmiştir.
27/08/2008	Gürcü web sitelerine yönelik son büyük saldırı 27 Ağustos'ta başlamıştır. Bu kez DDoS saldırısı şeklinde Gürcistan Dışişleri Bakanlığı ve bağlı siteler ana hedef konumuna koyulmuştur. 28 Ağustos'ta saldırılar yavaşlamaya başlamış ancak bu tarihten sonra bile düzenli trafikten ayırt edilemeyen olaylar tespit edilmiştir.

Kaynak: Tikk vd., 2010:69-71

[33] StopGeorgia.ru, Rusya tarafından Gürcistan'a yönelik kara, deniz ve hava saldırılarının başlamasından sonra geçen 24 saat içinde aktif hale gelen şifre korumalı bir forumdur. Burada her seviyeden bilgisayar korsanına yönelik hedef listeleri, Gürcü hükümetinin web sitelerine saldırmak için kullanılacak kötü amaçlı yazılımlar ve bu yazılımlara bağlantılar ve acemi bilgisayar korsanları için uzmanlardan gelen tavsiyeler paylaşılmaktadır (Carr, 2012:106). Örneğin 13 Ağustos'ta, Güney Osetya'daki kurbanlar için yas ilan edilen bu günde, forumda bir hedef listesi yayımlanarak her düzeyden siber korsana bu listedeki adreslere saldırı yapılması için çağrıda bulunulmuştur (Rios vd., 2009:37).

[34] Yapılan açıklamada Rusya'nın bir siber saldırı başlatarak başta Dışişleri Bakanlığı'nın olmak üzere birçok web sitesine ciddi zararlar verdiği ifade edilmiştir (Cyber Attacks Disable Georgian Websites (11.08.2008), http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html).

Gürcistan'a yönelik siber saldırılar, Gürcistan yönetimine ve toplumuna bilgi akışını kesmeyi amaçlayan bir bilgi savaşanın yansıması olmuştur. Çünkü siber saldırganlar, Rus işgali sonrasında kendi devleti ve toplumu üzerinde kontrolünü kaybettiğini düşündükleri Saakashvili rejiminin kırılganlığını dünyaya göstermeyi amaçlamış; bir yandan da morallerini ve hükümete olan inançlarını sarsmak ve kendi propagandalarını yapabilmek için Gürcistan toplumunun bilgiye erişimini keserek yanlış bilgi verebileceklerini ve kamuoyunu şekillendirebileceklerini düşünmüşlerdir. Ancak siber korsanlar, hükümet web sitelerinin hızlı restorasyonu ve Google gibi şirketlerin desteği sayesinde bu amaçlarına tam anlamıyla ulaşamamıştır (Kozlowski, 2013:239).

Estonya saldırılarıyla kıyaslandığında, Gürcistan'ın bilgi teknolojileri altyapısının daha az gelişmiş olması nedeniyle yaşanan hizmet aksamalarının da karmaşıklığı düşük kalmıştır. Ayrıca Gürcistan saldırılarının bir diğer farkı da botnet kullanılarak etkisi arttırılan DDoS saldırılarının yanı sıra, tanımlanması daha zor olan ve bir botnet saldırısına göre daha az bilgisayar gerektiren Yapısal Sorgulama Dili (SQL)[35] enjeksiyon saldırılarını da içermesidir. Bu açıdan da Estonya saldırılarına kıyasla daha yüksek bir uzmanlık gösterdiği söylenebilir (Ashmore, 2009:10-11).

Estonya saldırılarıyla benzer yönü ise, saldırıların sponsorluğundan Kremlin'in sorumlu tutulması olmuştur. Ancak Rusya bir kez daha saldırıların sorumluluğunu üstlenmeyi reddetmiştir. NATO tarafından Gürcistan saldırılarıyla ilgili yayımlanan raporda da saldırıların eşgüdümlü ve talimatlı görünmesine ve medyadaki tüm işaretlerin Rusya'yı göstermesine rağmen, Estonya'da olduğu gibi, DDoS saldırılarının arkasında kimin olduğuna dair kesin bir kanıt olmadığı sonucuna varılmıştır (Rid, 2012:14). Ancak gönüllü bir kuruluş olan Project Grey Goose uzmanları tarafından hazırlanan raporda *"önceden hazırlık ve keşif seviyesi incelendiğinde, Rus bilgisayar korsanlarının, Rus hükümeti ve/veya ordudaki yetkililer tarafından saldırıya hazırlandığı güçlü bir şekilde görülüyor"* şeklindeki açıklamaları bir gerçeği ortaya koymaktadır (Krebs, 2008).

Ayrıca Ekonomist tarafından dünyanın en önde gelen siber suç örgütü ve NATO tarafından ise büyük bir tehdit olarak tanımlanan Rus İş Ağı (Russian Business Network/RBN) Gürcistan'a yönelik saldırıları kolaylaştırmakla suçlanmıştır. RBN başkanı Flyman'ın St.Petersburg'lu üst düzey bir politikacının akrabası olduğu iddiaları, örgütün internet ağlarının kapatılmaması ve üyelerinin hiçbirinin Rus yetkililer tarafından tutuklanmaması ayrıca doğrudan bir kanıt oluşturmasa da siber korsanların RBN tarafından kullanılan araçlar ve saldırı komutlarının aynısını kullanmaları ve bazı saldırıların RBN tarafından kontrol edildiği bilinen bilgisayarlardan başlaması Gürcistan'a yönelik siber saldırılardaki Rus bağlantısı iddialarını güçlendirmiştir (Markoff, 2008; Klimburg, 2001:49-50). Ayrıca saldırıları analiz eden farklı uzmanlar, siber alanda düşmanca

[35] SQL, *"ilişkisel veri tabanlarıyla etkileşim kurmak için kullanılan yapısal bir dildir"* (Anley, 2002:3). Veri tabanı şeması oluşturma ve değiştirme, verilerin alınması ve yönetimi için tasarlanmıştır. SQL enjeksiyon ise, *"bir uygulamanın veri tabanı katmanında oluşan bir güvenlik açığından yararlanan bir kod enjeksiyon tekniğidir"* (Tikk vd., 2010:114).

eylemler gerçekleştirme konusunda uzmanlığı temsil eden RBN teknisyeni Alexandr A. Boykov ve Andrey Smirnov'un Gürcistan'a yönelik saldırıların failleri olabileceğini belirtmiştir (Kozlowski, 2013:239).

Sonuç olarak 2008 yılında Gürcistan'da yaşananlar, hibrit savaş özelliği gösteren bir çatışma olarak literatürde yerini almıştır. Hibrit savaş özelliği taşımasında konvansiyonel vuruşların ve siber saldırıların koordinasyonunun payı büyüktür. Medya ve iletişim tesisleri konvansiyonel vuruşların listesine dâhil edilmemiş; siber saldırılara bırakılmıştır. Ayrıca, Gürcistan ve Estonya'da yaşananlardan elde ettiği tecrübeler ile birlikte Rusya, 2009 yılında hibrit savaş niteliği taşıyan yeni stratejisi, *Gerasimov Doktrini'ni* ilan etmiş ve 2014 yılında yaşanan Ukrayna krizinde tüm yönleriyle uygulamaya koyabilmiştir (Darıcılı, 2014:8; Kozlowski, 2013:239). Gürcistan'da yaşananlarla ilgili dikkat çeken bir başka detay ise, Gürcistan'ın o dönemde NATO üyesi olma isteğine rağmen henüz üyeliğin gerçekleşmemesi sebebiyle koruma şemsiyesi altına girememiş olmasıdır. Yine de saldırıların ardından CDMA bünyesinde bir uzman bölgeye gitmiş ve incelemelerde bulunmuştur (Bıçakçı, 2014:122-123).

3.2.3. Rusya'nın Ukrayna Müdahalesi

2013 yılının Kasım ayında, dönemin devlet başkanı Viktor Yanukovich tarafından AB ile ortaklık müzakerelerine devam edilmeyeceğinin açıklanmasının ardından başlayan, Batı yanlısı protestolar ve ayaklanmalarla hız kazanan; 2014 yılının Şubat ayında Yanukovich'in yönetimden uzaklaştırılması ve ardından Rusya'nın Kırım'ı ilhakı birlikte boyut atlayan Ukrayna Krizi, daha önce bahsedilen hibrit savaş konseptinin başarılı uygulamasının bir örneğini teşkil etmektedir (Karabulut, 2016:34).

Aslında Ukrayna'ya yönelik bilgi savaşı amaçlı siber saldırılar krizden çok daha önce başlamıştır. Ukrayna Güvenlik Servisi (SBU) hükümet yetkililerini 2010 yılından beri Rus casus yazılımlarının (Snake, Uroboros ya da Turla olarak bilinen) hedefi oldukları konusunda uyarmıştır (Jaitner, 2015:90). Ancak Kırım ve esas olarak Rusya ile ilişkilendirilen saldırılar Şubat 2014'te başlamış ve Aralık 2018'e kadar boyut ve şekil değiştirerek devam etmiştir. Şubat 2014'te, Yanukovich'in ülkeyi terk etmesinden bir süre sonra, Kırım'daki Sevastopol ve Simferopol uluslararası havaalanlarında bir askeri bölge, daha sonra Vladimir Putin tarafından Rus birlikleri olduğu kabul edilen askerler tarafından ele geçirilmiştir. Eş zamanlı olarak silahlı askerler, Ukraynalı telekom şirketi UKRTelecom tesislerine baskın yaparak fiber optik kabloları hedef almışlardır. Bu yolla şirkete, hem yarımadada hem de yarımada ile Ukrayna'nın geri kalanı arasında iletişim ve internet bağlantı sağlama teknik kapasitesini kaybettirmek amaçlanmıştır (Maurer ve Janz, 2014). Ardından SBU şefi Valenty Nalyvaichenko tarafından yapılan açıklamada ise üst üste iki gün boyunca Ukrayna Parlamentosu üyelerinin cep telefonlarına siber saldırılar düzenlendiği ifade edilmiştir (Lee, 2014).

Rus birliklerinin 2 Martta Kırım'a girmesiyle birlikte Ukrayna devlet web sitesi (www.kmu.gov.ua) 72 saat boyunca erişime kapatılmıştır. *Cyber Hundred* ve *Null Sector* gibi bazı Ukrayna hacker grupları ise, yaşananlardan sorumlu tuttukları Rusya'nın Kremlin ve Merkez Bankası web sitelerine karşı DDoS saldırı başlatarak misilleme yapmıştır (Maurer ve Janz, 2014). Bunun yanı sıra, Rusya'nın en büyük haber kanallarından biri olan Russia Today kanalının da web sitesi hacklenmiş ve sitedeki *Rusya* kelimeleri *Nazi* kelimesi ile değiştirilmiştir (İkinci cephe siber savaş (15.03.2014), https://www.yenisafak.com/dunya/ikinci-cephe-siber-savas-626007). 3 Mart'ta Ukrayna Bağımsız Haber Ajansı bir dizi DDoS saldırısının hedefi olduğunu ve saldırıların geçici olarak çevrimdışı olmasına neden olduğunu açıklamıştır (Foxall, 2016:4).

İlerleyen günlerde Ukrayna Ulusal Güvenlik ve Savunma Konseyi, Kırım Yüksek Konseyi ve Kırım bağımsızlık referandum web siteleri de aynı saldırıların hedefi olmuştur (Foxall, 2016:4). Bu saldırılardan biri 22 Mayıs 2014 tarihinde Ukrayna'da cumhurbaşkanlığı seçiminden üç gün önce Seçim Komisyonuna yönelik gerçekleştirilmiştir. Rus yanlısı adaya yardım etmek ve Ukraynalı adayı yıpratmak için yapılan bu saldırıda, Ukraynalı uzmanlar seçim gününe kadar sistemi düzeltmeyi başarmış ve saldırganlar da polis tarafından yakalanmıştır (Windrem, 2016). Rus bilgisayar korsanları 24 Mayıs 2014 tarihinde ise bu kez Merkez Seçim Komisyonu sunucusuna bir dizi siber saldırı düzenlemiştir. Sonuçları görüntülemek için kullanılan sayfanın bir benzerini oluşturan bilgisayar korsanları, seçimlerin bittiği saat olan 20.00'dan sonra görüntülenecek, aşırı sağcı ve Rus karşıtı bir aday olan Dmytro Yarosh'un seçimi kazandığını gösteren bir grafik oluşturmuşlardır. Esasından Yarosh oyların %1'inden daha azını alabilmiştir. Rusya ise bu saldırıyla Ukrayna'nın sert hatta faşist figürlerle yönetildiği propagandası yaymaya çalışmış ancak saldırı Ukrayna siber güvenlik şirketi InfoSafe tarafından engellenmiştir (Kramer ve Higgins, 2017).

Kendilerine *Cyberberkut* adını veren Rus yanlısı bir hacker grubu Ukrayna, AB ve ABD'li yetkililer arasındaki telefon kayıtlarına ve e-posta yazışmalarına eriştiğini iddia etmiş ve bunu kanıtlamak için bazı içerikleri yayımlamıştır. Aynı zamanda bu grup birçok NATO web sitesini tahrif etmiştir (Jaitner, 2015:91). Dönemin NATO sözcüsü Oana Lungescu ise yaptığı açıklamada, saldırıların NATO sistemlerinin bütünlüğünü etkilemediğini belirterek *"cumartesi akşamı başlayıp pazar gününe kadar devam eden saldırılar sonucu zarar gören sistemlerin onarıldığını"* ifade etmiştir (Spiegel, 2014). 27 Haziran 2017 tarihinde gerçekleşen bir başka siber saldırıda ise Ukrayna'daki finans ve enerji sektörleri hedef alınmış ancak saldırı ülkedeki diğer Avrupa ve Rus işletmelerini de etkileyerek yayılmıştır. Ukrayna'ya yönelik diğer bir saldırı ise 24 Ekim 2017 tarihinde *BadRabbit* fidye yazılım kullanılarak gerçekleştirilmiş, başkent Kiev'deki metro hattı ve Odessa Havalimanı işletim sistemleri etkilenmiştir. İki saldırının da arka planında Rusya'nın olduğu öne sürülmüştür (Batchelor, 2018). Ayrıca Ukrayna'da başkan yardımcılığı görevini yürütmüş olan Dmytro Shymkiv'in 2017 yılında verdiği bir röportajda Ukrayna'ya karşı

gerçekleştirilen siber saldırıların %99 oranında Rusya bağlantılı olduğunu ifade etmesi de iddiaları destekler niteliktedir (Timtchenko, 2017).

2018 yılına gelindiğinde saldırılar kesilmemiş, Haziran ayında siber polis şefi Seghiy Demedyuk yaptığı açıklamada Rus bilgisayar korsanlarının Ukrayna'daki bankalar ve enerji altyapı şirketleri de dâhil olmak üzere birçok şirkete kötücül yazılım yerleştirme amaçlı saldırılar yapıldığını açıklamıştır (Polityuk, 2018). Demedyuk'un Ağustos ayında yaptığı başka bir açıklamada ise SBU ile ortak hareket ederek, Rusya kaynaklı birçok siber saldırı kaydedildiğini ve engellendiği ifade edilmiştir (UNIAN: Ukraine's cyber police report constant cyberattacks from Russia, (12.082018), https://www.kyivpost.com/ukraine-politics/unian-ukraines-cyber-police-report-constant-cyberattacks-from-russia.html). 8 Ekim akşam saatlerinde başlayıp 9 Ekim 2018'e kadar devam eden bir dizi DoS saldırısı ile Ukrayna maliye sistemi hedef alınmış; bu süreçte kullanıcılar kişisel hesaplarına ve mali servisin web sitesine erişememiştir. Ukrayna Ulusal Güvenlik Servisi yaptığı açıklamayla Ocak 2018'den itibaren ülkedeki tesislere ve veri tabanlarına 35 siber saldırı gerçekleştiğini belirtmiştir (Zubkova, 2018).

2019 yılında gerçekleştirilen cumhurbaşkanlığı seçimlerinde de 2014 yılında olduğu gibi, Rusya kaynaklı siber saldırılar beklenmiştir. Ukrayna Ulusal Güvenlik Servisi'nden Aleksandr Klimcuk yapılması planlanan dezenformasyon ve siber saldırılara gerekli cevabın verileceğini ifade etmiştir. Ukrayna İçişleri Bakanı Arsen Avakov beklenen siber tehditlerle ilgili *"son iki gündür bu durumu aktif bir şekilde gözlemliyoruz. Kiev ve Rusya'daki bazı internet adreslerinden merkezi seçim sistemimize erişim sağlama girişimlerinin yaşandığını görüyoruz; ancak uzmanlarımız sistemimizi çok iyi koruyor, müdahale girişimlerini takip ediyor ve engelliyorlar"* şeklindeki açıklamasıyla saldırı beklentisini doğrulamıştır (Üret, 2019). 2020 yılında Rus istihbarat örgütü Glavnoye Razvedyvatel'noye Upravleniye (GRU) tarafından gerçekleştirildiği iddia edilen son saldırıda ise ABD eski Başkan Yardımcısı Joe Biden'ın oğlu Hunter Biden'ın da bir dönem yönetim kurulunda bulunduğu Ukraynalı *Burisma* enerji şirketi hedef alınmış ve çalışanların e-posta şifreleri ele geçirilmiştir. Ancak esas hedefin niteliği ve ele geçirilen bilgilerin içeriği hakkında kesin bir görüş ortaya konmamıştır (Rusya Ukrayna Skandalının Kilit Şirketine Siber Saldırı Düzenledi (14.01.2020), https://www.amerikaninsesi.com/a/rusya-ukrayna-skandal%C4%B1n%C4%B1n-kilit-%C5%9Firketine-siber-operasyon-d%C3%BCzenledi-/5245207.html).

Rusya tarafından geldiği iddia edilen, örnekleri aktarılan karmaşık siber saldırılara rağmen daha önce Estonya'da yaşananlar gibi kritik altyapıları tamamen işlevsiz hale getirmeyi hedefleyen

büyük çaplı siber saldırılar yoğun olarak gözlenmemiştir.[36] Aslında örneğin Ukrayna Telekom altyapısının büyük bölümü, Sovyetler Birliği'nin parçası olduğu bir dönemde inşa edilmiş ve bu yüzden günümüzde Rus etkisine karşı da savunmasız kalmıştır. Bu açıdan, genel olarak iletişim ve internet sistemine zarar verilmiş ancak birçok uzmanın ifade ettiği gibi[37] Rusya siber saldırılarda etkiyi sınırlı tutmayı seçmiştir (Polityuk ve Finkle, 2014).

Etkinin sınırlı olmasının ikinci bir sebebi de, yukarıda da bahsedildiği gibi, Ukrayna'da yaşananların başlı başına bir siber savaş olmasından ziyade Rusların, Ukraynalıların ve uluslararası kamuoyunun gelişen olayları algılama şekillerini de etkilemeye çalışan bilgi savaşının bir tezahürü olmasıdır. Şöyle ki hem ulusal hem uluslararası kamuoyunu etkileme temelli hareket edilmiş ve bu yöntem başarılı olmuş gibi gözükmektedir. Tercih edilen bu yöntemin başarısı ise iki örnekle ortaya konulabilir. Birincisi, olayların devam ettiği 2014 yılında Levada Araştırma Merkezi tarafından yapılan bir anket, Rus katılımcıların % 69 oranında Rus medyasının Ukrayna'daki krizi nesnel bir şekilde ortaya koyduğuna inandığını göstermektedir (Blank, 2017:91). İkincisi, 2015 yılında Pew Research Center tarafından yapılan bir ankette ise Rusların Ukrayna'daki çatışma için %50 oranında Batı'yı suçladığını ortaya çıkarmıştır (Poushter, 2015).

Sonuç olarak Rusya'nın yaşanan krizi siber saldırılar yoluyla propaganda, dezenformasyon ve bilgi savaşına dönüştürdüğü Ukrayna krizi, Rusya'nın beşinci harekat alanından bir sapması olarak okunmamalıdır. Aksine Ukrayna'ya karşı girişilen hibrit savaş, Kremlin'in bilgi savaşına en az konvansiyonel savaş kadar önem verdiğini göstermiştir. Ayrıca uygulanan bilgi savaşı; elektronik, psikolojik ve siber savaşın birleşimi şeklinde ortaya çıkmıştır (Foxall, 2016:4). Bir bilgi savaşının başarısını ölçmek çok kolay değildir ancak dezenformasyon temelli siber saldırıların Kırım'da yaşananlar konusunda hem Kiev hem de uluslararası toplumun net bir resim oluşturmasını zorlaştırdığı ve bu yolla karar verme süreçlerinde kesintiler yaşattığı söylenebilir. Sofistike olmayan siber saldırıların bile medyanın her daim dikkatini çektiği bir durumda, bu saldırıların aynı zamanda sistemlerde ve güvenlik mimarilerinde genel güvensizlik yaratmaları operasyonel siber savaşın önemini bir kat daha arttırmaktadır (Jaitner, 2015:91).

[36] Bunun bir istisnası 23 Aralık 2015'de Rusya tarafından gerçekleştirildiği iddia edilen ve Ukrayna'daki bir enerji şirketinin üç ayrı dağıtım merkezini hedef alan bir saldırıdır. Uzaktan erişim kullanarak dağıtım merkezlerini çevrim dışı hale getiren saldırganlar 220.000'den fazla Ukraynalının kesintiden etkilenmesine neden olmuştur (Vogler ve Connell, 2017:20). Ayrıca bu olay ABD İç Güvenlik Bakanlığı tarafından da onaylanmış ve böylece bir bilgisayar virüsünün elektrik kesintisine sebep olduğu ilk kez ABD hükümeti tarafından da kabul edilmiştir (U.S. government concludes cyber attack caused Ukraine power outage (26.02.2016), https://www.itsecurityguru.org/2016/02/26/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage/). Elektrik şebekesine yönelik diğer bir saldırı ise 17/18 Aralık 2016 tarihinde gerçekleşmiş ve Kiev'in kuzeyinde elektrik kesintisi oluşturan bir siber saldırı Kiev elektrik şebekesini vurmuştur (Polityuk, 2016).

[37] CIA eski kıdemli yönetim subayı Marty Martin yaptığı açıklamada Moskova'nın sadece Ukrayna'nın internet ve iç iletişim sistemine zarar vereceğini düşündüğünü belirtmiş sebebini ise "*istihbarat akışından yaralanmak için bir şeyleri tamamen kapatmak yerine izlemek daha iyi olur"* şeklinde açıklamıştır. Washington'daki Stratejik ve Uluslararası Araştırmalar Merkezi'nde akademisyen Jim Lewis ise, Ukrayna'daki trafiğin çoğunun Rusya üzerinden geçtiğini belirtmiş ve daha fazlasını yapmamalarının sebebini *"muhtemelen karlı çıkacaklarını dair güvenleri var ve bu konuda kimsenin yapabileceği bir şey yok"* sözleriyle ifade etmiştir (Polityuk ve Finkle, 2014).

3.2.4. Stuxnet

Stuxnet, geleneksel bir sabotaj casusluk girişiminin; yüksek düzeyde teknik beceri, yetenek, planlama, fonlama gibi özelliklerini bünyesinde barındıran ve bu özelliklerin, bugüne kadarki tüm siber olayların ötesine geçen bir etki üretmek için araya gelmesini sağlayan bir operasyondur. Operasyona ismini veren Stuxnet solucanının, 2006 yılında ABD'de *Olympic Games (Olimpiyat Oyunları)*[38] adıyla başlatılan ve önce George W. Bush; ardından B. Obama yönetimi tarafından devam eden, İran'ın uranyum zenginleştirmesini sekteye uğratmayı amaçlayan ve toplam maliyetinin 300 milyon dolar olduğu tahmin edilen, uzun soluklu bir programın ürünü olduğu iddia edilmektedir (Maness ve Valeriano, 2015:151-152).

Kimi uzmanlara göre *bugüne kadar hedeflenmiş bir saldırı için geliştirilen, teknolojik olarak en gelişmiş kötü amaçlı yazılım* (Matrosov vd., 2010:70); kimilerine göre de *hassas, askeri düzeyde bir siber füze* (Clayton, 2010) olan Stuxnet solucanının teknik özellikleri incelendiğinde, uzak erişim bilgisayar sistemlerine yarı-özerk bir şekilde nüfuz/etki ve kontrol etmek için tasarlanmış, karmaşık bir bilgisayar programı olduğu görülmektedir. Siber uzaydaki seçilmiş hedeflere karşı kullanılabilecek olan *ateşle-unut* özellikli kötü amaçlı yazılımların en bilindik temsilcisi olan Stuxnet solucanı, tecrit edilmiş/kapalı sistemlere; daha açık bir ifadeyle genel kullanıma açık internete bağlı olmayan sistemlere, etki etmek için USB bellek gibi aracı cihazların kullanımını gerektirmiştir. Stuxnet solucanı dört adet *sıfır gün (zero day)* güvenlik açığı kullanmakta ayrıca Siemens yazılımı için güvenlik açığı içermektedir. Örneğin bu açıkların keşfedilenlerinden biri olan MS10-046 (Naraine, 2010), uzaktan kod yürütülmesine izin veren bir açıklıktır (Farwell ve Rohozinski, 2011:24).

Stuxnet diğer zararlı yazılımlara nazaran daha karmaşık bir kod ve daha büyük bir boyut içermektedir. Ayrıca birden çok programlama dilinden oluşturulmuştur. İkinci olarak kimlik doğrulama için JMicron ve Realtek firmalarından çalınan iki sertifika tarafından dijital olarak imzalanmıştır. Üçüncü olarak Stuxnet solucanı, sistemlere başarıyla bulaştıktan sonra sistem içinde kendini gizlemek için bir kök kullanıcı takımı kurmuş ve Malezya ve Danimarka'daki komut ve kontrol sunucularına bağlanmaya çalışmıştır (Chen, 2010:3). Tablo 11; *1) Hedefleme, 2) Hedef*

[38] Olmypic Games (Olimpiyat Oyunları) iddialara göre ABD Ulusal Güvenlik Ajansı (NSA), CIA, İsrail gizli servisi (MOSSAD), İsrail Savunma Bakanlığı ve İsrail SIGINT Ulusal Birimi tarafından yürütülen ortak bir ABD-İsrail projesidir. Ancak süreç içinde ABD ve İsrail'in Hollanda, Almanya ve Fransa olduğu düşünülen üç ülkeden daha yardım alması sembolü beş halka olan olimpiyat oyunlarının kod adı olarak seçilmesinin temelini oluşturmuştur. Nükleer tesislerde kullanılan Alman Siemens marka sistemler nedeniyle Almanya ve Fransa'nın teknik bilgi şeklinde istihbarat sağladığı düşünülürken; Hollanda için durum biraz daha farklıdır. Çünkü Natanz'da kullanılan santrifüjlerin tasarımının 1970'lerde Hollandalı bir firmadan çalınan tasarımlara dayandığı iddia edilmektedir. Pakistanlı bir bilim insanı olan Abdul Qader Khan tarafından Pakistan'ın nükleer programını oluşturmak için çalınan bilgiler daha sonra İran ve Libya dâhil diğer ülkelere satılmıştır. Bu sebepten iddialara göre Hollanda istihbaratı, İran'ın nükleer programının oluşturulmasında rol oynayan Avrupalı danışmanlar ve paravan şirketlerin tedarik ağına ve İran savunma teşkilatının e-posta sistemine sızmıştır (Zetter, 2019).

Tipi, 3) Boyut, 4) Zayıflık, 5) Kimlik Doğrulama gibi farklı boyutlarla Stuxnet ve daha önce karşılaşılan diğer zararlı yazılımlar arasındaki farkları ortaya koymaktadır.

Tablo 11: Stuxnet ve Diğer Zararlı Yazılımlar Arasındaki Farklar

İşlev	Stuxnet	Diğer Zararlı Yazılımlar
Hedefleme	Son derece seçici	Rasgele/Ayırt edilmeyen
Hedef Tipi	SCADA/ICSs	Bilgisayarlar
Boyut	500 Kb	500 Kb'tan az
Zayıflık	Dört sıfır-gün açığı	Bir sıfır-gün açığı
Kimlik Doğrulama	Geçerli sertifikalar (çalıntı)	Sahte

Kaynak: Collins ve McCombie, 2012:86

Stuxnet, en temel açıklamasıyla, İran'ın nükleer programında kullandığı santrifüjleri, SCADA[39] olarak isimlendirilen sistemlere sızma aracılığıyla yok etmek için tasarlanmıştır. Stuxnet solucanının SCADA sistemindeki özel hedefi, *Programlanabilir Lojik Kontrolörler (PLC)* olmuştur. Anahtarlar, röleler ve zamanlayıcı/sayıcılar gibi elektrikli donanım tarafından icra edilen işlevleri kontrol eden küçük bilgisayarlar olan PLC'ler içinde; Stuxnet solucanının tutunmaya çalıştığı PLC ise uranyum zenginleştirilmesinde kullanılan santrifüjleri kontrol edenler olmuştur (Collins ve McCombie, 2012:84).

PLC'leri programlamak için ise yöneticinin, cihazı standart bir Windows bilgisayara bağlaması ve kullanıma hazır hale getirmesi gerekmektedir. Bu nedenle, örneğin, santrifüjlerin hızı arttırılacaksa PLC, kendisiyle iletişim kuran ve yeni talimatlar yükleyen bir yazılım parçası çalıştıran bir Windows bilgisayara bağlanması gerekir. Stuxnet virüsü, PLC'ye bağlı bilgisayara bulaştıktan sonra, sisteme karşı *ortadaki adam (man in the middle)*[40] saldırısı gerçekleştirir. Bu şekilde Stuxnet solucanı, PLC'ye başlangıçta gönderilen komutları engeller ve bunun yerine kendi talimatlarını gönderir. Bununla birlikte yazılım, talimatların yüklendiği orijinal bilgisayara, sahte olarak rapor gönderir; bu yolla Stuxnet solucanı kendini gizlemeyi başarmış ve gelecekteki işlemleri tekrarlama fırsatı elde etmiş olur. (Shakarian vd., 2013:226-227) Stuxnet solucanı, hedeflediği PLC programları olan Siemens marka SIMATIC WinCC ve Step 7 programlarını çalıştıran Windows işletim sistemlerine erişmek için ise Siemens'in varsayılan şifrelerini

[39] SCADA sistemleri, tam bir kontrol sistemi olmaktan ziyade daha çok denetim seviyesine odaklanır. Ayrıca bu sistemler sadece çelik üretimi, enerji üretimi ve dağıtımı, kimya gibi endüstriyel işlemlerde kullanılmaz; aynı zamanda nükleer füzyon gibi bazı deney tesislerinde de kullanılır (Daneeles ve Salter, 1999:339).

[40] Ortadaki adam (man in the middle) saldırısı *"oturum başlatmak üzere ya da oturumu başlamış olan kullanıcıların iletişim kurmak üzere paylaştığı paketlerin, saldırgan tarafından ele geçirilerek, trafiğin kendi üzerinden geçecek şekilde ayarlanması"* işlemidir. Bu yolla saldırgan tarafından, gerekli bilgileri elde etmenin yanı sıra sistemde değişiklik yapma şansına da erişilmiş olur (Yüksel ve Öztürk, 2017:304).

kullanmıştır. Stuxnet solucanının yeteneği, bir bilgisayar hedefini vurabilmesi ve tekrar programlayabilmesi olmuştur (Farwell ve Rohozinski, 2011:24).

Endonezya[41], Hindistan[42], Azerbaycan[43], Pakistan[44], Malezya[45] gibi başka birçok ülkedeki sunucuları etkilese de; İran'ın[46] 2003'ten beri, Stuxnet solucanının bulaşma aralığı olan 807-1,210 Hz'de çalışan PLC tipine sahip olması ise, solucanın Natanz Nükleer Tesisine özel oluşturulduğunu kanıtlar niteliktedir. Şöyle ki, IR-1 santrifüj rotorunun[47] mekanik olarak dayanabileceği maksimum hız yaklaşık 1,400 Hz'dir. Stuxnet solucanının saldırı kodu, PLC'ye 15 dakika boyunca 1,410 Hz'e (solucanın saldırı sırasında ayarladığı maksimum hız) kadar hız vermesi; daha sonra 27 gün boyunca nominal hız olan 1,064 Hz'e dönmesi; daha sonra 50 dakika boyunca 2 Hz'e kadar yavaşlaması (bu hız uranyum zenginleştirmek için çok düşüktür) ve daha sonra 27 gün boyunca 1,064 Hz'de normale dönmesi ve tüm bu diziyi süresiz olarak tekrarlaması şeklinde işlemektedir. Bu şekilde frekans sürekli değiştirilerek zenginleştirme sürecinde kesinti yaratmak amaçlanmıştır. Natanz'ın amaçlanan hedef olduğuna dair güçlü bir başka kanıt ise saldırı kodu ve Natanz Nükleer Tesisi arasındaki uyumda göze çarpmaktadır. Şöyle ki, uranyum zenginleştirme işlemini optimize edebilmek için, sistemi bir dizi faza ve her fazda çalışan birden fazla santrifüje ayırmak gerekmektedir. Tesiste 15 fazlı ve 164 santrifüjlü bir sistem kullanılmakta ve saldırı kodu Natanz Nükleer Tesisi yapılandırmasıyla tamamen eşleşen, 15 düzensiz grup olarak organize edilmiş 164 parça dizilimi tanımlamaktadır. Natanz Nükleer Tesisi'nin altyapısı ve saldırı kodu arasındaki bu uyumun tesadüf olmadığı dile getirilmektedir (Lindsay, 2013:383-384; Shakarian vd., 2013:229).

Uranyum zenginleştirme çalışmalarını bu denli etkileyen Stuxnet solucanının varlığına dair Tahran hükümetinden ise çeşitli açıklamalar kamuoyuna yansımıştır. Dönemin cumhurbaşkanı Mahmud Ahmedinejad yaptığı açıklamada, *"elektronik cihazlara kurdukları yazılımla sınırlı sayıda santrifüjümüz için sorun çıkarmakta başarılı olmuşlardır… Neyse ki uzmanlarımız sorunların köklerini keşfettiler ve bugün (İran düşmanları) bu eylemleri tekrarlayamıyorlar"* (Erdbrink, 2010) sözleriyle sistemlerinin etkilendiğini doğrulamış ancak spesifik olarak Stuxnet'in varlığını açıkça tanımlamaktan kaçınmıştır. İran Atom Enerjisi Kurumu Başkanlığı görevini de yürütmüş Ali Akbar Salehi ise İran'ın bir bilgisayar saldırısına hedef olduğunu kabul etmiş ve *"virüsü tam olarak nüfuz etmek istediği yerde keşfettik ve herhangi bir donanıma zarar vermesini engelledik"* (Erdbrink, 2010) sözleriyle Stuxnet'in varlığını doğrulamıştır. Her ne kadar Tahran

[41]45,46,47,48 ve 49. Dipnottaki veriler solucanın 2010 versiyonu (v.1.3) için geçerlidir. Solucanın enfekte olduğu sunucu yüzdesi: 17,83 (Falliere vd., 2011:6)

[42] Solucanın enfekte olduğu sunucu yüzdesi: 9,96

[43] Solucanın enfekte olduğu sunucu yüzdesi: 3,40

[44] Solucanın enfekte olduğu sunucu yüzdesi: 1,40

[45] Solucanın enfekte olduğu sunucu yüzdesi: 1,16

[46] Solucanın enfekte olduğu sunucu yüzdesi: 58,31

[47] Makinelerin dönen bölümünü ifade etmektedir.

hükümeti 2010 yılının sonlarında solucanın nükleer programları üzerinde minimum etkisi olduğunu iddia etse de güvenlik uzmanı Ralph Langer, casus yazılımdan dolayı İran'ın nükleer programının tekrar yoluna girmesinin iki yıl alacağını ifade etmiştir (Katz, 2010). Çünkü Stuxnet'in neden olduğu hasar zor fark edilen biçimdedir. Bu nedenle donanım arızasına solucanın sebep olup olmadığını ilişkilendirmek zordur. Ayrıca solucanın üretken doğası nedeniyle, bulaştığı tüm bilgi işlem cihazlarını tespit etmek ve temizlemek çok zordur. İran'ın Kasım 2010'da Natanz'daki zenginleştirme operasyonlarını geçici olarak ve açıklanmayan nedenlerle durdurmasının sebeplerinden birinin bu olduğu söylenebilir (Shakarian vd., 2013:232).

Stuxnet saldırısıyla birlikte siber uzayın kendine has özelliği olan atfetmenin zorluğu bir kez daha akıllara gelmiştir. Virüsün ortaya çıkarılmasından sonra İran; İsrail ve ABD'yi saldırılara katılmakta suçlamıştır. İran Ulusal Güvenlik Konseyi Genel Sekreteri Saeed Jalili bir ropörtajında, Stuxnet'in arkasındaki isimler sorulunca *"umutsuz ve zayıflamış düşmanlarımız"* cevabını vermiş ve Stuxnet solucanının verdiği zarara değinmeden saldırının uzmanlar tarafından durdurulduğunu belirtmiştir ('We Have to Be Constantly on Guard' (18.01.2011), https://www.spiegel.de/international/world/iran-s-chief-nuclear-negotiator-we-have-to-be-constantly-on-guard-a-739945.html). Hatta İranlı yetkililer bir adım ileri giderek Alman firması Siemens'i de faillerin içine dâhil etmiş ve nükleer tesislerini sabote etmek için İsrail ve ABD'ye yardım ettiğini ifade etmiştir (Iran accuses Siemens of helping launch Stuxnet cyber-attack (17.04.2011), https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack). ABD ve İsrail'e yönelik suçlamaların kesin olarak reddedilememesi de İran'ın iddialarını güçlendirmiştir. Ayrıca Edward Snowden 2013 yılında verdiği bir röportajda Stuxnet solucanının kodlarını NSA ve İsrail'in birlikte yazdığını belirtmiştir (The NSA and Its Willing Helpers (08.07.2013), https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html). Stuxnet solucanının, sistemlere ilk olarak ne şekilde bulaştığıyla ilgili ise dönemin istihbarat bakanı Haydar Moslehi tarafından 2010 yılının Ekim ayında yapılan açıklamada, saldırıyla ilişkili olarak sayısını belirtmediği *nükleer casusun* gözaltına alındığı ifade edilmiştir (Iran arrests 'nuclear spies' accused of cyber attacks (2.10.2010), https://www.bbc.com/news/world-middle-east-11459468).

2019 yılında yaşanan bir gelişme ise Stuxnet solucanının, Natanz Nükleer Tesisi'ne nasıl sızdırıldığını ortaya çıkarmış gibi gözükmektedir. CIA ve MOSSAD adına Hollanda istihbarat birimi AIVD tarafından görevlendirilen İranlı bir mühendis, solucanı geliştiren ABD'deki mühendislere Natanz'daki sistemleri hedeflemelerine yardım edecek kritik bilgiler sağlamıştır. İranlı köstebek tecrit edilmiş sistemlere Stuxnet solucanını bulaştırması gerekince de bir USB bellek aracılığıyla ihtiyaç duyulan erişimi sağlamıştır. Esasında İranlı köstebek, Natanz Nükleer Tesisine sızmak için iki paravan şirket kurmuş ancak ilk kurduğu şirket tesise sızmayı başaramamıştır. İsrail destekli ikinci şirket sayesinde sızma işlemi başarılmış; gerekli bilgiler toplanarak solucana sürekli güncel yazılımlar ilave edilebilmiştir. (Zetter, 2019)

Sonuç olarak, 2010 yılında VirusBlockAda olarak bilinen küçük bir Belarus firması tarafından keşfedilen ve Microsoft firmasının incelemeleri sonucunda sistemlere etkisinin 2009 yılında başladığı düşünülen Stuxnet solucanının; hedef seçimi, gelişmişlik düzeyi ve gelecekteki kötü amaçlı yazılımlar için etkileri, onun diğer kötü amaçlı yazılımlardan farklı bir noktada konumlanmasına neden olmuştur (Chen, 2010:2). Mevcut güvenlik varsayımlarında kusurlar ortaya çıkaran Stuxnet solucanı, sistemleri internet bağlantısından soyutlamanın etkili bir savunma olmadığını ayrıca dijital olarak imzalanmış sertifikaların güvenli olacağı varsayımının da geçersiz olabileceğini ve motive olmuş bir grubun içeriden sağlanan bilgi, geniş ekonomik kaynaklar ve ileri beceri düzeyi kombinasyonu sayesinde bu derece karmaşık bir kötü amaçlı yazılımı ortaya çıkarabileceğini göstermiştir (Shakarian vd., 2013:234; Chen ve Abu-Nimeh, 2011:93).

3.2.5. Night Dragon

Bilgisayar korsanları hükümet ve askeri sistemleri hedeflemişler ancak 2010'ların başında ticari sektöre yönelik girişimlerde de bulunmuşlardır. Özellikle enerji sektörüne odaklanan ilk saldırılardan biri de *Night Dragon (Gece Ejderhası)* siber casusluk saldırısı olmuştur (Pentland, 2011). Kasım 2009 yılında başladığı düşünülen ve 2010 yılında ortaya çıkarılan siber casusluk operasyonunda, küresel petrol, enerji ve petrokimya şirketlerine yönelik koordine edilmiş, gizli ve hedefli siber saldırılar gerçekleştirilmiştir. Bu saldırılarda amaç, hedef sistemdeki işleyişi bozmak yerine; petrol ve gaz arama sahaları ve teklifler hakkında proje detayları ve finansal bilgileri bulmaya yönelik olmuştur (Wueest, 2014:11).

Değerli bilgiler peşinde koşan saldırganlar, elde ettikleri bilgileri enerji ve petrol arama gibi alanlarda rakipleriyle aynı düzeye gelmek isteyen şirketlerle ve ülkelerle paylaşarak hem maddi kazanç hem de prestij/ün gibi manevi kazançlar elde edebilirler. Örneğin bir firma, yeni müşteriler kazanmak için, rakip firmaya kötü şöhret ve olumsuz müşteri deneyimi kazandırma konusunda istekli olabilir. Ayrıca siber korsanlar için bir başka motivasyon kaynağı, şirketlerden çalınan bilgiler kullanılarak kritik altyapılara yönelik gerçekleştirilebilecek sabotaj saldırılarında bulunabilmek olmuştur (Wueest, 2014:16). Night Dragon siber casusluk saldırıları sonucu hassas dokümanların yanı sıra tescilli endüstriyel işlemlerin de kopyalanmasına McAfee firmasının üst düzey yöneticilerinden olan, dönemin başkan yardımcısı Dmitri Alperovitch *"bu bilgiler son derece hassastır ve rakipler için büyük miktarda paraya değecektir"* sözleriyle dikkat çekmiş ve saldırının maddi kazanç motivasyonu yönünü ortaya koymuştur (Bartz, 2011).

McAfee firması tarafından yayımlanan bir raporda (McAfee, 2011:3-4) bu saldırılarda sosyal mühendislik yöntemleri, kimlik avı, Microsoft Windows işletim sistemleri güvenlik açıklıkları, uzaktan yönetim araçları da dâhil olmak üzere çeşitli teknikler kullanıldığı ifade edilmiştir. Basit açıklamasıyla, siber korsanlar önce şirketin internet sitesindeki açıklığı kullanarak uzaktan komut

yürütülmesine izin vermiş, ardından yaygın bulunan bilgisayar korsanlığı araçlarını kullanarak hassas dâhili bilgisayarlara ve sunuculara erişim kazanmışlardır. Sonra sisteme yükledikleri kötücül yazılım sayesinde ek kullanıcı adlarına ve şifrelere erişim sağlamışlar bu sayede hassas dokümanlara daha fazla erişim şansı elde etmişlerdir. Son olarak kötücül yazılım yüklenen bilgisayarlardan internete doğrudan erişim etkinleştirilmiş; bu sayede yöneticilerin bilgisayarlarının gizliliği ihlal edilmiş, e-posta arşivleri ve diğer hassas dokümanlarla ilgili bilgiler firma dışına çıkarılabilmiştir. Siber casusluk saldırısıyla ilgili Dmitri Alperovitch yaptığı açıklamada *"saldırıların sofistike olmadığını ancak hedeflerine ulaşma konusunda çok başarılı olduğunu"* ifade etmiştir (Bartz, 2011).

Night Dragon siber casusluk saldırıları, her ne kadar sofistike olmasa da özel araçlar, uzmanlık ve deneyim gerektirmesi bakımından büyük olasılıkla bir devlet, büyük bir şirket ya da organize bir grup tarafından koordine edilen ya da sponsor olunan bir grubun eseri olduğu düşünülmektedir. Çünkü örneğin kötücül yazılımın nasıl tespit edilmeden etkili bir şekilde çalışacağını bulmaları ve sahip oldukları uzmanlığı işe yarayacak bir şeye nasıl dönüştüreceklerini bilmeleri gerekmiştir (Naraine, 2011). McAfee (2011:18) yayımladığı raporda saldırıların kaynağıyla ilgili doğrudan kanıtlar sunmasa da dolaylı kanıtlarla Çinli bilgisayar korsanlarına işaret etmiştir. Saldırılara birçok aktör katılım gösterse de saldırganlara önemli komut ve kontrol altyapısı sağlayan[48]; Çin'in Shandong eyaleti, Heze şehrinde yaşayan bir kişiyi tespit etmişlerdir. Bu kişinin saldırıların arkasındaki tek isim olduğu düşünülmese de saldırılardan sorumlu kişilerin, grupların ya da kuruluşların bir kısmını tanımlamaya yardımcı olabilecek bilgilere sahip olduğu düşünülmektedir.

Saldırıların Çin kaynaklı olduğunu gösteren bir başka detay ise, yine aynı raporda (McAfee, 2011:18) ortaya konulan tüm veri sızdırma etkinliğinin Çin'in çalışma saatlerinde aktif olan Pekin merkezli IP adreslerinden gerçekleşmesi ve saldırganların Çin merkezli bilgisayar korsanlığı forumlarında yaygın olan *hack araçlarını*[49] kullanması olarak ifade edilebilir. Çin Dışişleri Bakanlığı sözcüsü Ma Zhaoxu basın toplantısında yaptığı *"bu durumu gerçekten anlamıyorum ancak bu tür raporları sık sık duyuyoruz"* şeklindeki açıklamayla siber casusluk faaliyetinden haberdar olmadığını ifade etmiştir (Branigan, 2011). Ancak Tablo 12'de görüldüğü gibi Çin, siber casusluk faaliyetlerinin dış politika taktiği olarak kullanılmasında en aktif ülkelerden biridir. Çin, ABD'nin yanı sıra Japonya, Vietnam, Filipinler, Tayvan, Kuzey Kore, Hindistan ve Pakistan gibi başka ülkelerde de siber casusluk operasyonları yürütmekte ve bu yolla başta ABD olmak üzere rakiplerinin gücüne karşı koymayı amaçlarken; aynı zamanda rakiplerini savunma harcamalarını

[48] Bahsi geçen kişi, 100 mb alan için yılda yaklaşık 10 dolar gibi düşük bir ücretle kayıt tutulmadan ABD'de barındırılan sunucu sağlayan bir şirket işletmektedir. Night Dragon siber casusluk saldırılarında hedef alınan şirketlerde, makineleri kontrol etmeye yarayan zwShell komut kontrol uygulaması, bahsi geçen şirketin ABD tabanlı kiralık sunucularında barındırılmıştır.

[49] Bunlar, Hookmsgina ve WinlogonHack olarak bilinen, Windows oturum açma isteklerini engelleyen ve kullanıcı adlarını ve parolaları ele geçiren araçlardır.

arttırmaya teşvik ediyor gibi gözükmektedir (Valeriano ve Maness, 2015:91-93). Her ne kadar Çin, Night Dragon siber casusluk olaylarına katılımını reddetse de aktarılan nedenlerden ötürü saldırıların arkasındaki isim olarak ileri sürülmüştür.

Tablo 12: Kamuoyunda Bilinen Siber Casusluk Olayları ve Operasyonları [50]

Kaynak	Hedef	İsim	Başlangıç	Bitiş	Atıf[51]-Şiddet[52]
Çin	ABD	Titan Rain	1.1.2003	4.1.2006	1-2
Çin	ABD	Ghost Net	27.5.2007	8.1.2009	1-2
Çin	ABD	Night Dragon	11.1.2009	2.11.2011	1-2

Kaynak: Valeriano ve Maness, 2015:91-93

3.2.6. GhostNet

Mart 2009'da ortaya çıkarılan ve GhostNet adı verilen bir siber casusluk ağının; 103 ülkede 1295 virüslü bilgisayarla yüksek değerli hedeflerden bilgi çaldığı ortaya çıkarılmıştır (Hui vd., 2010:490). Hedef alınan yerler arasında birçok ülkenin büyükelçilikleri, dışişleri bakanlıkları ve diğer devlet kurumlarının bilgisayarları bulunurken; Tibet'in ruhani lideri Dalai Lama ve onun Hindistan, Brüksel, Londra ve New York'ta bulunan merkezlerindeki bilgisayarlara da casus yazılım yüklenmiş ve bu yerler de saldırıların hedefi olmuştur (Markoff, 2009). Bu saldırıda ağlara, e-posta kimlik avı girişimi sayesinde erişilmiş ve kötücül yazılım sisteme bir kez girdikten sonra bilgisayarların kamera ve ses donanımını yetkisiz bir şekilde çalıştırarak ses kaydı ve görüntü aktarabilecek şekilde tasarlanmıştır (Valeriano ve Maness, 2015:131).

Aslında kimlik avı yöntemi ve uzaktan erişim aracı olarak bilinen bir truva atı türü olan kötücül yazılım stratejileri kullanılması yeni bir yöntem değildir. Ancak GhostNet yazılımının başarısı bu yöntemin iyi bir uygulamasının sonucudur. Şöyle ki, kurbanlara gönderilen e-posta iletisinde *Sürgündeki Tibetliler için Özgürlük Hareketi Kimlik Kitabı Çevirisi* başlığı yer almıştır. Ayrıca e-posta iletisinde Sürgündeki Tibet Hükümeti'nin amblemi de bulunmuş ve dosyaya tıklandığında normal bir şekilde açılmış ancak arka planda kullanıcının bilgisayarındaki bir açıklık kullanılarak kötü amaçlı yazılım yüklenmiş; yüklendikten sonra kötü amaçlı yazılım kontrol sunucusuyla bağlantı kurmaya çalışmış ve kontrol sunucusunun ara yüzüne erişimi olan herhangi bir kullanıcı virüs bulaşan bilgisayarın tam kontrolünü ele geçirebilmiş ve bağlı olduğu ağa erişebilmiştir (Carr, 2012:146-147). Bu nedenle potansiyel olarak hassas bilgileri kaynaktan

[50] Tablo 12'nin orijinalindeki veriler toplam, 9 ülke ve 36 siber olayı aktarmaktadır. Ancak bu tabloda yalnızca bu çalışmanın konusunu oluşturan 3 siber casusluk faaliyeti aktarılmıştır.

[51] Atıf, bir devletin siber casusluk faaliyetine dâhiliyesini kabul edip etmemesidir. 0: yorum yok, 1: red, 2: onay, 3: çoklu atıf

[52] Şiddet, beş en şiddetli olmak üzere, 1-5 arası artan bir ölçeği yansıtmaktadır.

toplama gücünün yüksek olması GhostNet saldırılarının en önemli özelliklerinden birini oluşturmuştur (Kaminski, 2010:82).

Saldırıların arka planındaki birey, grup ya da devlet yapısı hakkında kesin bir netlik ortaya konamasa da tespit edilebilen komuta ve kontrol yapısının Çin'e kadar uzanıyor oluşu ayrıca Çin'in siber uzaydaki hareketliliği gözlerin onlar üzerine çevrilmesine neden olmuştur (Flaten ve Lund, 2014). Kanada'da Toronto Üniversitesi *Munk Uluslararası Araştırmalar Merkezli* gelişmiş bir araştırma faaliyeti olan *Information Warfare Monitor* araştırmacılarının ortaya koyduğu raporda ise atıfta bulunmak için birkaç olasılık sıralanmıştır. Elde edilen kanıtların işaret ettiği en somut şey, yüksek profilli hedefler setinin Çin devleti tarafından askeri ve stratejik istihbarat amaçları için kullanılmış olabileceğidir. Gerçekten de saldırının yöneldiği Hindistan, Butan, Bangladeş, Vietnam, Filipinler, Hong Kong, Tayvan gibi ülkelerin çoğu Güney ve Güney Doğu Asya'da bulunan, Çin dış ve savunma politikasına açıktan bağlı yüksek profilli hedeflerdir (Deibert ve Rohozinski, 2009:48).

Raporun ortaya koyduğu bu iddialara rağmen, Mart 2009'da New York'taki Çin konsolosluğu sözcüsü GhostNet'e ülkesinin dahiliyesini reddeden bir açıklama yapmıştır. Sözcü Wenqi Gao, *"bunlar eski hikayeler ve hiçbir anlamı yok... Çin hükümeti hertürden siber suçu kesinlikle yasaklamıştır ve tam karşısındadır"* sözleriyle ülkesini savunmuştur (Markoff, 2009). Ancak yine aynı dönemde GhostNet'in hedef listesindeki Filipinler'de yerel bir gazete olan *Inquirer* bir rapor yayımlayarak Filipinler Dışişleri Bakanlığı bilgisayar ağının Çin merkezli bilgisayar korsanlarının saldırısına uğradığını iddia etmiştir (Krekel, 2009:74).

Information Warfare Monitor araştırmacılarının atıfa ilişkin ortaya koyduğu ikinci iddia ise virüs bulaşan bilgisayarların, herhangi bir politik çıkarı olmayan birey ya da gruplar tarafından, Çin için stratejik öneme haiz yüksek profilli hedeflerin de dahil olduğu rastgele seçilmiş hedefler olabileceğidir. Son olarak, olası başka bir senaryo ise, bu yüksek değerli hedeflerin bir birey ya da grup tarafından kar amacı güdülerek hedeflenmiş olabileceğidir. Şöyle ki, devlet ya da özel şirkete yönelik GhostNet siber casusluk saldırıları sonucu ele geçirilen finansal bilgiler ya da kritik veriler bunları talep eden müşterilere satılmak amacıyla çalınmış olabilir. Vatansever bilgisayar korsanlarının bile kendi iradeleri ya da mensubu oldukları devletin örtülü onayı ile GhostNet gibi operasyonları gerçekleştirebiliyor oluşu bu ihtimalleri anlamlı kılmaktadır (Deibert ve Rohozinski, 2009:48).

3.2.7. Titan Rain

Siber casusluk operasyonlarının büyük ölçüde Çin'e atfedilmesine neden olan olaylardan biri 2003-2006 yılları arasını kapsayan ve gayri resmi olarak Titan Rain olarak adlandırılan siber saldırı silsilesidir. Saldırıların birincil amacının ABD'deki resmi kurumlardan büyük miktarda veri

sızdırılması olduğu ifade edilmiştir. Hedeflenen kuruluşlar arasında başta ABD Savunma Bakanlığı olmak üzere, Savunma Bilgi Sistemleri Ajansı, Sandia Ulusal Laboratuvarı, Dünya Bankası, Lockheed Martin ve NASA gibi yüksek profilli kuruluşlar bulunmaktadır (Shakarian vd., 2013:124). İlerleyen yıllarda ise aralarında Almanya ve İngiltere'nin de bulunduğu bir dizi Batı Avrupa hükümeti aynı saldırılara maruz kaldıklarını duyurmuştur. İngiliz Güvenlik Servisi (MI5) direktörü Jonathan Evans, alışılmadık bir adım atarak Çin tehdidine karşı uyarı niteliğinde bir mektup hazırlayarak 300 yönetici ve güvenlik danışmanına göndermiştir (Inkster, 2010:55).

Titan Rain siber casusluk saldırılarında Çin'in, ABD Ordusu Bilgi Sistemleri Mühendislik Komutanlığı, Deniz Okyanus Sistemleri Merkezi, Füze Savunma Ajansı ve Sandia Laboratuvarı'ndan gelen verilerin bulunduğu Sınıflandırılmamış İnternet Protokolü Yönlendirici Ağı üzerinden 10-20 terebayt arası veri çaldığı iddia edilmiştir (Carr, 2012:4). Düzenleme gereği internete bağlı askeri ve hükümet sistemleri gizli veri içermemektedir. Ancak bu veriler arasında teknoloji ve yeniliklerle ilgili veriler olabilir (Shakarian vd., 2013:126-127). Örneğin Titan Rain saldırılarında ABD Ordusu Havacılık ve Füze Komutanlığı'ndan çalınan veriler içinde ordu ve hava kuvvetleri tarafından kullanılan *Falconview 3.2* için spesifikasyonlar, ABD Ordusu helikopterlerinin havacılık–misyon-planlama sisteminin teknik özellikleri ve NASA'nın Mars yörüngesinde keşif ve araştırma yapmak için tasarladığı *Mars Yörünge Kaşifi'nin* sevk sistemi, güneş panelleri ve yakıt tanklarının şemaları olduğu iddia edilmiştir (Thornburgn, 2005).

Sandia Ulusal Laboratuvarı'nda ağ güvenlik analisti olarak çalışan Shawn Carpenter, Federal Soruşturma Bürosu (FBI) için karşı istihbaratta çalışırken Titan Rain saldırılarının izini Çin'in güneyindeki Guangdong eyaletine kadar sürebilmiştir. Saldırıların, yerel bir ağdan internete ilk bağlantı noktası olarak görev yapan üç Çinli yönlendiriciden kaynaklandığını tespit etmiş; üç yönlendiricinin her birinin arkasında ise altı ile on iş istasyonu olduğunu ve bu istasyonların yirmi dört saat boyunca çalıştığını tahmin ettiğini belirtmiştir. Devlet kurumları ve özel teşebbüslerden çalınan bilgiler ise Guangdong'a gönderilmeden önce Güney Kore'deki sunucularda saklanmıştır. Siber uzaydaki atfetme sorununu aşmaya çalışan bu tespit ise çarpıcı bir atılım olarak nitelendirilmiştir (Thornburgn, 2005).

Sonuç olarak Titan Rain, siber casusluk operasyonlarının temel prensiplerini gözler önüne sermiştir: önce ayrıntılı bir keşif, ardından hedef sistemlere sızma. Saldırganlar hedef sistemlere erişim sağlandıktan sonra ise hızlı ve verimli bir çalışmayla istenilen verileri hedef sistemlerden çıkarmayı başarmışlardır. Siber casusluğun nispeten düşük bir giriş maliyetine ve riske sahip olması bu alanın sömürülmesine olanak tanımıştır. Saldırıların kaynağının tespit şansı çok düşüktür ve Titan Rain örneğinde olduğu gibi tespit edilebilse bile atıf yapmak imkansıza yakındır. Şöyle ki, saldırıların çoğunun Çin kaynaklı olduğu iddia ve bazen tepsit edilse de doğrudan kanıt eksikliği nedeniyle suçlama yapmak çok zordur. Bu durumda da Çin'in başvurduğu inkar yöntemi anlam kazanmaktadır. Çin olaylara katılımını inkar etmiş ancak saldırıların kaynağının araştırılması

noktasında da herhangi bir girişimde bulunmamış gibi gözükmektedir (Shakarian vd, 2013:127; Adkins, 2013:9).

3.2.8. Conficker

Kasım 2008'de, daha sonra Conficker (resmi olarak W32/Conficker.worm; Downup, Downadup ve Kido olarak da bilinir) olarak anılacak bir bilgisayar solucanı, Microsoft Windows işletim sistemi bileşenlerindeki bir güvenlik açığından yararlanarak binlerce bilgisayarı etkilemiştir. Conficker solucanı, 1990'ların sonlarında ortaya çıkan, kendinden yüklemeli ve yayılmalı ve bilgisayarları bir botnet ordularına dönüştüren ilk kötü amaçlı yazılım parçalarından biri olmuştur (Schmidt, 2012:456). Conficker kötücül yazılımı tarafından enfekte olan cihazlar, uzak bir bilgisayara bağlanmış ve bu yolla kötücül yazılımı kullanan bilgisayar korsanının kontrolü altında performans gösterme potansiyeli olan bir botnet ağının parçası haline gelmiştir. Conficker solucanı, sistemdeki güvenlik bileşenleri tarafından kaldırılmasını önlemek için çeşitli savunma mekanizmaları kullanırken; ağ üzerindeki diğer bilgisayarları çıkarılabilir sürücüler (usb bellek gibi) ya da zayıf parolalar aracılığıyla etkilemiştir. Kasım 2008-Nisan 2009 arasındaki dönemde Conficker solucanının, her biri gelişmişlik ve tespit edilmekten kaçınmaya karşı önlemler geliştiren, beş çeşidi tespit edilmiştir (Kaska, 2012:6).

Conficker solucanının, dünya genelinde 2-10 milyon arası bilgisayarı etkilediği tahmin edilmektedir.[53] Microsoft ise yaptığı açıklamada dünya genelinde üç milyon bilgisayarın virüslü kaldığını ifade etmiştir (Krebs, 2009). 2011 yılında TÜBİTAK tarafından açıklanan verilere göre ise solucanın dünya genelinde 15 milyon bilgisayarı etkilediği ifade edilmiştir (İnternette 'Conficker' solucanı alarmı (30.01.2009), https://www.hurriyet.com.tr/ekonomi/internette-conficker-solucani-alarmi-10887623). Sayıların bu kadar yüksek ve geniş bir skalada olması solucanın teknik özelliklerinden de kaynaklanmıştır. Şöyle ki, Conficker solucanı Stuxnet solucanının aksine belirli bir sistemi değil, herhangi bir savunmasız sistemi etkileyecek şekilde tasarlanmıştır. Bu açıdan solucandan gerek özel (şirketler gibi) gerekse kamusal (ulusal ve yerel yönetimler, ordu gibi) ve kişisel bilgisayarlar ve sistemler etkilenmiştir (Kaska, 2012:16).

Conficker solucanından etkilenen kamusal kuruluşlardan biri, ABD'nin Texas eyaletindeki Houston kenti mahkeme sistemidir. 2009 yılının Şubat ayında kötücül yazılımın bulaşması sonucu polis küçük suçlar için tutuklamaları geçici olarak durdurmak zorunda kalmış ve mahkeme tüm duruşmaları ileri bir tarihe ertelemiştir (Olson vd., 2009). Conficker solucanından etkilenen kamusal kuruluşlardan bir diğeri de İngiltere Parlamentosu olmuştur. Solucan 2009 yılının Mart

[53] ESET firmasının virüs raporlama yazılımı ThreatSense tarafından ortaya konulan verilere göre %8.85 oran ile Conficker solucanı 2009 yılında dünyada en çok görülen kötücül yazılım olmuştur. Rapora göre kötücül yazılım 2009 yılı için en çok, %28.08 oranla Ukrayna'da görülürken; %18.69 oran ile Rusya ve %15.21 oran ile Güney Afrika Ukrayna'yı takip etmektedir. Türkiye'de ise bu oran %5.98 olmuştur (Conficker hala en tehlikeli virüs! (06.11.2009), https://www.milliyet.com.tr/teknoloji/conficker-hala-en-tehlikeli-virus-1158824).

ayında Parlamentonun ağına sızmış ve ağa bağlı bilgisayarları etkilemiştir (Arthur, 2009). İngiltere Savunma Bakanlığı'nın da solucandan etkilendiği iddia edilmiş ve hatta savaş gemilerinde internet ve e-posta erişimi de dahil olmak üzere, bilgi teknolojilerini etkileyen bir kötücül yazılımın Kraliyet Donanması'nın iletişim sistemlerini etkilediği de iddia edilmiştir. Savunma Bakanlığı'ndan yapılan açıklamada bilgi teknolojilerini sistemlerinin performansının etkilendiği kabul edilmiş ancak herhangi bir silah ya da navigasyon sisteminin etkilenmediği ve hassas bilgilerin bulunduğu ağlarda bulaşı tespit edilmediği ifade edilmiştir (Wattanajantra, 2009b). Conficker solucanından etkilenen bir diğer sistem ise *Intramar* adı verilen Fransız donanması bilgisayar ağıdır. Yapılan açıklamada hassas nitelikte belgelerin ve iletişimin yürütüldüğü *Sicmar Ağı'nda* solucan tepsit edilmemiş ancak bazı sistemlerin etkilenmesinden dolayı bir süre savaş uçakları önlem amacıyla havalanamamıştır (Willsher, 2009).

Conficker solucanı sağlık ve ulaşım sisteminde de aksaklıklara neden olmuştur. İngiltere'de beş (Wattanajantra, 2009a); İskoçya'da ise iki hastanenin sistemlerinin kötücül yazılımdan etkilendiği belirtilmiş ve kanser hastalarının randevularının etkilendiği ifade edilmiştir (Leyden, 2009). Solucan ABD'de de etkili olmuş, ülke genelinde çeşitli hastanelerdeki bilgisayarlar, kalp atış monitörleri ve manyetik rezonans görüntüleme cihazları da dahil olmak üzere kritik tıbbi ekipmanlar etkilenmiştir (Mills, 2009). Conficker solucanının tıbbi cihazlar üzerinde etkili olmasına olanak tanıyan koşullardan biri, bu cihazların çoğunun ağdaki diğer bilgisayarlar gibi izlenmemesi ve bu yolla siber saldırganlara ağa giriş için bir geçit sağlaması olarak açıklanmıştır (Palmer, 2020). Solucan Türkiye'de de etkisini göstermiş, Atatürk Havalimanı'nda bilet check-in ve bagajlama işlemleri için kullanılan ve uluslararası bir firma tarafından işletilen *SITA CUTE* isimli sisteme solucanın enfekte olması sonucu dış hatlar terminalinde bagajlama ve biletleme işlemleri manuel olarak yapılmak zorunda kalınmıştır. Yapılan açıklamada *"solucanın temizlenme işleminin 400'e yakın sistemde devam ettiği"* ve *SITA CUTE* sistemini kullanan *"Miami, Los Angeles, Orlando, JFK, Bremen gibi önemli havalimanlarında da sorun yaşandığı"* ifade edilmiştir (Ünlü virüs Atatürk Havalimanı'nda (30.01.2009), https://www.ntv.com.tr/turkiye/unlu-virus-ataturk-havalimaninda,uVcwpKeXLEqXo6d99N2fuw).

Sistemlere etkisi bu denli yüksek olan solucanın ortaya çıkardığı tehdidin üstesinden gelmek için siber uzayda işbirliği çabaları arttırılmıştır. Microsoft, kendi sistemlerindeki bir açıklığı kullanarak etkili olan solucanın kod yazıcılarının yakalanmasına yardım edecek bilgiler için 250.000 dolar ödül teklif etmiştir. Ardından bir adım ileri giderek, işbirliğinin sadece bir şirketin çabalarından fazla sonuç vermesi amacıyla üyeleri arasında ICANN, NeuStar, VeriSign, Symantec, F-Secure, M1D Global, AOL, Afilias gibi kurumların ve araştırmacıların bulunduğu bir çalışma grubu kurmuştur (Carr, 2012:13). Bütün bu çabalara rağmen solucanın yazılımını yapan kişi yada gruplar hakkında herhangi bir netlik ortaya koyulamamıştır. Kötücül yazılımın bazı özelliklerinden

dolayı araştırmacılar, yazılımı yapan kişi ya da kişilerin Ukrayna kökenli[54] olabileceğini düşünmüşler ancak ortaya konan doğrudan kanıtlar eksik kalmıştır. Yine de Conficker'ın karmaşıklık derecesi ve hızlı uyum yeteneği incelendiğinde dikkate değer maddi kaynakların varlığına işaret etmektedir. Bu açıdan bir suç örgütü ya da ulus devletin Conficker'ın geliştiricisi olması muhtemeldir ancak bunu destekleyen kanıtlar sınırlı kalmıştır (Kaska, 2012:18-19).

Sonuç olarak, siber suç faaliyetlerinden, siber savaşa göre daha az endişe duyulsa da Conficker'ın potansiyeli suç işleme potansiyeli nedeniyle değil, bilgisayar ağlarında bir siber savaş başlatma potansiyeli nedeniyle korkutucu olmuştur. Conficker solucanını ilk farkeden bilgisayar bilimcilerden Phil Porras'ın açıklamaları kötücül yazılımın ortaya çıkardığını tehdidin niteliğini ortaya koymaktadır: *"Conficker'ın yayılma tarzı bize tam ölçekli bir siber saldırının nasıl görünebileceğine dair net bir tablo verdi… Sadece, neyse ki, sonuçları olmadan"* (Bowden, 2019).

3.2.9. Orchard Operasyonu

Siber saldırının konvansiyonel güçle birlikte kullanımına dair en çarpıcı örneklerden biri, 6 Eylül 2007 tarihinde Suriye'nin kuzeyinde Deyr ez-Zor'daki nükleer reaktör sahasına İsrail Hava Kuvvetleri'ne bağlı F-15I ve F-16I savaş uçakları tarafından gerçekleştirilen ve *Orchard (Meyve Bahçesi) Operasyonu* olarak bilinen bombalı saldırıdır. Esasında saldırı kararının temeli 2006 yılında gerçekleştirilen bir operasyona dayanmaktadır. O dönemde Suriye Hükümeti'nden üst düzey bir yetkili bir dizi görüşme gerçekleştirmek için Londra'da bulunurken kişisel bilgisayarını otel odasında bırakıp dışarı çıkmış ve onu takip eden MOSSAD ajanları bilgisayarın uzaktan izlenmesine izin veren bir Truva atını sisteme gizlice yüklemiştir. Ajanlar bilgisayarı incelemeye başladıklarında ise daha önemli bir detay dikkatlerini çekmiştir. Kuzey Kore nükleer programının yöneticilerinden biri olan Chon Chibu ve Suriye Atom Enerjisi Komisyonu başkanı İbrahim Othman Suriye çölünün ortasında keşif yaparken çekilmiş bir fotoğrafına denk gelmişlerdir. Ele geçirilen diğer belgelerle birlikte Suriye'nin nükleer silah yapımında önemli bir eşik olan plütonyum zenginleştirmek için Kuzey Kore'nin yardımıyla gizlice al Kibar tesisini inşa ettikleri ortaya koyulmuş ve önlem alma gerekliliği doğmuştur (Singer ve Friedman, 2014:126-127).

Gelişmiş bir Suriye nükleer programının varlığı, İsrail devleti tarafından varoluşuna yönelik büyük bir tehdit olarak görülmüş; bu durum da nükleer tesisi vurma kararını beraberinde getirmiştir (Hughes, 2018:75). Bu saldırılar esnasında Suriye'nin hava savunma sistemi[55] tam anlamıyla

[54] FBI, solucanın yazılımını yapan dört Ukraynalı, bir İsveçli beş kişiden şüphelenmiştir. 21.07.2011 tarihinde FBI ajanı Norm Sanders ve Ukrayna polisinin ortak operasyonuyla Sergey Kamratov, Dmytro Volokitin ve Yevgen Fatyeyev isimli üç Ukrayna vatandaşı tutuklanmıştır. Kişisel bilgisayarları incelendiğinde Conficker'ın arkasındaki kodlama çalışmaları ve planlamalarıyla ilgili bağlantılar tespit edilmiştir. İsveçli Mikael Sallnert Danimarka'da tutuklanmış ve ABD'ye iade edilip 48 ay hapis cezasına çarptırılmıştır. Beşinci isim Victor Mauze ise iddianamede ismi geçmesine karşın yargılanmamıştır (Bowden, 2019).

[55] O dönemde radarların da dâhil olduğu hava savunma sistemi 1979'da hizmete giren Rusya ürünü BUK-M1 SAM sistemidir (Dygnatowski vd., 2019:285). Aynı dönemde İran'da hava savunma sistemlerini Moskova'dan almıştır.

körleşmiş ve Suriye hava sahasına giren, bölgeye baskın düzenleyen sonra da ayrılan İsrail savaş uçaklarını tespit edememiştir (Rid, 2012:16). Esasında Suriye hava savunma sistemini oluşturan radarlar düzgün çalışmıştır. Ancak gerçekleştirilen bir siber saldırı sonucu radar operatörlerinin görüntülediği ekranlar üzerinde değişiklik yapılmıştır. Gerçekleştirilen siber saldırı, modern savaşların değişen yüzünü ortaya koyması bakımında önem taşımaktadır. Şöyle ki, İsrail bölgede bulunan radar sistemlerine silahlı bir saldırı düzenlemek yerine siber saldırı düzenleyerek hedefi doğrultusunda istenen görüntüyü sistemlere yükleyebilmiş ve bunu büyük bir gizlilik altında gerçekleştirmiştir (Keleştemur, 2015:153).

Siber saldırının nasıl gerçekleştirildiği konusunda henüz bir netlik ortaya konamamış olsa da belirli tahminler yapılmıştır. İlk olarak tesisin bombalanmasından önce Türkiye sınırına yakın Tel Abyad'daki Suriye radar sahasına İsrail kuvvetleri tarafından saldırılmış böylece sistem hasar görmüş ve devre dışı kalmıştır. Ancak bombalama operasyonunun tamamı boyunca hava savunma sistemlerinin ve radarların devre dışı kalması akıllara iki programın kullanımını getirmiştir: *Senior SUTER*[56] ve *Ağ merkezli ortak hedefleme (Network-centric collaborative targeting/NCCT)*[57]. NCCT hedefi tanımlayıp, yerini belirlediğinde Senior SUTER devreye girmiş ve böylece sistemi kullanan operatörlerin düşman iletişimlerini ve bilgisayar ağlarını, özellikle de entegre hava savunma sistemleriyle ilişkili olanları ele geçirmesini sağlarken, düşman operatörlerin ise saldırıyı anlamasını ve buna karşı koymasını engellemiştir (Gasparre, 2008b). Bu noktada, İsrail'in Suriye hava sahasına özel boyayla boyanmış bir Heron insansız hava aracı sokmuş olabileceği ve Heron'un Senior SUTER programı kullanılarak radar sinyallerini yakalayıp aynı frekansta sinyaller göndererek radar sistemini devre dışı bırakmış olabileceği de ifade edilmiştir (Clarke ve Knake, 2010:9).

Saldırının gerçekleştirilme yöntemine dair ikinci olasılık ise, İsrail ya da müttefikleri adına çalışan bir ajanın, Suriye'de konuşlu Rus yapımı hava savunma sistemini kontrol eden bilgisayar programına bir truva atı yerleştirmiş olabileceğidir. Bu sayede tuzak program, belirli bir elektronik sinyal geldiğinde hava sahasını boş gösterecek şekilde programlanarak radar ekranlarının saldırını anında temiz görünmesini sağlamış olabilir. Üçüncü olasılık ise İsrail ordusunun, Suriye'deki fiber

Dolayısıyla hava savunma sisteminin bu şekilde devre dışı kalması aynı sistemi kullanan Tahran yönetimi tarafından da şaşkınlıkla karşılanmıştır. Yine bu noktada dolaylı olarak İran'ın da hedef olduğu iddia edilmiştir. İsrail ordusunun, hiç beklemediği bir anda Tahran yönetimini de vurabileceği konusunda gözdağı vermek istediği ifade edilmiştir (Keleştemur, 2015:152-153).

[56] Birinci nesil SUTER, düşman radarlarının gördüklerini izlemeyi başarmıştır. İkinci nesil, düşman ağı ve sensörleri üzerinde kontrol sahibi olmaya izin vermiş; üçüncü nesil ise roket atarlar ve radarlar da dâhil olmak üzere ağ sistemlerinin tam kontrolünü ele geçirmeyi sağlamış ve operatörün sistemin doğru çalıştığına dair temelde yanlış olan inancını güçlendirmiştir (Dygnatowski vd., 2019:285).

[57] Bu sistem, bir sensör ağının minimum insan müdahalesi ile bir hedefin yerini belirlemesine yardımcı olur. İnsan müdahalesinin en aza indirilmesiyle NCCT, bir hedefi bulmak için gereken süreyi saat veya dakikadan, saniyelere indirmektedir. Çalışma prensibi ise Barb Carson tarafından insan merkezi sinir sisteminin tehdit edici bir sesin geldiğini yöne anında gözlerini çevirmesine benzetilmiş ve *"bir düşman varlığı iletişim kurduğunda veya hareket ettiğinde sensör platformu üzerinde yön çizgisi alır ve diğer sensörleri düşman varlığına odaklanmak için uyarır. Düşmanın kimliği ve konumu hakkında destekleyici kanıtlar sağlar"* şeklinde açıklanmıştır (Gasparre, 2008a).

optik kablolarda oynama yapmış olabileceğidir. Suriye hava savunma sistemine ait fiber optik kablo ağı yalnızca askeri tesislerle korunan bölgelerde değil ülkenin dört bir yanına dağılmış durumdadır. İsrail ordusunun bu kabloları keserek, kendi kablolarını hava savunma sistemine bağlamış ve bir komut yazarak tuzak kapısını etkin hale getirmiş olabileceği ifade edilmiştir (Clarke ve Knake, 2010:10).

Suriye'ye yönelik operasyona İsrail'in yanı sıra ABD'nin de dahil olduğu iddia edilmiştir. Şöyle ki, operasyondan önce istihbarat amacıyla kullanılan fotoğraflar, ABD'nin casus uyduları aracılığıyla çekilmiştir (Keleştemur, 2015:152). Ayrıca saldırı esnasında kullanılan Senior SUTER sistemine ABD'nin sahip olduğu ifade edilmiştir (Clarke ve Knake, 2010:9). İsrail Başbakanı Ehud Olmert, saldırıdan önce Amerikalıların desteğinin alınması gerektiğini deklare etmiş; en azından NATO üyesi bir ülke olan Türkiye'nin sınırları ve askeri üslerine çok yakın bir bölgeye uçaklarını göndermek için ABD'nin zımni rızasına ihtiyaç olduğu vurgulanmıştır (Follath ve Stark, 2009).

İlginç olan bir nokta ise hem hedef olan Suriye hem de İsrail ve ABD kanadı başlarda böyle bir olay meydana gelmemiş gibi davranmışlardır. Saldırının gerçekleştiği gün Şam merkezli Suriye Haber Ajansı hava sahasının ihlal edildiğini ifade ederken, Suriyeli bir askeri sözcü ise savaş uçaklarının hava savunma sistemlerinin karşı koyması sonucu herhangi bir can ya da mal kaybına neden olmadan ıssız alanlara mühimmat bıraktıktan sonra ayrıldıklarını açıklamıştır. İsrail hükümeti radyosu askeri bir sözcünün *bu olay hiç gerçekleşmedi* açıklamasını aktarmıştır. ABD Dışişleri Bakanlığı sözcüsü ise birbiriyle çelişen yalnızca ikinci el raporlar duyduğunu ifade etmiştir (Follath ve Stark, 2009). Olaydan iki yıl sonra Suriye Devlet Başkanı Beşar Esad verdiği bir röportajda bombalanan tesisin nükleer bir tesis olmadığını, askeri bir tesis olduğunu iddia etmiş; toprakta tespit edilen uranyum izleri için de İsrail kanadını suçlamış ve onların havadan bırakmış olabileceğini ima etmiştir ('Peace without Syria Is Unthinkable' (19.01.2009), https://www.spiegel.de/international/world/spiegel-interview-with-syrian-president-bashar-assad-peace-without-syria-is-unthinkable-a-602110.html).

Sonuç olarak, bu çapta bir operasyonun siber ayağının İsrail ordusu siber güvenlik birimi ve NSA'ya eşdeğer olan Birim (Unit) 8200 tarafından gerçekleştirildiği düşünülmektedir. Ayrıca radar sistemlerinin siber saldırılar sonucu etkilenmesi, Orchard Operasyonunun siber ayağının İsrail'in Suriye'ye yönelik saldırısında başarılı olmasının kilit taşlarından birini oluşturduğunu kanıtlar niteliktedir. Yalnızca siber saldırıların kullanımı, bir varlığı fiziksel olarak yok etmede yetersiz kalsa da daha büyük bir askeri operasyonun entegre bir parçası olarak kullanılması durumunda ortaya çıkan etki daha büyük olmaktadır (Rid, 2012:17). Orchard Operasyonu göstermiştir ki, siber savaş geleneksel savaştan önce gelmekte; düşmanın geleneksel savunmalarını ortadan kaldırmadan önce siber saldırılar vasıtasıyla radar, hava savunma, füze sistemleri ve diğer kritik sistemler kolayca devre dışı bırakılabilmektedir (Clarke ve Knake, 2010:23).

3.2.10. RSA Saldırısı

Mart 2011'de bilgisayar ve ağ güvenliği firması RSA, bilgisayar sistemlerine gerçekleştirilen sofistike bir siber saldırı sebebiyle dünya genelinde 40 milyon kullanıcı ve 25.000'den fazla şirket tarafından kullanılan çok farktörlü kimlik doğrulama sağlayan *SecurID* sistemini zafiyete uğratacak kritik verilen çalındığını ve sistemin etkinliğinin tehlikeye girdiğini açıklamıştır. Gerçekleştirilen saldırı RSA firması yönetim kurulu başkanı Art Coviello tarafından "*yetenekli, motive olmuş, organize ve iyi finanse edilen siber saldırganların gerçekleştirdiği gelişmiş sürekli tehdit*[58] *saldırısı*" olarak nitelendirmiştir (Lee, 2015:202).

Bilgisayar ve ağ güvenliği firmasından verilerin çalınma yöntemi de dikkat çekicidir. Sosyal mühendislik yöntemi kullanılarak bir grup çalışana *2011 İşe Alım Planı* başlıklı e-posta ve ona ekli bir excel dosyası gönderilmiştir. Gönderilen bu dikkat çekici e-posta birçok çalışanın gereksiz posta kutusuna düşse de bazı çalışanlar bu gönderiyi ve ekli dosyayı açmıştır. Ekte bulunan excel dosyası, Adobe Flash yazılımında bulunan bir sıfır gün açıklığı aracılığıyla, aktive edilen sisteme arka kapı yüklenmiş ve böylece siber saldırganın sisteme ve ağ üzerinden diğer bilgisayarlara erişimine olanak tanınmıştır (Krombholz vd., 2014:8). Siber saldırganın bilgisayarları uzaktan kontrol etmesine izin veren sistem yüklendikten sonra ise çalışanlara ait birkaç hesap şifresi çalınmış ve bunlar hassas verilere erişim izni olan diğer çalışanların erişebileceği sistemlere girmek için kullanılmıştır. Son aşamada ise siber saldırgan RSA dosyalarını sunuculara aktarmış ordan da kendi bilgisayarına yönlendirmiştir (Richmond, 2011).

RSA firmasına düzenlenen siber saldırıyla ilgili dikkat çekici bir nokta ise, bu saldırılardan elde edilen veriler kullanılarak ABD'nin önde gelen teknoloji ve havacılık şirketi Lockheed Martin'in de siber saldırıların hedefi olmasıdır. Savaş uçakları, casus uydular ve diğer gizli ekipmanları üreten Lockheed Martin şirketinden yapılan açıklamada önemli verilerin gizliliği ihlal edilmeden önce saldırıların farkedildiği ve engellendiği vurgulanmış; bu ihlalle birlikte, bilgisayar ağlarına uzaktan erişimi korumak için kullanılan ve RSA firmasından temin edilen *SecurID* sisteminin güvenliği hakkındaki endişelerin doğrulandığı ve diğer şirketler ya da devlet kurumlarının da saldırılara karşı savunmasız olabilecekleri hakkındaki endişelerin arttığı dile getirilmiştir (Drew, 2011).

Sonuç olarak önce RSA ve ardından Lockheed Martin şirketlerine yönelik saldırılar, bazı siber saldırıların birden çok aşaması olduğunu göstermiştir. Bir yerde yaşanan güvenlik ihlali daha büyük ve daha karmaşık bir ihlale olanak tanıyan bir aşama olabilir. Böylesine aşamalı bir

[58] Gelişmiş Sürekli Tehditler, bir devlet ya da kuruluşa yönelik gerçekleştirilen ve sahip oldukları varlığı ele geçirene kadar devam eden *"uzun süreli erişime sahip olarak veri elde etme"* amaçlı siber tehdit çeşidini tanımlamaktadır. Gizli yürütülen, bir hedefi olan, uyarlanabilir ve veri merkezli olması bu tehdit çeşidi için temel kavramlardır (Akın ve Sağıroğlu, 2017:2).

saldırının unsurları da önemli ölçüde farklılaşacağı için parçaları bir araya getirmek zorlaşır ve tespit olanaksız hale gelir (Rid ve Buchanan, 2015:22). Bu durumda da siber alanda etkin bilgi paylaşımı ve karşı önlem geliştirmek daha değerli hale gelmektedir.

SONUÇ

Soğuk Savaş sonrası devlet güvenliğinde yeni bir boyut olan siber suç, siber terör, siber saldırılar ve siber savaşlar, internet kullanımının yaygınlaşması, ülkelerin elektrik, su, ulaşım, enerji, finans, telekomünikasyon gibi kritik altyapılarının giderek ağ bağlantılı hale gelmesi ve bilgi ve iletişim teknolojilerinin zaman içinde gelişim göstermesiyle etki boyutunu arttırmış ve gelecek dönemde de arttıracak gibi görünmektedir. Bu gelişen ve sürekli değişen alana uyum sağlamak isteyen devletler de siber güvenliğin sağlanmasına ilişkin strateji belgeleri yayımlamakta, karar alıcı kademelerde siber birimler oluşturmaktadırlar. Ayrıca NATO, BM, AB gibi uluslararası örgütler bünyesinde de çalışmalar yapılmakta ve gelişen tehdide karşı ortak bir yanıt verilmesine yönelik çabalar sürdürülmektedir.

Siber uzayın sağladığı anonimlik bu alanda faaliyet gösteren aktörlerin siber olaylar karşısındaki sorumluluklarını da belirsizleştirmektedir. Geleneksel saldırı yöntemlerine kıyasla siber uzaydan gelen saldırılarda, saldırı kaynağının tam olarak tespit edilemiyor oluşu uluslararası hukuk açısından atıf problemini de ortaya çıkarmakta alınacak tedbirleri ve yaptırımları da etkilemektedir. Ayrıca aktörün tespit edilemiyor oluşu siber caydırıcılığı da zayıflatmakta ve tehdidin değişen niteliğini ortaya koymaktadır.

Siber olayların artış göstermesi, aktörler açısından maliyetin düşük olmasının da bir sonucudur. Geleneksel saldırı yöntemleriyle kıyaslandığında siber saldırıların maliyeti kullanılan araçların farklılaşması sebebiyle çok daha düşük kalmaktadır. Bazen internet bağlantısı olan bir bilgisayar bile basit bir saldırı için yeterli olabilmektedir. Ayrıca siber olayların kritik altyapıları hedef alabilmesi sebebiyle hem fiziksel hem de ağlar üzerinde etkili olması ve ortaya çıkan etkinin belirli bir bölgeyle sınırlı kalmaması siber olayların artış hızını yükselten bir başka faktör olarak ön plana çıkmaktadır. Stuxnet'in siber güvenlik algısında meydana getirdiği değişim bu yüzden önemlidir. Çünkü artık siber saldırıların fiziksel olarak da etki doğurabildiğini gözler önüne sermiştir.

İncelenen örnek olayların da ortaya koyduğu gibi siber saldırılar çok hızlı bir şekilde gerçekleşmektedir. Bu açıdan Orchard Operasyonunda da görüldüğü gibi bazen saldırıya uğrayan taraf bunun farkına varana kadar sistemleri hasar görmekte ve saldırı sona ermektedir. Ayrıca siber saldırıların sınır aşan bir nitelik taşıması sebebiyle hedef çeşitliliği de yüksek olmaktadır. Yani bir aktör siber saldırılar vasıtasıyla aynı anda birçok hedefe zarar vermekte ve bazen gözle görülür etkiler oluşmadığı için hasar tespiti yapmak zorlaşmaktadır.

Örnek olaylar incelendiğinde, siber savaşların aktörler tarafından başlı başına bir müdahale yöntemi olarak kullanılmasından ziyade; hibrit konseptte hâlihazırda devam eden bir konvansiyonel savaş esnasında operasyonel amaçlarla kullanımının daha büyük etki oluşturduğu görülmüştür. Özelikle Rusya tarafından Gürcistan ve Ukrayna müdahalelerinde kullanılan bu yöntem, toplum mühendisliği ve psikolojik araçların kullanımını denkleme dâhil etmekte ve bu sayede bilgi kirliliği oluşturmak ve algı yönetimi yapmak amaçlanmaktadır. Ayrıca RSA firmasına düzenlenen siber saldırıda olduğu gibi bazı saldırıların aşamalı olduğu gözükmektedir. Yani bir siber saldırı sonucu ele geçirilen kritik bilgiler, başka siber saldırılarda kullanılabilmektedir. Bu da siber uzayın dinamik yapısını ortaya koymakta ve siber güvenliğin sağlanmasının toplumun her kesimi için önemli olduğunu göstermektedir.

Siber güvenlik özelinde incelenen siber savaşların ve siber saldırıların uluslararası ilişkileri hem teorik hem de olgusal bağlamda değiştirdiği söylenebilir. Realist teori açısından temel analiz birimi olarak alınan devlete yapılan vurgu siber uzayda aşınmaktadır. Devletler ekonomik ve askeri olarak büyük kaynaklara sahiptir ve hala sistemdeki en büyük güçtür. Ancak siber uzayın kendine has özellikleri sayesinde süreç içinde devlet dışı aktörlerin de sisteme dâhil olması ve güvenliği tehlikeye atabilmesi aktör algısında değişiklikler meydana getirmiştir. Çünkü belirli durumlarda saldırının isnat edilebileceği aktör bile netlik taşımamaktadır.

Yapısal realizmin büyük güçlere odaklanma eğilimi de belirli açılardan geçerliliği sorgulanır hale gelmiştir. Çünkü siber uzayda aktörlerin kapasiteleriyle ilgili net bir çıkarım yapmak mümkün olmamaktadır. Ekonomik çıktılar ve askeri kapasite sıralamasında büyük güçler arasına giremeyen ülkelerin bile saldırı ve savunma yoluyla siber alanda aktif olabildiği göz önüne alındığında kimin büyük güç olduğunun nasıl belirleneceği konusu netlik taşımamaktadır. Devletlerin yanı sıra, örneğin, Gürcistan'a yönelik siber savaşın en önemli yönlendiricilerinden olan RBN gibi siber suç örgütleri dahi kimi durumlarda gelişmiş ülkelerden daha aktif olmakta ve tehlike arz etmektedir.

Siber saldırılar yoluyla ele geçirilen hassas bilgilerin güvenliği tehdit etmesi sonucu daha önce realistler tarafından düşük politika konusu olarak görülen siber güvenliğin de artık yüksek politika konusu içinde değerlendirilmesi gerekliliği ortaya çıkmıştır. Ayrıca realizmin insan doğasına yönelik olumsuz bakış açısı belirli durumlarda değişime uğramıştır. Siber saldırıların öznesi olan bilgisayar korsanları daima kötü niyetli olmamakta, beyaz şapkalı hackerlar siber güvenliği tehdit eden saldırıları bertaraf etmek için kamu ve özel sektörle işbirliği içinde çalışmaktadırlar.

Realist teori ve alt alanları için geçerli bir yaklaşım olan, sistemi yöneten bir üst otoritenin olmaması sebebiyle anarşik olduğu nitelemesi siber uzay için de bazı noktalardan benzeşiyor gibi gözükmektedir. ICANN, ITU gibi özel ya da NATO, AB, BM gibi uluslararası örgütler bünyesinde

yönetişim amaçlı girişimler gerçekleştirilse de siber uzayda da tam anlamıyla bir üst erkin varlığından söz edilememektedir. Ancak devletler kimi durumlarda bir üst erk rolüne bürünerek güvenliklerini tehdit ettiğini iddia ettikleri internet sitelerine erişim engeli getirebilmekte ya da bunları kapatma yoluna gidebilmektedirler. Bu çabaların ötesinde Kuzey Kore, Çin, İran gibi ülkeler ise insanlığın ortak kullanımında olan internete ilişkin daha ileri kısıtlamalar getirebilmekte ve yalnızca kendi süzgeçlerinden geçen kullanımlara izin vermektedir. Ancak bu kısıtlamaların bile sadece ülke sınırları içinde geçerli olduğu, bölgesel ya da küresel özellik taşımadığı ifade edilebilir.

Liberal teori bazı açılardan siber güvenlik konusunu Uluslararası İlişkiler içerisinde daha iyi açıklayabiliyor gibi görünmektedir. Örneğin demokratik devletlerin birbirleriyle savaşmayacağı varsayımının bir benzeri siber uzayda da görülmektedir. Demokratik devletlerarası siber saldırılar nadir görülmekte; şiddet düzeyi genellikle siber suç seviyelerinde kalmaktadır. Ayrıca liberalizmin devlete yaptığı vurgu siber güvenlik konusu için daha doğru gözükmektedir. Devletler, merkezi bir aktör olma özelliklerini devam ettirmektedirler ancak sahneyi devlet dışı örgütler ve sermaye sahibi şirketlerle paylaşmaktadırlar. Bu sebepten etkin bir siber güvenliğin sağlanması içim kamu-özel işbirliği gereklidir.

Siber savaşlar ve siber saldırılar analiz edilirken, sosyal inşacı teorinin kimlik algısına yapmış olduğu vurgu önem taşımaktadır. Çünkü aktörler kimlik algısı etrafında şekillenmekte ve dost-düşman sınıfına koyulmaktadır. Stuxnet örneğinde görüldüğü gibi solucanın yazılımcıları olduğu iddia edilen ABD ve İsrail siber alanda olduğu gibi fiziksel alanda da dost ve müttefik ülkelerdir. Buna karşın İran ile ilişkiler ise her iki ülke tarafından tarihi süreçte düşman kimliği çerçevesinde şekillenmektedir. Ayrıca sosyal inşacılıkta dilin işlevine yapılan vurgu siber güvenlikle ilgili kavramları tanımlanır ve açıklanırken gerçek ve siber olan arasında analojiler kurma işlevini yerine getirmektedir.

Bir siber olayın suç, saldırı ya da savaş kategorisine koyulması için çerçeveleme yapmak önem taşımaktadır. Bu açıdan siber güvenlik incelemelerinin ivme kazanmasında güvenlikleştirmenin ortaya koyduğu bu yaklaşımın payı büyüktür. Çünkü bir olayı siber suç ya da siber saldırı şeklinde nitelemek onunla ilgili alınacak önlemleri ve verilebilecek cevapları şekillendirmektedir. Ayrıca güvenlikleştirmenin vurguladığı beş güvenlik sektörünün yanı sıra liberal teorinin yaptığı vurguyu destekler nitelikte kamu-özel sektör işbirliğinde yeni bir siber güvenlik sektörünün oluşumu desteklenmektedir.

Son olarak küreselleşmenin fiziksel sınırları belirsizleştirmesi internetin sınırsızlığıyla birleşince hem olumlu hem olumsuz sonuçlar doğurmuştur. Dünyada internet ve bilgi teknolojilerinin kullanımının giderek yaygınlaşması bir tuşla bilgi edinimini kolay hale getirmiştir. Ancak bunun yanında kötü niyetli aktörlerin de varlığı tehdit kaynağını genişletmekte ve olumlu sonuçlar olumsuza dönüşebilmektedir. Ülkelerin elektrik, su, ulaşım, enerji, finans,

telekomünikasyon kritik altyapılarının giderek ağa bağımlı hale geliyor olması ayrıca birçok hassas dokümanın bilgisayar ortamına aktarılması siber saldırılar yoluyla bunların tehdit edilebilir olmasını da mümkün kılmaktadır. Etkili bir siber savunma için uluslararası düzeyde etkin işbirliği sağlanmalı ve nükleer ya da belirli konvansiyonel silahlarda olduğu gibi bağlayıcılığı olan kurallar konulmalıdır.

YARARLANILAN KAYNAKLAR

Adams, James (2001), "Virtual Defense", **Foreign Affairs**, 80(3), 98-112.

Adkins, Gary (2013), "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism", **Journal of Strategic Security**, 6(3), 1-9.

Agius, Christine (2017), "Sosyal İnşacılık", A. Collins (Ed.), **Çağdaş Güvenlik Çalışmaları** (N. Uslu, Çev.), *içinde* (87-103), Uluslararası İlişkiler Kütüphanesi, İstanbul.

Akgül-Açıkmeşe, Sinem (2011), "Algı mı Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", **Uluslararası İlişkiler**, 8(30), 43-73.

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

Anderson, Alison (2003), "Risk, Terrorism, and the Internet", **Knowledge, Technology, & Policy,** 16(2), 24-33.

Anderson, Robet H. ve Anderson Richard O. (1997), "Emerging Challenge: Security and Safety in Cyberspace", John Arquilla ve David Ronfeldt (Ed.), **In Athena's Camp: Preparing for Conflict in the Information Age,** *içinde* (231-251), Rand, Ca.

Andress, Jasan ve Winterfeld, Steve (2011), **Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners**, Elsevier Inc., Waltham, Ma.

Anley, Chris (2002), Advanced SQL Injection In SQL Server, **an NGS Software Insight Security Research (NISR) Publication** , 3-25.

Arı, Tayyar (2013), **Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği,** Mkm Yayıncılık, Bursa.

Arıcak, Tolga (2015), **Siber Alemin Avatar Çocukları,** Remzi Kitapevi, İstanbul.

Arquilla, John ve Ronfeldt, David (1997), "Cyberwar is Coming!", John Arquilla ve David Ronfeldt (Ed.), **In Athena's Camp: Preparing for Conflict in the Information Age,** *içinde* (23-60), Rand, CA.

Arthur, Charles (02.04.2009), "Conficker is a lesson for MPs – especially over ID cards", https://www.theguardian.com/technology/2009/apr/02/conficker-parliament-security-charles-arthur, (29.04.2020).

Aschmann, Michael vd. (2015), "Cyber Armies: The Unseen military in the grid", **Proceedings of the 10th International Conference on Cyber Warfare and Security ICCWS-2015** (20-29), Academic Conferences and Publishing International Limited, Reading.

Ashmore, William. C. (2009), "Impact of Alleged Russian Cyber Attacks", **Baltic Security & Defence Review**, 1(11), 4-40.

Aslay, Fulya (2017), "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum" **International Journal of Multidisciplinary Studies and Innovative Technologies**, 1(1), 24-28.

Badie, Bertrand (2001), "Realism under Praise, or a Requiem? The Paradigmatic Debate in International Relations", **International Political Science Review,** 22(3), 253-260.

Balzacq, Thierry vd. (2016), "Securitization Revisited: Theory and Cases", **International Relations,** 30(4), 494-531.

Barkin, J. Samuel (2003), "Realist Constructivism", **International Studies Review,** 5(3), 325-342.

Barletta, William A. (2008), "Cyberwar of cyber-terrorism: The Attack on Estonia", **International Seminar On Nuclear War And Planetary Emergencies—38th Session,** (481-486).

Bartz, Diane (10.02.2011), "Chinese hackers infiltrated five energy firms", https://www.reuters.com/article/us-energy-cyber-china/chinese-hackers-infiltrated-five-energy-firms-mcafee-idUSTRE7190XP20110210 (23.04.2020).

Batchelor, Tom " (04.10.2018), "Russia cyberattacks timeline: when and where the GRU are accused of targeting western institutions, https://www.independent.co.uk/news/world/europe/russia-cyberattack-timeline-gru-when-where-netherlands-opcw-porton-down-fco-wada-a8568616.html (21.04.2020).

Bayraktar, Gökhan (2014), "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat", **Güvenlik Stratejileri Dergisi,** 10(20), 119-147.

_____ (2015), **Siber Savaş ve Ulusal Güvenlik Stratejis**i, Yeniyüzyıl Yayınları, İstanbul.

Baysal, Başar ve Lüleci, Çağla (2011), "Kopenhag Okulu ve Güvenlikleştirme Teorisi", **Güvenlik Stratejileri,** (22), 61-96.

Bendiek, Annegret ve Metzger, Tobias (2015), "Deterrence Theory in the Cyber-Century", **Lecture Notes in Informatics (LNI), Gesellschaft für Informatik**, 553-570.

Bendrath, Ralf vd. (2007), "From 'Cyberterrorism' to 'Cyberwar', Back and Forth: How the United States Securitized Cyberspace", Johan Eriksson ve Giampiero Giacomello (Ed.), **International Relations and Security in the Digital Age,** *içinde* **(**57-82), Taylor & Francis, New York.

Bıçakçı, Salih (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu" **Uluslararası İlişkiler,** 9(34), 205-226.

_____ (2014), "Nato'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik" **Uluslararası İlişkiler,** 10(40), 101-130.

Billo Charles ve Chang Welton (2004), **Cyber Warfare: an Analysis of the Means and Motivations of Selected Nation States,** Hanover: Institute for Security Technology Studies at Dartmouth College.

Bissell Kelly vd. (2019), **The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study**, Ponemon Institute LLC., Michigan.

Blank, Stephen (2017), "Cyber War and Information War à la Russe", George Perkovich ve Ariel E. Levite (Ed.), **Understanding Cyber Conflict: Fourteen Analogies**, *içinde* (81-98), Georgetown University Press, Washington.

Blomfield, Adrian, "Estonia calls for Nato cyber-terrorism strategy" (18.05.2007), https://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html (02.04.2020).

Booth, Ken (1997), "Secuirty and Self: Reflections of a Fallen Realist", Keith Krause ve Michael C. Williams (Ed.), **Critical Security Studies,** *içinde* (83-120), University of Minnesota Press, Minneapolis.

Bowden, Mark (29.06.2019), "The Worm That Nearly Ate The Internet", https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html (29.04.2020).

Branigan, Tania (11.02.2011), "Chinese hackers targeted energy multinationals, claims McAfee", https://www.theguardian.com/world/2011/feb/11/chinese-hackers-targeted-energy-multinationals (23.04.2020).

Brenner Susan W. ve Goodman Marc D. (2002), "in Defense of Cyberterrorism: an Argument for Anticipating Cyber-Attacks", **Journal of Law, Technologhy & Policy**, 1-57.

Brown, Chris ve Kirsten, Ainley (2005), **Understanding International Relations,** Palgrave Macmillan, NewYork.

Burchill, Scott (2005), "Liberalism", Scott Burchill ve Andrew Linklater (Ed.), **Theories of International Relations,** *içinde* (55-83), Palgrave Macmillan, New York.

Buzan, Barry (1996), "The timeless wisdom of realism?", Steve Smith vd.(Ed.), **International Theory: Positivism & Beyond**, *içinde* (47-65), Cambridge University Press, New York.

_____ (2008), "Askeri Güvenliğin Değişen Gündemi", **Uluslararası İlişkiler,** 5(18), 107-123.

Buzan Barry ve Ole Waever (1998), **Security: A New Framework for Analysis,** Lynne Rienner Publishers, Colorado.

Carr, Jeffrey (2012), **Inside Cyber Warfare,** O'Reilly Media, Inc, California.

Cartwright, James. E. (2011), **Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operation**, Department of Defense, Washington DC.

Cavelty, Myriam D. (2005), **a Comparative Analysis of Cybersecurity Initiatives Worldwide,** International Telecommunation Union, Cenevre.

_____ (2008), **Cyber-Security and Threat Politics: US efforts to secure the information age,** Taylor and Francis, Oxon.

Center for Strategic & International Studies (CSIS) (t.y.), "Significant Cyber Incidents Since 2006", https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3G1QKa (10.05.2020).

Chen, Thomas M. (2010), "Stuxnet, the Real Start of Cyber Warfare? [Editor's Note]", **Ieee Network,** 24(6), 2-3.

Chen, Thomas. M., ve Abu-Nimeh Saeed (2011), "Lessons from Stuxnet", **Security,** 44(4), 91-93.

Choucri Nazli ve Clark David D. (2013), "Who controls cyberspace?", **Bulletin of the Atomic Scientists,** 69(5), 21-31.

Choucri, Nazli (2012), **Cyberpolitics in International Relations,** MIT Press, Londra.

Clark, David (2010), "Characterizing Cyberspace: Past, Present and Future", **MIT Csail**, 1-3.

Clarke, Richard A. ve Knake K. Robert (2010), **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehditi,** (Çev., M. Erduran), İstanbul Kültür Üniversitesi, İstanbul.

Clayton, Mark (21.09.2010), "Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?", https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant (11.04.2020)

Collins, Alan (2005), "Securitization, Frankenstein's Monster and Malaysian Education", **The Pacific Review,** 18(4), 567-588.

Collins, Sean ve McCombie Stephen (2012), "Stuxnet: the emergence of a new cyber weapon and its implications", **Journal of Policing, Intelligence and Counter Terrorism,** 7(1), 80-91.

Connell Michael ve Vogler Sarah (2017), **Russia's Approach to Cyber Warfare,** CNA, Washington.

Çifci, Hasan (2017), **Her Yönüyle Siber Savaş**, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Ankara.

Damodaram Radha ve Valarmathi M.L. (2010), "Security Measures of Randvul Keyboard", **International Journal on Computer Science and Engineering (IJCSE)**, 2(3), 619-625.

Daneels, A ve Salter, W (1999), "What is Scada?", **International Conference on Accelerator and Large Experimental Physics Control Systems,** (339-343).

Darıcılı, Ali. B. (2014), "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi", **U.U. International Journal of Social Inquiry / U.Ü. Sosyal Bilimler Enstitüsü Dergisi,** 7(2), 1-16.

_____ (2016), "NATO'nun Siber Güvenlik Stratejisinin Analizi", **VII. Uludağ Uluslararası İlişkiler Konferansı –Uluslararası Sistemde Yeni Düzen Arayışları-,** (407-417), DORA, Bursa.

_____ (2017), "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", **Ulisa: Uluslararası Çalışmalar Dergisi,** 1(1), 1-24.

_____ (2019), "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi", **Tesam Akademi Dergisi,** 6(2), 11-33.

Dashora, Kamini (2011), "Cyber Crime in the Society: Problems and Preventions", **Journal of Alternative Perspectives in the Social Sciences,** 3(1), 240-259.

Dennesen, Kristen (2011), **Latin American Cyber Threat Landscape and 2011 Trends**, VERISIGN, Cancun.

Denning, Dorothy E. (2001), "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", John Arquilla ve David Ronfeldt (Ed.), **Networks and Netwars: The Future of Terror, Crime, and Militancy**, *içinde* (239-288), RAND Corporation, Santa Monica.

Doğrul, Murat vd. (2011), "Developing an international cooperation on cyber defense and deterrence against cyber terrorism", **3rd International Conference on Cyber Conflict,** *içinde* (29-43), CCD COE Publications, Tallinn.

Donnelly, Jack (2005), "Hobbes and classical realism", Scott Burchill ve Andrew Linklater (Ed.), **Theories of International Relations,** *içinde* (29-54), Palgrave Macmillan, New York.

Drew, Christopher (03.06.2011), "Stolen Data Is Tracked to Hacking at Lockheed", https://www.nytimes.com/2011/06/04/technology/04security.html (04.05.2020).

Dygnatowski, Sławomir vd. (2019), "The Analysis of Using Structural Solutions in Cybersecurity Based on Orchard Operation", **Journal of KONBiN,** 49(1), 281-298.

Economist Intelligence Unit (2011), **Cyber Power Index: Findings and Methodology,** The Economist.

Emmers, Ralf (2017), "Güvenlikleştirme", Allan Collins (Ed.) **Çağdaş Güvenlik Çalışmaları,** (Çev. N. Uslu), *içinde* (131-144), Uluslararası İlişkiler Kütüphanesi, İstanbul.

Erdbrink, Thomas (29.11.2010), "Ahmadinejad: Iran's nuclear program hit by sabotage", https://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html (14.04.2020).

Falliere, Nicolas vd. (2011), **W32.Stuxnet Dossier**, Symantec.

Farwell, James P. ve Rohozinski, Rafal (2011), "Stuxnet and the Future of Cyber War", **Survival**, 53(1), 23-40.

Filiol, Eric (2011), "Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct", Daniel Ventre (Ed.), **Cyberwar and Information Warfare**, *içinde* (245-284), ISTE, London.

Finkelstein Claire O. ve Govern Kevin H. (2015), "Introduction: Cyber and the Changing Face of War", Jens D. Ohlin vd (Ed.), **Cyberwar*:* Law and Ethics for Virtual Conflicts**, *içinde* (x-xx). Oxford University Press, Oxford

Finn, Peter (27.05.2007), "Cyber Assaults on Estonia Typify a New Battle Tactic", http://www.worldsecuritynetwork.com/Other/Finn-Peter/Cyber-Assaults-on-Estonia-Typify-a-New-Battle-Tactic (31.03.2020).

Fischer, Stanley (2003), "Globalization and Its Challenges", **American Economic Review,** 93(2), 1-30.

Flaten Ola ve Lund Mass S. (2014), "How Good are Attack Trees for Modelling Advanced Cyber", **Norwegian Information Security Conference** (NISK).

Follath, Von Erich ve Stark, Holger (02.11.2009), "How Israel Destroyed Syria's Al Kibar Nuclear Reactor" ", https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html (02.05.2020).

Foxall, Andrew (2016), "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain", **Russia Studies Centre Policy Paper,** (9), 1-15.

Freedman, Lawrance (1986), "The First Two Generations of Nuclear Strategists", Peter Paret (Ed.), **Makers of Modern Strategy from Machiavelli to the Nuclear Age**, *içinde* (735-778), Princeton University Press, New Jersey.

Gasparre, Richard. B. (09.03.2008a), "The Israeli 'E-tack' on Syria – Part I", https://www.airforce-technology.com/features/feature1625/ (01.05.2020).

_____ (10.03.2008b) , "The Israeli 'E-tack' on Syria – Part II", https://www.airforce-technology.com/features/feature1669/ (05.01.2020).

Giacomello, Johan Eriksson (2006), "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", **International Political Science Review,** 27(3), 221-244.

Gibson, William (1982), **Burning Chrome**, Arbor House Pub Co.

_____ (1984), **Neuromancer**.

Giddens, Anthony (1990), **The Consequences of Modernity,** Polity Press, Padstow.

Glaser, Charles. L. (2017), "Realizm", Alan Collins (Ed.), **Çağdaş Güvenlik Çalışmaları**, (Çev. N. Uslu), *içinde* (14-27), Uluslararası İlişkiler Kütüphanesi, İstanbul.

Goodman, Will (2010), "Cyber Deterrence Tougher in Theory than in Practice?", **Strategic Studies Quarterly**, 102-135.

Goodrich, Michael ve Tamassia, Roberto (2014), **Introduction to Computer Security**, Pearson Education Limited, Londra.

Govern, C. O. (2015), "Introduction: Cyber and the Changing Face of War", Jens D. Ohlin vd. (Ed.), **Cyberwar: Law and Ethics for Virtual Conflicts,** *içinde* (s. x-xx), Oxford University Press, Oxford.

Guiora, Amos N. (2017), **Cybersecurity Geopolitics, law and policy**, Taylor & Francis Group, New York.

Gurjar, L. R. (2015), **Cyber Crimes**, http://assets.vmou.ac.in/PGDCL04.pdf (30.12.2019)

Güntay, Vahit (2017b), "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği", **Güvenlik Bilimleri Dergisi,** 6(2), 81-108.

_____ (2018), "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri Dergisi,** 14(27), 79-111.

Hansen, Lene ve Nissenbaum, Helen (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", **International Studies Quarterly,** 53, 1155-1175.

Hathaway, Oona A. vd. (2012), "The Law of Cyber-Attack", **California Law Review**, 817-885.

Held David ve McGrew Anthony (1998), "The End of the Old Order? Globalization and the Prospects for World Order", **Review of International Studies**, 24(5), 219-245.

_____ (Ed.) (2003), **The Global Transformations Reader: An Introduction to the Globalization Debate,** Polity Press, Cambridge.

Herzog, Stephen (2011), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, 4(2), 49-60.

Hughes, Daniel. P. (2018), "Archer's Stakes in Cyber Space: Methods to Analyze Force Advantage", Henry Prunckun (Ed.), **Cyber Weaponry: Issues and implications of digital arms**, *içinde* (71-86), Springer, Sydney.

Hui Peter vd. (2010), "Towards Efficient Collaboration in Cyber Security", **2010 International Symposium on Collaborative Technologies and Systems** (489-498), IEEE.

Huth, Paul. K. (1999), "Deterrence and International Conflict: Empirical Findings and Theoretical Debates", **Annual Review of Political Science,** 2, 25-48.

Inkster, Nigel (2010), "China in Cyberspace", **Survival**, 52(4), 55-66.

Isnarti, Rika (2016), "A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War", **Andalas Journal of International Studies**, 5(2), 151-165.

Jaitner, Margarita L. (2015), "Russian Information Warfare: Lessons from Ukraine", Kenneth Geers (Ed.), **Cyber War in Perspective: Russian Aggression against Ukraine,** *içinde* (87-94), NATO CCD COE Publications, Tallinn.

Johnson Neil F. ve Jajodia Sushil (1998), "Exploring Steganography: Seeing the Unseen", **Computer**, 31(2), 26-34.

Johnston, Pamela E. (2000), "What a Good Idea! Frames and Ideologies in Social Movement Research", **Mobilization: An International Quarterly,** 5(1), 37-54.

Jordan, Tim (2003), **Cyberpower**, Taylor & Francis Group, New York.

Kalja, Ahto (2002), "The X-Road Project: A Project to Modernize Estonia's National Databases", **Baltic IT&T review**, (24), 47-48.

Kaminski, Ryan T. (2010), "Escaping the cyber state of nature: cyber deterrence and international institutions", **NATO Cooperative Cyber Defence Centre of Excellence Conference on Cyber Conflict** (79-94), CCD COE, Tallinn.

Karabulut, Ali N. (2016), "Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması", **Uluslararası İlişkiler,** 13(49), 25-42.

Karla, Kush (2017), "Emergence of Cyber Crimes: a Challenge for the new Millennium", **Bharati Law Review,** 86-103.

Kaska, Kadri (2012), **Conficker: Considerations in Law and Legal Policy**, CCD COE, Tallinn.

Katz, Yaakov (15.12.2010), "Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years", https://www.studentnewsdaily.com/daily-news-article/stuxnet-virus-set-back-irans-nuclear-program-by-2-years/ (15.04.2020).

Keleştemur, Atalay (2015), **Siber İstihbarat**, Level Kitap, İstanbul.

Kelsey, Jeffrey T. (2008), "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", **Michigan Law Review,** 106(7), 1427-1452.

Klimburg, Alexander (2001), "Mobilising Cyber Power", **Survival**, 53(1), 41-60.

Knutsen, Torbjorn L. (1992), **A History of International Relations Theory,** Manchester University Press, Manchester.

Koçer, Gökhan (2004), "Küreselleşme ve Uluslararası İlişkilerin Geleceği", **Uluslararası İlişkiler,** 1(3), 101-122.

Kolodziej, Edward A. (2005), **Security and International Relations,** Cambridge University Press, Cambridge.

Korhan, Sevda (2017), "Siber Uzayda Güç-Aktör İlişkisi", **Cyberpolitik Journal**, 2(4), 75-104.

Kozlowski, Andrzej (2013), "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan", **1st International Scientific Forum** (236-245), European Scientific Institute, Tiran.

Kramer Andrew E. ve Higgins Andrew (16.08.2017), "In Ukraine, a Malware Expert Who Could Blow the Whistle on Russian Hacking"**,** https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html, (21.04.2020).

Krebs, Brian (16.10.2008), "Russian Hacker Forums Fueled Georgia Cyber Attacks", http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (09.04.2020).

_____ (13.02.2009), "Cyber Security Community Joins Forces to Defeat Conficker Worm", http://www.csl.sri.com/users/porras/public/WP-Conficker-2-13-09.pdf (28.04.2020).

Krekel, Bryan (2009), **Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,** Northrop Grumman, McLean, VA.

Krombholz, Katharina vd. (2014), "Advanced Social Engineering Attacks, **Journal of Information Security and Applications**, 1-11.

Kurnaz, İbrahim (2016). "Siber Güvenlik ve İlintili Kavramsal Çerçeve", **Siber Politikalar Dergisi**, 1(1), 56-77.

Lan, Tang ve Xin Zhang (2010), "Can Cyber Deterrence Work?", Andrew Nagorski (Ed.), **Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway**, *içinde* (1-3), The EastWest Institute, New York.

Lander, Mark ve Markoff, John, "Digital Fears Emerge After Data Siege in Estonia" (29.05.2007), https://www.nytimes.com/2007/05/29/technology/29estonia.html (02.04.2020).

Lau, F. vd. (2000), "Distributed denial of service attacks", **2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'**, 2275-2280, IEEE.

Lee, Dave (05.03.2014), "Russia and Ukraine in cyber stand-off", https://www.bbc.com/news/technology-26447200 (19.04.2020).

Lee, Newton (2015), **Counterterrorism and Cybersecurity: Total Information Awareness,** Springer International Publishing, CA.

Lewis, James. A. (2002), **Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,** Center for Strategic and International Studies (CSIS), Washington.

Leyden, John (09.03.2009), "Scottish hospitals laid low by malware infection". https://www.theregister.co.uk/2009/03/09/scot_hostpitals_malware_infection/ (29.04.2020).

Libicki, Martin. C. (2009), **Cyberdeterrence and Cyberwar**, RAND Corporation, Santa Monica, CA.

Liff, Adam P. (2012), "Cyberwar: A New 'Absolute Weapon? The Proliferation of Cyberwarfare Capabilities and Interstate War", **Journal of Strategic Studies**, 35(3), 401-428.

Lin, Herbert S. (2010), "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy**, 63-86.

Lindsay, Jon R. (2013), "Stuxnet and the Limits of Cyber Warfare", **Security Studies,** 22(3), 365-404.

Linklater, Andrew (1995), "Neo-Realism in Theory and Practice", Ken Booth ve Steve Smith (Ed.), **International Relations Theory Today**, *içinde* (241-261), Polity Press, Cambridge

Lupovici, Amir (2011), "Cyber Warfare and Deterrence: Trends and Challenges in Research", **Military and Strategic Affairs**, 3(3), 49-62.

Mann, Ian (2008), **Hacking the Human Social Engineering Techniques and Security Countermeasures**, Gower Publishing Limited, Hampshire.

Markoff, John (12.08.2008), "Before the Gunfire, Cyberattacks" https://www.nytimes.com/2008/08/13/technology/13cyber.html?auth=login-google (09.04.2020).

_____ (28.03.2009), "Vast Spy System Loots Computers in 103 Countries", https://www.nytimes.com/2009/03/29/technology/29spy.html (24.04.2020).

_____(26.10.2010), "A Silent Attack, but Not a Subtle One" https://www.nytimes.com/2010/09/27/technology/27virus.html (02.05.2020).

Matrosov, Aleksandr vd. (2010), **Stuxnet Under the Microscope,** ESET LLC.

Maurer Tim ve Janz Scott (17.09.2014), "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context", https://css.ethz.ch/en/services/css-partners/partner.html/13306 (19.04.2020).

Mazari, Ali Al vd. (2016), "Cyber Terrorism Taxonomies: Definition, Targets, Patterns, RiskFactors, and Mitigation Strategies", **International Journal of Cyber Warfare and Terrorism**, 6(1), 1-12.

McAfee, (2011), **Global Energy Cyberattacks: "Night Dragon",** McAfee Foundstone Professional Services and McAfee Labs.

McGraw, Gary (2013), "Cyber War is Inevitable (Unless We Build Security In)", **Journal of Strategic Studies,** 36(1), 109-119.

Mearsheimer, John J. (2001), **The Tragedy of Great Power Politics,** W. W. Norton & Company, Inc., New York.

_____ (2013), "Structural Realism", Tim Dunne vd. (Ed.), **International Relations Theory Discipline and Diversity,** *içinde* (77-93), Oxford University Press, Oxford.

Mills, Elinor (24.04.2009), "Conficker infected critical hospital equipment, expert says" https://www.cnet.com/news/conficker-infected-critical-hospital-equipment-expert-says/ (29.04.2020)

Miş, Nebi (2011), "Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi", **Akademik İncelemeler Dergisi,** 6(2), 345-381.

Morgenthau, Hans J. (1997), **Politics Among Nations: The Struggle For Power and Peace**. McGraw-Hill.

Morse, Edward L. (1971), "Transnational Economic Processes", **International Organization,** *25*(3), 373-397.

Nakashima, Ellen (27.05.2013), "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies", https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html (06.12.2019).

Naraine, Ryan (02.08.2010), "As attacks escalate, Microsoft ships emergency Windows patch", https://www.zdnet.com/article/as-attacks-escalate-microsoft-ships-emergency-windows-patch/ 12.04.2020).

_____ (12.02.2011), "Night Dragon attacks: Another reason to care about consumer malware" , https://www.zdnet.com/article/night-dragon-attacks-another-reason-to-care-about-consumer-malware/ (23.04.2020).

Nissenbaum, Helen (2005), "Where Computer Security Meets National Security", **Ethics and Information Technology,** (7), 61-73.

Nye, Joseph S. (2004), **Soft Power: The Means to Success in World Politics**, Public Affairs, New York.

_____ (2010), "Cyber Power", **Belfer Center for Science and International Affairs,** 1-24.

Olson, Bradley vd. (06.02.2009), "Computer virus shuts down Houston municipal courts", https://www.chron.com/news/houston-texas/article/Computer-virus-shuts-down-Houston-municipal-courts-1742589.php (28.04.2020).

Onuf, Nicholas (1998), "Constructivism: A User's Manual", Vendulka Kubalkova vd. (Ed.), **International Relations in a Constructed World**, *içinde* (58-78), Taylor & Francis, New York.

Owens, William A. vd. (2009), **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**, The National Academies Press, Washington.

Önok, Murat (2013), "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,** 19(2), 1229-1269.

Özdemirci, Fahrettin ve Torunlar, Mehmet (2018), "Bilgi-Değişim-Siber Güvenlik-Bağımsızlık", **Bilgi Yönetimi Dergisi**, 1(1), 78-83.

Özgöker, Uğur ve Yılmaz, Serdar (2016), "New Security Threads within the Context of Globalization: Cybercrimes", Hasret Çomak vd. (Ed.), **Uluslararası Güvenlik: "Yeni Politikalar, Stratejiler ve Yaklaşımlar**, *içinde* (157-166), Beta, İstanbul.

Palmer, Danny (10.03.2020), "How poor IoT security is allowing this 12-year-old malware to make a comeback", https://www.zdnet.com/article/how-poor-iot-security-is-allowing-this-ten-year-old-malware-to-make-a-comeback/ (29.04.2020).

Pellerin, Cherly (12.03.2013), "Cybercom Builds Teams for Offense, Defense in Cyberspace", https://archive.defense.gov/news/newsarticle.aspx?id=119506 (22.01.2020).

Pentland, William (19.02.2011), "Night Dragon Attacks Target Technology in Energy Industry", https://www.forbes.com/sites/williampentland/2011/02/19/night-dragon-attacks-target-technology-in-energy-industry/#77be9d8b1d49 (22.04.2020).

Podhorec, Milan (2012), "Cyber Security within the Globalization Process", **Journal of Defense Resources Management,** 3(1), 19-26.

Polat, Doğan Ş. (2016), "Siber Terörizmle Mücadele", Hasret Çomak vd. (Ed.), **Uluslararası Güvenlik: "Yeni Politikalar, Stratejiler ve Yaklaşımlar"**, *içinde* (167-180), Beta Yayınları, İstanbul.

Polityuk Pavel ve Finkle Jim (04.03.2014), "Ukraine says communications hit, MPs phones blocked", https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304 (20.04.2020).

Polityuk, Pavel (20.12.2016), "INTERVIEW-Ukraine investigates suspected cyber attack on Kiev power grid", https://www.reuters.com/article/ukraine-crisis-cyber-attacks/interview-ukraine-investigates-suspected-cyber-attack-on-kiev-power-grid-idUKL5N1EF39K (20.04.2020).

_____ (26.06.2018), "Exclusive: Ukraine says Russian hackers preparing massive strike", https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-russian-hackers-preparing-massive-strike-idUSKBN1JM225 (21.04.2020).

Poushter, Jacob (10.06.2015), "Key findings from our poll on the Russia-Ukraine conflict", https://www.pewresearch.org/fact-tank/2015/06/10/key-findings-from-our-poll-on-the-russia-ukraine-conflict/ (19.04.2020).

Radu, Sintia (01.02.2019), "China, Russia Biggest Cyber Offenders", https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows (20.01.2020)

Rein, Martin ve Schön, Donald (1993), "Reframing Policy Discourse", Frank Fischer ve John Forester (Ed.), **The Argumentative Turn in Policy Analysis and Planning,** *içinde (145-166)*, Duke University Press, London.

Reus-Smit, Christian (2005), "Constructivism", Scott Burchill ve Andrew Linklater (Ed.), **Theories of International Relations**, *içinde* (188-212), Palgrave Macmillan, New York.

Richelson, Jeffrey T. (2016), **The U.S Intelligence Community**, Westview Press, Boulder.

Richmond, Riva (04.02.2011), "The RSA Hack: How They Did It", https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/ (03.05.2020).

Rid, Thomas (2012), "Cyber War Will Not Take Place", **Journal of Strategic Studies,** 35(1), 5-32.

Rid, Thomas ve Buchanan, Ben (2015), "Attributing Cyber Attacks", **Journal of Strategic Studies,** 38(1-2), 4-37.

Rios Maria José vd. (2009), "The Georgia's Cyberwar", **International Conference on Global Security, Safety, and Sustainability** (35-42), Springer, Berlin.

Rohozinski, Rafal ve Deibert, Ron (2009), **"Tracking GhostNet: Investigating a Cyber Espionage Network"**, Ottawa.

Sağıroğlu, Şeref ve Akın, Murat (2017), "Gelişmiş Sürekli Tehditler", **Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi,** 10(1), 1-10.

Sağıroğlu, Şeref ve Alkan, Mustafa (2018), **Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık**, Grafiker Yayınları, Ankara.

Samuel Kuboye Oluwafemi vd. (2014), "Cyber Terrorism Attack of the Contemporary Information Technology Age: Issuesi Consequences and Panacea", **International Journal of Computer Science and Mobile Computing**, 3(5), 1082-1090.

Sanger, David E. (31.07.2015), "U.S. Decides to Retaliate Against China's Hacking", https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html (27.12.2019).

Schmidt, Andreas (2012), "At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker", **Telecommunications Policy,** 36(6), 451-461.

_____ (2013), "The Estonian Cyberattacks", Jason Healey (Ed.), **A Fierce Domain: Conflicts in Cyberspace, 1986 to 2012**, *içinde* (174-193), Atlantic Council, Washington: D.C.

Shakarian, Paulo (2013), **"Introduction to Cyber-Warfare: A Multidisciplinary Approach",** Elsevier, Waltham.

Shimko, Keith L. (1992), "Realism, Neorealism and American Liberalism", **The Review of Politics,** 281-301.

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

Smith, Gerry (24.01.2013), "John Kerry: Foreign Hackers Are '21st Century Nuclear Weapons", https://www.huffpost.com/entry/john-kerry-hackers_n_2544534 (24.12.2019).

Snyder, Glenn H. (2002), "Mearsheimer's World-Offensive Realism and the Struggle for Security: A Review Essay", **The MIT Press,** 27(1), 149-173.

Sommer, Peter ve Brown, Ian (2011), **Reducing Systemic Cybersecurity Risk**, Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3.

Spiegel, Peter (16.03.2014), "Nato websites disabled by cyber attack on eve of Crimea vote", https://www.ft.com/content/b822d5cc-ace6-11e3-8ba3-00144feab7de (21.04.2020).

Strayer, W.Timothy vd. (2008), "Botnet Detection Based on Network Behavior", Wenke Lee vd. (Ed.), **Botnet Detection Countering the Largest Security Threat,** *içinde* (1-24), Springer Science+Business Media, LLC., New York.

Tarhan, Kamil (2017), "Siber Uzayda Realist Teorinin Değerlendirilmesi", **Siber Politikalar Dergisi**, 2(3), 105-124.

Thomas, Douglas ve Loader, Brian D., (2000), **Cybercrime: Law Enforcement, Security and Surveillance in the Information Age.** Routledge, London.

Thomas, Timothy. L. (2009), "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia", **Journal of Slavic Military Studies,** (22), 31-67.

Thornburgh, Nathan (05.09.2005), "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them", https://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm (26.04.2020)

Thornburgh, Tim (2004), "Social Engineering: The "Dark Art", **Proceedings of the 1st annual conference on Information security curriculum development** (133-135), Acm., Kennesaw.

Tikk Eneken vd. (2010), **International Cyber Incidents: Legal Considerations,** Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn.

Timtchenko, Ilya (17.11.2017), "Shymkiv: Ukrainians not prepared for cyber attacks", https://www.kyivpost.com/business/shymkiv-ukrainians-not-prepared-cyber-attacks.html?cn-reloaded=1 (21.04.2020).

Todd, Graham H. (2009), "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition", **The Air Force Law Review**, 65-102.

Tuli, Preeti ve Sahu, Priyanka (2013), "System Monitoring and Security Using Keylogger", **International Journal of Computer Science and Mobile Computing (IJCSMC)**, 2(3), 106-111.

United Nations (1990), "Resolutions Adopted on the Reports of the Third Committee", https://undocs.org/en/A/RES/45/121 (10.05.2020).

URL, "2016-2019 Ulusal Siber Güvenlik Stratejisi" (t.y.), https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf (30.09.2019).

___, "Ülke Künyesi" (t.y.) http://www.mfa.gov.tr/estonya-kunyesi.tr.mfa (28.03.2020).

___, "The Birth of the Web" (t.y.), https://home.cern/science/computing/birth-web (28.09.2019).

___, "Where the Future Becomes Now" (t.y.), https://www.darpa.mil/about-us/darpa-history-and-timeline (07.05.2020).

___, "Worldmeters" (t.y.), https://www.worldometers.info/world-population/? (02.10.2019)

___, “Conficker hala en tehlikeli virüs! (11.06.2009)”, https://www.milliyet.com.tr/teknoloji/conficker-hala-en-tehlikeli-virus-1158824 (29.04.2020).

___, "Convention on Cybercrime” (23.11.2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (30.12.2019).

___, “Çin'in gizli "süper ordu"su ortaya çıktı” (27.05.2011), http://www.milliyet.com.tr/dunya/cinin-gizli-super-ordusu-ortaya-cikti-1395440 (22.01.2020).

___, “Iran accuses Siemens of helping launch Stuxnet cyber-attack” (17.04.2011), https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack (14.04.2020).

___, “Iran arrests 'nuclear spies' accused of cyber attacks” (02.10.2010), https://www.bbc.com/news/world-middle-east-11459468 (14.04.2020).

___, “İkinci cephe siber savaş” (15.03.2014), https://www.yenisafak.com/dunya/ikinci-cephe-siber-savas-626007 (20.04.2020)

___, “İnternette ’Conficker’ solucanı alarmı” (30.01.2009), https://www.hurriyet.com.tr/ekonomi/internette-conficker-solucani-alarmi-10887623 (28.04.2020).

___, “Military expenditure by country, in constant (2017) US$ m., 1988-2018” (2019), sipri.org: https://www.sipri.org/sites/default/files/Data%20for%20all%20countries%20from%201988%E2%80%932018%20in%20constant%20%282017%29%20USD%20%28pdf%29.pdf (16.01.2020)

___, “Peace without Syria Is Unthinkable” (19.01.2009), https://www.spiegel.de/international/world/spiegel-interview-with-syrian-president-bashar-assad-peace-without-syria-is-unthinkable-a-602110.html (02.05.2020).

___, “Rusya Ukrayna Skandalının Kilit Şirketine Siber Saldırı Düzenledi” (14.01.2020), https://www.amerikaninsesi.com/a/rusya-ukrayna-skandal%C4%B1n%C4%B1n-kilit-%C5%9Firketine-siber-operasyon-d%C3%BCzenledi-/5245207.html (21.04.2020)

___, “The NSA and Its Willing Helpers” (08.07.2013), https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html (14.04.2020).

___, “U.S. government concludes cyber attack caused Ukraine power outage” (26.02.2016), https://www.itsecurityguru.org/2016/02/26/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage/ (20.04.2020).

___, "UNIAN: Ukraine's cyber police report constant cyberattacks from Russia" (12.08.2012), https://www.kyivpost.com/ukraine-politics/unian-ukraines-cyber-police-report-constant-cyberattacks-from-russia.html (21.04.2020).

___, "Ünlü virüs Atatürk Havalimanı'nda" (30.01.2009), https://www.ntv.com.tr/turkiye/unlu-virus-ataturk-havalimaninda,uVcwpKeXLEqXo6d99N2fuw (29.04.2020).

___, "We Have to Be Constantly on Guard" (18.01.2011), https://www.spiegel.de/international/world/iran-s-chief-nuclear-negotiator-we-have-to-be-constantly-on-guard-a-739945.html (14.04.2020).

___, "What is a computer worm, and how does it work?" (t.y.), https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html (30.12.2019).

___, "Creation of a global culture of cybersecurity (31.01.2003)", https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf (10.05.2020).

___, "Global Social Media Users Pass 3.5 Billion (t,y), https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion (2.11.2019).

___, "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security" (2.12.2008), https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/Shanghai+Cooperation+Organization+Agreement+on+Cooperation+in+the+Field+of+International+Information+Security+6-16-2009.pdf (15.05.2020).

Ünal, A.N. ve Yarman, B. S. B. (2014), "Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü", **7th International Conference on Information Security and Cryptology,** (278-284), İstanbul.

Ünver Mustafa vd. (2011), **Köle Bilgisayar ve Köle Bilgisayar Ağları Zombi ve Botnetler,** Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Üret, Ataberk (04.02.2019), "Ukrayna'nın seçim sistemine müdahele girişimi", https://www.ukrayna.com/ukrayna-nin-secim-sistemine-mudahele-girisimi/ (21.04.2020).

Valeriano, Brandon ve Maness, Ryan C. (2015), **Cyber War versus Cyber Realities: Cyber Conflict in the International System,** Oxford University Press, New York.

Vasquez, John A. (2004), **The Power of Power Politics**, Cambridge University Press, Cambridge.

Ventre, Daniel (2011), "Cyberconflict: Stakes of Power", D. Ventre (Ed.), **Cyberwar and Information Warfare**, *içinde* (113-244), Iste Ltd., London.

Viotti, Paul R. ve Kauppi, Mark V. (2012), **International Relations Theory,** Pearson Education, Inc., Glenview.

Waever, Ole (2003), "Securitisation: Taking stock of a research programme in Security Studies", 1-36, https://docplayer.net/62037981-Securitisation-taking-stock-of-a-research-programme-in-security-studies.html (07.05.2020).

Wall, David (2001), "Cybercrimes and the Internet", David Wall, **Crime and the Internet: Cybercrimes and Cyberfears**, *içinde* (1-17), Routledge, London.

Waltz, Kenneth (1979), **Theory of International Politics**, Addison-Wesley Publishing Company.

Wattanajantra, Asavin (23.06.2009a), "Conficker worm hits hospital PCs in Sheffield", https://www.itpro.co.uk/609615/conficker-worm-hits-hospital-pcs-in-sheffield (29.04.2020).

_____(16.06.2009b), "Royal Navy systems hit by computer virus", https://www.itpro.co.uk/609550/royal-navy-systems-hit-by-computer-virus (29.04.2020).

Weimann, Gabriel (2005), "Cyberterrorism: The Sum of All Fears?", **Studies in Conflict & Terrorism,** 28(2), 129-149.

Wendt, Alexander (1992), "Anarchy is what States Make of it: The Social Construction of Power Politics", **International Organization,** 46(2), 391-425.

_____ (1995), "Constructing International Politics", **International Security**, 20(1), 71-81.

_____ (1999), **Social Theory of International Politics,** Cambridge University Press, Cambridge.

Willsher, Kim (07.02.2009), "French fighter planes grounded by computer virus", https://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (29.04.2020).

Windrem, Robert (18.12.2016), "Timeline: Ten Years of Russian Cyber Attacks on Other Nations", https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111 (21.04.2020)

Wolf Jr., Charles (2000), "Globalization: Meaning and Measurement", **Critical Review,** 14(1), 1-10.

Wueest, Candid (2014), **Targeted Attacks Against the Energy Sector**, Symantec.

Yar, Majid (2006), **Cybercrime and Society**, SAGE Publications, London.

Yayla, Mehmet (2013), "Hukuki Bir Terim Olarak Siber Savaş". **TBB Dergisi**, 104, 177-202.

Yılmaz, Onur (2017), "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", **Siber Politikalar Dergisi,** *2*(4), 22-43.

Yüksel, Merve ve Öztürk, Nihat (2017), "SIP Saldırıları ve Güvenlik Yöntemleri", **Bilişim Teknolojileri Dergisi,** 10(3), 301-310.

Zehfuss, Maja (2004), **Constructivism in International Relations**, Cambridge University Press, Cambridge.

Zetter, Kim (02.10.2019), "Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran" , https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html (15.04.2020).

Zubkova, D. (09.10.2018), "State Fiscal Service Under Cyber Attack", https://ukranews.com/en/news/588643-state-fiscal-service-under-cyber-attack (21.04.2020).

ÖZGEÇMİŞ

Buğrahan EMİR, 23.01.1995 tarihinde Trabzon İli Vakfıkebir İlçesi'nde doğdu. 2005 yılında Kıbrıs İlkokulu'nu; 2008 yılında Kıbrıs Ortaokulu'nu; 2012 yılında Yatağan Anadolu Lisesi'ni; 2017 yılında Uludağ Üniversitesi – İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü'nü bitirdi. 2018 yılında Karadeniz Teknik Üniversitesi – Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalında yüksek lisans programına başladı.

EMİR, bekâr olup iyi düzeyde İngilizce ve başlangıç düzeyinde Almanca bilmektedir.