T.C.
BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER BİLİM DALI

SİBER GÜVENLİĞİN STRATEJİK BAKIŞ ÇERÇEVESİNDE KONUMLANDIRILMASI: TEHDİT/CAYDIRICILIK BAĞLAMINDA ÖRNEK KRİZ İNCELEMELERİ

Doktora Tezi

Tezi Hazırlayan:

Ahmet Emre KÖKER

İstanbul, 2021

T.C.
BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER BİLİM DALI

SİBER GÜVENLİĞİN STRATEJİK BAKIŞ ÇERÇEVESİNDE KONUMLANDIRILMASI: TEHDİT/CAYDIRICILIK BAĞLAMINDA ÖRNEK KRİZ İNCELEMELERİ

Doktora Tezi

Tezi Hazırlayan:
Ahmet Emre KÖKER

Öğrenci No:
140715002

Orcid: 0000-0002-8032-4237

Danışman:

Dr. Öğr. Üyesi Mustafa SUNDU

İstanbul, 2021

YEMİN METNİ

Doktora Tezi olarak sunduğum "Siber Güvenliğin Stratejik Bakış Çerçevesinde Konumlandırılması: Tehdit/Caydırıcılık Bağlamında Örnek Kriz İncelemeleri" başlıklı bu çalışmamın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. 04/02/2021

Ahmet Emre KÖKER

TEZ ONAYI

Beykent Üniversitesi Lisansüstü Eğitim Enstitüsü ***Siyaset Bilimi ve Uluslararası İlişkiler Doktora*** öğrencisi ***140715002*** numaralı ***Ahmet Emre KÖKER'***in hazırladığı ***"Siber Güvenliğin Stratejik Bakış Çerçevesinde Konumlandırılması: Tehdit-Caydırıcılık Bağlamında Örnek Kriz İncelemeleri"*** konulu DOKTORA TEZİ ile ilgili TEZ SAVUNMA SINAVI Lisansüstü Öğretim ve Sınav Yönetmeliğinin ilgili maddesi uyarınca 04.02.2021 günü saat 15:30'da Microsoft Teams programı aracılığıyla on-line olarak yapılmış, sorulan sorulara alınan cevaplar sonucunda adayın tezinin ***KABULÜ'***ne ***OYBİRLİĞİ'***yle karar verilmiştir.

JÜRİ ÜYESİ	KANAATİ	İMZA
Dr. Öğr. Üyesi Mu***** SU*** (Danışman) (İstinye Üniversitesi)		
Prof. Dr. Bu*** Samih GÜ**** (Üye) (İstanbul Üniversitesi)		
Doç. Dr. Mi** Mu****** AF**** FI****** (Üye) (Beykent Üniversitesi)		
Doç. Dr. Ar***** Em** ÇA*** (Üye) (Marmara Üniversitesi)		
Doç. Dr. Oz** ÖR**** (Üye) (İstanbul Kent Üniversitesi)		

Adı ve Soyadı : Ahmet Emre KÖKER
Danışmanı : Dr. Öğr. Üyesi Mustafa SUNDU
Türü ve Tarihi : Doktora Tezi,2021
Alanı : Uluslararası İlişkiler
Anahtar Kelimeler : İnternet , Siber Uzay, Güvenlik, Strateji, Savaş, Tehdit, Caydırıcılık, Çatışma, İttifak

ÖZ

SİBER GÜVENLİĞİN STRATEJİK BAKIŞ ÇERÇEVESİNDE KONUMLANDIRILMASI: TEHDİT/CAYDIRICILIK BAĞLAMINDA ÖRNEK KRİZ İNCELEMELERİ

Uluslararası ilişkilerdeki tehdit, caydırıcılık ve güvenlik kavramlarının zaman içindeki değişimleri ve savaş araçlarında yarattığı dönüşüme vurgu yapılarak örnek krizler bağlamında günümüzde siber çatışma döneminin yaşandığı belirtilmiştir. Siber çatışmada, siber silah kavramına odaklanarak siber kavramların ulusların milli güvenliklerinde oynadıkları rolün güçlü ve zayıf yönleri stratejik perspektifte tespit edilmeye çalışılmıştır. Böylece 21. yüzyılda asimetrik tehditlerin ortaya çıkmasıyla aktörler arasında yaşanan rekabet ve güç elde etme yarışının ciddi bir küresel siber kriz yaşanması ihtimalini oluşturduğu değerlendirilmektedir.

Bu doğrultuda siber silahların konvansiyonel veya nükleer bir savaşa girmeden aynı sonuçları sağlayabilecek şekilde etkin ve etkili olduğu, kritik alanlara yönelik etkilerinin ve sonuçlarının domino etkisiyle büyük zararlar verebileceği, iç hukukta buna yönelik önlemler alındığı fakat uluslararası alanda henüz düzenlemeler gerçekleştirilmediği üzerinde durulmuştur. Siber güvenlik alanında tüm aktörlerin özgürlüklerini, eşitliklerini, haklarını ölçecek bir işbirliği modelinin geliştirilmesine yönelik siber uzaydaki faaliyetlerin kolay ölçülebilebileceği kuralların ve bu kuralları denetleyecek bir üst otorite kurumunun zorunluluğu vurgulanmaktadır.

Sonuç olarak teknolojik gelişmeler sonucunda geleneksel güvenlik algılamalarının ve sınırlarının yerine aktörler arasında yaşanacak çatışmaların siber alanda gerçekleşerek uluslararası ilişkilerde hakim inanış haline dönüşeceği değerlendirilmektedir. Bu değerlendirme neticesinde gelecek düzen hakkında öngörüler belirlenerek küresel anlamda çözüm için bazı model önerileri sunulacaktır.

Name and Surname : Ahmet Emre KÖKER
Supervisor : Assist. Prof. Mustafa SUNDU
Degree and Date : Phd, 2021
Major : İnternational Relations
Key Words : The Internet, Cyber, Security, Strategy, War, Threat, Cooperation, Conflict, Deterrence

ABSTRACT

POSITIONING CYBER SECURITY WITH A STRATEGIC PERSPECTIVE: CASES ANALYSIS WITH THE CONTEXT OF THREATS/DETERRANCE

Emphasizing the changes in the concepts of threat, deterrence and security in international relations over time and the transformation they have created in war vehicles, it was stated that the cyber conflict period is experienced today in the context of exemplary crises. In cyber conflict, focusing on the concept of cyber weapons, the strengths and weaknesses of the role of cyber concepts in the national security of nations have been tried to be determined in a strategic perspective. Thus, in the 21st century, with the emergence of asymmetric threats, it is considered that the competition between actors and the race to gain power creates the possibility of a serious global cyber crisis.

In this direction, it has been emphasized that cyber weapons are effective and effective in such a way that they can provide the same results without entering a conventional or nuclear war, their effects and results on critical areas can cause great damage due to the domino effect, measures have been taken in domestic law, but regulations have not been made in the international area yet. In the field of cyber security, it is emphasized that the rules that can be easily measured for the activities in cyber space and the necessity of a higher authority institution to control these rules are emphasized to develop a cooperation model that will measure the freedom, equality and rights of all actors.

As a result, it is considered that as a result of technological developments, instead of traditional security perceptions and limits, conflicts between the actors will take place in the cyber space and turn into the dominant belief in international relations. As a result of this evaluation, predictions about the future order will be determined and some model proposals for a global solution will be presented.

İÇİNDEKİLER

Sayfa No.

İKİNCİ BÖLÜM

SİBER GÜVENLİK VE SİBER UZAY KAVRAMI

ÜÇÜNCÜ BÖLÜM

SİBER SAVAŞ

DÖRDÜNCÜ BÖLÜM

FARKLI ÜLKELER ve ULUSLARARASI KURUMLAR ÖZELİNDE SİBER GÜVENLİK ANLAYIŞLARININ VE POLİTİKALARININ KARŞILAŞTIRMALI ANALİZİ

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ARGE : Araştırma ve Geliştirme
ARPA : İleri Seviye Araştırma Projeleri Kurumu
ARPANET : Amerikan Gelişmiş Savunma Araştırmaları Dairesi Ağı
BM : Birleşmiş Milletler
DARPA : İleri Savunma Araştırma Projeleri Ajansı
DDOS : Dağıtılmış Hizmet Reddi ve Ağ Saldırısı
DNS : Alan Adı Sistemi
ENISA : Avrupa Birliğinin Ağ ve Bilgi Güvenliği Kurumu
IEN : Internet Erişim Noktası
IOT : Nesnelerin İnterneti
ISS : Internet Servis Sağlayıcıları
ITU : Uluslararası Telekominikasyon Birliği
LAN : Yerel Bilgisayar Ağları
NATO : Kuzey Atlantik Antlaşması Örgütü
NCIRC : NATO Bilgisayar Olayları Karşılama Kapasitesi
NPT : Nükleer Silahların Yayılmasını Önleme Anlaşması
OGSP : Ortak Güvenlik ve Savunma Politikası
START : Stratejik Nükleer Silahların İndirimi Anlaşması
TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
ULAKBİM : Ulusal Akademik Ağ ve Bilgi Merkezi
ULAKNET : Ulusal Akademik Ağ
USOM : Ulusal Siber Olaylara Müdahale Merkezi
VPN : Sanal Özel Ağ
WAN : Geniş İletişim Ağı
WWW : Dünya çapında ağ

GİRİŞ

Uluslararası anarşik sistem içerisinde tarih boyunca sürekli savaş araçları, tehdit unsurları ve güvenlik algısı teknolojik gelişmeler sonucunda değişmiştir. Bilgi devrimi ile birlikte internet teknolojisinin hayatımıza girmesi sonucunda siber uzay adı altında beşinci bir boyutta yeni bir alan ortaya çıkmıştır. Bu yeni alanda bireyler, devlet dışı örgütler ve küçük devletler, büyük ve güçlü devletlere karşı asimetrik bir güç kazanmıştır. Bu bağlamda aktörler arasında geçen mücadele, milli yazılıma sahip olma, büyük veriyi kontrol etme, en az maliyet ve kayıpla rakiplere karşı üstün gelme, caydırıcılık yaratarak gücünü kabul ettirme, dijital dünyanın sınır güvenliğini sağlama, yapay zekâyı kontrol etme, siber ordular oluşturarak güç ve tehdit unsurlarını kontrol etme vb. noktalara dönüşmüştür. Yani, dijitalleşmeyle birlikte hayatın her alanı dijitalleşerek siber tehdit ve risklerin önemi artmıştır. Aynı zamanda siber uzayın sahip olduğu özelliklerden dolayı tehdit algılamaları, küresel güvenlik ortamındaki güvensizliği, belirsizliği ve istikrarsızlığı tetikleyici başat ögelerden birisi haline gelmiştir.

Bu çalışmada güvenlik teorileri üzerinden siber tehdit unsurlarının yeni savaşların en önemli araçlarından biri haline gelmesine yol açan sorunsallar işlenecektir. Bu sorunsallar çerçevesinde örnek çatışmalar incelenerek çözüm için yeni bir model sunulacaktır. Sunulan bu yeni modelde siber güvenliğin küresel düzeyde siber tehdit alanlarının belirlenmesi ve risklerin azaltılması için ihtiyaç duyulan kurallar ortaya konacaktır. Bu ihtiyaç kapsamında uluslararası/uluslarüstü düzeyde aktörlerin aldıkları güvenlik ve savunma önlemleri, caydırıcılık faaliyetleri, hukuki düzenlemeler, bölgesel ve küresel işbirlikleri ile birlikte saldırı ve savaş örnekleri uluslararası ilişkilerin temel kavramsal teorileri çerçevesinde kronolojik bir sıralama ile dönem incelemesi yapılacaktır. Dönem incelemsi yapılmasının nedeni, tarih boyunca sürekli olarak teknolojik inovasyonların, savaşın taktik ve stratejilerini değiştirip dönüştürmüş olmasıdır.

Buna ilave olarak, siber saldırıların ucuz, hızlı, etkili, uzaktan gerçekleştirilen, maddi ve manevi ciddi kayıplara sebep olan, uygulayıcısı tespit edilebileyemen özellikleri bulunmaktadır. Bu gibi özellikleri nedeniyle ülkeler siber savaş yeteneği kazanma konusunda motive olmaktadır. Geliştirdikleri siber savş yetenekleri ile siber savaşın sunduğu fırsatlardan faydalanma ve tehditlerlerden

korunma çabası içine girmektedir. Ayrıca askeri tehditlerin dışında da sosyal ve kültürel denge, ekonomik ve finans sistemi, sağlık ve ulaşım sistemi, enerji sistemleri ve boru hatları, nükleer tesisler vb. birçok alanda etkili olabilen siber silahlar dijital dünyada yaşanacak siber savaşın yıkımlarının nükleer savaş kadar etkili sonuçlar doğurma ihtimali bu bağlamda değerlendirebilir. Böylece, küreselleşmenin geçirdiği evrim ve teknolojik gelişmeler sonucunda 21. yüzyılda yaşanacak ana çatışmalar, güç parametreleri, caydırıcı unsurlar, tehdit ve güvenlik algılarının siber alanda gerçekleşecektir. Bu sebeple siber saldırılara yönelik hem ulusal hem de uluslararası alanda önlem alınması zorunluluğu vardır.

Yukarıda bahsedilen bağlamda tezin birinci bölümünde tezin sorunsalını teorik bir perspektif üzerinden tartışabilmek için, öncelikle uluslararası ilişkiler teorilerinin konuya yaklaşımı kısaca ele alınacak, ardından tezin teorik çerçevesi olarak neoliberal kurumsalcı yaklaşımın tercih edilme nedenlerine ve yaklaşımın sorunsala ilişkin argümanlarına yer verilecektir. Bu bölümde son olarak tehdit, çatışma ve güvenlik kavramları kullanılarak uluslararası rejimleri açıklamaya yönelik diğer teorilerin tartışmaya katkısı değerlendirilecektir.

İkinci bölümde, küresel olarak yaşanan dijital dönüşüm kavramları açıklanarak bilgi devrimi ile değişen toplum yapısı, geleceğe yön veren yeni nesil kavramlar ve teknolojik araçlardaki değişimler sonucunda siber risk ve tehditlere yönelik literatür irdelenecektir. Bu amaçla, siber risk ve tehditlerin artan rolü siber uzayda donanım ve yazılım güvenliğinin sağlanması, siber uzayın yeni bir boyut olarak konumlandırılması sonrasında uluslararası ilişkiler'de sağladığı üstünlük ve zayıflıkların belirlenmesi, yeni tür siber silahların kullanılırlığının artması şeklinde sorunsallar incelenecektir. Nitekim, siber uzayın gelişimiyle birlikte ortaya çıkan güçlü ve zayıf yönler tespit edilmeye çalışılmış ve bu tespitlerle siber güvenliği etkileyen silahlara değinilmiştir. Böylece siber silahların etkileri yapısal düzeyde ele alınarak ülkeler aleyhine yarattığı yıpratma, engelleme, diplomasi yürütme ve caydırma gibi faaliyetlerin siber silah yarışını tetiklediği sonucuna ulaşılmaktadır. Bu doğrultuda siber uzayın içerdiği muğlaklıkların giderilebilmesi için daha çok bilimsel çalışma yapılaması gerektiğine dikkat çekmektedir.

Üçüncü bölümde; siber kavramlarının tanımlaması yapılarak harbin beşinci boyutunu oluşturan Siber Savaş'lar açıklanmıştır. Bu açıklama gerçekleştirilirken

siber savaşların varlığını ve yaşandığını belli teoriler, kavramlar ve görüşler çerçevesinde bir temele oturtulmuştur. Böylece "savaş" kavramı ile yaşanan siber saldırılar arasında bir bağ kurularak domino etkisiyle kritik alanlara yönelik gerçekleştirilecek siber savaşın diğer savaş türleriyle arasındaki benzerlikler ve farklılıklar ortaya konulacaktır.

Dördüncü bölümde, tezde geliştirilen analitik çerçevede seçilen özellikle soğuk savaş sonrasında ortaya çıkan bu yeni çatışma boyutuyla birlikte gerçekleşen saldırılar, casusluklar, suç ve terör olayları ile birlikte savaşlar üzerinden en önemli aktörlerin siber savaş kabiliyetleri ve siber savaş faaliyetleri üzerinden çatışma örnekleri incelenecektir. Bu örnek vakalar üzerinden "mahkumun ikilemi" oyun madeline dayandırarak ABD, Rusya, Çin gibi ülkelerin yanında NATO ve AB gibi kurumlar özelinde gerçekleşen güç yarışına yönelik uluslararası alandaki bilinç ve farkındalığın tespit edilmeye çalışılacağı yeni bir yaklaşım getirmeyi amaçlamaktadır. Bunun yanında küresel anlamda siber savaşların önlenmesine yönelik uluslararası kurum yapısı ve kurallarına yönelik model önerisi sunarak sonlanacaktır.

Tezin sorunsalı, temel değişkenimiz olan insan doğası ve küresel düzenin anarşik yapısının siber güvenlik sorunları da doğuracağıdır. Burada insan doğası ve anarşik yapıyı içeren bağımlı değişkenimizdeki problemden yola çıkarak (botnet, virüs, solucan, ddos vb.) saldırıların günümüzde arttığını ve bu saldırılara ulusal ve küresel bazda önlemler alınması zorunluluğunu ortaya koymaktır. Burada bağımsız değişkenimiz yaşanan siber çatışmalar, bağımlı değişkenimiz ise ulsuslarası güvenlik ortamının yaratacağı tehditlerdir. Bu ilişkilerden harektele çalışmanın hipotezleri şu şekildedir:

H1: "*Siber alan uluslararası güvenlik açısından stratejik bir alandır.* "

H2:"*Siber uzayın getireceği tehdit ve fırsatlar stratejik yönetim ihtiyacı gerektirmektedir."*

H3: "*Siber tehditler uluslararası güvenlik sorunudur".*

Strateji kavramı güvenlikle, güvenlik kavramı ise tehdit ve risk kavramları ile birlikte değerlendirilmektedir. Dolayısıyla, güvenlik ve tehdit, karşılıklı ve sürekli olarak birbirlerini etkileyen bir yapıda olduğu için siber alanda tehdit belirleme ve

güvenlik stratejisi oluşturulmasının ana sebebi anarşik uluslararası sistemin sahip olduğu doğa durumudur. Bu doğrultuda, siber güvenlikte herkes güvende olmadan hiç kimse güvende olamaz. Bu durumda aktörler arasındaki karşılıklı etkileşim ile birlikte oluşan siber ortamın içerdiği bilinmezlik korkuyu, korkular tehdidi, tehditler ise güvenlik riskini ortaya çıkarmıştır. Tüm bu kavramlar ise strateji ve savaş kavramlarının konuşulmaya başlamasını zorunlu kılmıştır. Güvensizliğin hâkim olduğu siber uzay ortamında devletler sürekli "güvenlik ikilemi" yaşamış ve "güç dengesi" peşinde koşmuşlardır. Böyle anarşik bir yapıdaysa devletler askeri güçlerine güvenmek ve bu alanda kendi askeri güçlerini yeterli düzeyde tutmak zorunda hissetmişlerdir. Bu his sonunda da günümüzde askeri yapıların içerisinde siber ordu birimleri kurarak oluşabilecek güç boşluğunu doldurmak istemişlerdir. Bu durumun asıl sebebide aslında güvende olmama hali veya sürekli bir güvensizlik ve belirsizlik ortamının oluşturduğu tehdit algısıdır. Bu sanal tehdit algısı özellikle Soğuk Savaş sonrası dönemde, geçmiş dönemlerin aksine, klasik "düşman" nitelendirmesinin büyük oranda geçerliliğini yitirmesine yol açarak güvenlik algılamaları ve tehditler ile mücadele yaklaşımını ön plana çıkarmıştır.

Siber güvenlik stratejilerinin barışçıl, çatışmacı, caydırıcı ve savaş stratejilerinin belirlenmesi, planlanması ve uygulanması şarttır. Çünkü siber alanda savunmanın sağlanabilmesi kapsamlı bir yaklaşım ister. Bunların içinde eğitimler, hukuki düzenlemeler, tatbikatlar, arge faaliyetlerinin gelişimi, farkındalık yaratılması gibi çalışmaların yanında önleyici diplomasi, ittifak ve caydırıcı faaliyetlerde belirgin olarak kullanılmalıdır.

Bu faaliyetlerin ortaya konulabilmesi için saldırıların sorumlularının bilinmesi gerekmektedir.Saldırıların arkasında olan, kışkırtma yaptığına yönelik kanıtlar bırakan, sorumluluktan kaçmak için ortaya çıkmayan ve siber uzayın gizemiyle kimliğini saklamaya çalışan sponsor devletlere yönelik uluslararası hukuk kapsamında bir yasal rejim oluşturulması şarttır. Sponsor devletlere yönelik oluşturulacak bu yasal rejim sonucunda sanal mülkiyet oluşacaktır.

Yargı perspektifinden bakıldığında, gerçek alanda işlenen bir suçu mevcut yasalar çerçevesinde atamak kolayken siber alanda aynı suç işlendiğinde, atamak genellikle zordur. Fakat bu zorluğu hafifletmenin bir yolu vardır. Bu yol internetin

özünde bir bilgi ortamı olması sebebiyle siber alanda sanal mülkiyet kavramının oluşturulmasıdır.

Sanal mülkiyet kavramı kurumsalcı teoriyle değerlendirildiğinde sorumluluğun devletler tarafından üstlenilmelisi ve bu konuda politikalar geliştirilmesi gerekmektedir. Yani devletler kendi içlerindeki tüm alanların ve dışarıya karşı oluşabilecek tüm saldırıların özel veya kamu olsun sorumluluğunu alması gerekmektedir. Bu sorumlulukta üst otorite kurum ve kurallarla kontrol edilmelidir. Bu kontrol çabasıysa ulusal ve uluslararası ortak hukuk prensipleriyle var olabilir. Bu prensip siber uzayın ağ bütünlüğü içinde ele alınmasını ve ağ yöneticisinin astın eylemlerinden sorumlu olması gerekli kılacaktır. Eğer bu konuda anlaşılırsa internetin karanlık yüzü tarafından kötü amaçlar için kullanımı(botnet, virüs, solucan, ddos vb.) sınırlandırılabilir. Bu sınırlandırma sonucunda da ortak suçluların muamelesine yönelik bir model oluşturulmalıdır.

Avrupa Siber Suçlar Sözleşmesinden ve evrensel siber hukuk kurallarından yararlanılarak tarafların yükümlülükleri belirlenebilir. Uluslarası toplum ile birlikte uluslararası hukuk kuralları ortaya konur ve böylece ülkelerin kendini savunma esasları belirlenebilir. Böyle bir hukuki çerçeve ile saldırganlığın hangi koşullarda oluşacağı tarif edilebilir. Dolayısıyla her devletin sorumluluklarını yerine getirmesi mecburiyeti ortaya çıkar ve uluslarası toplumun bu konuda zorlayıcı tedbirler alması mümkün hale gelir.

Bir siber saldırıya uğrayan devlet saldırının geldiği devletteki sorumluların adalete teslim edilmesini veya cezalandırılmasını isteyebilmelidir. Bunun içinde siber silahlarla gerçekleşen saldırıların düzeyi diğer konvansiyonel veya nükleer silahlar düzeyine yükseltilmelidir. Dahası bu tezde gerçekleştirilmesini önerdiğimiz vekalet yasası, üst otorite kurulmasının zorunluluğu uluslararası norm ve kaidelerin zorunluluğuna yöneliktir. Bu doğrultuda savaş kuralları ve uluslararası kaideler günümüz tehditlerini tam olarak kapsamamaktadır. Bu yüzden bu kuralların siber savaş kriterlerini içine alacak şekilde revize edilmesi gerekmektedir. Bu revize işleminin gerçekleştirilmesinde ise küresel bir çaba olmalıdır.

Birleşmiş Milletler(BM) Sözleşmesi, Lahey ve Cenevre Sözleşmeleri ve ilgili antlaşmalar devletler arasındaki "kuvvet kullanımının hukuki sonucu", "güç kullanımı", saldırganlık ve savaş eylemlerini değerlendirmenin tek temelidir. BM

tarafından ortaya konacak yaptırımlar veya cezai eylemler siber saldırganlar için güçlü bir caydırıcılık yaratmalıdır. Aynı zamanda bu zorunluluk her devletin önleyici veya öngörülen siber saldırılara ve yaklaşmakta olan tehlikelere karşı kendini savunma hakkını veya her türlü misilleme gerçekleştirmesine de katkı sağlayacaktır. İnternet kullanıcıları ister birey ister devlet olsun çevrimiçi söyledikleri ve yaptıklarıyla ilgili yasal sorumluluk almak zorundadır.

Günümüz şartlarında; Devletlere ilişkin temel hukuki düzenleme olan BM Sözleşmesi'nde 51. maddede; klasik/fiili anlamda bir çatışmadan bahsedildiği, Madde 2 (7)'deki iç işlere müdahale edilmemesi maddesinin siber casusluk ve saldırıları kapsamadığı, Madde 2 (4)'deki tehdidi veya güç kullanımını yasaklayarak tüm üyelerin diğer devletlerin egemenliğine, toprak bütünlüğüne ve siyasi bağımsızlığına saygı duymaya çağırdığı maddelerin siber sınırları kapsamadığı üzerine kurulmuştur. BM Sözleşmelerinin bu maddelerinin yanında NATO'nun 5. Maddenin siber saldırıyı kapsamaması, uluslararası hukukta bir savaşa girmeyi meşru kılan unsurların siber savaşlarda tanımlanmamış olması sorunun kaynağı olarak kabul edilebilir.

Güncellenecek bu ilgili maddeler çerçevesinde ihlal edilen maddelere dayanılarak kuvvet kullanmanın dinamik yapısı göz önünde bulundurularak fiziki gücü içermeyen ancak silahlı saldırı ile aynı derecede somut zararlara sebep olabilen siber saldırılar, kuvvet kullanmaya eşdeğer olabilirler. Bu doğrultuda, uluslararası hukuk siber saldırıları sınırlayabilir mi? Ya da adil bir bilgi savaşını oluşturan nedir?, Siber savaşlarda tahmin edilenden daha büyük felaketler ortaya çıkabilir mi?, Sınır, zaman ve mekan tanımayan siber saldırılar "kim" tarafından ve "nasıl" tespit edilecektir?, Eylem ve fail arasındaki sorumluluk ilişkisi ya da illiyet bağı "ne şekilde" kurulacaktır? Siber saldırılara karşı verilecek ceza kişilere mi yoksa devlete mi verilmelidir? Burada devletlerin anlaşabileceği ortak bir standart konulabilir mi?, Siber güvenlikle ilgili uluslararası hukukta siber saldırılara karşı yapılacak mukabele ile misillemenin şekli ve sınırları nasıl çizilecektir?, Siber saldırıları önleme, tespit etme ve karşılık verme aşamasında bilgi paylaşımı konularındaki uluslararası iş birliği kurumsal teori çerçevesinde ne şekilde sağlanabilir?, Uluslararası İlişkiler alanında, caydırıcılık ve siber silahlar arasında nasıl bir bağ vardır?, Siber saldırıların kritik alt yapıları etkileme gücü ne oranda bir yıkım yaratır?, Siber çatışmaları savaş

olarak nitelendirebilir miyiz? Nitelendirirsek de ne tür bir savaştır veya bu tezde belirtilen "World Wide Web Dünya Savaşı" gerçekleşmeden yasaklana bilir mi?, Siber çatışmaların amaç, araç ve hedefleri nelerdir?, Siber uzayın düzenlenmesi için bir üst otorite kurulması şart mıdır?, Siber uzayın sınırlarının olmaması ve küresel boyutta yaşanması ona ne gibi avantajlar ve dezavantajlar sağlar?, Geçmişten günümüz siber çatışmalarına kadar savaş araçları, güvenlik ikilemi, tehdit, caydırma ve güç kullanımı bakışı ne şekilde gelişmiştir?, Siber uzayın stratejik bakışta ele alınmasının sebebi nedir? Bunlar ve benzeri sorular çerçevesinde siber uzayda adil bir bilgi savaşı oluşturulabilmesi için siber saldırıların tehdidinin tanımlanması şarttır. Birleşmiş Milletler Şartı'nın özellikle 39, 41, 42 ve 52. Maddeleri siber uzaya yönelik bir yol haritasının sunulabilmesi için çok önemlidir. İlgili maddelerin içerdiği muğlaklıkların giderilmemesi sonrasında aktörleri caydıracak veya cezalandıracak bir mekanizmanın da olmamasıyla birlikte uluslararası ilişkilerde gerçekleşen siber çatışma riski devam edecektir.

Bu doğrultuda siber ihlallerden kimin sorumlu ve yükümlü olduğu genellikle net olmadığından BM'nin yetkilendireceği ITU (Uluslararası Telgraf Birliği) tarafından getirilecek kurallar evrensel kabul görmeli; meşru kabul edilmelidir. Birleşmiş Milletler müzakereleri zor ilerleyen konuları kapsadığından bir alt kurum altında sürecin geliştirilmesi ilerlemeleri hızlandıracaktır. BM tarafından ITU'nun yetkilendirilmesi ve ilgili kuralların düzenlenmesiyle birlikte devletler özelinde gerçekleşecek saldırılar kontrol altına alınabilir.

Aynı zamanda siber silah yarışının yarattığı kaygan zemin çok taraflı siber uzay sisteminin temelini zayıflatmaktadır. Siber silahların sınırlandırılması, kısıtlanması, etkisinin azaltılması, izinsiz ve haksız olarak kullananlara yönelik cezalandırmaların gerçekleştirilmesi gibi konularda mevcut durumda sistemsel etkisi negatiftir. Kullanım sınırlanmazsa ve belli kurallar altına alınmazsa riskler artacaktır. Aslında, maliyetleri düşük tutmak için diğer ülkelerden kullanıma hazır teknolojilerin kullanımı siber risk ve tehditleri arttırmaktadır. Eğer bu oluyorsa dijital araçlara yönelik siber güvenlik standartları ve bu araçların siber güvenliklerini düzenleyecek ve sağlayacak bir mekanizma oluşturulmalıdır. Böylece bu mekanizmayı inşa eden ve işleten tüm aktörler sorumluluğu üzerine almış olacaktır. Oluşturulacak bu mekanizma bu sorunu ortadan kaldıracaktır.

Burada siber silahların içerdiği en temel sorun dijital anlamda gelişmiş devletlerin aynı zamanda siber tehditlere karşı en hassas konumda olmalarıdır. Mayıs 2015'te Rusya ve Çin arasında siber uzay için "Saldırmazlık Paktı" imzalanması, başta ABD başta olmak üzere AB ve NATO gibi örgütlere üye devletleri de siber güvenliklerini sağlayabilme konusunda endişelendirmektedir.

Diğer taraftan, siber operasyonların daha kapsamlı değerlendirilmesi ve karakterize edilmesi yönünde bir yaklaşım sunan Schmitt Analizi, siber silahlarla kuvvet kullanımındaki nicel ve nitel boşluğu kapatmaya çalışmaktadır. Stanford Üniversitesi tarafından hazırlanan "Siber Suç ve Terörizmle İlgili Uluslararası Bir Sözleşme Önerisi" daha büyük bir uluslararası işbirliğinin sağlanabilmesi için siber saldırılara karşı mücadelede çeşitli argümanlar sunmuştu. Avrupa Konseyi Siber Suç Sözleşmesindeki kriterler ve yasalar ile edindikleri kazanımlar zaten, siber savaşların önemini ve bilinilirliğini ortaya çıkararak olumsuz etkilerini sürekli eritmektedir.

Bunlara ilave olarakta siber silahlardan gelecek tehditleri öngörebilmek için oluşturulan veri modelleme ve veri geliştirme süreçleri ile Saldırı Tespit Sistemleri uluslararası anarşik sistemde gerçekleşen siber çatışmalarda kullanılmaktadır. Bu Saldırı Tespit Sistemleri (IDS)'ni gerçekleştirmek için oluşturulan birçok örnek vardır. Tezde de bu tespit sitemlerinden ADAM projesi ve MINDS projesi üzerinde durulmuştur. Örneğin; veri madenciliği tekniklerinin bir IDS oluşturmak için nasıl kullanılabileceğini göstermek amacıyla Columbia Üniversitesi tarafından İngilizce ismi "Audit Data Analysis and Mining" olan ADAM projesi, daha sistematik ve otomatik bir şekilde normal ağ davranışını saldırı gerçekleşmeden öğrenmeye yarar. Bir diğer örnek Minnesota Üniversitesi tarafından gerçekleştirilen MINDS projesi kapsamında veri madencilik teknikleri kullanılarak bilgisayar ağları ve sistemleri üzerine gerçekleştirilebilecek saldırıların nasıl otomatik olarak tespit edilebileceğini göstermektedir. Bu sistemlerin hiçbiri 7/24 güvenli bir yapı asla sunamaz. Bu sistemler sadece alternatif yöntem sağlayarak riski azaltan bir ön uyarı mekanizması oluşturur.

Bu çerçevede, iki kullanıcı arasındaki şifrelemeyi sağlayan Kuantum anahtar dağılımı (QKD) protokolleri, silahlardan en yaygın kullanılanları oltalama(phishing), kötücül yazılım(malware), bot net, hizmeti engelleme(DOS/DDOS) saldırıları ve sosyal mühendislik saldırılarına karşı geliştirilen güvenlik duvarları şeklinde sayıları

artan güvenlik yaklaşımları çok taraflı anarşik yapıyı destekleme potansiyeli taşımaktadır.

Burada ulus devletlerarasında ciddi görüş farklılıkları bulunmaktadır. ABD uluslararası siber uzaya yönelik sistemde kullanılması ve kontrolün sağlanması için ICANN'ın kurulmasını ve herkesin üye olmasını desteklemiştir. Fakat Çin ABD'nin internet üzerindeki hâkimiyetini arttırmamak ve kendi ulusal internet ağını dışa bağımlı yapmamak için ICANN'a karşı soğuk bakmıştır. Türkiye'de İnternet Tahsisli Sayılar ve İsimler Kurulu adıyla hizmet veren ICANN(Internet Corporation of Assigned Names); tüm internet kullanıcılarının geçerli adresler bulabilmesi için DNS teknik unsurlarının yönetimini yapmaktadır. Üst düzey alan adlarının (.com, .info vb.) kullanılma yetkilerini dağıtarak kontrollerini sağlamaktadır. Mevcut internet yönetişimi rejimini içeren ICANN düzenlemesiyle, Çin'in tercihleri ile iki farklı şekilde çatışmaktadır. Birincisi, Çin'deki geleneksellik yerine, internet'in liberalizmin mirası olmasıdır. Yani, internet faaliyetlerinin ve sosyal kullanımlarının özgürce, özel sektör temelli ve ulus ötesi yönetişim biçimini temel alacak şekilde ekonomik ve politik normlarla bağlantılı olmasıdır.

Bu karşıt iki görüş içerisinde ITU sorun çözücü bir görev üstlenebilirdi. ITU tarafından, internetle ilgili konularda hem teknik hem de politika ile ilgili hususları kapsayan 101, 102, 133 sayılı alınan kararlar bu yönde olumlu bir ışık vermişti. Ayrıca internetle ilgili kaynakların dünya çapında yoğun bir şekilde konuşlandırılması ve doğrudan ağa bağlı IP özellikli tüketici cihazlarının entegrasyonu ile IPv4 adreslerinin tükenmesi sorunu ve IPv6'nın konuşlandırılması konusunda daha iyi farkındalık yaratılması amacıyla 2002, 2005 ve 2008 yıllarında düzenlenen çalıştaylar çok taraflı müzakerelerinin ITU komitesince gözden geçirilmesi sürecini daha etkili kılmaya yönelik girişimlerin ilk adımları olarak ortaya çıkmıştır.Söz konusu müzakerelerde karşılaşılan zorluklar ise konuya ilişkin hassasiyetleri ortaya koymaktadır.

Bu itibarla, belirli bir teorik perspektif (neoliberal kurumsalcılık) temelinde, "BM'nin temsil ettiği çok taraflı siber uzay sisteminin tehditlerinin zayıflatması nasıl sağlanabilir?", "Devletler ile BM ilişkisinin nasıl düzenlenmelidir?" sorularına cevap aranacaktır. Avrupa Birliği özelinde gerçekleştirilen kurallar ve bu kuralları uygulayacak ENISA (Avrupa Ağı ve Bilgi Güvenliği'nin oluşturulması Ajansı)

özelinde geliştirilen bölgesel siber güvenlik anlaşması çerçevesinde mevcut durumu analiz edecek ve geleceğine ilişkin projeksiyonları ortaya çıkaracaktır. Bu projeksiyonlar özelinde ulaşılacak temel tespitse siber mücadele yürütebilmek için savunma sanayisinde %100 milli yazılım kullanılmalı, hukuki düzenlemeler sürekli güncellenmeli, kendi siber silahlarımız üretilmeli ve yazılım, dijital dönüşüm araçlarına bağımlılık mümkün olduğunca azaltılmalıdır.

Son olarak tezde siber çatışmaların azalmasına ve stratejik konsensüs sağlanmasına yönelik bilincin arttırılması en önemli katkı olarak düşünülmektedir. Ayrıca, Türkiye'de uluslararası ilişkiler teorileri bağlamında değerlendirilen siber çalışmaların görece sınırlı olduğu görülmektedir. Bu bağlamda, tezin anılan literatüre katkıda bulunması beklenmektedir.

Araştırmanın Konusu

Tarih boyunca savaşlarda kullanılan strateji, yöntem, taktik ve silahlar sürekli olarak değişse de savaşların mantığı ve hedefi günümüz siber çatışmalarına yönelik hedeflenen stratejik bakışlardan çok farklı değildir. Bu bağlamda, siber kavramların özelliklerini inceleme, mantığını anlama ve konvansiyonel savaşlardan hangi yönlerden ayrıldığını stratejik açıdan açıklama temeline dayanan bu tez siber savaşın çıkış noktası olarak konvansiyonel veya nükleer bir savaşın oluşmaması için alternatif bir yol oluşturmasını esas almaktadır. Bu amaç doğrultusunda öncelikle günümüzde yaşanan siber çatışmalar bir Siber Savaş sürecine dönüşme ihtimaliyle her aktörün aklında sürekli var olan bir korku psikolojisi yaratmaktadır. Sıcak savaşa dönüşmesini beklemediğimiz bu döneme ait tehdit algıları, risk potansiyelleri ve caydırıcılık oluşturan politikalar Soğuk Savaş (1945-1990) benzeri bir yapı içerse de kendine özgü özellikleri vardır. Bu yapı, her ülkenin, kurumun ve örgütün birbirini hackleyebildiği ve aynı zamanda açık hedef olduğu anarşik bir yapı içermektedir. Soğuk Savaştan farkı ise sadece belli iki farklı gruba ait bir tehdit ortamı yerine tüm dünyayı aynı anda tehdit eden bir risk ortamı yaratmasıdır. Bu kapsamda günümüz literatüründe kullanılan siber savaş kavramına yönelik var olan tehdit ve caydırıcı unsurları engellemek için oluşturulması gereken siber güvenlik faaliyetleri bu çalışmanın ana çerçevesini oluşturacaktır.

Bu tezde belirtilen bir diğer nokta hayatın her alanının sürekli siber uzaya taşınmasıyla birlikte teknolojinin sağladığı avantajların yanında ciddi derecede

nesnelerin interneti, bulut bilişim ve yapay zekâ gibi kavramların tehdit oluşturacak siber risk unsurlarını tetiklemesidir. Bu yüzden günümüzde yaşanan siber çatışmaların öneminin devletler tarafından anlaşılmasını sağlayarak her ne kadar zorlu bir süreç olsa da bir üst otorite oluşturulması gerektiği yönünde bir tanı ortaya koymaktır. Bu zorluklar ve üst otoritenin gerektiği yönündeki kavramsal tartışma ortaya koyabilmek için siber uzayda alınan önlemler, gerçekleştirilen siber saldırılar ve mevcut örnekler bu tezde ayrıntı şekilde incelenecektir. Böylece, aktörler tarafından ekonomik, siyasi, askeri ve stratejik amaçlı yürütülen siber savaş ve siber saldırı (siber güvenlik ya da siber çatışmalarını içine alan) kavramların temeli ortaya konacaktır.

Ayrıca teknolojik gelişmeler sonucunda ortaya çıkan asimetrik tehditlerle birlikte uluslararası sistemin güvenlik dinamikleri değişmiştir. Böylece çok yönlü anarşik yapı ve güvenlik ikileminin beslendiği bu yeni boyut daha dinamik bir güvenlik kavramını ortaya çıkarmıştır. Bu durumda devletlerin birbirlerine daha bağımlı iç içe geçmiş ilişkilere sahip olmasına yol açmıştır. Bu sebeple bu çalışmada stratejik çalışmalar, savaş stratejisi, taktik, planlama ve güç stratejilerini içerecek şekilde siber dünyayı domine eden aktörler özelinde siber çatışmaların tanımı ve gelişmesine yönelik perspektifler açıklanacaktır.

Son olarak, anarşik uluslararası sistemde bu yeni alan üzerinde yaşanan rekabet ve güç elde etme yarışı silah kavramı üzerinden açıklanmıştır. Bu doğrultuda siber silahların artmasıyla birlikte siberin yaygınlaştığı yönünde stratejik açıdan önemli figürlerin görüşleri çerçevesinde çatışma süreci açıklanmıştır. Siber silahların kullanılmasıyla birlikte her alanda olduğu gibi devletlerarası diplomatik ilişkilerde de klasik diplomasiye yeni bir boyut kazandırarak "dijital diplomasi" adıyla yeni bir politika alanı oluşmuştur. Böylece devletlerin geleneksel savaş yöntemlerinin yanında neden bu yeni savaş türünü kullanmaya yöneldiği, siber savaşın aktörleri, yapılan siber mücadeleler ve siber uzayın geleceği bu tezde ele alınarak dünyayı derinden sarsacak bir siber kriz yaşanmasını önlemeye yönelik çözüm için bir model önerisi ortaya konacaktır.

Amacı

Bu çalışmada varılmak istenen temel amaç siber kavramların özelliklerini incelemek ve konvansiyonel/nükleer savaşlardan hangi yönlerden ayrıldığını veya

benzeştiğini stratejik açıdan açıklamaktır. Bu amaç doğrultusunda savaş çeşitleri arasında yaşanan benzer tehdit unsurlarını ve caydırıcılık yaratan araçları ortaya koymak en temel amaçtır.

Bu çalışmanın bir diğer amacı, siber sözcüğü ve savaş metaforunu birlikte açıklayarak siber uzayın bugünkü önemi vurgulamak, bunun yanında siber savaş, siber saldırı, siber terörizm ve siber suç gibi siber kavramları ayrıntılı bir şekilde açıklayarak hukuki bir üst yapı ve uluslararası işbirliği mekanizmaları oluşturulması yönünde teklifler geliştirmektir.

Bu tezde amaçlanan bir diğer husus ortaya daha önce hiç olmayan bir şey koymak yerine literatüre bir katkı sağlayarak uluslararası ilişkilerdeki çatışma, güvenlik ve savaşlar tarihine daha önce bakılmayan bir yerden bakılmasını ve Türkiye'de bu alanda önlem alınmasını sağlayacak bilinci oluşturmaktır. Bu bilincin oluşması içinde özellikle gerçekleşen çatışmalar üzerinden tarihsel süreç incelenerek bu konu hakkında uluslararası kuralların, normların ve kurumların oluşturulması yönünde bir model ortaya koymaktır. Bu modeli ortaya koyarken de ülkemizde dijital dönüşüm kavramlarının gelişmesine yönelik mevcut ilerlemenin yeterli olmadığı belirtilerek ülkemizde siber uzayın bilinilirliği ve farkındalığına katkı sağlamak planlanmaktadır.

Bu çalışmanın son amacı, siber çatışmalar sonucunda ortaya çıkan potansiyel tehditleri keşfetmek ve alınacak savunma önlemleri için bir perspektif oluşturmak, etkin siber güvenlik stratejilerinin oluşturulmasını sağlamak ve siber uzay literatürü hakkında farkındalığı arttırmaktır.

Önemi

Bu tezin önemi; bugün "Siber Savaş" kavramının konuşulmasının altında stratejik bir çerçevenin var olup olmadığını inceleyip bugünkü siber yapının geçmiş kökenlerle bağlantısının ve karşılaştırmasının yapılmasıdır. Siber konuların gelecekte daha da önemli olacak olması, Türk literatüründe tezimizin başlığında direk yazılmış bir tez bulunmaması, uluslararası düzeyde de sınırlı çalışma bulunması gibi sebeplerse tezimizin önemini ortaya koyacak hususlardır.

Bunun yanında daha önce hiç olmayan bir şey ortaya koymak yerine literatüre bir katkı sağlayarak uluslararası ilişkilerdeki çatışma, güvenlik ve savaşlar tarihine daha önce bakılmayan bir yerden bakılmasını ve Türkiye'de ulusal çapta icra

edilecek siber güvenlik çalışmalarına yönelik farkındalığın ve bilincin arttırılmasına yönelik önemli bir katkı sağlanması planlanmaktadır.

Son olarak bu çalışma ile mevcut bulunan akademik çalışmalardan farklı olarak siber uzay kavramı, siber güvenlik stratejileri, tehdit ve caydırıcılık unsurları, savaşları, saldırıları ve kullandıkları siber silahları, geçmiş geleneksel yöntemlerle kullanımıyla bir arada mukayeseli olarak anarşik uluslararası sisteme vurgu yapılarak ülkelerin siber saldırılara karşı dijital sınırlarını korumak maksadıyla siber güvenlik stratejileri geliştirme zorunluluğunun gelecekte daha da artacak olmasından dolayı şimdiden bu tezde belirtilen kural ve kurumların oluşturulmasının gelecekte ortaya çıkabilecek tehditlerin önleyebilecek olmasıdır. Bu iddianın çıkış noktası ise Milletler Cemiyeti, Birleşmiş Milletler ve Nükleer Silahsızlanma Anlaşması gibi üst otorite anlaşmaların büyük savaşlar sonrasında oluşmasıdır.

Bir diğer yandan ülkeler tarafından resmi olarak ilan edilecek bir siber savaş senaryosunda ABD, Çin ve Rusya gibi ülkelerin birbirine girmesi dünyadaki her sektörü kilitleyebilir, bu kilitlenme ülkelerin birbirine bağımlı olmalarından kaynaklı domino etkisiyle dünyada hızlıca yayılabilir. Bu sonucunda hiçbir devlete fayda sağlamayacağı vurgulanarak devletlerin asıl amacının yok etmek yerine zarar vermek, durdurmak, kontrol etmek, bilgileri ele geçirmek gibi ufak çaplı boyutlarda kalması için siber silah geliştirilmesinin belirli kurallar altında sınırlandırılarak kontrol altına alınmasının "*World Wide Web Dünya Savaşı*" olarak adlandırdığımız savaşın ortaya çıkmasını engelleyebileceğinin önemi ortaya konmaya çalışılacaktır.

Böylece bu çalışma sayesinde sanarşik yapının içinde barındırdığı özelliklerle her geçen gün devletlerin üstündeki psikolojik baskıyı arttırarak devam eden siber saldırıları, siber tehditleri ve siber savaşları öngörerek siber silahlardan gelebilecek tehditleri tespit etme yeteneklerinin geliştirilerek siber savaşa ilişkin teknoloji ve hukuki normları düzenleyen uluslararası geniş çaplı bir uzlaşının ya da bu uzlaşı zeminini denetleyecek kurumun oluşabilmesi için gerekenler hakkında bir rol model sunulmuştur.

Bu tezde vurgulanmak istenen bir diğer nokta siber uzay alanında yapılan siber savaşta geleneksel savaşlarda kullanılan taktiklerin benzerleri kullanılıyor olsa da geleneksel savaşlardan farklı olarak bir cephesi olmadığıdır. Her sektörün ve her alanın tehdit unsuru olarak kullanılabildiği siber uzayda zaman ve mekân sınırı

bulunmamaktadır. Bu yüzden günümüzde yaşanan siber çatışmalarda 7/24 saldırı ve savunma zorunludur. Böylece tehdit ve caydırıcılık boyutu artarak devam eden küreselleşen dünyada siber güvenliğin sağlanması, kritik bilgi ve altyapıların korunması gibi hususlar her geçen gün önem kazanacaktır. Siber tehdidin her geçen gün artan bu boyutu uluslararası ilişkilerdeki anarşiyi arttırmakta ve devletlerin siber alanı bir hâkimiyet unsuru olarak görmelerine yol açmaktadır. Bu kapsamda, devletlerin siber güvenliklerini sağlayabilmeleri için dijital dönüşüm teknolojilerine yönelik yerli endüstri oluşturmaları gerektiği yönünde bilinç oluşturulması yönündeki çabaların önemi üstünde durulacaktır.

Varsayımlar

Bu tezde, Çatışma boyutu her geçen gün artarak devam eden siber uzayda siber güvenliğin sağlanması, 7/24 saldırı ve savunma olması, tehditlerin bertaraf edilmesi, siber silahların etkisinin azaltılması, rekabet ortamında caydırıcılığının artması ve kritik bilgi ve altyapıların korunmasının giderek önem kazanacak olmasından dolayı geleneksel güvenlik algılamalarının ve sınırlarının yerine ‘’siber’’ kavramı kullanılmıştır.

Bu tezde belirtilen bir diğer varsayım savaşlarda kullanılan strateji, yöntem, taktik ve silahlar tarih boyunca sürekli olarak değişse de savaşların mantığı ve hedefinin aynı olması gelecekte bu kavramın realist anlayışın ana çerçevesini oluşturacağını iddia etmemize yol açmaktadır.

Son olarak aktörler arasında yaşanan siber korku ve psikolojik harbin stratejik savaş kültürünün bir devamı şeklinde günümüzde siber savaş adıyla devam ettiği varsayımına dayanmaktadır. Hayatın her alanının sürekli siber uzaya taşınmasıyla birlikte veri saklama ve depolama merkezlerinin farklı lokasyonlarda oluşturulmasının zorunluğunu doğuracağıdır. Sürekli yayılan ve genişleyen bu tesislerin varlığı ise verilerin korunma riskini arttırarak siber güvenliği tetikleyecektir. Artan bu riskler saldırıları arttıracak ve çatışma süreci artarak genişleyecektir. Bunu bir başka şekilde ifade edersek; nasıl sanki hayatımızda hep varmış gibi hissedilen internet teknolojisi ve mobil teknoloji 20 yıllık bir süreçse, 20 yıl sonra ne olacağını da kestirebilmek çok zordur. Nasıl 1945 yılında 2. Dünya Savaşı’nın bittiği ilk sıralarda yaşanan gelişmelerin Dünya’yı bir Soğuk Savaş’a

dönüştürdüğü tam olarak tanımlanamadıysa ama bu durum gerçekse, şuan günümüzde yaşanan olayları siber savaş dönemi olabileceği değerlendirilmektedir.

Sınırlılıklar

Temel alınan ve öncelikli olan faktörler şunlardır: dijital dönüşüm araçları, teknolojik gelişmeler, Soğuk Savaş sonrası kaos ve hiyerarşik yapının bozulması, tehdit, güvenlik ikilemi, anarşik yapı, strateji, siber caydırıcılık, rekabet ve güç elde etme mücadelesi gibi kaynaklardır.

Soğuk savaşın bitişi, asimetrik tehditleri ön plana çıkararak çok yönlü ve daha dinamik bir güvenlik kavramını ortaya çıkarmıştır. Anarşik yapı, caydırıcılık, korku, tehdit ve güvenlik ikileminin beslendiği bu boyut teknolojik alandaki gelişmelerden ve özellikle dijital dönüşüm süreçlerinden daha keskin şekilde etkilenmektedir. Sorular ve yaşanan örnek vakalar çerçevesinde uluslararası düzen, kavramlar ve kurumlara yönelik doğrudan veya dolaylı olarak stratejik tespitler ortaya konacaktır.

Konuya uluslararası güvenlik politikaları açısından yaklaşacak olursak siber savaşlar için örgütler, uluslararası kuruluşlar ve devletler düzeyindeki farklılık, analiz düzeyini inşacı teoriye yaklaştırmaktadır. Aynı zamanda güvenlikleştirme teorisi kapsamında siber dünyayı domine eden ve ulusal siber güvenlik stratejisi bulunan aktörler özelinde soğuk savaş sonrası oluşan yeni durum ve şartları içine alan çatışmalarla konu sınırlandırılmıştır.

Yöntem

"Siber Güvenliğin Stratejik Bakış Çerçevesinde Konumlandırılması: Tehdit/Caydırıcılık Bağlamında Örnek Kriz İncelemeleri" başlıklı bu çalışmada siber uzayın yeni gelişen bir alan olması sebebiyle nitel yöntemli tanımlayıcı bir araştırma tasarımı kullanılmıştır. Nitel araştırma boyutuyla toplanan veriler ikincil kaynaklardan elde edilen verilerden (bilimsel makaleler, raporlar, endeksler vs.) elde edilen bilgilerden oluşmaktadır.

Bir diğer yandan Uluslararası İlişkiler Teorileri (Realizm, İdealizm vs.) kapsamında siber uzayın teorilerle ilişkilendirilmesiyle elde edilen bilgiler doğrultusunda araştırma anlamlı hale gelerek doğa ve toplumsal olaylar ilişkilendirilip, sınıflandırılıp, düzenlenip yorumlanacaktır. Bunun sonucunda ise bilgilerle bilim arasında teorik olarak ilişki kurulacaktır.

Buna ilave olarak siber caydırıcılığın uygulanması noktasında uluslararası arenada kilit rol oynayan devletler, örgütler ve kurumlar tarafından ortaya konan önlemler ve gerçekleştirilen siber saldırılar mevcut örnekler üzerinden incelenerek (siber özelinde) bir hipotez belirlenecektir. Bu hipotez sonucunda da silah kavramı özelinde günümüzde gerçekleşen çatışmaları yeni bir savaş türü özelinde açıklayabilmek için tehdit, caydırıcılık ve güvenlik yaklaşımlarıyla teoriler arasında bir ilişkilendirme kurulmuştur. Bu ilişkilendirme gerçekleştirilirken de özellikle kavramların metodoloji içermesi, bilimsellik içermesi, tarihsellik içermesi, geleneksel savaş yöntemlerinde kullanılan taktik ve stratejilere benzerlik göstermesi, uluslararası ilişkilerin ana teorileri olan realist ve idealist akımların iddialarını karşılaması gibi yöntemler ortaya konarak karşılaştırmalı bir perspektif oluşturularak analiz gerçekleştirilmiştir.

Gerçekleştirilen bu analizler sonucunda siber çatışma dönemine yönelik bu vurgu gerçekleştirilirken de internetin gelişimine genel bir vurgu yapılarak siber kavramların ulusların milli güvenliklerinde oynadıkları rolün güçlü ve zayıf yönleri ortaya konarak siber silahların önemi ve bu silahların kullanılmasını engelleyecek uluslararası kuralların ve kurumların belirlenmesi ve uygulanması vurgulanacaktır.

Sonuç olarak; Devletler ve aktörler özelinde siber güvenlik anlayışları ve politikalarının karşılaştırmalı analizi gerçekleştirilerek siber caydırıcılığın uygulanması noktasında uluslararası arenada kilit rol oynayan devletler, örgütler ve kurumlar tarafından ortaya konan uygulamalar, önlemler ve gerçekleştirilen siber saldırılar mevcut örnekler (siber özelinde) karşılaştırılarak elde edilecek bilgiler çerçevesinde problemler, varsayım (lar)/hipotez(ler) belirlenecektir. Böylece, nitel bir teorik perspektif oluşturularak belli başlı sorunlar somutlaştırılacaktır.

Araştırmanın Sorunsalı

Siber suç, casusluk ve terör saldırılarının sayılarında her geçen gün artış yaşanması bu konudaki söylemlerin ve istatistiklerin incelenmesini zorunlu hale getirmiştir. Benzer nitelikte uluslararası arenada yaşanan çatışmalar ve bu çatışmalardan elde edilen sonuçlar ışığında günümüz uluslararası anarşik sistemi eleştirel bir şekilde yorumlanarak sistemdeki anarşinin çözümüne ilişkin öneriler geliştirmek bu tezin en önemli sorunlarının başındadır.

Bu bağlamda siber alanla ilgili daha önceden yazılan tezlerin, makalelerin ve kitapların eleştirel bir şekilde yorumlanması sonucunda günümüzde her an psikolojik bir korku ve tehdit yaratan bir siber çatışma dönemi yaşandığı tezi ortaya atılmıştır. Ortaya atılan bu tezde siber uzayın karakteristik özelliği olan bilinmezlik ve tahmin edilmezlik gibi özelliklerin içinde barındırdığı problemler, riskler ve tehditler bu çalışmada belirlenerek, sonrasında bu sorunlarla ilgili literatür ve alan üzerinden ulaşılan bilgiler, örnekler ve veriler üzerinden olayları tek tek incelemek yerine olgu olarak betimleyip siber savaş dönemine atıf yapılacaktır.

Bu tez ortaya atılırken tezin çıkış problemi insan doğasına vurgu şeklinde belirlenmiştir. Öncelikle insan doğasına vurgu yapılırken anarşik yapı baştan doğru baştan kabul edilip eleştirel bir yaklaşımla sorgulama gerçekleştirilecektir. Bu sorgulama gerçekleştirilirken de güç, ittifak, çatışma, tehdit, güvenlik, caydırıcılık, savaş ve strateji gibi kavramlar çerçevesinde uluslararası ilişkilerin ana teorileriyle siber uzay da üst otorite bir kurum ile etik ve hukuki kuralların olmaması problemine ulaşılacaktır.

Bir diğer yandan siber uzayda günümüzde görülenin dışında sanal bir evren olduğu, yaşanan bu yenidünyanın güvenliğinde de en önemli halkanın insan olması bu problemi desteklemektedir. Çünkü uluslararası ilişkiler teorileri kapsamında insan doğasına vurgu yapılarak tez bu doğru üzerinde inşaa edilecektir. Baştan doğru kabul ettiğimiz anarşik ve kötü olan bu süreçte yasaların oluşturulması, işbirliği modelleri ve kurumsallaşma gibi bağımlılık ve işbirliği temelli liberal politikalar üzerinden bu probleme çözüm yolları aranacaktır.

Aynı zamanda bu tezde siber güvenliğin ve gerçekleşen saldırıların problem olarak görülmesinin asıl sebebi günümüzde önemi ve etkinliği her geçen gün artan siber dünyada bir devletin, kurumun ve örgütün %100 güvenli olmasının mümkün olmamasıdır. Dolayısıyla aktörler tarafından oluşabilecek tehdidin farkında olunması, tedbir alınması, dirençli olunması ve bekalarını sürdürebilmeleri amacıyla güvenli bir ortam yaratılması gerekmektedir. Siber tehdidin sürekli değişime uğrayan yapısı ona karşı alınacak tedbirlerin de dinamik olmasını gerektirmektedir. Bu yüzden ulusların kritik altyapılarına karşı gerçekleştirilen siber saldırıları önlemek, siber saldırılara karşı uluslararası güvenlik açığını azaltmak ve siber saldırılar tarafından oluşacak hasarları ve hasarların iyileşme sürecini en aza indirmeye

yönelik stratejileri incelemek bu tezin ana problemidir. Bu problemi çözebilmemiz içinde kronolojik bir çalışma yaparak tarihten dersler çıkarılması şarttır.

Bunlara ek olarak günümüz dinamik yapısının içinde küresel çapta ekonomik, siyasi, askeri vb. her alanda yeni bir araç olarak internetin kullanım oranlarının hızla artması aktörlerin uluslararası güvenlikleri açısından siber güvenliği birinci önceliğe almasına yol açmıştır. Bu öncelikte doğrudan maddi kazanç sağlama, isim yapma, itibar kazanma, itibarı zedeleme, herhangi bir şeyi protesto etme, ses getirme, bilgi çalma vb. devletlere, kurumlara ve örgütlere karşı yürütülen siber saldırı çeşidini arttırmıştır. Bu bağlamda, bu yöntemlerin geleneksel yöntemlerden tamamen ayrılmadan birbirleriyle bağlantılı ve tamamlar şekilde olması gerektiği üzerine bir sonuca ulaşılması gerekmektedir.

Bu çalışmada üzerinde durulan bir diğer önemli problem siber kavramların hayatın tüm alanlarını birbirine bağımlı hale getirmesinin tehditleri domino etkisiyle yayma riskidir. Siber saldırıların ana hedefi ülkelerin güvenliği, silah sanayindeki teknolojik gelişmeleri, askeri silahların çalışma kodlarını, çevresel sorunları, sağlık sistemi, enerji tesisleri ve araçları, ulaşım sistemleri, haberleşme araçları, barajları ve su aktarma merkezleri, bankacılık ve finans yapısı, kamu hizmetleri vb. gibi her türlü alanı etkileyebilmektedir. Bu çerçevede, kritik altyapılara karşı gerçekleştirilen siber saldırıları önlemek, siber saldırılara karşı uluslararası siber güvenlik açığını azaltmak ve siber saldırılar tarafından oluşacak hasarları ve hasarların iyileşme sürecini minumum seviyeye indirmeye yönelik stratejileri incelemek bu tezin ana problemidir.

BİRİNCİ BÖLÜM

TEHDİT, CAYDIRICILIK, ÇATIŞMA VE GÜVENLİK KAVRAMLARI

A) Uluslararası İlişkilerde Güvenlik

1.1. Tarihsel Süreç İçinde Tehdit Algılamaları ve Değişen Güvenlik Anlayışı

Daha önce tehdit olduğu kabul edilen bir şeyin artık tehdit olarak inşa edilmemesi anlamına gelen "güvenlik dışılaştırması" kavramına göre, askeri sektördeki güvenlikleştirme belirli dönemlerde sürekli değişim yaşamıştır.1 Nasıl Soğuk Savaş sonrasında batı kapitalizmi hem komünizm hem de üçüncü dünya ideolojisine hâkim geldiyse ve tehdit parametrelerini değiştirdiyse benzer süreç günümüzde de mevcuttur.[2]

İnsanlık sürekli olarak farklı dönemlerde farklı araçlar ve bu araçlar sayesinde farklı yaşamlar sürmüştür. Yaşanan değişimler ekonomiden, kültüre, sosyal hayattan askeri yaşama kadar her alanı değiştirip dönüştürmüştür. Bu sebeple uluslararası ilişkileri belirleyen temel unsurların başında gelen güvenlik kavramı, zamana, mekâna ve dönemin koşullarına göre farklılık göstermektedir. Doğal olarak değişen şartlarla birlikte güvenliği etkileyen tehdit unsurları da zaman içerisinde değişmektedir. Örneğin; dış tehlikelere karşı ilkel dönemlerde insanoğlu ateş, taş, orak ile kendini savunurken zaman içerisinde niteliği ve niceliği değişen risk ve tehditlere karşı kullanılan savunma araçları ve stratejileri değişime uğramıştır.[3] Yâda geçmişte topraklarını genişletmek isteyen bir devlet, diğer devletler tarafından tehdit unsuru olarak görülmekteyken günümüzde teröre destek veren, siber saldırılar düzenleyen, silahsızlanma koşullarına uymayan ya da nükleer/kimyasal silahlardan arınmayan devletler tehdit unsuru olarak görülmektedir.[4]

---

[1] Barry Buzan, "Askeri Güvenliğin Değişen Gündemi", Uluslararası İlişkiler, Cilt 5, Sayı 18, (Yaz 2008), ss. 107-123.

[2] Barry Buzan, New Patterns Of Global Security İn The Twenty-Frst Century International Affairs (Royal Institute Of International Affairs 1944-), Cilt. 67, No. 3(Temmuz, 1991), ss. 431-451

[3] Selahaddin Bakan ve Sonay Şahin, "Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler", The Journal of International Lingual, Social and Educational Sciences cilt 4, Sayı 2, 2018

[4] Beril Dedeoğlu. "Uluslararası Güvenlik ve Strateji", Yeni Yüzyıl Yayınları, 2014

İletişim ve ulaşım imkânlarının geliştiği günümüz dünyasında yeni tehditlerin ortaya çıkmasına, var olan tehditlerin şekil değiştirmesine ya da daha etkili hale gelmesine teknolojik değişimler neden olmaktadır. Özellikle Soğuk Savaş'ın bitmesinden sonra küreselleşme çerçevesinde küresel uluslararası sistemde meydana gelen köklü değişimler, güvenlik ve politika yaklaşımlarını değiştirerek yeni bir tehdit boyutunun ortaya çıkmasına sebep olmuştur. Örneğin; 11 Eylül terörist saldırısı güvenlik kavramlarına yönelik tehdit ve risk algılamalarını önemli ölçüde değiştirmiştir. Böylece, 21. yüzyıl başlarına kadar belirgin olan tehdit kavramı, çok yönlü, belirsiz ve değişken bir hale gelmiştir. Yeni asimetrik tehdit kavramının, çok yönlü, belirsiz ve değişken bu yapısı güvenlik alanında yeni bir yaklaşımın ihtiyacını ortaya çıkarmıştır.

Güvenlik kavramı en temel anlamıyla tehditten uzak durma halidir. Dolayısıyla bu iki kavram birbirinden ayrı düşünülemez. Yani tehdit ne kadar artarsa güvenlik riskimizde o derecede artar. Bu sebeple anarşik uluslararası sistem içerisinde güç dengesinde meydana gelebilecek her değişim güvenlik ikilemini tetiklemektedir. Teknolojinin gelişmesi doğal olarak savaş araçlarını da doğrudan etkilemektedir. Böylece aktörlerin silahlanması, saldırı yöntemleri ve caydırıcılıkları da günün teknolojik şartlarıyla yeniden şekillenmiştir.

Günümüz güvenlik yaklaşımında devletlerin tehdit algılamaları Soğuk Savaş öncesi dönemlere göre farklılık ve çeşitlilik göstermektedir. Bu durumun en önemli sebepleri; dijital dönüşüm araçları ile birlikte ortaya çıkan teknolojik gelişmeler, sonucunda çok yönlü asimetrik tehdit algısının ortaya çıkmasıdır. Bu doğrultuda değişen ve dönüşen günümüz savaşları cephesiz, üniformasız askerlerle, ne zaman, ne şekilde, nasıl ve hangi hedefe yönelik yapılacağı bilinemeyen, silahı bilgisayar ve internet sistemleri olan bir yapıya dönüşmüştür. Bütün bu bilinmez yeni yapılar insanları, devletleri ve uluslararası örgütleri korkutmakta, korku ise tehdidi ortaya çıkarmaktadır. Bu tehditlere karşı iç ve dış güvenlik stratejilerinin oluşturulması ise zorlu bir süreçtir. Çünkü siber uzay hakkında tüm yetkili personellerin teknik, kavramsal ve psikolojik olarak eğitilmesi, kurumların yasal yapılarının oluşturulması ve gerekli arge faaliyetlerinin yürütülmesi gerekmektedir. Bu yüzden asimetrik tehditlerin bu yeni hali risklerin, tehlikelerin, korkuların, güç boşluklarının ve güvensizliklerin artmasına yol açmaktadır.

Bunların yanında; küreselleşme pratiği ve teknolojik gelişmeler sonucunda tehdit algılamaları da değişmektedir. Küreselleşme süreci tüm dünyada homojen ve uyumlu bir şekilde işlememekte ve aynı sonuçları doğurmamaktadır. Esasen küreselleşme süreci dünyanın farklı bölgelerinde farklı şekilde gelişmektedir. Dolayısıyla Samuel Huntington'un belirttiği ülkeler ve kültürler arası çatışmanın gerçekleşmesi çok normaldir. Samuel Huntington'a göre çatışma ve işbirliği serüvenindeki dünya siyasetindeki sınırları belirleyen temel faktör kültürdür. Buna ilave olarak farklı kültürlere sahip halklar ve ülkeler parçalanırken benzer kültürlere sahip halklar ve ülkeler ortaya çıkmaya başlamıştır.[5]Küreselleşme ise kültürleri tehdit eden bir baskı unsurudur. Küreselleşmenin motoru olan şirketler küresel ticaret ağını e-ticaretle birlikte daha da geliştirmiştir. Böylece; zaman, mekân, ulusal sınır, dil, gelenek ve ideolojik farklılıkları dikkate almadan sadece kar amacıyla ellerindeki teknoloji ve kaynakları internetle birlikte tüm dünyaya yayma çabasına girmişlerdir.[6] Bu yayma süreci doğal olarak güvenlik yaklaşımlarını da doğrudan etkilemektedir.

21. yüzyılın başlarında yaşanan tüm bu yukarıdaki çabaların yanında ABD'ye karşı düzenlenen 11 Eylül megaterörist saldırıları ve asimetrik tehditler; geleneksel tehditlerle etkin bir biçimde mücadele etme konusunda yetersiz kalındığını herkese göstermiş ve güvenlik yaklaşımını yeniden şekillendirmiştir. Bu yeniden şekillenmeyle birlikte güvenlik kavramı, pasif yapıdan, sürekli değişen ve takip edilmeyi gerektiren aktif bir yapıya geçmiştir. Bu sebeple görünüşte birbirlerinden bütünüyle farklı olan bu gelişmeler dünya düzeninin şuan ki yapısı ve devletlerin güçleri üzerinde yıkıcı bir etki yaratmıştır. Güvenlik kavramındaki bu genişlemeye paralel olarak risk ve tehdit kavramları askeri konuların yanı sıra siyasi, sosyal, ekonomik ve çevresel konuları içine alan ve devletin bütün organlarını ilgilendiren bir özellik kazanmıştır. Bu yüzden tehdit alanları sadece askeri olmamakla birlikte ekonomik, siyasi, çevresel, insani, sosyal, toplumsal ve teknolojik öğelerin yer aldığı geniş bir tehdit yelpazesinde hayatın her alanını bu tehdit algısının bir parçası haline dönüştürerek güvenliği gerçekleştirebilmek için detaylı ve öngörülü değerlendirmelerin yapılmasını zorunlu hale getirmiştir.

---

[5] Samuel P. Huntington, "The Clash of Civilizations and the Remaking of World Order", Simon and Schuster Journal, USA, 1996, ss.2-6.

[6] Richard J. Barnet. ve, John Cavanagh. "Küresel Düşler: İmparator Şirketler ve Yeni Dünya Düzeni", çev. Şen, G. Sabah Yayınları, İstanbul, 1995.

Hayatın her alanının bir tehdit unsuru ve saldırı aracı haline bu denli gelmesinde internet (siber uzay) etkili olmuştur. Nesnelerin internetiyle birlikte internet kullanılan bilgisayar ve akıllı cihazlar yaygınlaşmıştır. Ayrıca uzaktan erişimin kolaylaşması kurumsal ağlara fiziksel bağımlılığı azaltarak güvenlik riskini arttırmıştır. Ağların daha karmaşık hale gelmesi sonucundaysa bulut sunucuları yaygınlaşmış ve devletler sahip oldukları kritik verileri tek bir lokasyonda tutamaz hale gelmiştir. Bu durum siber tehditleri çok daha karmaşık hale getirmiştir. Karmaşıklığın yanında öngörülemeyen ve bilinmeyen tehditlerse yapay zekânın gelişmesine yol açmıştır. Yapay zekâ ile birlikte teknolojideki gelişmeler daha da hızlanmış ve değişen tehditler, belirsizlik ve tahmin edilemezliğin en önemli özelliği olduğu çok yönlü "asimetrik tehdit" haline dönüşmüştür.

Bu asimetrik tehditleri içeren çatışma sürecinin ortaya konulmasında insanın evrimini itaatsizlik eylemleriyle tamamlamayan Erich Fromm'un sözleri çerçevesinde değerlendirebilir. Erich Fromm'a göre; "İnsanoğlunun tarihi itaatsizlikle başladı ve ne yazık ki itaatle sona erecektir. Eğer itaatsizlik yetisi insanlık tarihinin başlangıcını oluşturuyorsa itaat, insanlık tarihinin son bulmasına neden olacaktır. Bu son bulmayla eğer insanoğlu kendini öldürürse, bu ölümün nedeni ölüm düğmesine basmayı emredenlere itaat etmek olacaktır."[7] İnsanoğlunu koşulsuz itaate sürükleyecek günümüzdeki en büyük tehlike her türlü kurumsal hafızanın depolandığı bulut, bunu işleten yapay zekâ ve ortaya çıkan siber tehditlerin birlikteliğidir. Bunu önleyecek mekanizma ise siber güvenliktir.

İnsanların aldıkları kararlar çoğu zaman taraflı, göreceli ve duygusal olabilmektedir. Makineler ise duygudan arınmış ve tümüyle rasyonel bir karar mekanizmasına sahiptir. Akıllı teknolojilerle birlikte robotların yapay zekalarının gelişmesi ve sahip oldukları bilgileri big data merkezleriyle depolamalarıyla ciddi bir güç elde etmeye başlamışlardır.[8] Günümüzde ve gelecekte tüm aktörleri bekleyen asıl sorun robotların internet yoluyla birbirleriyle iletişime geçmeleri sonucunda sürecin insanların kontrolünden daha da çıkabilme ihtimalidir.

Soğuk Savaş'ın bitmesi sonrasında gelişen dijital dönüşüm araçları ile birlikte büyük güçlerin güç kullanmasının maliyeti, karşılıklı bağımlılıklar, serbest piyasa

[7] Erich Fromm, "İtaatsizlik Üzerine Denemeler", Yaprak Yayınları, Çeviren Sayın, A. İstanbul, 1987, ss.7-8.
[8] Bilal Aksu, Big Data Bilginin Gücü, Pusula Yayınları, İstanbul, 2017, ss.87-88.

ekonomisi, ekonomik entegrasyon, internet 'in ortaya çıkması ve uluslararası ticaret gibi gelişmeler ulus altı gruplar ve ulus ötesi toplulukların politik rollerini arttırmıştır. Örneğin; 1973 OPEC petrol krizi uluslararası ticaretteki bağımlılığın etkisini ve küçük zayıf bir devletin güçlü ülkelere karşı elde edebileceği gücün önemlini tüm dünyaya göstermiştir. Ya da konuya siber güvenlik açısından baktığımızda "Tor" isimli siber silahın 2009 yeşil devrim ve 2011 Arap Baharı'nda kullanıldığı iddiasında yeni teknolojilerin gelişimi ve dağıtılmasının geleneksel diplomasinin ötesine geçerek yeni bir diplomatik silah şekline dönüşmesidir.[9] Bu süreçte sistemin yaşadığı çıkmazlara yeni gerçekçiliğin bir çözüm getirememesi ve olacakları önceden tahmin edememesi sonucunda yeni-gerçekçiliğin yetersizliğine tepki olarak yeni liberalizm teorisi gelişmiştir.

Teoriler çerçevesinde Soğuk Savaş sonrası dönemi daha ayrıntılı bir şekilde açıklamaya çalışırsak şu noktalara değinmemiz gerekmektedir. Teknolojik, ekonomik ve kültürel değişimin hızlandığı Soğuk Savaş sonrası dönem içinde belirsizliği barındıran büyük bir iktidar çatışması yaşanmaktadır. Bu sürecin savaş olarak tanımlanmasının sebebiyse "Savaş" kavramının içinde sayısız aktiviteyi kapsayan bir terim olmasıdır. Yaşanan bu süreçte küresel güç çatışmaları, nükleer silahların caydırıcı etkileri, azalan kaynaklar ve bölgesel çatışmaların hepsi bu gerginlik sürecinin devam etmesine yol açmaktadır.

Bu durumu bir başka şekilde ifade edersek, 19. yüzyılda uranyum güç kaynağı değildi. Fakat günümüzde uranyumun zenginleştirilmesi çok önemli bir güç kaynağı haline gelmiştir. Soğuk Savaş'ın başlangıcından günümüze kadar geçen süreçte uluslararası sistemde gerçekleştirilen temel mücadelelerin başında rakip güçlerin nükleer bir güce sahip olmasını engellemek vardı. Bu strateji günümüzde de siber uzay aracılığıyla gerçekleştirilmektedir. Bunun en güzel örneğini İran dışında birçok ülkeyi de alarma geçirerek önlem almalarına yol açan stuxnet olayında görmekteyiz. Kısaca stuxnet çatışma süreci'ni açıklarsak;

İran'a göre nükleer gelişim kendisi için hak ve olması gereken bir şeyken ABD ve İsrail'e göre bu durum; kötü 'nün resmedilmiş hali olan ve ''Şer Ekseni'' olarak adlandırılan ülkelerden biri olan İran'ın daha büyük kötülük yaratma mücadelesidir. Bu sebeple; ABD ve İsrail'e göre İran'ın güçlü nükleer alt yapısı

[9] P.W Sınger, ve Allan Frıedman, "Siber Güvenlik ve Siber Savaş", Çeviren Atav, A. Buzdağı Yayınları, Ankara, 2018, ss.151.

çökertilmelidir. Askeri bir müdahalenin çok daha büyük etkileri olacağından Amerika Birleşik Devletleri ve İsrail'in çözümü uluslararası alanda suç olarak görülmeyen Stuxnet solucanını yaymak olmuştur. Siber Savaş'ın bir aracı olarak karşımıza çıkan bu virüs siber savaş kavramının etkisinin ne kadar büyük olabileceğini tüm dünyaya göstermiştir. Böylece, siber savaş enstrümanları sayesinde güç santralleri, fabrikalar ve birçok teknolojik tesisin kontrolsüz bir silaha dönüşebilecek bir güç olabileceği herkesçe görülmüştür.

Tarihteki, fiziksel etkisi doğrudan görülebilen ilk 'ciddi' siber saldırı olarak kayıtlara geçen ve 2010 yılında İran'ın uranyum zenginleştirme tesislerine yapılan bu saldırılarda kullanılan stuxnet isimli solucan, eğer bulaştığı bilgisayarda SCADA yazılımı bulunuyorsa, kendini aktive ederek bilgisayar ağına zarar verme özelliği taşıyordu. Stuxnet virüsünün bir yıldan fazla bir süre İran ağlarının içinde bulunarak nükleer bilim adamları tarafından farkına varılmamasıysa stuxnetin mükemmel bir bütünlük içinde sinsiliğini ortaya koymuştur.

İran'ın, ABD ve İsrail tarafından ortaklaşa olarak kendisine gerçekleştirildiğini iddia ettiği bu saldırı, endüstriyel sistemleri gizlice gözetleyen, gerektiğinde kendini yeniden programlayabilen siber silahların karışık bir siber savaş aracı olarak kullanıldığının ve tehlike boyutunun bir göstergesidir.[10] Yani ABD ve İsrail'in Ortadoğudaki projelerinde rakip gördüğü ve özellikle Rusya tarafından örtülü bir şekilde desteklenen İran'ın nükleer faaliyetlerini durdurma hedefi doğrultusunda Stuxnet virüsünün yayılması gibi etmenler bu savaşın olduğunu göstermektedir. Bu yüzden nükleer güce sahip tüm aktörler bu alanda ciddi bir tehdit altında kalmıştır. Çünkü nükleer tesislere gerçekleştirilecek siber saldırılar yoluyla radyoaktif patlamalar gerçekleşebilir. Bu durum ise Çernobil benzeri bir tehdidin yaşanma riskini içinde barındırır.

Siber savaşlar sanıldığı gibi geleceğe ait bir mesele değildir. Sadece "Siber Savaş" tanımı ve tehdidi, dünya geneli tarafından 2007 yılında idrak edilmiştir. Geleneksel savaşlarla bağlantılı bir şekilde siber uzayı nasıl anlayacağımız ve tecrübe edeceğimizde tartışmaları içinde barındırmaktadır.[11] Bu bağlamda bir

[10] David. E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, The Newyork Times, 01.06.2012 https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html ET.10.10.2019.
[11] Ramazan Kurtoğlu," Biyo- Politik Savaşlar", Destek Yayınları İstanbul, 2018.

devletin dış politika ve güvenlik stratejisinin oluşturulmasında siber stratejiler çok önemli bir yer tutmalıdır. Çünkü siber stratejiler dünyada gelişen olaylara göre sürekli yenilenmektedir.

Günümüz siber dünyasında nükleer güce sahip devletlerin nükleer güç sistemlerini elektronik ortamda muhafaza etmesi, kontrol etmesi ve geliştirmesi rakip veya düşman bir aktör tarafından yapılabilecek bir saldırı ihtimalini kuvvetle ortada tutmaktadır. Nükleer santral ve nükleer silahlara sahip olan devletlerin kendi iradeleri dışında uzaktan erişim ile başka aktörler tarafından sistemlerinin kullanılıp imha edilebilme riski insanlık doğasında çok ciddi bir riski ortaya çıkarmaktadır. Yapay zekâ, loT, big data, biyomühendislik, bulut bilişim ve siber saldırılar artık güç kavramlarının etkisini çok ileri boyutlara taşımıştır. Yani teknoloji hiçbir milletin tek başına çözemeyeceği çapta varoluşsal tehditler yaratarak her şeyi değiştirmiştir. Bu yüzden artık günümüzde 2 önemli düşman vardır. Bunlardan biri nükleer savaş, bir diğeri ise içinde yapay zekâ, loT ve bulut bilişim kavramlarını barındıran siber savaş oluşma ihtimalidir. Siber saldırılarda saldırganların kimliğini saklayabilmeleri bu ihtimali sürekli canlı tutmaktadır. Dolayısıyla siyasi, ahlaki, askeri, ekonomik veya kültürel hangi alanda olursa olsun anarşik uluslararası sistemin beşinci boyutu olan siber ortam küçümsenecek bir konu değildir.

Yukarıda bahsedilen tüm bu bilgiler ışığında uluslararası ilişkilerin yeni bir mücadele alanı olan siber uzay sürecini, teorilerin ve düşünce okullarının hiçbiri kendi başına tamamen açıklamada yeterli değildir. Bu yüzden her teori çerçevesinde siber uzayın düşüncel alt yapısı bu tezde sağlam bir temele oturtulmaya çalışılmıştır. Bu yapılırken de günümüzde yaşanan teknolojik değişimler, internetin hayatın her alanına etki etmesiyle oluşan belirsizlikler ve artan riskler hızlı bir güç geçişi döneminde olduğumuz konusunda güçlü bir fikir birliği yaratılmaya çalışılmaktadır. Siber uzayın şuan ki gücünün oluşumu ise Thucydides'ten bu yana tarihçiler ve siyasi gözlemcilerin, hızlı güç geçişleri ve büyük güç çatışmalarının önde gelen yapısal nedenler olduğunu belirtmelerinden yola çıkarak koyabiliriz. Bu doğrultuda ticaret ve savaş gibi tarih boyunca uluslararası alanda yaşanan tüm yapısal gelişmeler ve değişimler 4 tip etkileşimi doğrudan içermiştir. Bunlar; [12]

[12]Jr. Joseph S. Nye ve Robert O. Keohane, "Transnational Relations and World Politics", International Organization, Cilt. 25, No. 3, (Yaz, 1971), ss. 329-349.

1) Bilginin hareketi: İnanç, fikir ve doktrinlerin iletimi dâhil olmak üzere her türlü iletişim,

2) Ulaşım: savaş malzemesi ve kişisel eşyaların yanı sıra mallar dâhil olmak üzere tüm fiziksel nesnelerin hareketi,

3) Finans, para hareketi ve kredi araçları,

4) Seyahat, kişilerin hareketi.

Hem ticaret hem de savaş kavramları koordineli bilgi hareketleri, fiziksel nesneler, para ve insan hareketlerini gerektirir. Ulus devletler tarafından başlatılan ve sürdürülen küresel etkileşim savaşlarının çoğu, büyük miktarda uluslararası iletişim ve kayda değer ticaret ilişkilerini içerir. Bununla birlikte, ulus ötesi iletişim, nakliye, enerji, finans, seyahat vb. diğer etkileşimler "ulus ötesi" şeklinde sivil toplum aktörlerini-bireyleri veya kurumları içermektedir. Günümüzdeyse siber uzay bu 4 ana tip etkileşimin en yoğun olarak kullanıldığı alanlar olarak ortaya çıkmaktadır. Siber uzayın "asimetrik" ve "eşitsizlikleri" içinde barındıran yapısı ulus ötesi ilişkilerin belirsiz veya çelişkili yapısını etkileyerek zengin, modern ve teknolojik açıdan gelişmiş kesimleri güçlendirmektedir. Aynı zamanda siber faaliyetlerde itiraz edebilecek özerk bir yapının bulunmaması sebebiyle karşılıklı bağımlılık yoluyla belirli devletlerin diğerlerini etkileme kabiliyetleri artmıştır. "Sibernetik" teorisyen okulu ve "neo-işlevselci" yaklaşıma göre bu durum; ulus ötesi ilişkilerde hükümetleri kısıtlayarak politikalarını daha işbirlikçi yapması yönünde etkilemektedir. [13]

Konvansiyonel veya nükleer gücün hâkim olduğu dünyada güçlü ve büyük devletler kendi politikalarının ulus ötesi ilişkiler sistemi üzerinde kabul edilmesinde daha etkilidir. Bu yüzden bağımlılık ve karşılıklı bağımlılıkla baş etmek, küçük devletlere göre büyük devletler için daha özel problemler doğurur. Bu durum siber ortamda da aynı şekildedir. Örneğin; ABD yüz yüze kaldığı siber güvenlik riskinden dolayı NATO içerisinde özellikle Estonya örneğinde de olduğu gibi bir ittifak sistemi oluşturmaya çalışmaktadır.

Günümüzde yaşanan siber çatışmalar sayesinde artık teknolojik bir kültüre sahip ülkeler, biranda büyük bir kriz yaşayabilir. Böylece iç ve dış dengesini bir anda kaybederek hızlıca yok olabilir. Teknolojik gelişmeler sayesinde geri plandayken bir

[13] Nye ve Keohane, a.g.e. ss.339.

anda üst noktalara çıkabilir. Aynı zamanda en üst noktada yaşamını sürdürürken bu konumunu kaybedebilir. Yani teknoloji ve siber uzay aslında tüm devletlere güvenlik politikalarını oluşturmalarında hem avantaj hem de dezavantaj sağlamaktadır. Bugün dev Amerikan siber güvenlik alt yapısı bile çökertilebilmektedir. Örneğin; 2001 yılında bir Amerikan casus uçağı ile Çin jeti pasifikte çarpışmıştır. Çin jeti düşünce Çinli hackerler Beyaz Saray'ın sitesine saldırmıştır. Amerika'nın en büyük sitelerinden twitter, spotify, netflix, amazon, reddit, gibi uygulamalara yönelik Ddos siber saldırıları düzenlenmesi sebebiyle tüm halkın bu uygulamalara erişimi kesilmiştir. [14] Bu olay sonrasında ise; Amerika, siber güvenliğe yönelik ilk belgesi olan 2003 tarihli The National Strategy to Secure Cyberspace adlı belgeyi yayınlamıştır.

Bu belgenin yayınlanmasının en önemli sebebi bilgi teknolojisi ve biyo-güvenlik gibi teknolojik kavramların ortaya çıkması küresel gözetim, ağ iletişimi, akıllı silah kullanımı, robotik uçak, gerçek zamanlı simülasyon ve özel hızlı dağıtım, ağa bağlı teknolojiler ve internet gibi yeni bir savaş şekli olan kuvvetlerin riskinin artmasıdır. Tüm bu gelişmeler doğrultusunda kritik altyapılara yönelik gerçekleşecek saldırılara yönelik siber ortamın önemi hakkında topluluklar kurmak (totaliter rejimlerle savaşan gruplar dâhil) için 9/11 tarihinde Clinton yönetimi 'siber güvenliği' tanıdığını belirtmiştir. [15] Çünkü toplumun savaş ve savaşçılarla ilişkisi teknolojik gelişmelerle birlikte temelden değişime uğramıştır. Günümüzde teknolojik olarak yönlendirilen savaş senaryosu siber güvenliği içermektedir. Teröristlerin veya diğer kötü huylu aktörlerin fiziksel ve dijital saldırılarla neden olduğu tehditler kritik altyapıları ve küresel iletişim ağlarını derinden etkilemekte ve etkileri yıkıcı olmaktadır. Bu sebeple siber güvenlik tartışmaları ciddi dijital güvenlik açıklarına ve önlenmesi için özellikle ABD'de ciddi stratejik çalışmalar gerçekleştirilmesine işaret etmektedir.

Bu durum ve bilinmezlikler anarşik yapıyı daha da arttırmaktadır. Anarşik yapının en doğal sonucu olarak ortaya çıkan her savaş türü bir sonraki savaş türünün nedeni ve sonucudur. Soğuk Savaş siber savaşın doğmasının bir nedenidir. SSCB'nin

[14]Reuters. Dijital Dünyada Kaos Yaşanıyor: 3. Dalga Başladı, Sputniknews, 22.10.2016, https://sptnkne.ws/c4W4, ET.30.01.2020.

[15] Barry Buzan, and Hansen, Lene. "The Eciltutıon Of Internatıonal Securıty Studıes", Cambridge University Press,2009, ss. 248.

ekonomik ve teknolojik yapıdaki değişime ayak uyduramaması bu savaşın bitmesine yol açmıştır. Bu sebep ise aynı zamanda siber savaşın başlangıcı olan internetin doğuşu, gelişimi ve yükselişini ortaya çıkarmıştır. Nasıl 1. ve 2. dünya savaşları tamamen birbirinden farklı bir savaş modeliyse, Soğuk Savaş ve siber savaşta birbirinden farklı savaş modelidir. Doğal olarak çözümü içinde farklı bir modelleme gerekmektedir. Soğuk Savaş'ın sonucu nükleer bir savaşın önlenmesine yönelik bir çaba geliştirildiğinde siber savaşın tetiklenmesine yol açmıştır. Joseph S. Nye eski savaşları ve gelecekteki savaşları bir nedensellik içinde açıklayıp gerçekçiliğin gücü ve sınırları ile birlikte alınabilecek önlemleri açıklamaya çalışmıştır.[16] Hatta siber tehditler literatüründe siber tehditlerin elektronik bir pearl harbor yaratıp yaratmayacağını tartışmaktadır.[17]

Bu tartışmalar doğrultusunda stratejik, operatif ve taktik seviyede geleceğin savaş alanı siber ortama kaymaktadır. Şuan yumuşak bir şekilde yükselme dönemini yaşayan siber uzay uluslararası ilişkilerde dış politika stratejilerinin belirlenmesi süreçlerinde aktif olarak kullanılmaktadır. Siber uzay hakkında uluslararası hukuk kurallarında misilleme yasağının bulunmaması, karşılıklılık ilkesinin olmaması, bilinmezliği içinde barındırması, kanunlara aykırı olmaması gibi sebeplerden dolayı çatışmalarda sıklıkla kullanılmaktadır. Bu bağlamda gerçekleşen tüm çatışmalar savaş hukukunda veri iletişimi ve veri koruması süreçlerine yönelik gerçekleşen siber savaş dönemi olarak gösterilmektedir. [18] Çünkü siber uzayda gerçekleşen çatışmalar, uluslararası barış ve güvenliği doğrudan ve somut bir şekilde tehdit etmektedir. Tüm devletlerin bağımsızlığını, toprak bütünlüğünü, siber alt ve üst yapılarını, bilgilerine erişimini, alt yapılarına zarar vermeye yönelik saldırıları sonlandıracak bir üst yapı organizasyon kurulamaması halinde de bu anarşik yapının etkisi artacaktır.

Kısaca özetlemek gerekirse şuana kadar küresel olarak yaşanan bütün büyük savaşların sebebi ondan bir önceki savaşlardır. 2. Dünya Savaşı 1. Dünya Savaşı'nın sonucu olarak ortaya çıkmıştır. Soğuk Savaş'ın(üçüncü küresel savaşın) kökleri ise 2. Dünya Savaşı sonucunda ortaya çıkmıştır. Günümüz siber savaşları yani dördüncü

[16] Joseph S. Nye, "Power in the Global Information Age From Realism To Globalization", Routledge Journal, 2004, ss 11-37.
[17] Joseph S. Nye, "Nuclear Lessons For Cyber Security?" Strategic Studies Quarterly, Cilt.5, No.4, Kış 2011, ss:18-36.
[18] Hans Joachim Heintze ve Pierre Thielbörger, "From Cold War To Cyber War, The Eciltution Of The İnternational Law Of Peace And Armed Conflict Over The Last 25 Years", Springer, Germany,2016, ss.24.

küresel savaş ise Soğuk Savaş'ın bir sonucudur. Soğuk Savaş'ın nasıl sona erdiğini anlamadan veya nasıl uygulandığını bilmeden siber savaşı anlayamayız. Bir başka açıdan günümüzde nükleer güçlerin ve nükleer toplumların çoğalma tehlikesi konvansiyonel savaş olmama durumunu veya sahte barış dönemini sürdürmekte ve siber savaşların artmasına sebep olmaktadır. Ayrıca günümüzde siber savaşların yaşandığını gösterebilmemiz için öncelikle politikalara bakmamız gerekmektedir. Clausewitz bakışı gibi yukarıda belirtilen tüm küresel savaşları anlamamız için önce politikaları anlamamız gerekmektedir. Savaşlar da kullanılan tanklar, piyadeler, toplar, uçaklar, gemiler asimetrik diye tanımladığımız hacker vasıtasıyla da yürütülebilir. Bunu anladığımızda silah kavramlarını açıklamayı ve dolayısıyla da siber savaşı anlamamızı daha da kolaylaştıracağız. [19]

Aynı zamanda stratejinin mantığı hep savaşları en düşük maliyetle kazanmak olmuştur. Temeli ise amaç ve araç uyumuna dayanır. 1. ve 2. Dünya Savaşları da bu amaç/araç uyumunun bittiği dönemlerde ortaya çıkmıştır. Soğuk Savaş sonrasında devletlerin içinde bulundukları tehdit/güvenlik konseptinin değişmesi sonrasında devlet dışı aktörler rakip olmuştur. Siber uzayın kullanımı ise bu örgütlerin gücünü daha da arttırmıştır. Nükleer çağa kadar temel amaç savaş kazanmak iken nükleer çağda temel amaç savaş çıkmasını önlemek olmuştur. Aynı bakış siber savaş konusunda da günümüzde devam etmektedir.

Siber uzay dünya dengelerini değiştirebilecek ve herkesin siber uzayın bir aktörü olabileceği çok düşük maliyelerle çok büyük zararlar verebileceği bir alandır. Çünkü akıllı şebekeler, akıllı ev projeleri, akıllı şehir projeleri ve elektrik şebekesine paralel haberleşme sisteminin kurulması gibi projeler hayatımızın her alanını birbiri ile bütünleştirmiştir. Bu durum ise devletlerin hayatın her alanını daha kolay kontrol edebileceği bir güce sahip olmasına yol açmıştır. Örneğin; internetin mucidi ABD bu alandan çok büyük zararlar görebilmektedir. Bu örneği destekler şekilde Yevegeniv Primakov'a göre; günümüz dünyasında ABD'nin küreselleşmede lider rol oynaması dünyanın tek kutuplu olduğunu göstermemektedir. Tam tersine tüm bu eğilimler tek kutuplu değil, çok kutuplu bir dünyaya gidişe tanıklık edildiğinin göstergesidir.[20]

[19] Ramazan Kurtoğlu, Küresel Para Oyunları ve Psiko-Siber Savaş, Destek Yayınları, İstanbul, 2017, ss. 28-29.
[20] Yevegeniv Primakov, "11 Eylül ve Irak Müdahelesi Sonrası Dünya", Doğan Kitap, 2004.

Artık sadece güç kullanma ve etkileme aracı olarak askeri, ekonomik, siyasi, kültürel, etnik, dini ve mezhepsel araçlar yoktur. Günümüzde siber araçlar önemli bir savaş silahı olarak yeni bir araç şeklinde kullanılmaktadır. Çünkü siber uzay ülkelerin dış politika kodlarını (coğrafi/jeolojik konum, yüzölçümü, nüfus, doğal kaynaklar, dil, din, sosyo-kültürel özellikler) etkisiz hale getirebilecek potansiyele sahiptir. Bu sebeple teknolojinin ve internetin gelişmesiyle ve yaygınlaşmasıyla birlikte beşinci boyut alanı olan siber uzay alanında devletler ordular kurmakta, bütçeler oluşturmakta ve faaliyetler yürütmektedirler. Günümüz bilgi çağında devletlerin kurdukları bu siber orduların potansiyel güçleri, çalışma yapıları, tehditleri ve riskleri ise birbirlerinden farklıdır. Bu farklılıklar ise anarşi ortamını kuvvetlendirmektedir. Anarşi ortamının kuvvetlenmesinin en önemli sebebiyse klasik hayatta olduğu gibi günümüz siber dünyasında da iyi ve kötünün birlikte bulunmasıdır. Bundan dolayı uluslararası anarşik yapı içerisinde üst çatı ve kuralların belirlenmesi şarttır.

Siber saldırıların, doğası gereği nerden geldiğinin kesin olarak bilinememeside bir başka önemli husustur. Bu yüzden dünya da birçok siber saldırı gerçekleşmeye devam etmektedir. Siber saldırıların devam etmesini önlemek için gerçekleştirilen siber güvenlik faaliyetleriyse tam anlamıyla bir güvenlik sağlamamaktadır. Bu doğrultuda siber güvenlik kavramı her ne kadar teknoloji içerse de en önemli halka insan faktörüdür. Eğer siber güvenlik hakkında farkındalık yaratılmaz ve nitelikli insan gücü yetiştirilemezse alınan teknik önlemlerde etkisiz kalacaktır. Bu bağlamda; siber güvenlik tehditlerine karşı kritik öneme sahip alt yapıların korunması için kurum ve kuruluşların yapılandırılması, eğitim ve konferanslar düzenlenmesi, kullanıcı grupların artması, nitelikli personel sayısının arttırılması, ulusal kuralların oluşturulması ve son olarak halkın bilinçlendirilmesi yönünde bir stratejik kültür yaratma çabası olduğu görülmektedir.

Sonuç olarak yukarıda anlatılanlar ışığında siber strateji oluşturma sürecini tek bir teori, model veya bilim dalı ile açıklamak mümkün değildir. Bu durumun nedeni siber strateji oluşturma sürecini etkileyen birçok farklı faktör bulunmasıdır. Bu faktörler doğrultusunda farklı teori ve modellerle anarşik bir yapının hâkim olduğu siber çatışma sürecini alternatif yaklaşımlarla açıklamamız gerekmektedir.

1.2. Neorealizm ve Siber Güvenlik

Uluslararası İlişkilerde hiçbir kuram ya da yöntem geçerliliğini tam olarak yitirmemektedir. Sadece taraftar sayıları ve önem atfedilmesi zaman içinde değişmektedir. Örneğin; 1. Dünya Savaşı sonrası ütopyacı liberaller hâkimken, bu kuram 2. Dünya Savaşı'nın çıkması ile önemini yitirmiştir. Aynı şekilde Sovyetler Birliği'nin beklenmedik şekilde süper güç olarak ortaya çıkması yeni-gerçekçiliği ortaya çıkarmıştır. Soğuk Savaş'ın bitişini dönemin baskın kuramı yeni-gerçekçiliğin öngörememesi de, bu kuramın da kendinden öncekiler gibi popülerliğini kaybetmesine yol açmıştır. Bu değişimlerin hepsinin asıl sebebi dünyada gerçekleşen değişimlerin sorunları da değiştirmesidir.

Soğuk Savaş döneminde ve öncesinde devlet merkezli, askeri güç odaklı bir bakış açısı olan realizm anlayışıyla tehditler ve çıkarlar temelinde güvenlik yaklaşımı etkin olmuştur. Soğuk Savaş sonrası dönemde realist güvenlik yaklaşımının artan yeni tehditleri çözümleyememesi yeni yaklaşımları doğurmuştur. Soğuk Savaş'ın bitmesiyle birlikte şiddet, korku ve risk gibi kavramlar güvenlik çalışmalarında kullanılmaya başlamış ve böylece güvenlik çalışmalarının kapsamı değişen korku parametreliyle birlikte genişlemiştir.

Güvensizlik korku içinde yaşamayı ve tehlikeleri doğurur. İnsanlar güvensizliği hissettiklerinde güvenliğin ne olduğunu anlarlar. Hayatta kalmak için güvenlik gereklidir. Bu yüzden güvenlik tehditlerden biraz özgür olmaktır. Bireyler ve aileler için geçerli olan güvensizliklerin hayatları belirlemesi, ülkeler ve milletler için de geçerlidir. Burada önemli olan aktörler tarafından yaşamı etkileyen tehlikenin ve güvensizliğin ayırt edilmesidir. Çünkü bütün toplumların yaşamları, kendilerine yapılacak bir saldırı ile devrilebilir. Örneğin; 9/11 saldırısı sıradan bir saldırının geleceği saniyeler içinde değiştirebileceğini göstermiştir.

Kenneth N. Waltz "yapı", "teori", "insan doğası" vb. kavramlar hakkında yapısal gerçekçiliğinin bir bütünü olarak uluslararası sistemin anarşik durumu hakkında güçlü bir resim ortaya koymuştur. Kenneth Waltz'a göre; anarşik sistemin hâkim olduğu yapı içerisinde devletlerarasındaki etkileşimler savaş, diplomasi, ticaret, göç ve fikirlerin hareketi gibi etkileşimlerin hepsinin seviyesi ve türleri değişiktir. Devletlerin temel birim olduğu ve anarşinin hâkim olduğu bu yapı içerisinde uluslararası bir toplumun oluşması için toplumların ortak bir amaçtan daha

fazlasını içeren ortak bir kimlik unsuru, bir "bizlik" duygusu içermesi gerekir.[21] Bu stratejiyi uygulama yönünde tarafların kimler olduğu sorusuna verilebilecek en güzel cevap internete bağımlı olan birey, örgüt, kurum ve devlettir. Bir diğer yandan Kenneth Waltz'ın birey, devlet, toplum ile uluslararası sistem analiz düzeyleri üzerinden siber uzaydaki çatışma kavramına mikrodan makroya şeklinde yaklaşabiliriz. Örneğin;

- ✓ Bireyler, İçerdekiler, Hackerlar veya Teröristler

Tablo 1 Yıllara Göre Siber Savaş Alanın Bireysel Kullanıcıları

YILLARA GÖRE SİBER SAVAŞ ALANIN KULLANICILARI	
1980'ler	Meraklılar
1990'lar	Basit Suçlular
2000'ler	Aktivistler[22]
2010'lar	Devlet Destekli Gruplar
2020 ve Sonrası	Paralı Siber Askerler

- ✓ Ulus-devletler, (siber çatışmalarda en aktif rol oynayan siber ordulara sahip en önemli aktör)
- ✓ Ulusal-ulus altı gruplar (örn: Organize suç grupları, suç örgütleri, terör grupları, çıkar grupları, vb.), ulus ötesi veya ulus üstü gruplar (çok uluslu şirketler(Sanayi casusları, Yazılım Şirketleri),
- ✓ Hükümetler-dışı örgütler (NATO)
- ✓ Uluslararası sistem (Anarşik Yapı)şeklinde konuyu inceleyebiliriz.

Ayrıca, KennethWaltz'in neorealist teorisinde iddia ettiği gibi, çatışma insan davranışlarında endemik olabilir. Fakat savaşın kökenleri sosyal organizasyonda vardır. Gücü bir amaçtan ziyade bir araç olarak gösteren Waltz'a göre uluslararası

[21] Kenneth N. Waltz, "Theory of Intemational Politics", Reading, Mass,Addison-Wesley, 1979,ss. 93.
[22]Türk Dil Kurumu açısından **'eylemci'** ve **'etkinci'** olarak geçen **aktivist** kavramı özelde belli bir düşünceyi savunan ve bunun için farklı amaçlar doğrultusunda eylemler gerçekleştiren kişidir. İnandığı düşünce doğrultusunda doğru yanlış gerekli olanı yapmak için belli bir eylemi gerçekleştirebilmektedir. Hürriyet İnternet Gazetesi, Aktivist Ne Demek? Aktivist Nedir? Aktivist Tdk Kelime Anlamı , 29.03.2020, https://www.hurriyet.com.tr/gundem/aktivist-ne-demek-aktivist-nedir-aktivist-tdk-kelime-anlami-41480920, ET.24.11.2020.

sistemin anarşik doğası ve mücadeleleri sonucunda ortaya çıkan devletlerarasındaki güç dengeleri barışın sağlanmasından ziyade devletlerin kendi sınırları içerisindeki bağımsızlığını korumaları için bir ilkedir. Çünkü günümüzde sanal dünya üzerinde milli sınırlarını korumaya çalışan devletler bam başka sorunlarla yüz yüze kalmıştır. Örneğin; internet, bilgisayar ve akıllı telefonların yaygınlaşmasıyla birlikte uzaktan erişimin kolaylaşması kurumsal ağlara fiziksel bağımlılığı azaltarak güvenlik riskini arttırmıştır. Ağların daha karmaşık hale gelmesi sonucunda ise bulut sunucuları yaygınlaşmış ve devletler sahip oldukları kritik verileri tek bir lokasyonda tutamaz hale gelmiştir. Bu durum siber tehditleri çok daha karmaşık hale getirmiştir. Karmaşıklığın yanında öngörülemeyen ve bilinmeyen tehditlerse yapay zekânın gelişmesine yol açmıştır. Yapay zeka ile birlikte teknolojideki gelişmeler daha da hızlanmış ve nesnelerin interneti (IOT) teknolojileri kavramı ile bugüne kadar internete hiç bağlanmamış buzdolabı, televizyon, otomobil, güvenlik kamerası vb. aygıtların da çevrimiçi hale gelmesi ile günümüzde her araç ciddi birer tehdide dönüşmüştür. Bu yeni siber riskler ve tehditler ile birlikte tehditlerin karakteristik özellikleri de değişerek tehditler, belirsizlik ve tahmin edilemezliğin en önemli özelliği olduğu çok yönlü "asimetrik tehdit" haline dönüşmüştür. Bu asimetrik tehditlerle birlikte günümüzde zekâsı her geçen gün daha da artan makineler üretmek, toplumun farklı katmanları arasında yaşanan siber güç çatışmalarını önemli bir sorun haline getirmiştir. [23]

Ayrıca bilgisayar ve internetin kullanılır lığının artmasıyla birlikte *bilgi* en önemli tehdit ve fırsat unsuru haline dönüşmüştür. Bu sebeple; bilgisayar ve internet kullanımının yoğunlaştığı günümüz koşullarında milli güvenlik sorunlarını, siber uzayın küresel tehdit ve fırsatlarını dikkate almadan sadece geleneksel yöntemlerle halledebilmek mümkün gözükmemektedir. Yani; küresel meselelerin bütününü kavrayıp özetleyebilen ve herkesin üzerinde mutabık olduğu tek bir sorun olmadığı gibi kontrol da hiç kimsenin ya da yöntemin tekelinde değildir. [24]

Hiç kimsenin yönetiminin tekelinde olmadığının bir göstergesi olarak bu yenidünyada ortaya çıkan fiziksel değişiklikler ve küresel düzensizlikler sonucunda

---

[23] Mehmet Karaca, "İnsanlaşan Makinalar ve Yapay Zekâ", İTÜ Vakfı Dergisi Yayınları, Sayı 75Ocak-Mart2017,Http://Www.İtu.Edu.Tr/Docs/Default-Source/Haber-Sl%C4%B1der---Ekler/Sayi75.Pdf?Sfvrsn=2 ET:13.12.2019.

[24] Zygmunt Bauman, "Kureselleşme-Toplumsal Sonucları", Çev: Yılmaz. A. Arıntı Yayınları, İstanbul, 2010, ss.63.

bir dönüşüm geçirilerek günümüzde kaotik entropi[25] çağına girildiğinden bahseden Randall Schweller, her şeyin olabileceği ve çok az şeyin tahmin edilebileceği bir döneme girildiğinden bahsetmektedir. Coğrafyanın öneminin azaldığı bu yenidünyanın içinde bulunduğu entropi çağında, hiç kimse güvende değildir. Aynı zamanda bu yeni dönemde küresel karşılıklı bağımlılık artmakta ve güç dağınık bir hale gelerek çok taraflı işbirliğini azaltmaktadır. [26]

Savunmacı gerçekci Kenneth Waltz'ın temel varsayımlarının aksine saldırgan gerçekçilerden olan Randall Schweller ve John Mearsheimer gibi düşünürlerin görüşleri Kenneth Waltz'ın savunmacı yeni gerçekçiliğinin dayandığı devletlerin yalnızca egemen güç dengesini koruyarak uluslararası sistemdeki kendi konumlarını korumaya çalışan statüko güçler olduğu önyargısını düzeltmeyi amaçlamaktadır.

Bu çerçevede uluslararası İlişkilerde realist akımın temsilcilerinden John J. Mearsheimer, liberal kurumsalcıları sadece kurumsalcı olarak adlandırmaktadır. John Mearsheimer'a göre kalıcı barış için önemli bir görev üstlenen uluslararası kurumlar tam anlamıyla bütün çatışmaları bitirecek bir güce sahip değildir. Aynı zamanda Mearsheimer uluslararası kurumlarda gerçekçiliğin yanıltıcı bir mantığı olduğuna dair şu tespitte bulunmuştur. Mearsheimer'a göre; NATO'yu bir arada tutan şey Sovyet tehdididir.[27] Mearsheimer'ın buradaki çıkış noktası ise göreceli kazanç kaygısıyla "gerçekçi bir dünyada ..." aktörlerin işbirliği ile motive edilmesinin gerekliliğidir.

Başta John Mearsheimer olmak üzere gerçekci görüşlerin ortaya koyduğu endişeden yola çıkarsak, liberal kurumsalcıların sorun çözüm için sundukları kurumlar tek başlarına yeterli değildir. Fakat burada önemli olan kurumların anarşik yapıdaki tehditlerin risk oranlarını azaltmalarıdır. Bu tezde üst otorite bir kurumun

---

[25]**Entropi Nedir?** Termodinamik alanında icat edilen entropi terimi, gelecekte iş veya faaliyet gerçekleştirmek için sistem olarak tanımlanmaktadır. Termodinamik yasası çerçevesinde; entropisi olmayan bir sistemde çok fazla potansiyel; entropisi yüksek bir sistemde çok az şey vardır. Termodinamiğin ikinci yasası iş yapıldıkça entropinin arttığını, yani enerjinin azaldığını belirtir. Etkinlik kapasitesi tükendiğinde, sistem sonunda bir noktaya gelir. Kısacası, işin performansı, sistemin gelecekteki faaliyetler için yeteneğini azaltır. Sonuç olarak sistem çalışmadığında, sonunda bir maksimum entropi noktasına ulaşır. Entropi, tuhaf bir şekilde, kaosun bir ölçüsü olarak da düşünülebilir. Randall Schweller, Maxwell's Demon And The Golden Assle: Global Discord İn The New Millennium Johns Hopkins University Press, Baltimore, 2014. Ss.18

[26]Randall Schweller, "Maxwell's Demon And The Golden Assle: Global Discord İn The New Millennium", Johns Hopkins University Press, Baltimore, 2014. Ss.12-20.

[27] John J. Mearsheimer, "The False Promise of Institutions", International Security, Cilt 19, No.3, 1994/94, ss.7-11.

kurulmasına yönelik gereklilikte bu noktada ortaya çıkmaktadır. Özellikle Soğuk Savaş bittikten sonraki süreçte aslında günümüzde bir 'Siber Savaş' dönemi yaşanmaktadır. Sıcak savaşa dönüşmesini beklemediğimiz Siber Savaş, Soğuk Savaş (1945-1990) a sadece aktif konvansiyonel silahların kullanılmaması sebebiyle benzer bir yapı içermektedir. Bu yapı, her ülkenin, kurumun ve örgütün birbirini hackleyebildiği ve aynı zamanda açık hedef olduğu anarşik bir yapı içermektedir. Siber savaş; anarşik uluslararası sistemde konvansiyonel veya nükleer bir savaşın oluşmaması için ülkelere alternatif bir yol sunmaktadır.

Günümüzde yaşandığını iddia ettiğimiz siber savaşın konvansiyonel savaşla birlikte aleni olarak ilan edilmesi halinde tüm veriler ve kurumsal hafıza çökebilir. Bu sebeple tezde " World Wide Web War " şeklinde adlandırdığım konvansiyonel silahlarla birlikte gerçekleşebilecek bir siber savaşın yaşanmaması için liberallerin belirttiği gibi devletler tarafından anlaşılarak bir üst otorite oluşturulması gerekmektedir. Zaten siber savaşın çıkış noktası da konvansiyonel veya nükleer bir savaşın oluşmaması için alternatif bir yol sunmasıydı. Fakat bu amaç zaman içinde devletlerin bu süreçten kazandığı fayda sayesinde değişmiş ve birbirlerini her an tehdit eden yapıya dönüşmüştür. Bu yeni tür çatışma boyutuda dış politika davranışlarında siber diplomasiyi kullanmayı zorunlu kılmıştır. Uluslararası ilişkilerde yeni bir alan olan siber uzay ile birlikte teknoloji, her alanda olduğu gibi devletlerarası diplomatik ilişkilerde de böylece etkili olmuştur. Kısaca; internetin kullanım alanının yaygınlaşmasıyla klasik diplomasi yeni bir boyut kazanarak "dijital diplomasi" adıyla yeni bir politika sahası oluşturmuştur. Böylece; yumuşak güç politikası uygulayan devletler için dijital diplomasi, içerisinde bulunduğumuz bu modern çağda güvenliğin sağlanabilmesi için en önemli araçlardan biri haline gelmiştir.

Bir diğer yandan güvenlik, bireyden başlayıp toplumun bütün aşamalarını kapsayacak şekilde hem teorik hem de pratikte bir bütün olarak düşünülmelidir. Ken Booth tarafından öne sürülen "Dünya Güvenlik Teorisi" dünya politikasında yüzyıllardır süregelen anarşik yapının değişen araçlarla uluslararası politikada oynadığı belirleyici rolü realist bir bakış açısını ortaya koyarak kritik güvenlik çalışmalarının geliştirilmesine fayda sağlamıştır. Bu teori içinde; derin eşitsizlik, aklın reddedilmesi, küresel politik kurumların azgelişmişliği gibi konular çağdaş

dünya siyasetinin karşılaştığı tehdit ve zorluklar olarak gösterilmiştir. Ken Booth'a göre, güvenlik çalışmalarında temel sorun, hâkim güvenlik anlayışı olan realizmin "problem çözücü" niteliğinin güven(siz)lik yaratmasıdır. Bu yüzden Booth'a göre, akademik uluslararası politika disiplini içinde eleştirel güvenlik çalışmaları gereklidir. [28] Bu tezdeki en önemli çıkış yolumuz Ken Booth gibi geleneksel güvenlik, tehdit ve savaş gibi kavramlara eleştirel bir gözle bakarak alternatif yöntemlerin varlığına odaklanmaktadır. Ayrıca; Ken Booth'ın eleştirel güvenlik bakışı; güvenliğin temel parametrelerinin devlet merkezci, askeri kaygıları dikkate alan, erkeklere özgü indirgemelerine karşı çıkmaktadır. Ken Booth'ın bunu yaparken ki asıl amacı güvenlik çalışmalarındaki geleneksel söylemin zayıf yanlarını ve sorunlarını ortaya koyarken alternatif bir söylem geliştirmeyi ve bu sayede güven(siz)lik sorununa yönelik farklı bir çözüm bulmayı amaçlamasıdır.[29]

Ken Booth dışında sosyal faktörlerin önemini vurgulayan neorealist John Mearsheimer'a göre, Soğuk Savaş'ın bitmesiyle birlikte nükleer savaş korkusunun yerine içinde iktisadi ve siyasi konuları da barındıran milli güvenlik konuları gelmiştir. John Mearsheimer bu süreçte kültür, norm ve kimlik terimlerinin kolektif bir şekilde milli güvenlik üzerindeki etkisini vurgulamıştır. Siber uzay ise kültürü, normları ve aktörlerin kimliklerinin değişmesini, kontrol edilmesini veya yönlendirilmesini sağlayan en önemli yollardan biri haline gelmiştir. Bu bağlantı uluslararası ilişkilerde siber uzayın oynadığı rolü göstermektedir. Çünkü rasyonalistlere göre, aktörler kültür ve kimliği, diğer kaynaklar gibi kendi menfaatlerini arttırmak için stratejik olarak değerlendirmektedir.[30]

Ayrıca Mearsheimer'ın gerçekçi dünyasında agresif savaş tehdidi düşük olmakla birlikte, "her devlet sistemdeki en zorlu askeri güç olmak ister" ve Mearsheimer'ın güç gerçeklerine göre "kurumların devlet davranışları üzerinde bağımsız bir etkisi yoktur". Bu bağlamda kurumsal teori ve gerçekçilik, birkaç yönden farklıdır. Gerçekçilik, küresel genellemeler ile doludur. Kurumsalcılık uluslararası dönüşme isteklerini benimsemektedir. Aynı zamanda, kurumsalcı teori

[28] Ken Booth. "Realizm And World Politics", Routledge Journal, 2011, ss. 1-50.
[29] Ken Booth, a.g.e, ss. 185-200.
[30] Peter J. Katzenstein, "Milli Güvenlik Kültürü: Dünya Siyasetinde Normlar ve Kimlik", Çeviren Efe, İ. Sakarya Üniversitesi Kültür Yayınları, Sakarya, 2014, ss. 20-30.

faydacı ve rasyoneldir. [31] Ayrıca hem realistler hem de liberaller kurumları farklı değerlendirir. Zorunlu hale gelen ve sayıları her geçen gün artan kurumlar insan yaşamı için zorunlu olmasına rağmen, aynı zamanda tehlikelidir. Bu yüzden beklentiler ve inançlara göre oluşturulacak kurumlar tasarlanırken hesap verebilirlik kural mekanizmalarına dâhil edilmelidir. Buna ek olarak küresel kurumların üstün bir zorlayıcı gücü ve meşruluğu olmalıdır.

Randall Schweller'e göre içinde bulunduğumuz entropi çağı, dünyadaki iktidar mücadelesinde büyük bir değişim yaşatarak gelişmekte olan ülkelere bu gücün geçişini simgelemiştir. Kabaca bu güç değişimi batıdan doğuya geçişi simgeleyen bir kaos ölçüsüdür. Kaosun hâkim olduğu bu yeni düzende entropinin acımasız yükselişi ile her şey düzensiz, karışık ve tahmin edilemez şekilde yaygınlaşmıştır. Düzensizliğin yaygınlaşmayla birlikte bozukluk ve entropi artmış böylece insanlar birbirlerinden ve dünyadan daha şaşkın ve bağlantısız hale gelmiştir.

Entropi çağı ile birlikte kaos haliyle tanımlanan bu yeni dünya düzeni neorealizm çerçevesinde bir anarşi mantığına dayanır. Anarşik yapı çatışmacı ve rekabetçi olmak zorundadır. İç ve genel etkileşimlerin çeşitliliği sistemin karmaşıklığının göstergesidir. [32] Bu karmaşık yapıdaysa güvenlik olgusu uluslararası ilişkilerin ana mekanizmalarından birisi haline gelmiştir. Soğuk Savaş sonrası değişen dinamikler ile de yakından ilişkili olan güvenlik olgusundaki kuramsal dönüşüm yeni tehdit araçlarına ve geleneksel anlayıştan farklı olarak tehdit çeşitliliğe yol açmıştır.

Entropi çağı ile birlikte teknolojinin ve internetin yaygınlaşması sonucunda siber sınırları içerisinde güvenliklerini sağlamak isteyen devletler; ordular kurmakta, bütçeler oluşturmakta ve faaliyetler yürütmektedir. Günümüz bilgi çağında devletlerin kurdukları bu siber orduların hepsinin potansiyel güçleri, çalışma yapıları, tehditleri ve riskleri farklıdır.

Büyük güçlerin ordu birimleri kurarak bu denli önem verdikleri siber güvenlik hem saldırı hem de savunmayı bir arada bulundurur. Siber güvenlik sadece teknik bir konu değildir. Siber güvenlik; siber terörizm, siber saldırı, siber savaş,

[31]Richard K. Ashley, "The Poverty Of Neorealism", International Organization, Cilt. 38, No. 2 (İlkbahar 1984), ss. 225-286.
[32] Martin Griffiths, Steven C. Roach, And M. Scott Solomon, "Fifty Key Thinkers In International Relations", Routledge Journal, 2009, ss 211-224.

siber casusluk gibi başlıca siber tehditlerden sistemlerimizi korumayı hedefler.[33] Yani siber güvenlik bir çatıdır. Bu yüzden devletler tarafından siber güvenlik tatbikatları gerçekleştirilerek sistemin açıklıkları ortaya çıkarılıp gereken tedbirlerin alınması yönünde çalışmalar düzenlenmektedir.[34] Çünkü siber uzay her şeyden önce bir bilgi ortamıdır. Yaratılan, saklanan ve her şeyden önce paylaşılan dijital verilerden oluşur. Sanal olmayan boyutu ise bu sistemin kurulmasını sağlayan kablolar, uzay tabanlı iletişim, teknolojik aletler vb.dir.

Siber uzay küreseldir. Fakat devletsiz değildir. Yaşam gibi boyut ve ölçeği sürekli evrim geçirmektedir. Siber uzayın teknolojisiyle birlikte aktörler üzerinde yarattığı beklentilerde benzer şekilde evrim geçirmektedir. Siber uzayın coğrafyası fiziki gibi değildir. Bir tuşla değişebilir. Buda risk ve tehdidi arttırmaktadır. Risk ve tehditlerin önlenmeside siber güvenliği sağlamaya bağlıdır. Bu yüzden siber güvenlik, yirmibirinci yüzyılda uluslararası güvenliğin en yeni sorunudur. Bu yeni soruna karşı siber güvenliği sağlamak ve siber saldırılara karşı koymak için hazırlanacak stratejinin üç hedefi olmalıdır. Bunlar; savunma, tespit ve caydırmadır. Bunun düzgün bir şekilde sağlanabilmesi için ise siber güvenlik duvarları oluşturmak yeterli değildir. Oluşturulan bu siber güvenlik duvarlarının milli imkânlarla oluşturulması ve milli yapay zekâ ile makinelerin bu stratejiyi öğrenmesi sağlanmalıdır.

Realist bakışa göre; liberallerin savunduğu gibi siber uzay'da devletlerarasında işbirliğini zorlaştıran iki unsur vardır. Bunlar; aldatma ihtimali ve devletlerin göreceli kazançlara olan ilgisidir. Zaten siber güvenliğe yönelik uluslararası bir konsensüsün oluşmaması da bu sebepten kaynaklanmaktadır. Aldatma ihtimali ve devletlerin göreceli kazançlara olan ilgisinden dolayı günümüzde siber uzay aktörlere çok büyük fırsatlar sağlamaktadır. Birçok teorist siber uzayı uluslararası ilişkilerdeki güç mücadeleleri içerisinde hak ettiği yere konumlandırmamaktadır. Fakat 1. Dünya Savaşını tartışırken de göreceğimiz gibi, sık sık sapa yerlerdeki görece önemsiz krizler büyük çatışmaları hızlandırmıştır. Çünkü anarşik bir sistemde devletlerin temel amacı güvenliktir. Savaşı kaçınılmaz kılan şey ise korkudur. Yani birinin yükselmesinin diğerinde yarattığı endişedir. Bu

[33]P.W Sınger ve Allan Frıedman, "Siber Güvenlik ve Siber Savaş", Çev.Atav, A. Buzdağı Yayınları, Ankara, 2018.
[34] Sait Yılmaz, "21. yüzyılda Güvenlik ve İstihbarat", Alfa Yayınları, İstanbul, 2006, ss. 267.

peleponessos savaşında da böyleydi. Günümüz siber dünyasında da böyledir. Özetle; Atina ve Sparta güç mücadelesinden beri temel mantık hiç değişmemiştir. Ekonomik bağımlılık, ittifak ve güç arayışları, casusluk, hegemon olma mücadeleleridir. Siber uzay da meşru ve güvenilir yönetim kuralının henüz olmadığı "doğa durumu" hâkimdir. Bu bağlamda, siyaset felsefesi perspektifinde, siber uzayda iktidar ve yönetim sorunsalı devam etmekte buda Siber Güvenlikte "Güvenlik İkilemi" ni tetiklemektedir.

Ekonomik bağımlılık, ittifak ve güç arayışları, casusluk ile hegemon olma mücadelelerini tarihten siber uzay dönemine kadar realist bir bakışla incelediğimizde şu noktalara değinmemiz gerekmektedir.[35] 18.yüzyılda o dönemin hâkim güçlerinden olan İngiltere'nin amacı, merkezi sorun Fransızların Avrupa'ya hâkim olmasını engellemekti. 18. ve 19. yüzyıllarda askeri kaynaklar sınırlıydı ve deniz aşırı ticarete oldukça bağımlı genişleyen bir ekonomik ticareti koruma mücadelesi vardı. Bu durumda İngiltere'nin arttırmaya çalıştığı aslında hâkimiyet değil, ticaretiydi. 18. ve 19. yüzyıldaki bu strateji, ulusal amaçları güvence altına almak için doğrudan doğruya kara ve deniz muharebeleri ve güçler dengesi sistemiyle bağlantılıydı. 19. ve 20. yüzyılda bu durum emperyalizme dönüşerek tehdit aracı olarak nükleer güç kullanılmaya başladı. Aynı şekilde; günümüz anarşik uluslararası sistemi de kendi dinamikleri içinde beşinci bir boyut olarak konumlandırdığımız "siber uzay" alanında gerçekleşen siber saldırılar ve siber çatışmalarla sürdürülmektedir. Örneğin; günümüzdeki durum bu zamana kadarki geçen bütün tarihsel süreçlerden farklıdır. Artık kripto paralar (bitcoin vb.), elektronik ve online bankacılık ve finans sistemi üstünden ekonomik yapı işlerken ticari yapı ise artık denizler üzerinde değil "siber uzay" üzerinde E-Ticaret şeklinde gelişmektedir. Özellikle Çin e-ticaret üzerinden ciddi bir atılım gerçekleştirerek dünya ticaretinde hâkim bir konuma gelmiştir. Bu hâkimiyeti geliştirmek ve korumak içinde siber saldırıları aktif bir şekilde kullanmaktadır. Artık Çin gibi birçok devlet kendi internet sitelerini kurmakta, gümrük mevzuatlarını oluşturmakta ve yazılımlarını geliştirmektedir. Bunun en güzel örneğini ülkemizde de görebiliriz. Örneğin; PTT AŞ ile Katar Posta Teşkilatı arasında gerçekleştirilen işbirliği çerçevesinde www.turkishsouq.com adıyla e-ticaret platformu oluşturulmuştur. Yani artık devletler kendi aralarında ticari

[35] Paul Kennedy, "Büyük Güçlerin Yükseliş ve Çöküşleri", Çev. Karanakçı, B. Türkiye İş Bankası Yayınları, İstanbul, 2013.

ilişkilerini e-ticaret platformları üzerinden yürütür hale gelmiştir. Nasıl yirminci yüzyılda Avrupa'da Almanya'nın ortaya çıkışı sisteme karşı bir meydan okuma yaratmışsa, yirmi birinci yüzyılda da internet, bilgi teknolojileri, yapay zekâ ve bulut bilişim gibi kavramların ortaya çıkışı uluslararası sistemde yeni meydan okumaları, güç mücadelelerini, meşruiyet kavgasını ve rekabeti oluşturmuştur. Özellikle ABD, Çin, Rusya ve İsrail gibi ülkeler "Siber" yoluyla birbirlerine karşı caydırma stratejilerini ve taktiklerini kullanmaktadır.

Aktörlerin birbirlerine karşı caydırma taktiklerini uyguladıkları uluslararası anarşik sistemde siber uzayın devletler açısından kara, deniz, hava ve uzaydan sonra beşinci boyut güvenlik alanı kabul edilmeye başlaması internet'in küreselleşme sürecinin etkisinin her disiplinde olduğu gibi uluslararası ilişkileri de etkilemesine yol açmıştır. Beşinci bir boyut olan siber uzay (internet), zaman ve mekân algısını değiştirmiş ve insanlarda algılama, düşünme, öğrenme ve farkındalık biçimlerini dönüştürmüştür.

Ayrıca günümüz anarşik yapısının sahip olduğu çok kutuplu sistemdeki güç dengesi, ittifaklar kavramıyla da yakından ilişkilidir.[36] Siber uzay alanında güç dengesi ve ittifak sistemini oluşturma yönündeki ilk atılımları ise Estonya krizi sonrasında görmekteyiz. Estonya krizi sonrasında NATO tarafından oluşturulan merkezle devletlerin kendi siber güvenliklerini sağlamaları yönündeki ilk ittifak eğilimi örnekleri görülmüştür.

Enformasyon amaçlı siber uzay vasıtasıyla gerçekleştirilen savaşları açıklayabilmemiz için realist bakışın en önemli yöntem olarak ortaya koyduğu savaş kavramının özelliklerini incelememiz gerekmektedir. Savaş; bir devlet veya devletler grubunun, diğer bir devlet veya devletler grubuna karşı güç kullanarak diplomatik yollarla çözülemeyen sorunlarını çözmesi anlamına gelmektedir. Bir ülkenin politik ve sosyal yapısı, ekonomik gücü ve coğrafi konumu, silahlı kuvvetlerinin yapısını ve savaşın karakterini belirler. Bu durum siber savaşlar içinde geçerlidir. Şiddetin büyüklüğü, savaşın amacına ve araçlarına göre değişir. Politika bir araç olarak kullandığı savaşın amacını ve uygulanacak şiddetin derecesini belirler. [37]

[36] Joseph S. Nye ve David A. Welch, "Küresel Çatışmayı ve İşbirliğini Anlamak", Çev.Akman, R. Türkiye İş Bankası Yayınları. İstanbul, 2010, ss. 108-118.
[37] Nejat Eslen, "Tarih Boyu Savaş ve Strateji", Q-Matris Yayınları, İstanbul, 2003, ss.13-15.

Savaş politik bir amaca hizmet eden politik bir eylemdir. Bu sebeple politikadan ayrı düşünülemez. Politik amaca hizmet etmesi savaşın mantığını oluşturur. Savaşın yönetimi ayrı bir uzmanlık gerektirmekle birlikte kendine özgü prensipleri vardır. Savaşın ana hatları politika tarafından belirlenir. Siber uzay alanında ana hatlar siyasi irade tarafından belirlenmekle birlikte bu alanın yönetimi uzman ordu birimleri tarafından gerçekleştirilmektedir.

Savaş bir şiddet kullanma alanı olduğu ve sonrasında gözyaşı ve acı yaratması sebebiyle doğasında tehlike vardır. Siber alanda oluşan riskler ise siber tehdit kavramını ortaya çıkarmaktadır. Devletler siber saldırılara ve siber savaşlara karşı önlem alabilmek için siber tehdit kavramını önceliklerine almakta bu sebeple de günümüz devlet yapılanmalarında siber birimler kurarak can ve mal kayıplarına yönelik tehditlerin ve tehlikelerin önüne geçmeyi planlamaktadır.

Savaş belirsizlik alanıdır. Siber alanda aynı şekilde içinde belirsizlikleri barındırmaktadır. İçinde barındırdığı belirsizlik ve kolay gizlenebilme imkânıysa devletlerin bu yolu seçmesine yol açmaktadır.

Rastlantı ve şans alanı olarak görülen geleneksel savaş yöntemleri aynı şekilde siber savaş içinde geçerlidir. Çünkü Stuxnet gibi bir virüsün güvenlik imkânlarının en üst düzeyde sağlandığı bir tesise sokulması bir siber savaş olarak değerlendirilse de içinde rastlantı ve şansı barındırmaktadır.

Operasyonel siber savaş; adından da anlaşılacağı üzere mevcut bir fiziksel savaş sırasında kullanılır. Geleneksel savaş yöntemleri kullanılırken devletler siber saldırıları da gerçekleştirir. Bu onlara geleneksel savaş yöntemlerinde üstün olabilmek için ciddi bir güç kazandırmaktadır. Siber savaş tek başına belki faydalı olamayacak bile olsa geleneksel savaş yöntemleriyle birlikte kullanıldığında çok ciddi sonuçlar yaratabilir. Beklenmeyen bir anda ve doğru zamanda yapılan ani siber saldırılar çok etkili olabilir. Bu durum Gürcistan savaşında fazlasıyla kendini göstermiştir. Örneğin; Gürcistan savaşında da görüldüğü gibi günümüz siber savaşlarında "yıpratma", artık düşman ordularının gücünü savaş alanında aşındırma sorunu değildir. Gerçek hedef Clausewitz' terimiyle "ağırlık merkezi" artık bizzat ordular değildir. İnsan ve malzemeden ziyade bilgi teknolojisi ve internetin yayılması artık tüm düşmanların güç kapasitelerini dışarıdan etkileyebilme fırsatı sunmuştur. Aynı zamanda; günümüzde büyük güç aktörlerinin elinde "nükleer silahlar"

bulunması sebebiyle dünyada bloklaşmaları yaratacak bir "topyekün savaş" yaşanmasının yerine bu tarz siber yöntemlerin devletler tarafından kullanılacağı göstermektedir.

Aynı zamanda geleneksel savaşta önemli bir unsur olan insan faktörü siber savaşlar içinde geçerlidir. Özellikle hackerlar tarafından yürütülen siber savaşlarda artık beyaz şapkalı hackerlar bir araya toplanarak ülkeler tarafından siber ordular oluşturulmaktadır.

Geleneksel savaşlar ile günümüz siber savaşları arasındaki bir diğer önemli hususta moral değerleridir. Moral stratejisi insanları motive edecek imkânları kısıtlayarak, morallerini yüksek tutmalarını engelleyip savaşı kazanmayı hedeflerler. Örneğin; Rusya'nın siber saldırı kabiliyetini ortaya çıkaran 2008 yılındaki Gürcistan ve Rusya arasındaki Güney Osetya savaşı sırasında, Rusya tarafından gerçekleştirilen botnet ve ddos saldırıları sonrasında; Gürcistan'da hem halkın hem ordunun hem de yöneticilerin morali bozulmuştur. Çünkü günümüz siber savaşlarında yıpratma, sadece düşman ordularının gücünü savaş alanında aşındırma sorunu değildir.

Robert Gilpin uluslararası politikanın iki bin yıldır değişmediğini ve Thucydides'in bugünkü dünyayı anlamakta zorlanmayacağını ileri sürmüştür. Bu bağlamda siber savaş kavramı sadece bir araç değişimi olarak karşımızda durmaktadır. Hala güvenlik ikilemi hala ittifak arayışları (NATO gibi örgütlenmeler) devam etmektedir. Amaç hala aynıdır. Hayatta kalmak. Bu yüzden ''Siber Savaş'' kavramı sadece söz konusu sürecin yeni araçlar(silahlar) çerçevesinde yeniden belirlenmesidir.

Siber savaş, geleneksel savaş yöntemleriyle birlikte kullanıldığında çok ciddi sonuçlar yaratabilir. Beklenmeyen bir anda ve doğru zamanda yapılan ani siber saldırılar çok etkili olabilir. Geleneksel savaş yöntemlerinde üstün olabilmek için ülkelere ciddi bir güç kazandırabilir. Bu doğrultuda NATO ve Rusya arasında günümüzde yaşanan asimetrik siber savaş kavramları yeni güvenlik stratejilerinin yaratılmasına ihtiyaç duyulduğunun en önemli göstergesidir. Bu yeni savaş konsepti hızlı ve çok büyük değişimleri içinde barındırmakla birlikte yeterince anlaşılamadığından karmaşık, çok boyutlu, sınırsız ve öngörülemez bir gelecek planı ortaya koymaktadır. Örneğin; dönemin Rusya Genelkurmay Başkanı General Valery Gerasimov'in "hibrid savaş" olarak kavramsallaştırdığı "Gerasimov Doktrini" ile

birlikte Rusya'nın eski coğrafyasına yönelik gerçekleştirdiği politikalarında NATO üye ülkeleri üzerinde Soğuk Savaş dönemi benzeri bir baskı ve korku yaratmaktadır. Bu strateji temelde geçmişte George Kennan çevreleme politikasında ulaşmak istediği amaç neyse aslında Gerasimov'la birlikte bu amacın farklı bir çeşidini gerçekleştirmeyi planlamaktadır.

Bu doğrultuda uluslararası güvenlik çalışmalarına yönelik 4 temel soruya odaklanılmalıdır. Bunlar, kimin güvenliği korunmalı? Ordu, birincil güvenlik sektörü olarak görülmeli mi? Güvenlik yalnızca dış tehditlerle mi ilgilidir? Güvenlik politikalarındaki tehlike ve acil durum nedir?[38] Bu sorular çerçevesinde teknolojik gelişmeler çerçevesinde güvenliğe özgü yaklaşımlar daha rahat cevaplanabilir.

Anarşik uluslararası devletler sistemi içerisinde toplumun savaş ve savaşçılarla ilişkisi teknolojik gelişmelerle birlikte temelden değişime uğramıştır. Günümüzde teknolojik olarak yönlendirilen savaş senaryosu siber güvenliği içermektedir. Teröristlerin veya diğer kötü huylu aktörlerin fiziksel ve dijital saldırılarla neden olduğu tehditler kritik altyapıları ve küresel iletişim ağlarını derinden etkilemekte ve etkileri yıkıcı olmaktadır. Bu sebeple siber güvenlik tartışmaları ciddi dijital güvenlik açıklarına ve önlenmesi için ciddi stratejik çalışmalar gerçekleştirilmesine işaret etmektedir. [39] Aynı zamanda; bilgi teknolojisi ve biyo-güvenlik gibi teknolojik kavramların ortaya çıkması küresel gözetim, ağ iletişimi, akıllı silah kullanımı, robotik uçak, gerçek zamanlı simülasyon ve özel hızlı dağıtım, ağa bağlı teknolojiler ve internet gibi yeni bir savaş şekli olan kuvvetlerin riskini arttırmıştır. Buzan'a göre; tüm bu gelişmeler doğrultusunda kritik altyapılara yönelik gerçekleşecek saldırılara yönelik siber ortamın önemi hakkında topluluklar kurmak (totaliter rejimlerle savaşan gruplar dâhil) için 9/11 tarihinde Clinton yönetiminin 'siber güvenliği' tanıdığını belirtmiştir.[40] Yani siber güvenlik uluslararası anarşik sistemi domine eden ülke tarafından kabul edilmiştir.

Bunun yanında uluslararası düzeni sağlayacak bir uluslararası kuruluşun olmayışı aynı doğa hali gibi siber uzay alanında güçlü olanın her istediğini yapacağı ve haklı görüleceği bir duruma yol açmaktadır. Realist bakış doğa halinin kötü, vahşi

[38] Barry Buzan ve Lene Hansen, "The Eciltution Of International Security Studies", Cambridge University Press, 2009, ss.10.
[39] Buzan ve Hansen, a.g.e. ss.269.
[40] Buzan ve Hansen, a.g.e ss.248.

ve kısalığına vurgu yaptığından bu durumu normal görmektedir. Liberaller ise uluslararası hukukun ve örflerin varlığına işaret ederler. Bu yüzden bu tez siber uzay alanında düzeni sağlayabilmek için uluslararası bir kuruluş oluşturmanın gerekliliğini vurgulamaktadır. Uluslararası kuruluşlar her ne kadar tamamen barışın güvencesi olmasa da genişleyen nükleer cephanelikler sonucunda nükleer güce sahip aktörlerin insan varlığına yönelik durdurulamaz bir şekilde ölümcül tehditler vermeye başlamasını engellemek için siber uzaya yönelik uygulayıcı ve denetleyici uluslararası bir örgütün kurulması birçok sorunu çözüme kavuşturabilir.

Nasıl nükleer cephaneliklerin arttırılmasının serbest bırakılması nükleer tehdidin artmasının en büyük sebebiyse[41] siber silahların artmasının engellenmemesi de en büyük tehdit unsurudur. Siber silahlar ve nükleer silahlar arasındaki en önemli benzerlik her ikisinin de bütün yaşamı alt üst edebilecek bir kapasiteye sahip olmasıdır.

Siber silahlar ve nükleer silahlar arasındaki en büyük farklılık nükleer silahların sahip olduğu tehdit boyutlarının Hiroşima ve Nagazaki de test edilerek anlaşılmış olmasıdır. Tehdit boyutu anlaşıldığından dolayı nükleer silahların kısıtlanmasına yönelik uluslararası anlaşmalar çerçevesinde sınırlamalar, kurallar ve yasal mevzuatlar konulmuştur. Fakat siber silahlar için benzer bir uygulama henüz bulunmamaktadır. Buda siber savaşın sınırları konusunda uluslararası sistemin anarşik yapısını daha da destekler bir yapı ortaya çıkarmaktadır.

1.3. Güvenlikleştirilen Siber Uzay ve Neoliberal Kurumsalcı Teori

Soğuk Savaş'ın bitmesinden sonra ortaya çıkan ve devletlerin işbirliği yapmasına dayanan neoliberaller, sistemin anarşik yapısı içerisinde devletlerin rasyonelliğini kabul ederler. Ayrıca mutlak kazanca bakarak Realistlerin bu etkiyi abarttığını belirtirler. Bu çerçevede anarşik ortamda işbirliği geliştirilmesinde uluslararası kurumların payı büyüktür. Uluslararası kurumlar geleceğin belirsizliğini ortadan kaldırarak bilgi sağlarlar. Böylece de etkileşim, maliyetini düşürürler.

"Kurum" kavramı hem kamu örgütleri gibi formel örgütlenme biçimlerini, hem de gelenek gibi informel bireysel davranışları kapsayan belirli bir durum veya özellik kazanmış olan toplumsal bir düzen veya kalıptır. "Kurumsallaşma" ise

[41] Buzan, ve Hansen, a.g.e ss. 109.

"istikrarsız, gevşek yapılı ve dağınık etkinliklerden düzenli, istikrarlı ve toplumsal açıdan bütünleştirici kalıpların ortaya çıkması"'nı içeren bir tür kazanma süreci olarak tanımlanmaktadır. Bir başka ifadeyle kurumsallaşma ile birlikte kurumlar bir biçime, istikrarlılığa veya varlığını sürdürmeye dönüşmektedir. [42]

Uluslararası ilişkilerdeki toplumsal düzen yapıları veya araçları olarak kurumlar, toplum içinde aktörlerin eylemlerini şekillendiren istikrarlı ve tekrarlayan davranış kalıplarıdır. Bu sebeple kurumlar sosyal bilimler için çok önemlidir. Kurum kavramına atfedilen bu önem, kurumsallaşma süreci hakkında farklı yaklaşımların ortaya çıkmasına yol açmıştır.

Bu bağlamda; hem güvenlik hem de politik ekonomi konularında uygulanabilecek kurumsalcı teori anarşi altında işbirliğini temel alır. [43] Kurumsalcı teori, kurumları hem bağımsız hem de bağımlı olarak kavramlaştırmaktadır. Kurumlar bağımlıdır. Çünkü kurumlar devletler tarafından yaratılmıştır. Kurumlar bağımsızdır çünkü kurumlar insan eyleminin bir sonucu olarak değişmektedir. Bu durum mahkûmların ikileminde olduğu gibi ikiden fazla devlet içeren uluslararası sistemde başkalarını aldatma potansiyelinin yüksek olması sebebiyle aktörlerin anlaşmasında sorun ortaya çıktığını göstermektedir. Bu süreçte; göreceli kazanımlar ve kurumların rolünün önemli vurgulanmakta ve işbirliği ile potansiyel mutlak kazanımların gerçekleşebileceği belirtilmektedir.

Kurumların oluşturulmasındaki fonksiyonlar ise şunlardır; geniş çaplı şiddetin kullanımını sınırlandırmak, sonraki nesilleri savaşın tehlikesinden kurtarmak, yönetişimin ademi merkeziyetçiliğinin olumsuz dışsallığını sınırlandırmak, garanti sağlamak ve Büyük Buhran gibi dünya sistem bozulmalarıyla başa çıkmaktır. Fakat günümüzde en değerli meta olan bilgi güvenliğini korumaya yönelik herkesçe kabul görmüş kriterler belirlenememiştir. Bu durumda farklı görüşlerin artmasına yol açmaktadır. Bu durum uluslararası ilişkilerde yaşanan anarşik durumun aslında göstergesidir. Bu yüzden bu tanımlamadaki çeşitlilik NATO ve Rusya arasında gerçekleşen siber sorunlarında çözülememesine ve güvensiz bir yapıya yol açmaktadır.

---

[42]Tuncer Fidan, "Kurumsalcılık Yaklaşımları ve Yeni Kurumsalcılık Perspektifinden Eğitim Örgütleri", Medeniyet Eğitim Araştırmaları Dergisi, Cilt:1, Sayı:1, 2017, ss.1-16.

[43] Robert O. Keohane ve Lisa L. Martin, "The Promise of Institutionalist Theory", International Security, Cilt. 20, No. 1. Yaz, 1995, ss.43

Aynı zamanda; siber ortamdaki her türlü bilginin korunması şeklinde tanımlanan siber güvenlik, bilginin üretimi, depolanması, işlevsel kılınması ve iletimiyle de yakından ilgilidir. Böylece siber uzayın karmaşık ve çok boyutlu kendine has ortamı siber güvenlik nosyonunu öncelikli güvenlik sorunlarından biri haline getirmiştir. Bunun sonucunda da küreselleşme ve bölgeselcilik gibi kavramlarında tetiklediği devlet arasında yaşanan siber sorunlar kurumların oluşturulmasını zorunlu hale getirmektedir.

Küreselleşme ve bölgeselcilik gibi kavramlar çok kutuplu bir güç sistemi dengesine dönüşten başka bir şey değildir. Joseph Nye'a göre, bölgesel sınırlar siyasi liderlerin değişen güçlerini, normlarını ve çıkarlarını yansıtmaktadır. Siber feodalizm kavramı ile Peter Drucker ile Alvin ve Heidi Toffler bilgi devriminin hiyerarşileri yassılaştırdığını ve yerlerine ağ örgütlenmeleri geçirdiğini ileri sürmüştür. Böylece bir hacker ya da küçük bir devlet, güçlü ve büyük bir devlete karşı ciddi başarılar elde edebilme fırsatına sahip olmuştur. Peter Katzenstein ise iki kutupluluğun çökmesiyle birlikte bölgeselleşmenin dünya siyasetindeki öneminin arttığını belirterek küreselleşme ve bölgeselciliğin birbirlerini tamamlayıcı ve iç içe geçmiş süreçler olduğunu belirtmiştir. Eşzamanlı olarak meydana gelirler ve birbirlerini beslerler. Bu durumu bölgeselleşmenin en önemli örneği olan Avrupa Birliğinde de görebiliriz. Örneğin; Avrupa Birliğinde bu yeni siber alana yönelik bölgesel karmaşıklaşma içinde temel avantajlar sunan teknoloji kompleksleri, hukuki düzenlemeler, inovasyon ve üretim ağlarının önemi giderek artmaktadır. Bu bağlamda hem kurumsallaşma hem de bölgeselleşme örnekleminde önemli bir yer tutabilecek Avrupa Birliği'nin politikaları örnek çatışma vakalarını incelediğimiz bölümde ayrıntılarıyla sunulacaktır. Fakat şimdi Avrupa Birliği'nin siber uzay hakkındaki faaliyetlerini kısaca açıklarsak,

Avrupa Birliği'nin siber güvenlik politikaları ve güvenlik stratejilerinin temeli kritik alt yapıların korunmasını sağlamaktır. Bunu yaparken Avrupa Birliği siber güvenlik hakkında yasal düzenlemeler gerçekleştirmektedir. Bu çerçevede 2013 yılında yayınlanan Cybersecurity Strategy for the European Union (AB için Siber Güvenlik Stratejisi) en önemli belgedir. Bu belgeyle birlikte AB kritik alt yapılarla siber güvenlik arasındaki bağlantıyı vurgulayıp ortak bir siber güvenlik politikası oluşturulmasını, politikaların ve kurumların bu bağlamda işleyişlerini vurgulamıştır.

Uluslararası ortamda Avrupa Birliği'nin siber güvenlik hususuna verdiği bu önem uluslararası aktörler arasında siber güvenlik konusunun ne kadar önemsendiğini göstermektedir. [44]

Avrupa Birliği ve NATO örneklerinden yola çıkarsak küreselleşmiş bir dünyada gerçekleşecek yönetim için etkili kurumlar oluşturmak zordur ama gereklidir. Oluşturulacak Liberal-demokratik kurumlar sayesinde hesap verebilirlik ve katılım artacak böylece ikna, zorlama ve ilgi alanına dayalı pazarlık ile güvenlik daha kolay sağlanabilecektir. [45]

Küreselleşme ile ilgili bir diğer önemli husus mesafelerin daralmasıdır. Günümüzde yaşanan teknolojik gelişmelerle birlikte ağların ortaya çıkması dünyayı ekonomik, siyasi, çevresel ve sosyal olarak bağlantılı bir hale getirmiştir. Bu sebeple; her anlamda küreselleşen dünyada etkili yönetim için daha kapsamlı uluslararası kurumların oluşturulması ve işbirliğinin teşvik edilmesi çatışmaların çözülmesi için zorunlu hale gelmiştir. Böylece küreselleşme sonucunda ortaya çıkan karşılıklı bağımlılık bu gerekliliği desteklemiştir. Çünkü karşılıklı bağımlılığın önemli bir anlamı, fırsatlar sağlamasıdır. Bu durumda işbirliği ile yaşanacak çatışmalara alternatif geliştirerek her iki tarafa da potansiyel kazançlar yaratmaktadır. Fakat sistemik etkiler kurumlar tarafından oluşturulacak bir işbirliği sayesinde sağlanmazsa gelecekte, biyoteknoloji, yapay zeka, büyük veri, nesnelerin interneti, siber uzay, genetik manipülasyon ve henüz farkında olmadığımız teknolojiler ile bu bağımlılık, asimetrik tehdit aracı olan risk unsurlarını arttırabilir. Her geçen gün yenilenen teknolojilerin artmasıysa asimetrik riskleri ve tehditleri oluşturarak kayıt dışı şiddetin küreselleşmesi ve korkunun liberalizmi gibi olguları yaratmaktadır. Şiddetin küreselleşmesi ve korkunun liberalleşmesiyse tehlikenin kendisidir.[46] Bu yüzden günümüzde önemi ve etkinliği her geçen gün artan başta siber uzay olmak üzere iletişim teknolojileri hafife alınmamalıdır.

Bu durumu bir başka şekilde ifade edersek; tarih boyunca uluslararası sistemin içerdiği anarşik yapı siber uzay alanında da devam etmektedir. Bu yüzden devletler ulusal çıkarlarını sağlayabilmek için siber faaliyetlerini gizli olarak

[44] Mehmet Eren, "Avrupa Birliği'nin Siber Güvenlik Politikası", Beta Yayınları, İstanbul, 2017.
[45] Robert O. Keohane, "Power And Governance In A Partially Globalized World", Routledge, 2002, ss. 245-265.
[46] Robert O. Keohane, a.g.e ss. 272.

yürütmektedir. Aynı zamanda coğrafi konum ve yakınlık, jeopolitik gelenek gibi konularda öngörüleri ortadan kaldıran siber uzay tamamen sınırı olmayan ve herkesin herkese kolaylıkla saldırabileceği bir yapı sunmuştur. Buda ülkelerin kendi siber güvenlik duvarlarını oluşturmalarını zorunlu kılmıştır. Uluslararası bir kurumun oluşturulmasıysa realistlerin varsaydığı anarşinin etkisini hafifletecektir. Bu sebeple siber uzayda gerçekleşen sorunlar hakkında sorumlu bir uluslararası örgütün oluşturulması şarttır. Siber uzay hakkında tam anlamıyla yetkiye sahip bir şekilde oluşturulacak bu örgüt uluslararası hukuk kuralları çerçevesinde sistemde bir güç dengesi ve istikrar yaratacaktır. Aksi takdirde sistemin içinde barındırdığı anarşi artarak devam edecektir.

Siber stratejilerin gelişim sürecini incelediğimizde; 20. yüzyılda bilgisayarın ve internetin ortaya çıkışı ile ülkelerin saldırı ve savunma tekniklerindeki değişime paralel olarak barış ve işbirliği kavramlarının da dönüştüğü görülmektedir. Özellikle 20. yüzyılın son 10 yılında ve 21. yüzyılın başlarında yaşanan siber saldırılar, casusluk mücadeleleri, savaşlar, gerginlikler ve hareketler bilişim sistemlerindeki gelişmelerden etkilenmiştir. Bu sebeple, Dünyada birçok ülke kendi Ulusal Siber Güvenlik Stratejisini belirlemiştir. Aynı zamanda değişen dünya değerleri arasında ilk sırayı alan bilgiyi, koruma ve muhafaza etme biçimi de böylece değişiklik göstermiştir.

Günümüzde bilginin geliştirilmesi, aktarılması ve ele geçirilmesi için siber uzay kullanılmaktadır. Ülkelerde bilgiyi ele geçirmek için siber uzay üzerinden kanunsuz yöntemler kullanarak saldırı ve savunmalar gerçekleştirilmektedir. Siber uzay ve bilgi teknolojilerine olan bağımlılığın her geçen gün artması istihbarat, suç, terör ve savaş gibi geleneksel kavramların da dönüşmesine yol açmıştır. Bu yüzden de devletler en azından kendi içlerinde bu suçları engellemek için kanunlar, yönergeler ve yönetmelikler vasıtasıyla iç hukuklarını düzenlemektedir. Fakat uluslararası hukukta bu yönde geliştirilmiş bir fikir birliği ne yazık ki bulunmamaktadır.[47]

Bu tezde ayrıntılarıyla belirteceğim hukuki süreçlerle ilgili en önemli husus devletlerin en azından kendi içlerinde bu suçları engellemek için kanunlar, yönergeler ve yönetmelikler vasıtasıyla iç hukuklarını düzenledikleri halde

[47] Atalay Keleştemur, "Siber İstihbarat", Level Kitap Yayınevi, İstanbul, 2015, ss:417.

uluslararası hukukta bu yönde geliştirilmiş bir fikir birliğinin olmadığını göstermektedir. Robert Keohane ve Joseph Nye gibi Neoliberal düşünürlerin çatışma/işbirliği bakışı, ortak çıkarlar, güç dengesi ve barışçı ilişkiler üzerine kurulu bir uluslararası hukuk kodunun oluşturularak tehditlerin azaltılabileceği yönünde bir fikre dayanır. Robert Keohane'ye göre; hem sistemin hem de toplumun birbirinden ayrıldığı sınırların ve farklılığın üstesinden gelmek için bir tür dayanışma ve işbirliği modelinin gerekliliğinin altını çizmektedir.

Bilgi devrimiyle bağlantılı hem hükümetleri hem de uluslar ötesi aktörleri birleştiren siber savaş ve siber tehdit kavramları modern toplumların korunmasızlığıdır. Joseph Nye bu yeni kavramlar hakkında "Elektronik Pearl Harbor" gibi bir benzetmeyle konudan bahsetmiştir.[48] Aynı zamanda, Joseph Nye bu noktada devletlerin siber güvenliğine yönelik temel tehditleri devletlerin birbirlerine karşı oluşturduğu siber tehditler ve devlet dışı aktörlerin devletlerin siber güvenliğine yönelik tehditleri şeklinde iki ayrı bölüme ayırmıştır. Bu sınıflandırmaya göre siber çatışmalar ile ekonomik temelli casusluk ve istihbarat tehditleri daha çok devletler ile ilişkilendirmektedir. Siber ağlar aracılığıyla işlenen suçlar ve siber terörizm ise devlet dışı aktörler ile ilişkilendirmiştir.

Realistlere göre kültür ve kimlik, yeteneklerin dağılımının bir türevidir. Akılcılara göre ise, aktörler kültür ve kimliği kendi çıkarlarını daha da geliştirmek için kullanır. Yapısal neorealist geleneksel bakışa göre güvenliğin dar tanımı, askeri güçlerin devletler tarafından kullanımı ve kontrolüne odaklanmaktadır. Neoliberal kurumsalcılık ise devlet dışındaki grupları, bireyleri ve diğer devlet dışı aktörleri etkileyen askeri, politik, ekonomik, sosyal, çevresel ve zihinsel güvenlik tehditlerini önemser.

Neorealizm ve neoliberalizm, uluslararası anarşinin uluslararası politikanın analizdeki merkezi önemi üzerinde hemfikirdir. Neorealist ve neoliberal perspektifler arasındaki ayrım ise şu şekildedir. Neorealistlere göre anarşik bir uluslararası sistemin rekabet baskısı tarihte sabittir. Neoliberaller'e göre ise uluslararası kurumlar devletlerin çıkarlarını tanımlayabileceği ve çelişen politikaları koordine edebileceği

[48] Joseph Nye, "Nuclear Lessons For Cyber Security?" Strategic Studies Quarterly, Cilt.5, No.4, Kış 2011, ss.18-36.

alternatif bir yapısal bağlam sağlamaktadır.[49] Siber uzay içinde bu yapısal bağlam gerçekleştirilecek hukuki düzenlemeler ve oluşturulacak kurumlar ile sağlanabilir.

Robert Keohane'ye göre, hegemonya sonrası uluslararası politika, uluslararası anarşi koşullarının içerdiği belirsiz iktidar siyasetini yaşamak zorunda değildir. Bunu yaşamak yerine hegemonların kurumlar aracılığıyla yarattığı uluslararası düzen, uluslararası anarşi sorununu hafifletebilir. Bu kurumlar izlemeyi kolaylaştırır, politik şeffaflığı arttırır, belirsizliği azaltır ve politika ile ilgili bilgileri arttırır. Çatışmaların devam ettiği hegemonik bir sistemin kurumsal altyapısı böylece işbirliğiyle çelişkili politikaların koordinasyonunu kolaylaştırabilir. [50] Bu yüzden oluşacak tehditlerle mücadele edilebilmek için "Siber suç" ve "siber suçlu" gibi kavramların Birleşmiş Milletler gibi bir üst otorite tarafından hukuksal düzenlemelerinin yapılması şarttır. Örneğin; Birleşmiş Milletler kapsamında siber güvenliği incelediğimizde: uluslararası anarşik sistem üzerinde devletlerarasında meydana gelebilecek herhangi bir saldırıda başvurulacak temel kurum Birleşmiş Milletlerdir. BM Sözleşmesi'nde 51. maddede; klasik/fiili anlamda bir çatışmadan bahsedildiği görülmektedir. Bu ifadede herhangi bir şekilde siber saldırı ifadesi yer almamaktadır. [51]

Fakat ABD ve Rusya gibi ülkeler böyle bir uluslararası anlaşmanın imzalanmasının, anlaşmaya uyulmasının, denetlenmesinin ve devletler tarafından uygulanmasının imkânsızlığı gerekçesiyle istememektedir. Herkes tarafından görülen gerekçe bu uygulamanın imkansızlığı olsa da bu itirazın asıl altında yatan sebep siber saldırıların devletlere sağladığı güç avantajını kullanmaktır. Ama yine de uluslararası alanda siber güvenlikle ilgili ufakta olsa kıpırdanmalar gözükmektedir. Bunlardan bazıları ise şunlardır;

NATO Kapsamında Siber Güvenlik: Siber Güvenlik kapsamında yapılan uluslararası seviyede ilk çalışma NATO Siber savunma mükemmeliyet merkezi ve uluslararası bağımsız uzmanlar grubu tarafından hazırlanan "siber savaşta uygulanacak hukuk hakkında talinn el kitabı"dır. Cambridge Üniversitesi tarafından 2013 yılının Mart ayında yayınlanan bu el kitabı, uzman grubu görüşlerinden

[49] Robert Powell. "Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate," International Organization, Cilt. 48, No. 2, İlkbahar 1994, ss. 313-44.
[50] Robert O. Keohane, "After Hegemony: Cooperation and Discord in the World Political Economy", Princeton University Press, 1984.
[51] Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, Birleşmiş Milletler Sözleşmeleri, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/bm_yeni.html, ET.29.01.2020.

oluşmaktadır. Aynı zamanda " Talinn El Kitabı" NATO destekçi ülkelerinin görüşlerini ya da resmi bir NATO görüşünü temsil etmemektedir.[52] Fakat Clausewitz açısından baktığımızda bu el kitabının hazırlanması çok önemlidir. Çünkü bir müttefiki savaş alanına getiren manevra, muharebeyi kazanmak kadar önemlidir. Çünkü günümüz toplumlarında "Yıpratma" stratejisi klasik bir savaştan daha önemli bir güce sahiptir. Stratejik olarak yaklaştığımızda siber saldırılar ile ulaşılmak istenen asıl hedef rakip halkın ve toplumun moralini yok etmektir. Günümüzde de Clausewiz'in savaş bir bütündür bakışı doğrultusunda Estonya'da Talinn Merkezli bir NATO Siber Güvenlik Merkezi kurulması NATO'nun siber uzay olarak tanımladığımız savaş alanına konumlanmasının en güzel örneğini oluşturmaktadır.

Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi, Avrupa Konseyi bünyesinde siber suçlarla ilgili hazırlanan ilk resmi belge olma özelliği taşıyan bu belge, 23.11.2001 tarihinde Macaristan'da imzalanarak 01.07.2004 tarihinde yürürlüğe girmiştir. Türkiye'de ise Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi 10.11.2010 tarihinde imzalanmasına rağmen, 02.05.2014 tarihli ve 28988 sayılı resmi gazetede yayınlanan "6533 sayılı uygun bulma kanunu" ile yürürlüğe girmiştir.[53]

1.4.Siber Uzay'ın Tehdit Unsuru Olması ve Kopenhag Okulu

Buzan ve Waever'in başını çektiği Kopenhag Okuluna göre güvenlik kavramı, iletişim ve etkileşimler sonucu ortaya çıkar ve karşılıklı öznellik üzerinden açıklanabilir. Kopenhag Okulu temsilcilerine göre tehdidin gerçekte var olması gerekmemektedir. Yani bir durumun gerçekten tehdit olup olmadığı tecrübe edilmeden anlaşılamaz. Bu yüzden konun aktörlerin tehdit olarak adlandırmalarıyla tehdide dönüştüğü anlaşılmaktadır. [54]

Kopenhag Okuluna özgü bakış açısıyla; karşılaşılan tehdit yaşamsal (beka) ile ilgilidir. Bu yüzden önlem almakta gecikilirse çok önemli sonuçları olabilir. Bu yüzden güvenlik kavramı hem fayda hem de zararı içinde barındırır. Kopenhag

[52]Milli Güvenlik Kurulu Genel Sekreterliği, Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku), https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku ET.29.01.2020.

[53]Bakanlar Kurulu, Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun BulunduğunaDairKanun,ResmiGazete,22.04.2014,http://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm ET.29.01.2020.

[54]Başar Baysal ve Lüleci, Çağla. "Kopenhag Okulu ve Güvenlikleştirme Teorisi", Güvenlik Stratejileri Sayı: 22, Yıl: 2011, ss. 61-90.

Okulu'nun güvenlik kavramını sektörlere ayırması da aslında siber güvenlik kavramının konuşulmasına büyük fayda sağlamaktadır. Ana aktör olan devletler dışında Avrupa Birliği ve NATO gibi uluslar üstü örgütlerde güvenlik kavramını bir alt dala ayırarak siber güvenlik konusuna eğilmelmektedir. Özellikle Soğuk Savaş'ın sona ermesiyle birlikte küresel faktörlerin dünya siyasetindeki etkileri azalmış ve bölgesel güçlerin ağırlığı artmıştır. Bu sebeple uluslararası politika giderek daha fazla bölgesel, ulusal ve yerel dinamikler tarafından şekillenen bir hal almıştır.[55] Bu doğrultuda günümüz güvenlik sorunlarının kaynağının belirlenmesinde Kopenhag Okulu'nun güvenlik anlayışının önde gelen teorisyenlerinden olan Barry Buzan "İnsanlar, Devletler ve Korku" isimli kitabında güvenliği askeri, siyasi, ekonomik, sosyal (toplumsal) ve çevresel olmak üzere beş ayrı sektörde incelemiştir. [56] İnsan, Devlet ve Savaş'ı bir resmin üç önemli parçası olarak gören Buzan'a göre güvenliğin önemli bir parçası olan bu beş sektörde temel birimi devlet oluşturmakta ve sektörler devletlerin çıkarlarına göre şekil almaktadır.[57] Bu bağlamda Barry Buzan'ın 4 temel argümanı aşağıdaki gibidir:

1. Uluslararası ilişkilerin temel oyuncusu egemen devletlerdir

2. Uluslararası ilişkilerde, en az iki devletin birbirlerinin kararlarına etki edebildiği bir devletler sistemi vardır.

3. Uluslararası yapı anarşiktir.

4. Uluslararası sistemde devletler, ortak çıkarları ve değerleri çerçevesinde kendilerini sınırlandırdıkları ortak kurallar ve birlikte oluşturularak yürütülen kurumlar sayesinde "uluslararası toplum" içinde var olurlar.

Bu dört argüman çerçevesinde siber uzayı yeni bir alan olarak konumlandırmak ve bu alanda gerçekleştirilen mücadeleleri yeni bir savaş şekli olarak göstererek bir çözüm modeli sunmak bu tezin ana iddialarındandır. Çünkü günümüzde yaşanan küreselleşme ve teknolojik gelişmeler sonucunda anarşik bir yapının hâkim olduğu yapı içerisinde uluslararası toplumu oluşturan siber kurumların ortaya çıkışı ile uluslararası toplum daha kolay anlaşılabilecektir. Bu doğrultuda

[55]Peter J. Katzenstein, "Regionalism In Comparative Perspective. Cooperation And Conflict " Cilt.31, No.2, Haziran 1996, ss.123-59.

[56] Barry Buzan, "People, States And Fear: An Agenda For International Security Studies In The Post-Cold War Era", Harvester Wheatshef, 2nd Edition, London, 1991, ss.19-21.

[57] Ken Booth, Theory Of World Security, Cambridge University Press, United Kingdom, 2007, ss.162.

uluslararası toplum oluşturulurken *Bölgesel Güvenlik Kompleksi Teorisi* kapsamında oluşan uluslararası sistemin yeni çatışma ya da ittifaklarını sadece askeri güvenlik şeklinde ya da küresel kültürel, dinsel ve medeniyetsel ayrılıklar ekseninde değil, bölgelerin oluşturduğu alt-sistemler üzerinden yeni araçlarla birlikte açıklamamız gerekmektedir. Ayrıca uluslararası sistemin kuralsız, düzensiz ve anarşik yapısı sebebiyle sistemin teminatını sağlayacak tek çare olarak gösterdikleri güvenlik komplekslerinin oluşması için en önemli kriterler şu şekilde belirtilmektedir.[58]

- ✓ Devletlerarasında ortak bir tehdit algısının olması
- ✓ Ortak tehdit algısı ile karşılıklı olarak bağımlılığı olan devletlerarasında bir işbirliği sağlanması
- ✓ Güvenlik komplekslerini oluşturan dinamiklerin zaman içerisinde değişmesi
- ✓ Güvenlik kompleksi içerisinde yer alan devletlerin ihtiyaçlarının birbirlerine paralel olması
- ✓ Ülkelerin paylaştıkları güvenlik ihtiyaçlarının çeşitlilik göstermesi sebebiyle bir devletin aynı anda birden fazla kompleks içerisinde yer alması
- ✓ Güvenlik komplekslerinin barışın oluşması ve korunmasındaki rolü
- ✓ Soğuk Savaş sonrası dönemin güvenlik problemlerinin açıklanmasındaki faydası
- ✓ Devletlerin güçlerine göre düzeyinin değişmesi
- ✓ Küreselleşme ile birlikte artan farklı tehdit kaynaklarının devletleri işbirliğine yöneltmesidir.

Aslında tüm bu güvenlik kompleksleri Soğuk Savaş'ın bitmesiyle birlikte yaşanan teknolojik gelişmeler çerçevesinde oluşmuştur. Uluslararası sistemin güvenlik dinamiklerinin değişmesi çok yönlü anarşik yapıyı ve güvenlik ikileminin beslendiği daha dinamik bir güvenlik kavramını ortaya çıkarmıştır. Böylece devletler birbirlerine daha bağımlı, iç içe geçmiş ilişkilere sahip olmuştur. Bu bağlamda siber dünyayı domine eden ve ulusal siber güvenlik stratejisi bulunan aktörler daha önemli bir konuma gelerek güvenlik bakışını askeri, ekonomik, toplumsal, çevresel ve siyasi

[58] Buzan ve Hansen, a.g.e. ss. 212-225.

olarak her alanı kapsayan bir yapıya dönüştürmüştür. Bu bakışı Barry Buzan'ın güvenlik kavramı da şu şekilde desteklemektedir.[59]

- ✓ Askeri güvenlik, devletlerin silahlı saldırı ve savunma yeteneklerinin iki seviyeli etkileşimi ve devletlerin birbirlerinin niyetleri hakkındaki algıları ile ilgilidir.
- ✓ Siyasi güvenlik devletlerin örgütsel istikrarı, hükümet sistemleri ve onlara meşruiyet veren ideolojiler ile ilgilidir.
- ✓ Ekonomik güvenlik, kabul edilebilir refah ve devlet gücü seviyelerini sürdürmek için gerekli kaynaklara, finansmana ve pazarlara erişimi ilgilendirir.
- ✓ Toplumsal güvenlik, toplumsal kimlik ve kültür modellerini etkileyen tehditler ve güvenlik açıkları ile ilgilidir.
- ✓ Çevre güvenliği, diğer tüm insan girişimlerinin dayandığı temel destek sistemi olarak yerel ve gezegensel biyosferin bakımı ile ilgilidir.

Barry Buzan'a göre bu beş sektör birbirinden ayrı olarak işlemez ve hepsi güçlü bir bağlantı ağı içinde bir araya getirilir. Çünkü askeri tehditler ve silahlı çatışmaların büyük güçler arasında azalan belirginliği, güvenlik boşluğunu kuvvetlendirmekte bu durumda siyasi, ekonomik, toplumsal ve çevresel konuların uluslararası güvenlik gündeminin en üst sıralarına çıkmasına yol açmaktadır.

Buzan'ın bu teoride asıl amacı karar verme pratiğinden önce bilgiye ulaşmaktır. Bu sebeple "X nesnesi" araştırmasında 5 kategoriye bölünmüş şekilde sorulması geren sorular vardır. Bunlar; [60]

- ➢ Tarih: Kökenleri nedir? Nasıl gelişti?
- ➢ Yapı: ne şekildedir? Nasıl yapılmıştır?
- ➢ İşlev: nasıl çalışır? Dinamikleri nelerdir?
- ➢ Rol: Tabiatta ya da insan dünyasında ne işe yarar?
- ➢ Sınıflandırma: diğer şeylerle ilgisi nedir?

[59] Barry Buzan, "New Patterns of Global Security in the Twenty-First Century", Royal Institute of International Affairs, Cilt. 67, No. 3, Temmuz, 1991, ss. 431-451.
[60] Tony Buzan ve Barry Buzan, "Zihin Haritaları", Çevr. Tercanlı, G. Alfa Yayınları, İstanbul, 2019 ss. 103-104.

Bu beş soru çerçevesinde teze verdiğimiz şekil siber uzay'ın sahip olduğu güvenliğin karakteristik özelliklerini mantıksal bir çerçeveye oturtmamıza fayda sağlamıştır. Çünkü güvensizliği yaratan korku için üç argüman vardır. Bunlar korkunun kurumsallaşması, kurumsallaşan korkunun algıları tetiklemesi ve son olarak korkunun kendini yenileyerek sürdüren bir hal almasıdır. Bu argümanlar korkuyu dış politikanın kesin bir aracı haline getirmiştir. [61] Siber uzayda kullanılan siber silahlarda dış politikada kullanılan kesin bir korku aracı haline dönüşmüştür. Ayrıca şuan geleneksel bir savaş yaşanmıyor olması mutlak bir barış olduğu anlamına kesinlikle gelmemektedir**.** Örneğin; Soğuk Savaş'ın barış ortamında yaşanması Soğuk Savaş'ın gerçekleşmediğini göstermez. Gösterdiği tek şey konvansiyonel veya nükleer bir savaşın gerçekleşmemiş olmasıdır. Aynı şekilde günümüzde yaşanan çatışmaları, korkuları ve tehdit hallerini de göz önüne alarak savaş yaşandığını iddia etmemiz gayet doğaldır.

1.5. İnşacılık Yaklaşımı ve Siber Caydırıcılık

Geleneksel uluslararası güvenlik çalışmalarının merkezinde yer alan sosyal inşacı bakışla caydırıcılık teorisi misilleme güç tehdidine dayanmaktadır. Aynı zamanda caydırıcılık, bir hasmı kabul edilmez derecedeki tehditlerle yapmak istediği bir şeyi yapmaktan vazgeçirmektir. Akılcı caydırıcılık teorisinin analitik gücüyse devletlerin kendi yararlarını maksimize etmeye çalışmasıdır. Yani caydırıcılık kuramı güçlü bir materyal paha-fayda mantığı ve güçlü bir akılcılığı vurgular.[62] Bu bağlamda nükleer silahların ve kimyasal silahların kullanılmaması direk caydırıcılıkla alakalıdır. Bu kitle imha silahlarının kullanılmaması yasakçı normaların oluşturulmasıyla birlikte değerlendirilmelidir. Çünkü caydırıcılık mantığının özü misliyle mukabele korkusundan dolayı nükleer ve kimyasal silahların kullanılmamasına dayanır. Fakat nükleer ve kimyasal silahların kullanılmamasına dayanan normlar, akılcı açıklamalar ve caydırıcı araçlarla tek başına yeterli değildir.

Nükleer devrim sonucunda nükleer silahların gelişmesi, şiddete bağımlı olan toplumsal yapıdaki ilişkileri yeniden değerlendirmeyi zorunlu kıldı. Günümüzde nükleer silahların devamlılığı ve artan rolü ile birlikte aktörlerin şiddete meyilli

[61] Ken Booth, "Realizm and World Politics", Routledge Journal, 2011, ss.185.
[62] J. Peter. Katzenstein, "Milli Güvenlik Kültürü: Dünya Siyasetinde Normlar ve Kimlik", Çeviren Efe, İ. Sakarya Üniversitesi Kültür Yayınları, Sakarya, 2014, ss 137-149.

halleri karşılıklı bağımlılıkla birleşince ulusal, bölgesel ya da küresel güvenlik sonuçlarını doğurmaktadır.

Dünya düzenindeki aktörlerin güvenlik ve tehdit bakışı çerçevesinde nükleer silahları kullanmama normu sadece nükleer silahlara sahip ve bu oranda caydırıcılığı kullanan ülkelere aittir. Nükleer silahlara sahip bu devletler dünyanın çoğunluğu tarafından nükleer silah edinilmesinin ve kullanılmasının gayri meşru olduğunu diğerlerine kabul ettirmiştir. Bu durumu nükleer güce sahip olan devletlerin nükleer güce sahip olmayan aktörlere karşı Nükleer Zenginleştirme Anlaşmasında ortaya koydukları taahhütlerde açıkça görmekteyiz. Siber uzay vasıtasıyla gerçekleştirilen saldırılar bu taahhütleri yerine getirmeme, karşı tarafın gücünü etkileme gibi konularda ülkelere avantaj sağlamıştır. Bunun en güzel örneği stuxnet olayıyla yasaklamalara karşı uranyum zenginleştirme çabasında olan İran'da görülmüştür.

Caydırıcılıkla alakalı bir diğer konu da ittifak sistemidir. Hem birey düzeyinde hem de devletler düzeyinde uluslararası sistemde yaşanan tüm mücadeleler üç katmanda gerçekleşmektedir. Bunlar; resmi kurumlar (NATO vb.), egemenlik kuralları ve uluslararası hukuk unsurları ve son olarak, uluslararası dostluk ve düşmanlık kalıplarıdır. Harici bir tehdit sonucunda ortaya çıkan ittifakların kurulması öncelikle bu üç katmandaki potansiyel bir saldırganı caydırmaya dayanmaktadır. Devletler ittifak oluşturmada stratejik olarak iki hesap yapar. Bunlar; tehdidin belirlenmesi ve tehdide cevaben ittifak yapıl(ıp)mayacağı, yapılacaksa kiminle yapılacağının belirlenmesine dayanır. Çünkü tehdit dengesi yaklaşımı, yakın tehditler, nispi askeri güçten doğan akılcı bir maliyet ve fayda hesaplamasına dayanır. [63] Yukarıda kurumsalcı bakışta da açıkladığım gibi NATO içerisinde siber güvenlik alanında birlik oluşturma yönünde çabalar, demeçler, hukuki düzenlemeler ve kurulan kuruluşlar aynı zamanda caydırıcılık oluşturma yönünde bir çabanın göstergesidir.

Aynı zamanda anarşik yapının yapılmak zorunda bıraktırdığı ittifak sisteminde, kimlikte belirleyici bir rol üstlenmektedir. Çünkü niyetler ve ideolojik bakışlar tehdidin inşasında önemli bir bileşendir. Kenneth Waltz gibi neorealistlerin anarşik yapılar "benzer birimler" üretme eğiliminde olduğuna yönelik vurguları devletlerin kimliklerini ve milli güvenlik politikalarını etkiler. Devlet ve çevresi

[63] Stephen M. Walt, "Alliance Formation and The Balance Of World Power", The Mit Press, International Security, Cilt. 9, No. 4 İlkbahar, 1985, ss. 3-43.

arasındaki çatışma ve kültürel işbirlikleri çift taraflıdır. Çift taraflı çatışma ve işbirliği ilişkilerini şekillendiren bir diğer husus ise geleneksel caydırıcılık teorisinin dayandığı silahların ve teknolojilerin aktörlerin şahsi menfaatleri doğrultusunda kullanmamalarına dayanan sistemin doğasını sosyal inşacı bakışla bakarak kimyasal ve nükleer ampirik vakaların açıklanmasıdır. Bu kavramın siber uzay hakkında kullanılmasındaki açıklayıcı güç nihai belirsizliktir. Kenneth Waltz'in anarşik yapıların "benzer birimler" üretme eğiliminde olduğuna yönelik tespitlerini destekler nitelikte Peter Katzenstein konuya şu şekilde yaklaşmıştır.

Peter Katzenstein; büyük kısıtlamaların olduğu bir dünyada ulusal seçimlerin olasılığını korumanın küçük devletlerin ana stratejisi olduğunu belirtmiştir. Aynı zamanda hayatta kalmanın önemli olduğu bu uluslararası anarşik sistem içerisinde "meydan okuma" nın sıradan bir hal almış olması sebebiyle her büyük devlet 'in küçük bir devletten daha farklı ve fazla güvenlik açığıyla baş başa kalacaktır.[64] Buradaki asıl vurgu iki şekildedir. Birincisi, devletlerin içinde bulunduğu güvenlik ortamlarının sadece maddi değil, önemli ölçüde kültürel ve kurumsal olduğunu belirtmesidir. İkincisi, kültürel ortamların hem devlet davranışlarını hem de "kimlik" denilen devletlerin temel karakterini etkilediğini iddia etmesidir.[65]

Bu bağlamda; nasıl geçmişte yaşanan konvansiyonel tüm saldırılar yalnızca devletlerin topraklarını ve sınırlarını değil, yaşam tarzlarını, temel varsayımlarını ve ahlaki var olma haklarını etkilemişse günümüzde de siber saldırılar sadece askeri alanda değil tüm alanlarda psikolojik kargaşa yaratarak düzene karşı meydan okumaktadır. Bu meydan okumalar ve anarşik yapılar "benzer birimler" ve "kimlik" koruma mücadeleleri üretme eğilimindedir. Bu durumu daha da açarsak Peter J. Katzenstein dış kültürel ortamların devlet kimlikleri ve dolayısıyla ulusal güvenlik çıkarları ve politikaları üzerine yapabileceği en az üç etki öngörmektedir. Bunlardan birincisi devletlerin hayatta kalma mücadelesidir. İkincisi, ortamların sistemdeki durumunun zaman içinde değiştirmesidir. Son olarak, kültürel ortamların, belirli bir uluslararası sistem içindeki devletlerin karakterinde farklılığa neden olmasıdır. Bu değişikliklerin hepsi küreselleşme sonucunda internetin hayatın her alanına

[64] Peter Katzenstein, "Small States and Small States Revisited", Carfax Publishing, New Political Economy, Cilt. 8, No. 1, 2003, ss.9-30.
[65] Peter. J. Katzenstein, "The Culture of National Security: Norms, Identity, and Culture in World Politics", Columbia University Press, , New York, 1996, ss.1-27.

girmesiyle birlikte hızlı bir şekilde gerçekleşmiştir. Siber uzayla birlikte algı yönetimi, teknoloji transferi, kimlik yaratma ve dünya vatandaşlığı gibi kavramlarla ortak bir kültür yaratma gibi stratejiler kullanılmaya başlamıştır.

Peter J. Katzenstein'ın bu süreç içinde altını çizdiği nokta 1970'lerin sonuna gelindiğinde karşılıklı bağımlılık teorisi ile herkes ekonomiye odaklanırken sosyal etkilerin (kimlik ve kültür) gibi kavramların atlanmasıdır. Çevresel, kültürel veya kurumsal unsurlar normları, normlar ise ulusal güvenlik çıkarlarını, devletlerin kimliğini ve güvenlik politikalarını şekillendirir. Aynı şekilde devlet kimliğindeki değişiklikler, ulusal güvenlik çıkarlarını, rejimleri, güvenlik topluluklarının normatif yapılarını veya devlet politikalarını etkiler. Böylece etkilenen devlet politikaları kültürel ve kurumsal yapıyı yeniden üretir ve yeniden yapılandırır.[66]

"Sert" gücün öneminin azaldığını, "yumuşak" gücün öneminin arttığı ve gücün dönüşümü için kurumların ve kültürün öneminin arttığı Soğuk Savaş sonrasındaki süreç için; yeni-gerçekçilik, büyük ölçüde uluslararası devlet sistemindeki maddi güç dengesine odaklanmaya, neoliberalizm ise uluslararası kurumların devletlerarasındaki çatışmalar üzerindeki potansiyel olarak ılımlı etkilerine odaklanmaya başlamıştır.

Bunu ortaya koyarken inşacı (constructivist) olarak tanımlanabilecek kuramsal bir bakış açısına sahip Katzenstein'ın, anlaşmazlıkların tamamen çözümlenmesinin mümkün olmadığı, uzlaşılabilecek ve orta yolun sağlanabileceği konuların olabileceği yönündeki bakışı tezimizi desteklemektedir. Çünkü Peter Katzenstein, analitik uzlaştırmacılık (analytic eclecticism) yaklaşımı ile farklı bakış açılarının kuram ve epistemoloji gibi konularda anlaşmadan da birbirlerini tamamlayabileceğini, dünya siyasetini anlamlandırabilmek için faydacı bir yaklaşım kullanmanın gerekli olduğunu iddia etmektedir. Siber uzay alanı da içerisinde tehditleri barındırdığı kadar fırsatları da içermesinden dolayı faydacı bir yaklaşımla bakılması zorunludur.

Ayrıca Peter J. Katzenstein'a göre; ontolojik, epistemolojik ve metodolojik anlaşmazlıklar farklı dünya görüşlerinden doğdukları için bunları çözümlemeye

[66]Peter J. Katzenstein, "Conclusion: National Security in a Changing World, The Culture of National Security", Columbia University Press, New York, 1996. ss. 498-537.

çalışmak vakit kaybıdır. [67] Aynı şekilde siber uzayın da tamamen çözülmesi imkânsızdır. Çünkü,

- ✓ Siber savaşın ne zaman başladığını ve bittiğini bilmek, onu tanımlamaktan daha zordur.
- ✓ Siber savaşın çizgileri, izledikleri teknik ve yöntemleri bulanıktır.
- ✓ Nispeten Soğuk Savaş dinamiklerine benzer nitelikte psikolojik yapı, karşılıklı gerilim, her an saldırı yaşama korkusunu içeren ama teknolojinin gelişmesiyle birlikte bunu konvansiyonel ve nükleer savaş araçları vasıtasıyla değil de siber silahlar yöntemiyle uygulayan bir çatışma türüdür.
- ✓ 7/24 saldırı ve savunmanın hâkim olduğu, çok cepheli bir savaştır.

Tüm bu anlatılanlar ışığında ister neorealist ister se neoliberal teoriler şuan geleneksel bir savaş yaşanmıyor olmasını mutlak bir barış dönemi olarak gösteremez. Nasıl Soğuk Savaş barış içinde sonuçlandıysa, günümüzde yaşanan siber çatışmalarda bir barış dönemi şeklinde gelişmektedir. Eğer ülkeler savaşın kaçınılmaz olduğunu düşünürse, siber yöntemlerle geliştirilmiş geleneksel veya nükleer bir savaş dünyaya çok ciddi zararlar verebilir. Bu durumsa herkes için bir felaket olabilir. Soğuk Savaş döneminde Sovyetler Birliği tarafından saldırıya uğrama korkusuna sahip ülkeler günümüz siber dünyasında da bu hissi farklı boyutlarda yaşamaktadır. Rusya'nın izlemiş olduğu siber stratejilerin NATO üyesi ülkeleri korkutması bunun en güzel örneğidir.

Bir diğer yandan yukarıda bahsedilen özellikler hangi etkiye odaklanılırsa odaklanılsın güvenlik çalışmalarının sadece devletler ve askeri meselelerle sınırlandırılmaması gerektiğini göstermektedir. Siber uzayla birlikte artık her alan tehlikelidir. İnternetin ve bilgisayarın hayatımıza girmesiyle dünya siyasetindeki güvenlik ve tehdit gündemi genişlemiş ve güvenlik dışı çalışma alanları (ekonomik meseleler, teknolojik dönüşüm, gıda güvenliği, kritik tesisler, enerji tesisler, nükleer tesisler, barajlar, kitlesel göç korkusu vb.) ve devlet dışı aktörler bu yeni güvenlik alanında önemli bir unsur haline gelmiştir.

[67]Peter J. Katzenstein ve Rudra Sil, "Analytic Eclecticism in the Study of World Politics: Reconfiguring Problems and Mechanisms across Research Traditions Perspectives on Politics", Cambridge University Press, Ağustos 2010, ss 411-431.

Artık büyük devletler, küçük devletlere karşı bile her türlü silahlı saldırıdan ziyade ekonomik, siyasi, diplomatik ve siber yöntemleri kullanmaya başlamıştır. Bunun en güzel örneği; Özellikle Soğuk Savaş sonrasında Rusya'nın aktif bir güç unsuru olarak kullandığı siber stratejileri asimetrik bir tehdit olarak kültürel, kuramsal ve kimlik üzerinden her alanda şu şekilde resmedebiliriz. 21. yüzyılda bu alanı en başarılı kullanan Rusya'nın son yıllarda NATO üyesi Estonya'ya veya eski Sovyet coğrafyasında Gürcistan ve Ukrayna gibi ülkelere yönelik gerçekleştirdiği saldırgan hamlelerde görebiliriz. Bu hamleler, yeni bir dünya savaşına giden süreçte yeni bir alan olan siber uzayı Rusya'nın aktif bir şekilde kullandığını göstermektedir.

Bunlara ek olarak siber uzayla birlikte devlet dışı aktörler önem kazanmış ve milli unsurlar daha da önemli hale gelmiştir. Peter J. Katzenstein, Soğuk Savaş'ın sona ermesiyle birlikte, siyasi ve entelektüel iklimin değişmesi ile ortaya çıkan uluslararası politika sorunlarının ulusal güvenliğe etkilerini kültürel-kurumsal bağlam ve siyasi kimlik üzerinden incelemiştir. [68] Peter J. Katzenstein bu yeni dönemin hâkim güç unsuru olarak gösterdiği protean güç kavramı; etkileri görünmez, belirsiz ve kontrol edilemezliği temsil eder. Başka bir deyişle, protean gücün oynadığı bir dünya için "bir şeyi şansa bırakan tehdit" altındadır.[69] Siber uzayda etkileri görünmez, belirsiz ve kontrol edilemez bir yapıyı güvenlik literatürüne kazandıran yeni dönemin hâkim gücüdür. Bu alan farklı analitik bakış açılarının farklı ulusal güvenlik tanımları önermesinden dolayı siber uzayda anlaşmazlıkların tamamen çözümü imkânsızdır. Çünkü teknoloji insanları ve dolayısıyla diğer aktörleri yönlendirip kontrol etmektedir. Bu yönlendirmelerse devlet kademesinde krizleri ve görevden almaları doğurmaktadır. Bu durum 7/24 savunma yapmamız gereken bir güvenlik riskini ortaya çıkarmaktadır. Örneğin; siber uzayda devletler ve örgütlere yönelik saldırı gerçekleşmese bile bireysel anlamda kimlikler yani önemli liderler baskı altına alınabilir. Bu sebeple, bireyler veya önemli liderler, teknolojik cihazlar, ekonomik eğilimler ve dünyayı şekillendiren siyasi dinamikler sebebiyle korunmasızdır.

[68] Peter J. Katzenstein, "Introduction: Alternative Perspectives On National Security, The Culture Of National Security", Columbia University Press, New York, 1996, ss.1-32.
[69] Peter J. Katzenstein, "Protean Power And Uncertainty: Exploring The Unexpected İn World Politics", International Studies Quarterly Cilt.62, No.1, Yıl.2018, ss.80–93.

Tüm bunların yanında bireysel düzeyde içinde bulunulan tehditlerin yanında devlet düzeyinde de ülkeler milli güvenliklerini ve milli sınırlarını korumakta zorluk çekmektedir. Ülkeler kritik alt yapı hizmetlerini“ network“ adı verilen bilgi ağları üzerinden kontrol etmekte ve bu da sanal saldırıların çıkış noktasını oluşturmaktadır. Siber uzayla birlikte artık ulusal sınırları korumak güvenlik ihtiyaçlarını karşılamamaktadır. Yani devletler sadece askeri ve geleneksel olarak ulusal sınırlarını korumakla güvende değildir. Telekominikasyon, bankacılık, finans, elektrik enerjisi, petrol ve doğalgaz dağıtımı, su temini, nakliye, acil hizmetler ve devlet hizmetleri gibi ortak kritik alt yapılar siber saldırılar sayesinde müdahale edilebilecek kritik ulusal güvenlik alt yapılarını oluşturmaktadır. Sistem düzeyindeyse uluslararası sistemin sahip olduğu anarşik yapının doğasında riskler vardır. Her risk aynı zamanda bir tehdittir. Bu sebeple risk ve tehdit kavramlarının varlığı güvenlik kavramının ortaya çıkmasının en önemli sebebidir. Aynı zamanda; tehditleri belirlemek, analiz etmek, etkisini azaltmak ve fırsatları değerlendirmek devletlerin dış politika stratejilerini belirleyerek rakiplerine karşı mücadele edebilmeleri için bir zorunluluktur.

Gelecekte meydana gelmesi muhtemel bir olay, bir devletin, topluluğun veya bireyin varlığına veya refahına yönelik olası olumsuz etkileri bulunan bir tehdit eylemidir. Bu bağlamda tehdit tanımlaması üç biçimde ortaya çıkmaktadır. Bunlar; eldekini yitirme riski, başkasının elindekini ele geçirememe riski ve küresel tehditlerdir. [70] Yani; tehdit hem gerçek olgu ve olaylara hem de algı ve tahminlere dayanmaktadır. Bir tehdidin gerçek tehlike olup olmaması sadece gerçekleştiği zaman ortaya çıkar ve buda önlem alınması için geç kalındığını gösterir. Aynı zamanda hiçbir zaman gerçekleşmeyecek bir durumda tehdit olarak kabul edilebilir. Burada önemli olan algı ile olgu arasındaki mesafedir. Eğer mesafe açılırsa risk artar. Risk arttıkça ise tehdit artar. Böylece de güvensizlik durumu oluşur. Realist bakış ise bu güvensizlik durumuna karşı devletin temel amacının vatandaşları iç ve dış tehditlere karşı korumak olduğunu ileri sürer. Bu doğrultuda siber uzay salt askeri olmadan iç ve dış risklere karşı ülkeleri korumasız bırakabilecek ve önlem alınması zorunlu bir yapı sunmaktadır.

[70] Elke Krahmann, “From State to Non-State Actors: The Emergence of Security Governance, New Threats and New Actors in International Security”, Palgrave Macmillan, New York, 2005, ss.3-19.

Realist teori açısından bakıldığında siber uzay alanına yönelik ordu birimlerinin kurulması da bu alanda savaş verildiğinin en temel göstergesidir. Asimetrik tehdit kavramıyla doğrudan bağlantılı olan siber savaşlar güç kavramını sadece askeri nitelikte olmaktan çıkarmıştır. Asimetrik tehdit, özünde beklenmedik bir zamanda ve mekânda aniden "karşı tarafın zayıf taraflarına yönelme" ile ilgili olduğundan dolayı bu tehdit konvansiyonel savaş tehditlerinden ayrılmaktadır. Soğuk Savaş sonrasında önemi artan bu tehdit türü ile devletlerin güvenlik sorunları, tehdit algılamaları ve savunma doktrinlerinin yeniden gözden geçirilmesi zorunlu bir hal almıştır. Örneğin; ne konvansiyonel bir savaş ne de tam anlamıyla bir terör faaliyeti olmayan 9/11 olayı asimetrik tehdit kavramını daha belirgin hale getirmiş ve saldırıların boyutunu, etkisini, yöntemini ve sonuçlarını daha önceki geleneksel yöntemlerden ayırmıştır.

Geleneksel olmayan yöntemlere karşı etkin bir korumanın gerçekleştirilmesinde küreselleşme güvenliğe bakış yaklaşımında tam anlamıyla bir değişim ve dönüşüm yaratmıştır. Küreselleşmeyle birlikte teknolojik, ekonomik, sosyal, kültürel, siyasal vb. tüm alanlar iç içe girmiş bu durum ise tehdit algılamasını Soğuk Savaş öncesi döneme göre daha da genişletmiştir. Özellikle Soğuk Savaş sonrası dönemde kapitalizmin, küreselleşmenin ve internetin ortaya çıkmasıyla birlikte oluşan teknolojik gelişmelerin hızlanmasıyla tehdit algılamaları da farklılaşmıştır. Günümüzde tüm bu gelişmeler sonucunda ortaya çıkan siber uzay ise geleneksel güvenlik yaklaşımının yanında tüm bu güvenlik stratejilerini kapsayan bir tehdit algısı ortaya çıkarmıştır.

Asimetrik tehditlerin vücut bulmuş hali olan "Siber Savaş" kavramı tarafların nicelik veya nitelik bakımından büyük ölçüde eşit olmadığı, cephesi olmayan, hangi vasıtalarla nasıl vuracağının önceden kestirilemediği, tarafların birbirinin nitelik veya niceliksel eksikliğinden dolayı savaş hukukuna uygun davranmadığı bir savaş türüdür. Bu savaş türünde eylemin kapsamını, şiddetini, nasıl algılandığını ve etkisini dikkatlice analiz edebilmek çok zordur. Çünkü stratejik rekabette vurgu fiziksel alandan bilişim alanına, verilerin toplanıp işlenmesine, ağlara sızılmasına ve psikolojik manipülasyona kaymaktadır. Böylece, "siber uzay" kavramı fiziksel alanı sömürgeleştirerek hayatın her alanının dijital ortama aktarılmasına ve insan

faaliyetlerinin "verileşip", "ölçülebilir ve analiz edilebilir" hale gelmesine yol açmıştır. Bu süreci ise Henry Kissinger şöyle açıklamaktadır;

Günümüzde uluslararası sorunlar küresel boyutta yaşanmakla birlikte pek çok konuda fikir birliğine varılamamakta, bu durum ise gerilimi arttırmaktadır. Siber güvenlik konusu da tam bu durumda karşımıza çıkmaktadır. Siber uzay 1980'lerde varsayımsal bir terim iken, günümüzde hayatın her alanında kullanılan bir terimdir. Artık hemen hemen her aygıt internete bağlanmaktadır. Bu yüzden internetin akışını durdurmayı ya da dijitalleşmeye karşı direnmeyi hiçbir yönetim, hatta en totaliter rejimler bile başaramamıştır. Kitle imha silahlarının artması, nükleer santrallerin yayılması ve çatışmaların insan anlayışının ötesine taşınması ise teknolojik gelişmelerle birlikte tehdidi küresel düzeyde siber uzaya taşımıştır. Kissinger'a göre; siber uzay tüm tarihsel deneyimlere meydan okumaktadır. Çünkü siber uzay kaynaklı tehditler henüz belirsiz ve tam anlamıyla tanımlanmamıştır. Ayrıca kaynağının bulunması da zordur. Her yerde mevcut ancak kendi başına tehdit edici değil; tehlikesi ise kullanımına bağlıdır. [71]

Bu doğrultuda küresel olarak internete bağlanan cihaz sayısının artması ve bu cihazların insanların hayatına dâhil olmasıyla güvenlik ihlallerine maruz kalma riski de aynı oranda artmaktadır. Günümüzde bütün ülkeler siber saldırılara karşı hassas durumdadır. Elektrik sisteminden banka ve finans sistemlerine, televizyonlardan bilgisayara, Nükleer tesislerden Enerji trafo sistemlerine kadar her şey elektronik bir ağ içinde ve bir şekilde siber saldırı yöntemi ile bilgileri çalınabilir, sistemleri çalışamaz hale gelebilir hatta tamamen imha edilerek ciddi yıkımlara yol açabilir durumdadır. Örneğin; siber saldırılar kullanılarak devletlerin sahip olduğu kritik alt yapılar zarara uğratılabilir. Petrol dökebilir, gaz uçurabilir, nükleer tesisleri etkilenebilir, jeneratörü patlatabilir, trenleri raydan çıkarabilir, uyduları yörüngeden çıkarabilir, hava yollarını yere düşürebilir.

Siber saldırı stratejilerinin, devletler üstünde politik ve ekonomik baskı enstrümanı olarak kullanılması, askeri güce eşlik edecek şekilde devletlerin güvenliklerini etkilemek için bir silah olarak kullanılmaktadır. Robert Gilpin, dünya politikalarındaki savaş ve değişim üzerine yaptığı analizlerinde, revizyonist ve statüko güçleri arasındaki kimlik ve düzen ayrımını prestij ve itibar kavramlarıyla

[71] Henry Kissinger, "Dünya Düzeni", Çev.Gül, S.S. Boyner Yayınları, İstanbul, 2016, ss. 372-379.

birlikte uluslararası sistem içinde analiz etmektedir. Gilpin için uluslararası düzendeki prestij ve itibar, iç politikada otorite kavramına işlevsel ve ahlaki olarak eşdeğerdir. Güçten ziyade prestijin uluslararası ilişkilerdeki önemini vurgulayan Gilpin, özünde prestijin askeri veya ekonomik güce dayandığını iddia etmektedir. [72] Siber uzayda kullanılan siber saldırılar ve siber casusluklar sayesinde elde edilen verilerin kullanılması da ciddi derecede prestij ve itibar kaybına yol açabilmektedir. Yani bir devletin en mahrem bilgilerinin güvenliği delinerek ülkeler bundan zarara uğratılmaktadır. Siber uzayın rakiplerin güvenlik sistemlerini zaafiyete uğratarak karşı tarafın prestij ve itibar kaybına yol açabilecek güç unsurları mevcuttur. Bu güç unsurları çerçevesinde Brandon Valeriano, Benjamin Jensen ve Ryan C. Maness tarafından yazılan Siber Strateji İktidar ve Zorlamanın Gelişen Karakteri adlı kitapta; tezimizde belirttiğimiz bu hususları doğrular nitelikte Rusya, Çin ve Amerika'nın dış politikasında uyguladıkları çatışma/işbirliği dinamiklerinde siber uzayın rolü belirtilerek bu ülkelerin uluslararası sistemdeki ana siber güçler oldukları nitelendirilmiş ve siber çatışma, siber güvenlik, siber zorlama, siber stratejiler, bilgi savaşı konularında belirttiği hususlar tezimizin belirleyici kriterlerini oluşturmuştur. Sonuç olarak tüm bu gelişmeler, örnekler, tanımlamalar ve açıklamalar çerçevesinde "siber" ile ilgili şu hususlar asla unutulmamalıdır.[73]

- ✓ Siber baskının, geleneksel devletçilik ve iktidar araçlarının yerini almak yerine tamamlayıcı olduğu,
- ✓ Siber stratejilerin belirleyici savaş araçlarından ziyade siyasi savaş ve gizli eylem olarak işlev gördüğü,
- ✓ Siber çatışmanın uluslararası meselelerde zorlayıcı etkiler elde etmede kullanışlı ve yeni bir yolu olduğu,
- ✓ Siber silahların son yılların en önemli askeri yeniliği olduğu,
- ✓ Özellikle 2000 ve 2014 yılları arasında yaşanan gelişmeler ışığında uluslararası sistemde ana aktör olan devletler tarafından gerçekleştirilen zorlama yaklaşımının bir parçası olarak siber teknolojilerin hayatın her alanını bütünleştirdiği,

[72] William C. Wohlforth, "Gilpinian Realism and International Relations International Relations", Sage, USA, Cilt.25, No.4, Yıl.2011, ss.500-510.
[73]Brandon Valeriano ve Benjamin Jensen, "Cyber Strategy: The Evolving Character of Power and Coercion", Oxford University Press, 2018.

- ✓ Çağdaş bir gizli eylem ve politik savaş biçimi olduğu,
- ✓ Siber baskının, dijital sınırlarda stratejik amaç elde etmek için kullanıldığı,
- ✓ Siber operasyonlar rakip devletler arasında ağ saldırılarını askeri tehditler gibi diğer geleneksel devletçilik formlarıyla birleştiren daha büyük bir entegre zorlayıcı stratejinin bir parçası olduğu,
- ✓ Siber Stratejilerin birçok yöntemlerinin olduğu,
- ✓ Siber stratejilerin rakipleri zorlama, caydırma ve tehdit etme amacıyla kombine bir strateji olarak kabul edildiği,
- ✓ Rakip ülkelerin siber stratejileri özellikle bozma, casusluk ve bozulmama gibi amaçlarla kullandığı,
- ✓ Aktörler tarafından kullanılan siber savaşların gerçekleri doğrultusunda, uluslararası sistemde siber çatışmaların ve tehditlerin günümüzde yaşandığını

Son olarak, 21. yüzyıl uluslararası ilişkilerindeki güvenlik algısında yaşanan değişmeler sonucunda ulusal güvenliğe yönelik yeni tehditler ve güvenlik politikalarını şekillendiren siber öğeler siyasi, askeri ve ekonomik alanla etkileşim içindedir. Bu sebeple, siber stratejiler belirlenirken Uluslararası İlişkiler Teorileri tarafından sıklıkla kullanılan güvenlik kavramı, tarihsel süreç içerisinde farklı dönemlerde farklı koşullarda ortaya çıkan farklı araç tehdit ve risklerine göre şekillenmiştir. Özellikle, tarihi en başından günümüze kadar incelediğimizde güvenlik algısında yaşanan değişimlerin sebeplerinin teknolojik gelişmelerle bağlantılı olduğu açıkça görülmektedir. Bu yüzden her dönemin güvenlik algılamaları yine o döneme göre değerlendirilmelidir. Bunun yanında içinde yaşanan her dönemde bile her aktör için tehdit farklı anlamdadır. Aynı zamanda; aktörler aynı tür tehdidi bile algılasa iki farklı şekilde davranabilirler. Bu davranışlar tehdide karşı güç birliği yaparak karşı koyma da olabilir, karşılıklı bağımlılık anlamına gelen bir iş birliği ile sistemin bütünlüğünün güvenliğini sağlamaya yönelikte olabilir. Böylece; tehdit hayatın her alanında var olmakta ve güvenlikten bahsettiğimizde "bireylerin güvenliği, toplumun güvenliği, devletin güvenliği, coğrafi ya da işlevsel alt sistemlerin, bölgelerin güvenliği veya uluslararası sistemin bütünü ya da bütüne yakınının güvenliği" gibi her konuda aslında bir tehdidin varlığından

bahsetmekteyiz.[74] Bu çeşitlilik içinde tehdit algılamalarındaki ve davranışlarındaki güvenlik yaklaşımlarına hem teorik hem de stratejik olarak yaklaşmak zorunluluktur.

Aynı zamanda güvenlik kavramı küreselleşme kavramıyla da doğrudan bağlantılıdır. Ekonomik, sosyolojik, kültürel, toplumsal, siyasal ve daha da önemlisi teknolojik gelişmelerin doğal bir sonucu olan küreselleşme ile birlikte devletler güncel tehditler karşısında, bireyler, toplumlar ve ulus ötesi aktörler ile siber güenliklerini sağlamak için iş birliği yürütmek zorundadır. Çünkü, küreselleşme toplumların her yönüyle yaşam alanlarına nüfuz ederek teknolojik, siyasi, ekonomik veya askeri olarak güçlü ülkelerin amaçlarına uygun bir şekilde dünyayı yönlendirmelerine imkânı sağlamış ve dünya nüfusunun neredeyse üçte ikisinin milli güvenliklerini olumsuz yönde etkilemiştir.[75]

Dijital dönüşüm araçlarının birer silah haline gelmesiyle birlikte güçsüz olan aktörler kendilerinden görece güçlü olan ve kendilerine karşı tehdit oluşturan unsurlara karşı bir fırsat kazanarak ulusal ve uluslararası alanların iç içe geçmesine yol açmıştır.[76] Bunun yanında ulusal hükümetlerin gücünün azalması, dünya çapında serbest piyasa sisteminin yayılması, sosyal ve kültürel benzerliklerin yayılması, teknolojik yeniliklerin düzenlenmesi, küresel olarak işsizlik, eşitsizlik ve yoksulluğun artması, suç, uyuşturucu, terör, şiddet, iç savaş, hastalık ve çevresel yıkımların artması gibi birçok olgu küreselleşmenin bir sonucudur. [77] Uluslararası rekabet mücadelesinde sermaye ve teknoloji transferinin kolay, hızlı ve ucuz olması ise küreselleşmenin ulusal güvenlik üzerindeki risk/fırsat paradoksunu ortaya çıkarmaktadır. Bunun yanında nesnelerin interneti ile birlikte bilgisayar ve internetin kullanılırlığı artmakta bu da bilgiyi tüm teorilerin önemseyeceği en önemli tehdit ve fırsat unsuru haline dönüşştürmektedir. Bu sebeple; bilgisayar ve internet kullanımının yoğunlaştığı günümüz koşullarında milli güvenlik sorunlarını, siber uzayın küresel tehdit ve fırsatlarını dikkate almadan sadece geleneksel yöntemlerle halledebilmek mümkün gözükmemektedir. Yani; küresel meselelerin bütününü

[74] Barry Buzan, "People, States And Fear", Wheatsheaf Book, 1983.
[75] Zygmunt Bauman, "Küreselleşme Toplumsal Sonuçları", Çeviren. Yılmaz, A. Arıntı Yayınları, İstanbul, 2010, ss.83.
[76] Nasıh Sarp Ergüven, "Uluslararası Hukuk Açısından Güvenlik Kavramının Teorik Temelleri", Ankara Üni. Hukuk Fak. Dergisi, Cilt.65, No.3, 2016, ss.771-835.
[77] Paul Streeten, "Globalisation: Threat Or Ossortunity?", The Pakistan Development Review, Cilt.37, No.4, Yıl. Kış 1998 ss.51-83.

kavrayıp özetleyebilen ve herkesin üzerinde mutabık olduğu tek bir sorun olmadığı gibi kontrol da hiç kimsenin ya da yöntemin tekelinde değildir. [78]

B) Tehdit ve Caydırıcılık Kavramları

1.6. Farklı Yaklaşımların Tehdit Algılama Metodolojisi

1.6.1. Tehdit Kavramını Anlamak ve Açıklamak

Uluslararası sistemin sahip olduğu anarşik yapının doğasında riskler vardır. Her risk aynı zamanda bir tehdittir. Bu sebeple risk ve tehdit kavramlarının varlığı güvenlik kavramının ortaya çıkmasının en önemli sebebidir. Aynı zamanda; tehditleri belirlemek, analiz etmek, etkisini azaltmak ve fırsatları değerlendirmek devletlerin dış politika stratejilerini belirleyerek rakiplerine karşı mücadele edebilmeleri için bir zorunluluktur. Bu doğrultuda konuyu daha iyi anlayabilmemiz için ilk olarak tehdit kavramını açıklamamız gerekmektedir.

İngilizcesi " threatening " kelimesine karşılık gelen tehdit kavramı 1990'lardan sonra uluslararası sistemde yaşanan köklü değişimler, küreselleşmenin beraberinde getirdiği teknolojik gelişmeler ve modern dönemde yeni tehditlerin ortaya çıkmasıyla beraber birçok alanda kullanılmaktadır.

Türk Dil Kurumu sözlüğüne göre tehdit; "birinin gözünü korkutma, tehlikeli bir durum yaratma, korku verme ve gözdağı" olarak tanımlanmıştır.

5-6 Nisan 2007 tarihleri arasında TSK Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü tarafından düzenlenen "Türkiye'ye Yönelik Dış Kaynaklı Risk ve Tehditler Sempozyumu" sonuç raporunda ise tehdit; gerek kısa gerekse uzun vadeli hedeflerin gerçekleşmesini güçleştiren, yeri ve zamanı gelince ortadan kaldırılmasında milli güç unsurlarının kullanılmasını gerektiren her çeşit faaliyet olarak tanımlanmıştır. [79]

Somut bir tehlikeyi ifade eden tehdit, içerisinde öznellik barındırmasının yanında içerisinde makul bir oranda da nesnellik barındırmaktadır. Aynı zamanda; "mücadele edilebilir ve muhtemel zararlarına karşılık hazırlık yapılabilir" yapıda

[78] Zygmunt Bauman, a.g.e. ss.63.
[79] Ahmet Küçükşahin, "Türkiye'ye Yönelik Dış Kaynaklı Risk ve Tehditler Sempozyumu", T.C. Genelkurmay Başkanlığı Harp Akademileri Komutanlığı Saren, 05-06 Nisan 2007, ss.45.

olan tehdit kavramı, hükümetin politika seçeneklerinin çeşitliliğini önemli ölçüde daraltan ve aynı şekilde bireyler, topluluklar ve hatta tüzel kişileri etkileyen eylem veya eylemler dizisi olarak tanımlanmaktadır.[80]

Beril Dedeoğluna göre tehdit; eldekini kaybetme riski, diğer süjelerin etkisi ve küresel tehditler olmak üzere üç biçimde ortaya çıkan eylemler bütünüdür.[81]

Bir başka tanımlamaya göre gelecekte meydana gelmesi muhtemel bir olay olan tehdit kavramı, bir devletin, topluluğun veya bireyin varlığına veya refahına yönelik olası olumsuz etkileri bulunan bir eylemdir. Bu bağlamda tehdit tanımlaması üç biçimde ortaya çıkmaktadır. Bunlar; eldekini yitirme riski, başkasının elindekini ele geçirememe riski ve küresel tehditlerdir. [82] Her devlet, milli varlığına, bekasına ve güvenliğine yönelik bu tehditlere karşı tedbirler almak durumunda olduğundan ve iç tehditlerin devlet ve rejim güvenliğini tehlikeye atması sebebiyle birincil tehdit olarak tanımlanmaktadır. Devletlerin birincil tehdit olarak tanımladıkları iç tehditleri engellemeye yönelik ise iç hukukta gerekli düzenlemeler gerçekleştirilmektedir.[83] Ulusal alanda herkes tarafından kabul gören ortak iç tehdit algılamalarından bazıları ise şunlardır;

- ✓ Terörizm
- ✓ Silahlanma
- ✓ Organize suç ve mafya örgütleri
- ✓ Etnik çatışmalar ve yükselen milliyetçilik
- ✓ Dini radikalizm
- ✓ Kitlesel göç hareketleri
- ✓ Ekonomik dengesizlikler
- ✓ Çevre sorunları
- ✓ Siber Suç ve Siber Terör

Ulusal alanda bu tehdit alanlarıyla alakalı düzenlemeler gerçekleştiriliyor olsa da uluslararası alanda bu yönde çalışmalar yapılamamaktadır. Bunun en önemli sebebiyse karşılığı olmayan, denk gelmeyen, özünde beklenmedik bir zamanda ve

[80] Nasıh Sarp Ergüven, a.g.e. ss.771-835.
[81] Beril Dedeoğlu, "Uluslararası Güvenlik ve Strateji", Yeniyüzyıl Yayınları, İstanbul, 2008, ss.32-63
[82] Elke Krahmann, a.g.e. ss.3-19.
[83] Selim Dursun, "İç Tehditler ve Dış Politika: Gürcistan Dış Politikası Örneği (1991-2003)", AÇÜ Uluslararası Sosyal Bilimler Dergisi Cilt: 3, Sayı:2, Yıl: 2017, ss. 24-49.

mekânda aniden "karşı tarafın zayıf taraflarına yönelme" ile ilgili "asimetri" kavramı ile "tehdit" kelimesi birleşmesidir. Konvansiyonel savaş tehditlerinden ayrılan bu yeni tehdit türü Soğuk Savaş sonrasında önemini arttırmış ve bu tehdit türü ile birlikte devletlerin güvenlik sorunları, tehdit algılamaları ve savunma doktrinlerinin yeniden gözden geçirilmesini zorunlu kılmıştır.

Bu bağlamda; Ashton B. Carter, William J. Perry ve David Aidekman tarafından gerçekleştirilen asimetrik tehdit sınıflandırmasında; günümüzde özellikle haberleşme, bilgisayar, uydu teknolojileri, kitle imha silah sistemleri, enerji, finans, ulaşım sistemleri ve hükümet kurumlarına yönelik asimetrik saldırılarının gerçekleştirildiği belirtmiştir. [84] Gerçekleşen bu asimetrik tehditlerin en önemli özellikleri ise şunlardır;

- ✓ Görülmez,
- ✓ Anlaşılmaz,
- ✓ Bilinilmez,
- ✓ Tahmin edilmez
- ✓ Karşı koyulması zor,
- ✓ Savaşın normal özelliklerine benzemez
- ✓ Çok yönlülük içerir
- ✓ Öznellik içerir
- ✓ Sivil/asker ayrımı yapmaz
- ✓ Konvansiyonel bir savaşta başa çıkılamayacak bir hedef ile çarpışmak için alternatif bir yol sunar.

Colin S. Gray'a göre asimetrik tehditler; öngörülemez, bilinmediği için korkutuculuğu yüksek, cevap vermede orantısızlık içeren, hedef gözetmeksizin içerisinde çok yönlülüğü barındıran (askeri, iktisadi, sosyal, kültürel), zayıflıkları kullanan, psikolojiyi etkilemeyi temel alan, mali durumla bağlantılı ve teknolojiyi

[84] Ashton B. Carter, William J. Perry ve David Aidekman, "Countering Asymmetric Threats", Carter, A.B. ve White J.P. (der.) "Keeping the Edge Managing Defense for the Future", the Mit Press, Cambrigde,2001,ss.120-121 https://books.google.com.tr/books?id=hduWZJ3j_KEC&pg=PA1&lpg=PA1&dq=Keeping+the+Edge:+Managing+Defense+for+the+Future&source=bl&ots=lMtpNzU_4h&sig=ACfU3U0TNlwVxK1ocsGvmICr0pfH2ZbuFg&hl=tr&sa=X&ved=2ahUKEwj4ruSvg4XkAhVWhlwKHewwAeY4ChDoATABegQICRAB#v=oness&q=Keeping%20the%20Edge%3A%20Managing%20Defense%20for%20the%20Future&f=false .ET. 30.01.2020.

farklı konseptle kullanır yapıdadır. Bu yüzden düşmanlardan gelebilecek asimetrik tehditlerden etkilenmemek için caydırıcılığa sahip olunması, saldırı potansiyeli yüksek hedeflerin korunması ve geleneksel olmayan yöntemlere karşı etkin bir korumanın gerçekleştirilmesi gerekmektedir.[85]

Günümüzde popüler olan bu asimetrik tehditlerin vücut bulmuş hali olan "Asimetrik Savaş" türünün tarihsel arka planı ve fikirsel alt yapısı aslında yıllar önce Sun Tzu ve Clausewitz 'in ortaya koyduğu savaş stratejileri, prensipleri ve önerilerine kadar dayanmaktadır. Örneğin;

Sun Tzu'ya göre savaşta ustalık yenmek değil, kolaylıkla yenme becerisini göstermektir. Düşmanın planlarını bozmak, savaşmadan kazanmak ve dolaylı stratejinin üstünlüğünü vurgulamıştır. Günümüzde sıklıkla kullanılan ''siber uzay'' ve ''siber strateji'' kavramı Sun Tzu'nun yeniden keşfedilmesidir. Çünkü Sun Tzu tarafından önerilen prensipler ve değerlerle ''siber uzay'', ''siber strateji'' ve ''siber savaş'' gibi kavramların sahip olduğu değerlerle benzerlik göstermektedir. Her ikisi de güçle bağlantılı olsa da asıl amaç şekilsizliğe ulaşmaktır.

Sun Tzu'nun asıl olanın savaşmadan kazanmak [86] şekilsizliğe ulaşmak vurgusu da siber uzayı tarif etmektedir. Siber uzay devletlere savaşmadan, büyük kayıplar yaşamadan kazanma imkânını ve yaptıkları faaliyetlerin başkası tarafından kesin olarak öğrenilemeyeceği bilinmezlik yaratan bir güç alanı ortaya çıkarmıştır. Örneğin; siber risk ve tehditler, yaşamın tüm işleyişini etkileyebilecek derecede giderek daha önemli bir hale gelmektedir. Çünkü siber saldırılar elektrik kesintilerine, askeri ekipmanların arızalanmasına, ulusal güvenlik sırlarının ihlal edilmesine, tıbbi kayıtlar gibi değerli ve hassas verilerin çalınmasına, kritik alt yapıların çalışamaz hale gelmesine neden olabilmektedir. Siber uzayın bu kritik alanların hepsinde sahip olduğu etkileme gücü sayesinde güçlü devletlerarasında büyük bir çatışma çıkma ihtimali azalırken ufak ve gizliden yürütülen çatışmaların sayısı artmaktadır.[87]

Son olarak; Sun Tzu'nun "Mükemmellik her savaşta çarpışarak kazanmak değildir. En iyi strateji savaşmadan kazanmaktır.", "Kurnazlık ve gizlilik denilen

[85] Colin S. Gray, "Modern Strateji", Çeviren Öz, H. Truva Yayınları, 2008.
[86] Sun Tzu, "Savaş Sanatı", Hasan Alı Yücel Klasikleri Türkiye İş Bankası Yayınları, İstanbul, 2018.
[87] Us Commission On National Security, "21 Th Century, New World Coming", Washington, D.C, 15.10.1999, ss.8.

kutsal sanat! Senin sayende görünmez olmayı; senin sayende duyulmaz olmayı öğrenip, düşmanın kaderini elimizde tutuyoruz.", "Planlarını gece gibi karanlık ve geçilmez yap ve hareket ettiğinde bir yıldırım gibi in!" gibi sözlerinin hepsi aldatma, hile, gizlilik, kayıpsız kazanç ve sürprizin savaştaki önemi hakkındaki bakışı günümüzün asimetrik savaşlarındaki stratejik bakışla benzerlik göstermektedir. Aslında asimetrik tehdit kavramı ile mücadelenin yol haritası da o zamanlardan ortaya çıkmıştır.

Clausewitz'e göre de savaş bir düellodur. Clausewitz savaşları iki kategoriye ayırmıştır. Bunlar, siyasi amaçlarla yürütülen "sınırlı savaşlar" ve düşmanı alt edip istenilen barış koşullarını dikte ettirmek için yürütülen " topyekün savaşlar" dır. [88] Bu bağlamda günümüzde yaşandığını iddia ettiğimiz asimetrik savaşların bir türü olan siber savaşlar Clausewitz tanımlamasıyla "sınırlı savaş" olarak gösterilebilir. Aynı zamanda; tarih boyunca, birçok savaşta güç dengesizliğinden kaynaklanan asimetrik durum yaşanmıştır. Clausewitz'in ''Savaş politikanın başka araçlarla devamıdır''[89] ve ''Her çağ kendi savaşını yaratır.'' sözleri çerçevesinde Soğuk Savaş sonrası yeni dönem incelendiğinde, asimetrik savaşların bir parçası olan bu belirsizlik ve konvansiyonel savaşlara alternatif olma hali günümüzde siber savaş ya da hibrit savaş gibi yeni savaş yöntemlerinin ortaya çıkmasına yol açtığı görülmektedir. Böylece klasik savaştaki gibi savaş kavramı silahlı kuvvetler tekelinden çıkmıştır.

Hibrit yöntemler ve enformasyonun doğuşu ile bilgisayarın bu kadar önemli olması hakkında Alvin Toffler'in sözleri günümüz sistemini çok güzel özetlemektedir. Alvin Toffler'e göre; Bilgisayardan… "düşünülemez olanı düşünmesini ve daha önce düşünülmemiş olanı düşünmesini isteyebiliriz. Bilgisayar bugüne kadar harfiyen düşünülemez ve tahayyül edilemez olan yeni kuramlar, düşünceler, ideolojiler, sanatsal iç görüler, teknik ilerlemeler, ekonomik ve politik yenilikleri mümkün kılar. Bilgisayar böylece tarihsel değişimi hızlandırır ve 3. Dalga, toplumsal çeşitliliği ateşler. [90] Bu bağlamda bilgisayar ve internet temelli günümüz güvenlik stratejilerinin işleyişinde NATO üye ülkeleri ve Rusya arasında günümüzde yaşanan siber ve hibrit savaş kavramları, bu yeni güvenlik stratejilerinin

[88] Paul Kennedy, "Savaşta ve Barışta Büyük Stratejiler", Çeviren Fethi, A. Totem Yayıncılık, İstanbul, 2014, ss.43.
[89] C. Clausewitz, Savaş Üzerine, Çev. Koçak, S. Doruk Yayınları, 2015.
[90] Krishan Kumar, "Sanayi Sonrası Toplumdan Post-Modern Topluma Çağdaş Dünyanın Yeni Kuramları", Dost Yayınları, Ankara , 2013, ss. 19.

yaratılmasına ihtiyaç duyulduğunun en önemli göstergesidir. Bu yeni savaş konsepti hızlı ve çok büyük değişimleri içinde barındırmakla birlikte yeterince anlaşılamadığından karmaşık, çok boyutlu, sınırsız ve öngörülemez bir gelecek planı ortaya koymaktadır. Böylece aynı saldırının kendisine karşı yapılabilme ihtimali ülkelerin bu yeni silahı aleni kullanmalarını engellemektedir.

Ayrıca asimetrik bir tehdit olan siber tehditlerle ilgili bir diğer önemli husus nükleer silahlardır. Günümüzde nükleer silaha sahip ülkelerin bu gücünü korumak istemesi, bu silaha sahip olmayan devletlerin edinmesini engellemesi, bu silahlara sahip olmayan ülkelerin kendilerini tehdit altında hissetmelerine yol açmaktadır. Bu silahlara sahip olmayan devletlerin veya terör örgütlerinin bu silahlara sahip olması, ulaşabilmesi veya kullanması ciddi bir tehdittir. [91] Siber uzay ise siber silahlar kullanılarak bunun gerçekleşebileceğini stuxnetle birlikte göstermiştir.

Nükleer silahlarla gücün doğrudan kullanımının geçmişe oranla daha zor olması sebebiyle nükleer savaşın bir siyaset aracı, hatta tehdit unsuru olarak kullanımı önemli oranda azalmıştır.[92] Fakat; teknolojik gelişmelerle birlikte uluslar arasında artan bağımlılık satranç tahtasında kullanılan temel bileşen haline gelmiştir. Sonuç olarak teknolojik olarak nükleer enerji ile nükleer silah üretimi arasında önemli bir farkın bulunmaması nedeniyle, nükleer enerji teknolojisine sahip olmayan fakat olma yolunda çalışmalar yapan ülkelerin siber silahlarla birlikte tehdit paradoksu devam etmektedir.

Bu paradoksun devam etmesiyle birlikte tehdit zeakası kavramı önem kazanmaktadır. Günümüzde dijital dönüşüm araçlarıyla birlikte insanların ve makinelerin birlikte çalışmasıyla elde edilen tehdit zekâsı kavramı, saldırganın kimliği, motivasyonlarının ve kabiliyetlerinin ne olduğu, geçmiş ilişkileri ve tehditlerini tespit edebilmek için sistemde hangi göstergelerin aranacağı gibi olum(suz)lu soruları cevaplayarak milli güvenliğin sağlanmasına yardımcı olur. Çünkü milli güvenliği sağlayabilmek için fırsat ve başarılardan ziyade negatif olan tehdit ve başarısızlıklara odaklanmak gerekmektedir.

---

[91] Kadir Sancak, "21.yüzyılda Güvenlik Sorunları: Bir Tehdit Unsuru Olarak Nükleer Silahlar", The Journal of Academic Social Science Studies, Cilt.6, No.8, Ekim 2013, ss.499-510.

[92] Zbigniew Brzezinski, "Büyük Satranç Tahtası:Amerika'nın Küresel Üstünlüğü ve Bunun Jeostratejik Gereklilikleri", Çeviren:Türedi, Y. İnkılap Yayınları, ss:36.

Aynı zamanda tehdit zekâsı kavramı, dış politika oluşturma stratejilerinin altında bir stratejik kültür yaratmaktadır. Çünkü her ülke kendi şartlarına göre tehdit algılamakta bu durumda öznellik yaratmaktadır. Bir kişi veya ülke için tehdit olarak algılanabilecek bir durum diğer bir kişi veya ülke için avantaj olabilir. Bu yüzden aktörlerin tehdit algılamalarına etki eden faktörler arasında deneyimler, içinde bulunulan sosyal, siyasal, kültürel, çevresel durum, iç ve dış dinamikler başta olmak üzere pek çok etken bulunabilir.

Bu bağlamda; tehdit zekâsı genellikle üç alt kategoriye ayrılır. Bunlar;[93]

- ✓ Stratejik: Genellikle teknik olmayan bir kitleye yönelik daha geniş eğilimler
- ✓ Taktik: Daha teknik bir kitleye yönelik tehdit oyuncularının taktikleri, teknikleri ve prosedürlerinin ana hatları
- ✓ Operasyonel: Özel saldırı ve kampanyalarla ilgili teknik detaylardır.

Özetlemek gerekirse; tehdit hem gerçek olgu ve olaylara hem de algı ve tahminlere dayanmaktadır. Bir tehdidin gerçek tehlike olup olmaması sadece gerçekleştiği zaman ortaya çıkar. Buda önlem alınması için geç kalındığını gösterir. Aynı zamanda hiçbir zaman gerçekleşmeyecek bir durum da tehdit olarak kabul edilebilir. Burada önemli olan algı ile olgu arasındaki mesafedir. Eğer mesafe açılırsa risk artar. Risk arttıkça ise tehdit artar. Böylece de güvensizlik durumu oluşur. Realist bakış ise bu güvensizlik durumuna karşı devletin temel amacının vatandaşları iç ve dış tehditlere karşı korumak olduğunu ileri sürer. Bu doğrultuda realizmin odak noktası askeri güç olmuştur. Asimetrik tehditlerin ortaya çıkması ise güç kavramını sadece askeri nitelikte olmaktan çıkarmıştır. Ayrıca içsel, dışsal veya asimetrik tehdit olarak herhangi bir tehdidi analiz edebilmek için öncelikle, düşmanın kim ve tehdidin ne olduğunun tespit edilmesi gerekmektedir. Bu bağlamda güvenlik olgusundan söz edebilmek için tehdit tanımlamasının yapılması gerekmektedir.

[93] Zane Pokorny, "What Is Threat Intelligence? Definition And Examples", 30 Nisan 2019, https://www.recordedfuture.com/threat-intelligence-definition/ ET. 30.01.2020.

1.6.2. Tehdit Algılama Metodolojisi

Güvenlik kavramı, her şeyden önce güvensizliği ortaya çıkaracak bir tehdidin varlığı ve söz konusu tehdidi ortadan kaldıracak nitelikte bir güç ile mümkün hale gelmektedir. Bu yüzden güvenlik kavramının tanımlaması yapılmadan, tehdit kavramının açıklanması ve geçirdiği dönüşümün belirlenmesi mümkün değildir. Güvenlik en basit anlamıyla risk ve tehditten uzak durulmasıdır. Soğuk savaş sonrasına kadar güvenlik anlayışı geleneksel bir çizgide ilerlerken, Soğuk Savaş sonrasında farklı anlayış ve alanları içine alan kapsayıcı bir hal almıştır.

Tehdit algılaması ve güvenlik yapılanması aktörlerin dış politikasını oluşturan en önemli iki unsurdur. Güvenlik stratejilerinin oluşturulmasının ilk basamağı ise güvenliği tehlikeye sokacak öğelerdir. Devletler dış politika davranışlarını güvenliklerini tehlikeye sokacak öğeler ve tehdit algılamaları çerçevesinde belirlemektedir. Bu yüzden tehdit algılayan devletlerin tehdit unsuru oluşturan devlete karşı realist dış politika davranışına başvurması kaçınılmaz bir sondur. Tarihsel süreç içerisinde de devletler tarafından uygulanan dış politika davranışları başka bir rakip güç unsuru tarafından tehdit olarak algılandığında o devlet tarafından karşı devlete yönelik realist bir dış politika davranışı ortaya koyulduğu görülmektedir. Örneğin; tarih boyunca kullanılan çevreleme stratejisi, güç dengesi, ittifak stratejisi, güvenlik ikilemi, caydırıcılık vb. tüm dış politika hareketleri bu tehdit algısının bir sonucu olarak ortaya çıkmıştır.

Küreselleşme ise güvenliğe bakış yaklaşımında tam anlamıyla bir değişim ve dönüşüm yaratmıştır. Küreselleşmeyle birlikte teknolojik, ekonomik, sosyal, kültürel, siyasal vb. tüm alanlar iç içe girmiş bu durum da tehdit algılamasını Soğuk Savaş öncesi döneme göre daha da genişletmiştir. Özellikle Soğuk Savaş sonrası dönemde kapitalizmin, küreselleşmenin ve teknolojik gelişmelerin hızlanmasıyla birlikte tehdit algılamaları da farklılaşmıştır. Aynı zamanda, birey/grup veya ülkelerin her birinin tehdit algısının farklı olması tehditlerin algılanması, yorumlanması ve uygulanmasında da farklılaşmaya yol açmıştır. Günümüzde teknolojik gelişmeler sonucunda ortaya çıkan siber uzay ise geleneksel güvenlik yaklaşımının yanında tüm bu güvenlik stratejilerini kapsayan bir tehdit algısı ortaya çıkarmıştır.

Özetlemek gerekirse; uluslararası sistemde, sistemin bütün aktörleri benzer biçimde varlığını koruma ve sürdürme kaygısı taşıdığından benzer tehdit kaygıları

yaşasa da sistemi anlamaya, anlatmaya ve açıklamaya yönelik farklı yaklaşımları olabilmektedir. Bu yaklaşımların bir kısmı içerik bir kısmı da analiz yöntemiyle alakalıdır.Yaklaşımların bazılarıda birbirlerini tamamlamaktadır. Bu yaklaşımlardan bazıları ise şunlardır;

Mearsheimer'a göre, devletler birbirlerinden korkarlar ve sürekli olarak kendilerine rakiplerinin saldıracağından şüphelenirler. Bu sebeple, devletler birbirlerine karşı koşulsuz bir güven hissine sahip değildir. Çünkü uluslararası sistemin sahip olduğu anarşik yapı sebebiyle muhtemel bir tehdit anında, tehdit altındaki ülkenin başvurabileceği bir merkezi otorite bulunmamaktadır.[94] Bu anarşik durum da güvenlik çıkmazını ortaya çıkarmaktadır. Devletlerin kendi güvenliklerini sağlama sürecinde silahlanması, diğer rakipleri tarafından tehdit olarak algılanmaktadır. Böylece bu etki/tepki süreci bir devletin güvenliğiyle diğerinin güvensizliğini oluşturan bir güvenlik çıkmazı yaratmaktadır.

Tehdit algılamada önemli bir diğer tehdit yaklaşımıysa güç kullanımıyla alakalıdır. Devletler güç kullanma tehdidiyle rakiplerinin dış politika davranışlarını etkilemekte ve rakiplerini kendi isteklerine göre hareket ettirmeye zorlamaktadır.[95] Bu bağlamda; Kenneth Waltz ile birlikte Robert Gilpin, gücün sistemdeki dağılımı üzerinde yoğunlaşmıştır. Aynı zamanda; anarşik uluslararası sistemde bireylerin tehdidi nasıl algıladığı konusunda Waltz gibi neorealistler, güç gibi materyal faktörlerin zayıf aktörleri baskı altında tutmaya yarayan bir tehdit unsuru olarak kullanıldığını savunmaktadır. Bu bakışa göre tarih boyunca uluslararası sistem hep kendine has bir denge içermektedir. Dengenin bozulmaya başladığında da tehdit unsuru artarak sistem yeniden dengenin kurulabilmesi için savaşa sürüklenmiştir. Bu yüzden dönemin tek kutuplu, çok kutuplu veya hegemon olmasından ziyade güç dengesinin önemi ortaya koyulmuştur. Sürekli değişen ittifaklar ve güç kapasitesindeki değişimler teknolojik gelişmelerle birleşince farklılaşmayı, farklılaşma ise tehdit unsurunu ortaya çıkarmaktadır.

[94] John J. Mearsheimer, "The False Promise of International Institutions", International Security, Cilt.19, No.3, Kış 1994-1995, ss. 10-11.
[95] K. J. Holsti, "The Concept of Power in the Study of International Relations", Wiley on behalf of The International Studies Association, Cilt. 7, No.4, Şubat 1964, ss.179-194.

Robert Keohane ve Joseph Nye gibi Neoliberal düşünürlerin çatışma/işbirliği bakışı, ortak çıkarlar, güç dengesi ve barışçı ilişkiler üzerine kurulu bir uluslararası hukuk kodunun oluşturularak tehditlerin azaltılabileceği yönünde bir fikre dayanır.

Thomas Schelling de " The Strategy Of Conflict" adlı kitabında oyun kuramı ve strateji alanında literatüre ciddi bir katkı yaparak kuramsal analizlerde çatışma ve işbirliğinin önemini ortaya koymuştur. Aynı zamanda; dış politika stratejilerinin belirlenerek hedeflerin gerçekleşmesi için görüşmelerin, pazarlığın ve iletişimin önemini vurgulamaktadır. Savaşların ve diğer çatışmaları mutsuzluğun en önemli sebebi olarak gösteren Thomas Schelling her koşulda işbirliğinin önemini ortaya koymuştur.[96]

Tehdit çalışmalarında en detaylı ve gelişmiş çalışmalarından birini yapan Barry Buzan ise, people, states and fear adlı eserinde devletlerin karşılaşabileceği tehditleri askeri, politik, sosyal, ekonomik ve çevreyle ilgili tehdit başlıkları altında incelemiştir.[97] Böylece Barry Buzan tehdit yaklaşımının sadece askeri bir olay olmadığı karmaşık ve kapsamlı bir durumu içerdiğini belirtmiştir.

David Baldwin'in güvenlik yaklaşımı da; askeri, ekonomik, çevre, kimlik ve toplumsal güvenlik gibi kavramların hiçbirinin birbirlerinden farklı olmadığı sadece güvenliğin farklı bir türü olarak güvenlik yaklaşımını çeşitlendirdiğini belirtmiştir.[98]

Sonuç olarak; Soğuk Savaş dinamiklerini bireylerin öneminde ve kapitalist değerlerin doğasında gören revizyonistler, Soğuk Savaş sonrası dönemi teknolojinin ve kapitalizmin etkisindeki caydırıcılık ve tehdit kavramlarının değişmesinde bulur. Post revizyonistler ise, revizyonistlerin üzerinde durduğu ekonomik determinizm nedeniyle değil, anarşik sistem üzerindeki güvenlik ikilemine vurgu yapar. Bu güvenlik ikilemi Thucydides'in kaleme aldığı Atina ve Sparta arasındaki asırlar önceki krize kadar gitmektedir. Bu sebeple günümüzde aktörler arasında yaşanan güvenlik ikilemi farklı yapı ve şekillerde siber uzay üzerinde devam etmektedir. Çünkü siber uzay aslında tüm alanları içine alan büyük bir resimdir. Büyük resmi inceleyebilmek içinde büyük strateji ile konuya yaklaşılması gerekir. Büyük strateji özünde güçlüye ne kadar güce sahip olacağı, zayıfa ise kabul etmeye mecbur

[96] Thomas C. Schelling, "The Strategy of Conflict", Harvard University Press, Cambridge, 1980.
[97]Barry Buzan, "People, States And Fear The National Security Problem İn İnternational Relations" ,Whealsheal Books, 1983.
[98] David A. Baldwin, "The Concept Of Security, Review Of International Studies", British International Studies Association, Cilt.23, No.1, 1997, ss.5-26.

olduğunu kabul ettirmeye dayanır. Büyük strateji ekonomik, askeri, siyasi, diplomatik her şeyi içine alır. [99] Aynı zamanda büyük strateji doğası gereği tesadüfleri ve beklenmedik gelişmeleri yapısal olarak içine alan, kesintisiz bir biçimde yaşanan değişime tabidir.[100] Çatışmadan başka tercihin kalmadığı durumlarda da büyük strateji hem savaşmak hem de savaştan kaçınmak anlamına gelmektedir. Bu yüzden büyük strateji sadece savaşla ilgili görülmemelidir. Ekonomik, siyasi veya diplomatik değişikliklerde de kendilerini uyarlamaları gerektiğini belirtir. Büyük strateji de en önemli başarılar vazgeçilen savaşlarla alakalıdır. Bunun ise tarihte en güzel örneği Soğuk Savaştır.[101] Günümüzdeyse büyük stratejinin başarısı siber stratejiler sayesinde büyük savaşların engellenmesindedir.

1.6.3. Tehditlerin İnandırıcılığı ve Caydırıcılık

Uluslararası İlişkilerde tehditlerin inandırıcılığı kavramını açıklayabilmemiz için öncelikle caydırma teorisine bakmamız gerekmektedir. Caydırıcılık Teorisini açıklarkende en güzel örnek iki rakip süper güç arasında savaşla sonuçlanmayan bir gerginlik dönemi olan ve caydırıcılığın dış politika dinamiklerinde aktif olarak kullanıldığı Soğuk Savaş gösterilebilir. Soğuk Savaş döneminde çevreleme kavramıyla bağlantılı olarak kullanılan caydırıcılık kavramı, tehdit yoluyla karşının gözünü korkutma ve rakibin avantaj elde etmesini engelleme fikrine dayanır. [102] Kısaca caydırıcılık, kabul edilemez ölçüde sonuçlar doğuracağı tehdidinde bulunarak karşı tarafı davranışlarından vazgeçirmeye dayanan bir stratejidir. Özünde korkutarak karşının cesaretini kırmaya dayanan caydırıcılık kavramının kullanımı uluslararası ilişkilerde çok eskilere dayanmaktadır.

Caydırıcılığın başarısıda tehditlerin potansiyel saldırganlara inandırıcı gelmesine ya da bir başka deyişle saldırganın rakibinin mevcut askeri gücünü kullanmakta kararlı olduğuna inanmasına bağlıdır. Diğer yandan, saldırganın kendisine misilleme yapılacağı tehdidine inanması da bir başka önemli etkendir.

[99] Williamson Murray, Richard Hart Sinnreich ve James Lacey, "Büyük Stratejinin Oluşumu, Siyaset, Diplomasi ve Savaş", ÇevirenBaltacı, E. Avangard Yayınları, İstanbul, 2017, ss. 10.
[100] John Lewis Gaddis, "International Relations Theory And The End Of The Cold War", Iınternational Security, Cilt 17, Sıra 3, Kış 1992-1993, ss. 5-58.
[101] John Lewis Gaddis, The Cold War, The Penguin Press, New York, 2005.
[102] Nye ve Welch, a.g.e. ss. 191-195.

Tehditlerin inandırıcılığında, "askeri kapasite'', "pazarlık gücü'', "itibar'' ve " çıkarlar'' ise diğer önemli faktörlerdir. [103]

Özellikle Soğuk Savaş'ın bitmesiyle birlikte dünya her ne kadar tek kutuplu bir hal almış gibi gözükse de Rusya'ya dair kaygılar, İran uranyum zenginleştirme çabaları, Kuzey Kore'nin nükleer cephanelikleri, Çin'in askeri ve ekonomik olarak modernleşmesi, zenginleşmesi ve güçlenmesi uluslararası arenada ABD'nin tekel gücünü ve itibarını kırmaktadır. Bu tehdit durumlarının hepsi askeri güçlerin kullanımını azaltmıştır. Aynı zamanda; teknoloji, internet ve bilginin güç unsuru olarak kullanılması ve uluslararası alanda yayılması caydırıcılığı arttıran, aktörleri pazarlık yapmaya zorlayan ve askeri gücün kullanılmasını azaltan bir başka unsurdur. Çünkü geleneksel silahların yanında çok önemli bir rol üstlenen nükleer silahların kullanılma ihtimali aktörleri ciddi derecede tehdit etmektedir. [104] Bu sebeple stratejik caydırıcılık nükleer ve balistik füzelerin yanında diplomatik, ekonomik ve teknolojik alanları kullanan siber silahlar ile Soğuk Savaş benzeri bir caydırıcı unsur haline gelmiştir.

1.6.4. Tehdit Algılamalarındaki Değişim ve Siber Tehditlerin Sınıflandırılması

Güvenlik algılamaları tarih boyunca sürekli dönüşüme uğramıştır. Bu dönüşümle birlikte günümüzde gerçekleşen savaş ve çatışma kavramları evrensel, çok boyutlu, çok aktörlü ve esnek bir yapıya dönmüştür. Küreselleşme ve bilgi teknolojilerinde yaşanan süratli değişimlerse siber uzayın kullanımını arttırarak devlet dışı aktörlere daha önce hiç olmadığı kadar asimetrik avantaj sağlamıştır. Bu doğrultuda tüm devletler ve de uluslararası sisteme katılan devlet dışı aktörler güvenliklerini sağlamak için bu yeni durumda pozisyonlarını almıştır. [105]

Eleştirel güvenlik anlayışına göre, aktörlerin güvenliklerini sağlamak için alacakları pozisyonların göreceli olması, mutlak güvenliğin sağlanmasını mümkün kılmamaktadır. Bu yüzden asıl üzerinde durulması gereken güvensizliktir.

[103]Emre Gündoğdu, Uluslararası İlişkilerde Caydırma Teorisi, Marmara Üniversitesi Siyasal Bilimler Dergisi, Cilt 4, No.2, Eylül 2016, ss.1-22.
[104]Michael S. Gerson, "Conventional Deterrence in the Second Nuclear Age", Parameters, 2009, ss.32-48.
[105]Fatih Dedemen, "Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi", Güvenlik Bilimleri Dergisi, Cilt 5, No 1, Mayıs 2016, ss.141-176

Güvensizlik, tehditlerden doğan tehlikelerle dolu korku içindeki bir yaşamı ifade eder. Söz konusu tehditler, doğrudan şiddet içerebileceği gibi, dolaylı da olabilir. Tüm bu tehditlerin ve güvenlik risklerini bir bütün olarak sunan siber güvenlik kavramıysa her an, her tipten saldırıya hazır olmak ve kendimizi korumak noktasında bütünleşik güvenlik platformları ve entegrasyonları içermektedir. Bu yüzden; doğru ve tam bir siber güvenlik sisteminin sağlanabilmesi eş güdümlü bir halde fiziksel güvenliğin sağlanması ile gerçekleştirilebilir. Çünkü siber tehditler için kullanılan tanımlar, genelde geleneksel çatışma ve savaşlarda kullanılan tabirlerle benzerdir.

Soğuk Savaş döneminde ve öncesinde devlet merkezli ve askeri güç odaklı bir güvenlik yaklaşımı etkin olmuştur. Fakat kapitalizmin etkisi, teknolojik gelişmeler, Soğuk Savaş dönemindeki kırılma ve 11 Eylül saldırıları güvenlik ve tehdit algısında değişim yaşanmasını zorunlu kılmıştır. Böylece Soğuk Savaş sonrası değişen güvenlik algılamaları sonucunda yeni küresel dönemin yeni tehdit algılamaları ortaya çıkmış ve daha önce sadece askeri ve sert güçle ilgili olan tehdit kavramı asimetrik bir nitelik kazanarak siyasi, ekonomik, çevresel, toplumsal ve teknolojik gibi birçok alanı içine almıştır. [106]

Aynı zamanda teknolojik gelişmeler sonucunda devletlerin içlerinde oluşan toplumsal tehditler sadece kendi toplumlarını etkilemekte kalmamış küresel düzen üzerinde de ciddi etkilere yol açmıştır.[107] Ayrıca günümüzde teknolojinin hayatımızdaki rolünü ve etki sahasını giderek arttırmasıyla birlikte siber ortamla ilgili tehditler artmıştır. Bu artış bilgi hırsızlığından, rasgele bireysel saldırılara, bilinçli ve organize saldırılardan, siber ordular kurarak rakip ülkenin kritik altyapılarını çökertmeye kadar bireysel güvenlikten, ulusal güvenliğe her alanda kullanılmaktadır. Bu yüzden, henüz daha kullanımı çok yeni olan siber tehditler konusunda farkındalığın arttırılması ve gelecekte beka sorunu haline gelecek bu tehditlerin daha da artacağı göz önünde bulundurularak siber tehditlere ilişkin ulusal stratejiler ve eylem planları bir an önce kapsamlı bir şekilde hayata geçirilerek gerekli hukuki, teknik ve kurumsal alt yapılar oluşturulmalıdır. Çünkü asimetrik savaş türünde yeni bir cephe oluşmasına yol açan siber uzay çatışmalarda ekonomi,

[106] Muharrem Aksu ve Faruk Turhan, "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", Uluslararası Alanya İşletme Fakültesi Dergisi, Cilt 4, No 2, Yıl 2012, ss. 69-80.
[107] Richard A. Faik, "Dünya Düzeni Nereye? Amerikan Emperyal Jeopolitikası", Çeviri Domaniç, N. ve Arhan, N. Metis Yayınları, 2004 ss.38.

iletişim, medya gibi birçok unsuru bilgisayar ve internet ile bir araya getirmiştir. Bu durum yeni fırsatların doğmasına, bu yeni fırsatlar ise yeni tehditleri, mücadeleleri, çatışmaları, saldırıları ve savaşları doğurmuştur. Bu sebeple 21. yüzyılda asimetrik savaş; uzay, hava, deniz, kara ve son olarak siber uzay dâhil tüm boyutları içeren bir savaş türü haline gelecektir. [108] Soğuk Savaş'ın en büyük korkusu olan nükleer savaş tehdidi bile[109], günümüz siber silahları tarafından kullanılma tehdidini içinde barındırmaktadır.

Dijitalleşmeyle birlikte tehdit algısı da değişerek siber terör, siber suç, siber saldırı, siber casusluk ve siber savaş gibi yeni tehdit alanlarını ortaya çıkarmıştır.[110] Bu bağlamda siber tehditlerin önemi, kapsamı, silahları ve unsurlarına yönelik cevaplandırmamız gereken iki önemli soru vardır. Bunlardan ilki siber risklerin neden büyük tehdit olduğudur. Bu soruya vereceğimiz cevap devletlerin siber alanın kullanımını hayatın her alanına yaymasıyla birlikte siber risk ve tehditlerin, yaşamın tüm işleyişini etkileyebilecek derecede giderek daha önemli bir hale gelmesidir. Çünkü siber saldırılar elektrik kesintilerine, askeri ekipmanların arızalanmasına, ulusal güvenlik sırlarının ihlal edilmesine, tıbbi kayıtlar gibi değerli ve hassas verilerin çalınmasına, kritik alt yapıların çalışamaz hale gelmesine neden olabilmektedir.

Bir diğer soruda siber güvenlik tehditlerinin kaynağının kim olduğudur. Bu soruya vereceğimiz cevap siber güvenlik tehditlerinin belirlenmesinde anarşik yapı, aktörler arasındaki rekabet ve güç ilişkisi, bilgiyi koruma mücadelesi ve karşılaştırmalı üstünlükler gibi perspektiflerin kullanılmasıdır. Böyle anarşik bir ortamda internet sisteminin kullanıldığı her yerde risk tehdidi mevcuttur. Bu yüzden en önemli aktör olan devletler güvenliklerini sağlayabilmek için çeşitli yollar denemektedir. Bunlar; ittifak oluşturma, birbirleri ile karşılıklı olarak bağımlılıklarını arttırma, siber strateji oluşturma sürecinde stratejik bir bakış açısı gerçekleştirebilmek için kurumsal bir yapı oluşturma ve son olarak sorunlara çözüm

[108] Matai, D K. "The World Beyond 11 September Focus On Asymmetric Warfare", 1 Whitehall,RTC, 22.10.2001, ss 2-4. http://www.mi2g.com/cgi/mi2g/reports/speeches/221001.pdf ET.07.02.2021.
[109] Therese Delpech, "Nuclear Deterrence İn The 21st Century Lessons From The Cold War For A New Era Of Strategic Piracy", Rand Cooperation, 2012 ss:6.
[110] Hugo Taylar, "What Are Cyber Threats and What to Do About Them", Preyproject, 22.01.2020, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ ET.31.01.2020.

bulabilmek için büyük resmi görebilmedir. Büyük resimden kasıt ise internettir. İnternete bağımlı tüm sektörler ise bu resmin parçasıdır.

Bu büyük resim içinde aktörler ulusal hedeflerine ulaşabilmek için tehditler kadar fırsatları, kısıtlamalar kadar imkânları, yavaşlık kadar ilerlemeyi bir arada yaşamaktadır. Bu sebeple 21. yüzyıl güvenlik stratejileri ekonomik ve siyasi gücün askeri güç kadar etkili olduğu bir dönemi içermektedir. [111] Bunu devletlerin ulusal güvenliklerine ve kritik alt yapılarına yönelik gerçekleşen saldırılarda ve tehditlerde görebiliriz. Özellikle siber suç ve terör tehditleriyle yüz yüze kalan devletler bu alanda kendilerini korumak, için kamu-özel işbirliği modeli geliştirmekte ve ulusal bilgi güvenliği stratejisi oluşturmaktadır. [112]

Günümüz güvenlik yönetiminde bilgi güvenliği kritik bir öneme sahiptir. Bilgi yönetiminde amaç olay yönetimini yapmak, çok sayıda kaynaktan oluşan bilgiyi güvenli ve yönetilebilir bir ortamda toplamak, anlamlandırmak ve optimum kullanılmasına imkan tanımaktır. Aynı zamanda siber güvenlik dediğimizde aklımıza donanım, yazılım ve verilerin dijital saldırılara karşı korunması gelmektedir. Bu araçların yüksek derecede küresel bağlantıya sahip olması nedeniyle, siber saldırılar giderek daha sık ve daha şiddetli olmaya başlamıştır. Bu sebeple bilgi güvenliği, risk yönetimi, durum analizi, veri analizi, uygulamalı kriptografi, siber etik ve siber adli tıp ile ilgili temel bilgiler ve ileri düzey bilgilerin oluşturulması gereklilik halini almıştır.

Aynı zamanda tehdit ve çatışma yönetimi içerisinde; bilgisayar sistemleri ile ağ ve bulut altyapılarına yönelik gerçekleştirilen potansiyel güvenlik ihlallerine ilişkin riskleri ve saldırıları incelemek, bunların nasıl önleneceğini ve tespit edileceğini öğrenmek gibi amaçlarla uygulamalı deneyim testlerinin ve etik hacklemelerin arttırılması gerekmektedir. Bu çalışmadan sonra siber güvenlik risk değerlendirmesi, saldırı tespit ve önleme çabasıyla birlikte kritik altyapıların koruması için yapay zekâ ile makine öğrenimi ve tahmine dayalı analitik çalışmaların arttırılması sürecine götürecektir. Bu süreçten sonrada gerekli milli güvenli yazılım tasarımı oluşturularak kritik alt yapılardaki bilgi ve sistemlerin güvenlikleri

[111] Gary Hart, "Dördüncü Güç 21. yüzyılda Amerikan Büyük Stratejisi", Çeviren Karabaşoğlu, İ. Avangard Kitap, İstanbul, 2016, ss. 61.
[112] Robert P. Hartwig, "Cyberrisk: Threat And Ossortunity", İnsurance İnformation İnstute, New York, Ekim 2016, ss:11.

uygulamalı şifreleme ilkelleri, açık anahtar şifrelemesi, dijital imza, mesaj kimlik doğrulama kodları ve şifreleme protokolleri gibi kriptografik ve kripto analitik teknikleri çerçevesinde sağlanacaktır. Böylece mahremiyeti önemli olan konulara vurgu yapılarak geniş anlamda siber riskler, tehditler ve güvenlik açıkları tanımlanacak, tahmin edilerek öncelik verilecektir. Bu durum bilgi gizliliğinin sağlanması ve ulusal güvenliği tehdit edecek siber risklerin azalması yönünde bir strateji geliştirilmesine yol açacaktır. Oluşturulan bu yeni siber ulusal güvenlik ve dış politika stratejileri sayesinde rakiplere karşı rekabet avantajı sağlanacak, finansal kazanç elde edilecek, casusluk faaliyetlerinde ön plana geçilecek ve saldırılan ülke zayıflatılacaktır.

Sonuç olarak siber alanda aktörlerin kendi güvenliğinin sağlanması için aktörlerin gerçekleştireceği yukarıda belirtilen çatışma yönetim strateji süreci çok önemlidir. Uluslararası sistemdeki siber ortama yönelik anarşik yapı devam ettiği sürece bu yönetim süreci ulusal yönetilebilir bilgi güvenliğinin sağlanmasında teknolojik bir zorunluluktur. Ayrıca uluslararası alanda temel siber güvenlik ilkelerini belirleyerek küresel çevrimiçi dünyada aktörler arasında işbirliğini teşvik etmek için 24 Ocak 2020 tarihinde Dünya Ekonomik Forumu'nda Davos'ta hazırlanan "Küresel Risk Raporları" doğrultusunda Siber Güvenlik Teknoloji Anlaşması'nın gerçekleştirilmesi konuşulmuştur.[113] Bu yönde geliştirilen bu çabalar ve girişimler siber çatışma yönetiminin olumlu bir şekilde çözülebilmesi ve siber anlayışlı bir geleceği teşvik etmek için çok önemlidir. Fakat yeterli değildir. Çünkü tehdit yönetimi kapsamlı bir süreçtir ve asıl amaç, riskleri tanımlamak, niteliklerini analiz etmek, meydana gelme olasılığını değerlendirmek ve risklerin etkisini azaltmaktır. Yani tehditleri yönetmek 4 aşamalı (Tanımla, Analiz Et, Planla ve Yönet) bir süreci ifade eder. Bu süreci kısaca açıklarsak;

İlk aşama tanımlama aşamasıdır. Bu aşama tehditlerin doğası tanımlanarak tehditlerin fırsata çevirilmesini kapsar. Bu aşamayı kısaca açıklarsak;

Güvenliğimizi tehdit eden unsurları, ister geleneksel yaklaşım isterse yeni güvenlik yaklaşımı çerçevesinde değerlendirelim cevap değişmeyecektir. Tehditlerin varlığının asıl sebebi insan doğasına dayanmaktadır. Çünkü insanoğlu doğuştan kötü,

[113] Cybersecurity Tech Accord returns to the World Economic Forum, Tech Accord News, 24.01.2020 https://cybertechaccord.org/cybersecurity-tech-accord-returns-to-the-world-economic-forum/ ET.28.02.2020.

vahşi ve bencildir. İnsanoğlunun bu doğa hali doğal olarak devletleri ve daha üstte yapıyı da doğrudan etkilemektedir. Zaten Hobbes, Locke ve Rousseau gibi sözleşmecilerin devlet kurulması yönündeki açıklamaları da bu durumu destekler niteliktedir. Örneğin; Rouseau Toplum sözleşmesinde şu şekilde açıklar; birlikte oluşturulan bu tüzel kişiliğe eskiden site, şimdi ise cumhuriyet, siyasi gövde yada devlet denmektedir. Devlet egemen, güçtür ve tebaanın ona bağlı olacak şekilde tüm haklarını devretmiş olduğunu söyler. [114]

Bu yetkiyi almış devletler günümüzde sanal dünyada kendi sınırlarını korumaya çalışarak bu alanda hem kendi vatandaşları hem de dışarıdan gelecek saldırılara karşı tekrardan gücü ve kontrolü ele geçirebilmek için ciddi mücadele vermektedir.Tarihsel kapitalizmde nasıl insanlar, insan grupları siyasi mücadelelerini ve ana stratejik hedeflerini devlet iktidarını denetim altında tutmak üzerine kurmuşsa[115] bu mücadele sanal ortamda da devam etmektedir. Aynı zamanda, bir tehdidin söz konusu olması için ilişkinin doğası gereği iki tarafı bulunması gerekir. Bunun yanında tehdit kavramı doğası gereği koşullu olabileceği gibi aynı zamanda karşı tarafın ne yaptığına bakmadan direk koşulsuz olarak da gerçekleşebilir. Bu sebeple; tehdit kavramının doğası gereği oluşturulan dış politika stratejilerinde asıl hedeflenen amaçlar; güvenlik, statükoyu sağlama, caydırıcılık oluşturma, büyük güç olma, rakibi saf dışı etme, rakipler üzerinde nüfus kazanma, inşa etme, ittifak/koalisyon oluşturma ve son olarak barış dönemi stratejileri şeklinde sınıflandırılabilir.

Güvenlik çalışmalarına başlayabilmek için öncelikle risk ve tehditlerin belirlenmesi gerektiğini daha önce belirtmiştik. Bu kapsamda bir konunun tehdit veya risk olması, konunun kendi özelliğinden ziyade onu kabul eden kişi, kurum veya ülkenin kendi yetenek ve kabiliyeti doğrultusunda konuyu algılamasına bağlıdır. Devletler eğer kendi güçlü ve zayıf yanlarını bilirse hangi alanlara önem vermesi gerektiği ve tehditlerin nereden gelebileceğini görme imkânı bulur. Bu sebeple devletler güçlü ve zayıf yönleri ile tehdit ve fırsatlarını bir sentez haline dönüştürülerek iç ve dış politika stratejilerini belirlemelidir.

---

[114] Jean Jacques Rousseau, "Toplum Sözleşmesi", Çeviren Ilgaz, T. Kırmızı Yayınları, İstanbul, 2006, ss.43.

[115] İmanuel Wallerstein, "Tarihsel Kapitalizm", Çeviren. Alpay, N. Metis Yayınları, İstanbul, 2006, ss.40-41.

Realistler'e göre en önemli aktör olan devlet (Hobbes'un deyimiyle Leviathan) için ulusal sınırların güvenliği çok önemlidir. Kendi sınırlarını korumaya çalışan her devlet bu alanda ciddi mücadele vermektedir. Devletlerin kendi coğrafya ve sınırlarını korumak için gerçekleştirdikleri mücadele internetin hayatımıza girmesiyle farklı bir tehdit boyut almıştır. Bu yüzden internetin hayatımıza girmesiyle birlikte dijital dönüşüm araçlarına yönelik siber silahlarla gerçekleştirilecek saldırılara karşı güvenliğin sağlanabilmesi için milli imkanlarla gerçekleştirilecek aarge faaliyetlerine önem verilmesi zorunlu bir hal almıştır.

Mike Howard'a göre; araştırma ve geliştirme, "tehdit ve başarısızlık" ile "fırsat ve başarıları" birbirine bağlamaktadır. [116] Günümüzde bilgisayar ve internet teknolojilerinde yaşanan hızlı gelişme ve (Ar-Ge) çalışmaları sonrasında insanların ve makinelerin birlikte çalışmasıyla elde edilen yapay zekâ, büyük veri ve bulut bilişim kavramları bilinçli kararlar almamızı ve harekete geçmemizi sağlamaktadır. Siber tehdit kavramlarıda bu fırsatların başkalarının eline geçme riskine ortaya çıkarmaktadır. Aynı zamanda; devletlerin e-devlete dönüşüyor olması ve ülkelerin yabancı Telekomünikasyon cihazı ve yazılımı kullanmaları devletlerin siber tehdit unsurlarını arttıran diğer etkenlerdir. e- devlet, e-belediye ve e-demokrasi gibi kavramların geliştiği günümüzde yapay zekâ, toplumları ve yöneticileri yönlendirmede önemli bir görev üstlenmeye başlamış ve dünya çapındaki çatışma sayısı düşmeye başlamıştır.

Özetlemek gerekirse, uluslararası ilişkilerde hem tehditler hem de fırsatlar vardır. Devletler, risk olasılığını azaltmak, tehditleri belirlemek, analiz etmek, etkisini azaltmak ve fırsatları değerlendirmek için dış politika stratejilerini belirler ve rakiplerine karşı mücadele ederler. Günümüzde mücadelelerin gerçekleştiği iktisadi, siyasal, askeri, kültürel ve doğal kaynakların hepsinin küreselleşmesi, küresel asimetrik kavramlarında etkisiyle birlikte güçlü bir aktörün yanlış bir strateji uygulaması halinde nasıl güçsüz bir aktöre yenilebileceğini hem teorikte hem de pratikte göstermesidir.[117] Bu yüzden tehditler düzgün bir şekilde belirlenip önlem

[116]Mike Howard, "Threat or Ossortunity? Managing Risk Through" R&D, Epri Journal, Kasım-Aralık 2015, ss 1-2.
[117]Arreguin-Toft, Ivan, "How the Weak Win Wars: A Theory of Asymmetric Conflict", International Security, Cilt 26, No 1, Yıl 2001, ss.93-128.

alınabilirse fırsata rahatlıkla dönüşebilir. Fakat mutlak güvenlik yoktur. Çünkü insan doğası kötüdür.

İkinci aşama analiz aşamasıdır. Bu aşama tehdide karşı koymada bakış farklılıklarını ortaya çıkarmayı kapsar. Bu aşamayı kısaca açıklarsak;

Geleneksel neorealist bakış devletlerin uluslararası arenada yalnız olduğunu ve çatışmaların kaçınılmaz olması sebebiyle tehditlerin bitmeyeceği, güç ilişkisinin güvenlik ikileminin var olduğu sürece kaçınılmaz olduğunu vurgular. Neoliberaller ise karşılıklı bağımlılık ve işbirliği ile tehditlerin azalabileceği fırsatların ortaya çıkabileceği yönünde bir görüş ortaya koymaktadır.

Bu durumu başka bir şekilde ifade etmek gerekirse, çatışma şartlarında bir aktör diğer bir aktörün istemeyeceği bir şeyi yapması halinde onu cezalandıracağını söyleyerek tehdit eder. Bu durum karşısında gerçekleştirilebilecek davranışı her iki görüş açısından incelersek Realistler tehdidin inandırıcı olduğu ölçüde işe yarayacağını düşünecek ve tehdidi yerine getirmek, yani karşı tarafı cezalandırmak için her türlü maliyete katlanacaktır. Liberaller ise söz konusu maliyetlerin çok yüksek olacağını düşünerek aktörler arasında işbirliği ve karşılıklı bağımlılığı arttırarak çatışmanın ve dolayısıyla tehdidin azalacağını savunacaktır.

Aynı zamanda; çatışmacı güvenlik stratejileri kapsamında diplomatik, ekonomik, askeri vb. her alanda Realizm ve Liberalizm teorilerinin avantaj sağlama mücadelelerine yönelik bakışları farklıdır. Bu yüzden herhangi bir söylemin tehdit olarak değerlendirilebilmesi için eylemin kapsamı, şiddeti, nasıl algılandığı ve etkisi dikkatlice analiz edilmelidir. Günümüzde eylemin kapsamını, şiddetini, nasıl algılandığını ve etkisini dikkatlice analiz edebilmek çok zordur. Çünkü stratejik rekabette vurgu fiziksel alandan bilişim alanına, verilerin toplanıp işlenmesine, ağlara sızılmasına ve psikolojik manipülasyona kaymaktadır. Böylece, "siber uzay" kavramı fiziksel alanı sömürgeleştirerek hayatın her alanının dijital ortama aktarılmasına ve insan faaliyetlerinin "verileşip", "ölçülebilir ve analiz edilebilir" hale gelmesine yol açmıştır.

Üçüncü aşama planlama aşamasıdır. Bu aşama tehdit planlamasında oluşabilecek riskleri ortaya çıkarmayı kapsar. Bu aşamayı kısaca açıklarsak;

Bireysel, ulusal veya uluslararası şekilde gerçekleşebilecek tehditlerde en önemli temel değerler sorunu insan hakları ve temel insani ihtiyaçlar konusunda

nelerin ne kadar ve nasıl tehdit unsuru olarak kullanılabileceğinin bilinememesidir. Çünkü eğer tehdit eden taraf, tehdit edilen taraf istediğini gerçekleştirmezse her türlü askeri, fiziksel, ekonomik veya bir başka şekilde zarar verebilir. Böylece tehdit edilen taraf doğrudan veya dolaylı olarak zarara uğrayabilir. Uygulanacak stratejilerin planlama aşamasında genel kabul görmüş kriterler olmaması sebebiyle bir tehdidin önem derecesi onun ne çeşit bir tehdit olduğuna, tehdidin kim tarafından ve nasıl algılandığı, etkisinin boyutu, meydana gelme ihtimali ve sonuçları gibi soyut kriterlere bağlıdır. Örneğin; 11Eylül terörist saldırılarından sonra ABD'de karar alıcılar Osama bin Ladin'i öncelikli düşman, nefretle dolu, acımasız, alçak ve kalpsiz bir adam olarak algılamışlardır. Bu imge birçok kişi tarafından doğruda olabilir. Fakat bu konuda sosyal psikologlar özellikle yanlış algılama örüntüsüyle ilgilenmektedir.[118] Bu sebeple siber uzaydaki planlama aşamasında algıların risk ve fırsat konusunda öznel, değişken, hassas ve belirleyici olduğunun gözden kaçırılmaması gerekir.

Dördüncü ve son aşama yönetme aşamasıdır. Bu aşamada tehdidi etkileyen unsurlar ortaya konmaktadır. Bu aşamayı kısaca açıklarsak;

Dünya tarihinde hegemon güçlerin yerleri, coğrafyaları, anayasaları, nüfusları, kültürleri, kullandıkları teknolojileri, savaş araçları, savaşta ve barışta güvenlik anlayışları her zaman askeri nitelikli olmakla birlikte tehdidi etkileyen unsurları hep birbirlerinden farklı olmuştur. Günümüzde teknolojinin gelişmesiyle birlikte internetin hayatımıza girmesi sonucunda "bilgi devrimi" gerçekleşmiş ve güvenlik bakışı salt askeri olmaktan çıkarak siber yöntemleri askeri sonuçlar elde edilebilmede önemli bir unsur haline getirmiştir. Siber çağdan önce ulusların kapasitesi insan gücü, donanım, coğrafya, ekonomi ve moral karışımı üzerinden değerlendiriliyordu. Siber uzay ile birlikte tehdit yönetimi tüm bu kriterleri aşarak savaş ve barış dönemleri arasındaki kesin ayrımı sonlandırmıştır. Bu doğrultuda Endütri 4,0 ve Toplum 5.0 gibi gelişmeler çerçevesinde tehdit yönetimini etkileyen unsurları genel olarak açıklarsak;

- ✓ Algılama, aktörlerin öznel yapılarından dolayı bir durumu tehdit olarak değerlendirmeleri önemli bir unsurdur.

[118] E. Taylor Shelley, Letitia Anne Peplau ve David O.Sears, "*Sosyal Psikoloji"*, Çeviren Dönmez, A. İmge Yayınları, Ankara, 2007, ss.505.

- ✓ Geçmiş deneyimleri ve tarihsel çatışmaları aktörlerin güncel tehdit algılamalarını kuvvetlendirmekte ve bu yönde güvenlik politikalarının geliştirilmesini zorunlu kılan unsurlar arasında bulunmaktadır.
- ✓ Günümüz dünyasının belirsizlikler içeren yapısı tehdit oluşma riskini arttıran unsurlardan biridir.
- ✓ Zengin ve güçlü bir aktör ile zayıf ve güçsüz bir aktörün stratejileri, amaç ve hedef bakımından farklı özellikleri içinde barındırmaktadır. Bu durum ise güçlü/zayıf devletlerarasındaki tehdit algılamasında paradoks oluşturmaktadır. Örneğin; ekonomik, askeri, sağlık, enerji ve finans yapıları güçlü olan devletlerin siber alanda gelebilecek tehditlere karşı hassasiyetleri yükselmektedir.
- ✓ Bağımsızlık ve egemenlik gibi bir devleti devlet yapan en temel öğe ve değerleri kapsayan güvenlik hedefleri bir devletin en temel dış politika hedeflerini ve tehdit algı yönetimini şekillendirir. Bu durum siber uzayda da geçerlidir.

Günümüz savaşları artık cephelerde değil, doğrudan bir devletin, milletin kritik alt yapılarını, ekonomilerini ve unsurlarını hedef almaktadır. Bu durumun önüne geçmek içinde sanal dünyada ordular, polisler, istihbaratçılar kurulmuştur. [119] Fakat kurulan bu yapılar tehdit algısını ve güvenlik ikilemini arttıran bir unsur haline dönüşmüştür. Ayrıca, devletin toprak bütünlüğüne yönelik tehditler günümüzde siber sınırlar üzerinden gerçekleşmekte ve sadece askeri değil ekonomik, sağlık, finans, enerji ve sosyal her alanı etkileyebilme kapasitesine sahiptir. Örneğin Covid-19 ile başlayan sağlık tehdidi tüm dünyayı etkileyerek siber uzayın gelişmesine katkı sağlamıştır. Kısaca bu süreci açıklarsak;

Çin'in Wuhan kentinde 2019 yılının sonlarına doğru ortaya çıkan ve Covid-19 adı verilen hastalığa yol açan koronavirüs pandemisi, tüm dünyaya hızla yayılırken, milyonlarca insana bulaşarak yine milyonlarca can kaybına sebep olmuştur. Dünya sağlık örgütü bu salgını pandemi olarak ilan etmiş ve bu virüsten korunmak için tüm ülkelere büyük görevlerin düştüğünü belirtmiştir. Ülkeler de vatandaşlarını korumak ve can kayıplarını önlemek için tedbir olarak en başta sokağa çıkma yasakları

[119] Ramazan Kurtoğlu, a.g.e ss. 108

uygulamıştır. Bu yasaklarla birlikte insanlar evlerinde çalışmaya, eğitimlerini online almaya, toplantılarını sanal ortamda gerçekleştirerek tüm ihtiyaçlarını internetten almaya başlamıştır. İnternetin bu denli kullanılmaya başlanmasıyla birlikte siber güvenliğin önemi dahada artmıştır. Koronavirüs salgını küresel olarak yayılırken [120] salgının yarattığı yeni zorluklarla nasıl başa çıkabileceği konusunda McKinsey uzmanları tarafından yapılan araştırmada tek bir kilit alanda standartları korumanın zorlaştığına değinilmiştir.[121]

Yaşanan bu süreçte milyonlarca insan evden çalışmaya geçtikçe, bilgisayar ağları üzerindeki yük arttı ve bilgisayar korsanlığına karşı güvenlik açıkları ortaya çıktı. Bu yüzden bilgi güvenliği görevlileri (CISO'lar) ve ekiplerinin iki acil önceliği oluşmuştur. Bunlar; büyük çapta evden iş düzenlemelerini güvence altına almak ve hacimler arttıkça tüketiciye dönük ağ trafiğinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumaktır. Bu kapsamda; bilgi güvenliği görevlileri pandemiye yanıt vermek için iki önceliği dengelemek zorunda kalmıştır. Bunlar yeni siber tehditlere karşı koruma ve iş sürekliliğini sağlamadır. Bunun yapılması için ise 4 stratejik ilkenin sağlanması gerekmektedir. Bu ilkeler kritik işletim ihtiyaçlarına odaklanma, güvenlik ve teknoloji risklerini yönetmeye yönelik test planları, yeni siber tehditlerin izlenmesi ve korumanın iş sürekliliği ile dengelenmesidir.[122] Tüm bu anlatılanlar ışığında böyle çeşitli ve bazende birbiriyle rekabet eden ihtiyaçları bir kerede ele almak kolay değildir. Çünkü bu yeni çatışma alanında ortaya çıkan savaşın ana silahları belirli bir zaman ve verileri yok etme veya yeniden yazma amacıyla yazılıma zarar vermek üzere programlanmış mantık bombaları ve bilgisayar virüsleridir.[123] Aynı zamanda tehdit olarak görülen bu silahlar temel zorluklar arasında düzenlemeleri, bulutun benimsenmesini, sayısallaştırmayı ve yetenek

[120]Worldometers, "Covid-19 Coronavırus Pandemıc", 11 Nisan 2020, https://www.worldometers.info/coronavirus/ ET.11.04.2020.

[121] Aaron De Smet, "Our Best İdeas, Quick And Curated", McKinsey & Company, 10 Nisan 2020, https://www.mckinsey.com/~/media/McKinsey/Email/Shortlist/83/2020-04-10.html?hlkid=07a7b799568a4ce28798fa2250e79858&hctky=11508467&hdpid=fc2bbd7a-3c43-4a4e-976e-19849ec0222c ET.11.04.2020.

[122] Jim Boehm, James Kaplan ve Nathan Sportsman, "Cybersecurity's Dual Mission During The Coronavirus Crisis", McKinsey & Company, Mart 2020, https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis?cid=other-eml-shl-mip-mck# ET.11.04.2020.

[123] Lopamudra Bandyopadhyay, "Cyber-Security Threats, Information Warfare and Critical Infrastructure Protection", Global İndia Foundation, ss.1-14 https://www.globalindiafoundation.org/Cyber.pdf ET. 07.02.2021

boşluğunu da etkiler. [124] Örnek vermek gerekirse COVİD-19 krizi de her şeyden önce insani bir sorundur. Bu yüzden daha güçlü teknoloji kontrolleri arttıkça birçok insanın hissettiği ek stres onları sosyal mühendislik saldırılarına daha yatkın hale getirecektir.

Tüm bu anlatılanlar ışığında yeni dönemin bir küçük geçiş aşaması olarak görülen evden çalışma protokolü başladığından beri kişisel bilgisayarlara yönelik gerçekleşen siber saldırılarda da patlama gerçekleşti. Bunun en güzel örneğini Hindistan'da ulusal siber güvenlik ajansının ülkede COVİD-19 salgını sonrasında evden çalışmanın başlamasıyla birlikte siber saldırıların sayısında bir artış yaşandığına yönelik sözlerinde görebiliriz.[125] Bu yüzden küresel olarak kapsamlı bir siber güvenlik sınırının oluşturulması için düzenleyici, denetleyici, kural koyucu ve uygulayıcı bir üst otoritenin oluşturulması şarttır. Çünkü küreselleşme ve teknolojik gelişmelerle birlikte günümüzde artık sadece devletler değil aynı zamanda devlet dışı örgütler ve bireylerde ciddi tehdit unsuru olarak ortaya çıkmıştır. Böylece, devletler artık geleneksel yöntemlerdeki gibi tehdit süreçlerinde tekel bir konuma sahip değildir. Bu nedenle güvenlik ihtiyacı ve tehdit unsurları daha karmaşık ve zor bir hal almıştır.[126]

C) Siber Uzayda Çatışma Kavramı

1.7. Siber Çatışmanın Evreleri

1.7.1. Siber Çatışmalara Yönelik Felsefi Yaklaşım

Teknolojiler her zaman bir değiş tokuş yaratarak topluma yeni bir şey verip aynı zamanda o zamana kadar ki önemli görülen şeyleri de geri almıştır. Bu sebeple günümüzde çok önemli bir kavram olarak ortaya koyduğumuz siber uzay kavramını geçmişten ayrı tutulamayız. Hep bir bağımlılık ve bağlantı vardır. Geçmiş ve gelecek

[124] Report, The Cybersecurity Posture Of Financial-Services Companies: IIF/McKinsey Cyber Resilience Survey, McKinsey Company, Nisan 2020, https://www.mckinsey.com/business-functions/risk/our-insights/the-cybersecurity-posture-of-financial-services-companies-iif-mckinsey-cyber-resilience-survey?cid=other-eml-shl-mip-mck, ET.11.04.2020.

[125] PTI, Covid-19: Cert-In Flags Spurt In Cyberattacks On Personal Computers Since "Work From Home" Protocol Began, Yeni Delhi, 27.03.2020, https://www.deccanherald.com/national/Covid-19-cert-in-flags-spurt-in-cyberattacks-on-personal-computers-since-work-from-home-protocol-began-818277.html ET.09.04.2020.

[126] Cha, Victor D. Globalization and the Study of International Security, Journal of Peace Research, Cilt. 37, No. 3, 2000, ss. 391-403.

birbiriyle uyumlu olmak zorundadır. Birinin kaybı bir diğerinin kazancını doğurur bu da aslında uluslararası sistemin anarşik yapısının gerçeğidir. Bu yüzden rakipler ve düşmanlar olmak zorundadır. Örneğin; Alfabe matbaadan, matbaa telgraftan, telgraf telefondan, telefon ise bilgisayardan ayrı tutulamaz. Hep bir öncekinin kaybetmesi öbürünün kazancını doğurmuştur. Devletler de hayatları boyunca güvenlikleri için bu sürece ayak uydurmak zorunda kalmışlardır.

Teknoloji felsefesinin tarihçesi antik yunan felsefesine kadar uzanmaktadır. Tarihçiler tarihi incelerken keşif ve icatlara göre dönemlere ayırmıştır. Sabanın bulunması, tarım dönemini, buharın bulunması sanayi dönemini, bilgisayar ve internetin bulunması da bilginin hâkim olduğu dönemi başlatmıştır. Yani, Teknoloji ve bilim değişimin temel faktörüdür. Teknolojik olarak her ilerleme ve girilen her dönem, yapıcı ve yıkıcı unsurları içinde barındırmaktadır. Aynı zamanda, geçilen her yeni dönemde keşfedilen araçlar sayesinde dönemin tüm dinamiklerini değiştirmiştir. Örneğin; göçebe yaşamdan sonra yerleşik topluma geçilen aşamada tarımda kullanılan araç ve gereçlerin keşfi, tarımı kolaylaştırmıştır. 18. yüzyıl sonunda sanayi devrimiyle birlikte bilimsel ve teknolojik gelişmeler yaşanmış bunun sonucunda da makinelerin kullanımı yaygınlaşmıştır. 19. yüzyıldaki problem bilgi kıtlığı içindeki bir kültürde yaşayıp bilgiye ulaşma çabası içinde olmamızdı. Fakat 19. yüzyıl içerisinde özellikle 1840'dan itibaren yaklaşık yüzyıllık bir süreçte fotoğraf ve telgrafla başlayan süreç televizyon ve cep telefonuyla devam ederek zaman, mekân ve biçim sınırlarını çizmeye başlamıştır. Son aşama bilgi devrimi olarak gördüğümüz internetin hayatımıza girmesiyle gerçekleşmiştir. [127]

"Bilgi Devrimi" ile birlikte siber uzay bilgi ile dolu insanlar ve devletler yaratmıştır. İnsanların ve devletlerin bu bilgiyi nasıl kullanacaklarını bilememesiyse güvenlik riskini ortaya çıkarmıştır. Aynı zamanda kişisel özgürlükleri yok etmiş ve devleti daha egemen ve güçlü bir hale getirmiştir. Günümüzde yaşanan bu güvenlik tehdidinin altında yatan asıl sebep teknolojik olarak yaşanan tüm gelişmelerin insansız çözümler üretmek üzerine oluşturulmasıdır. Günümüzde gelişen yapay zekâ ve robotlar insanlarla beraber yaşamak zorundadır. Siber güvenlikte en önemli ve kritik halkayı da insanların oluşturması bu alandaki tehdidi daha da arttırmaktadır. Çünkü siber-fiziksel sistemlerin hüküm sürdüğü sanal dünya ile gerçek dünya

[127]Taner Altınok ve Haydar Çakmak, "Suç, Terör, Savaş Üçgeninde Siber Dünya", Barış Platin Yayınevi, Ankara, 2009, ss 6-16.

beraber işlemek zorundadır. Aynı zamanda Nesnelerin interneti (LOT) ile birlikte kullanım alanı ve kullanıcı sayısı her geçen gün artarak devam eden internet çağımızı domine eden ana araç konuma gelmiştir. Bu doğrultuda; Siber Güvenlik, Siber-Fiziksel Sistemler, Bulut Teknolojileri, Akıllı Fabrikalar, Nesnelerin İnterneti, Yapay Zeka, İnternet Servisleri, Öğrenen Robotlar, Büyük Veri, Sanal Gerçeklik ve 3 Boyutlu Yazıcılar gibi yüksek teknoloji içerikli bileşenler siber uzayın belirsizliğiyle birleşince korkuyu, korkular tehdidi, tehdit ise güvenlik riskini ortaya çıkarmaktadır. Güvenlik riski sonucunda oluşan ittifak, caydırıcılık, kurumsallaşma ve işbirliği gibi kavramlarda savaş kavramının özündeki örnek çatışmaları ortaya çıkarmaktadır. Yani, her yeni teknolojik icat tüm sosyal, kültürel, ekonomik, siyasi ve askeri hayatı etkilediği gibi savaşları da değiştirip dönüştürmüştür. Örneğin; ilkel toplumda savaş aracı olarak taş, tarım toplumunda mızrak, sanayi devriminde silah 1. Dünya Savaşında büyük savaş araçları ve otomatik makineli silahlar, 2. Dünya Savaşında nükleer silah ortaya çıkmışken günümüzde de bilgisayar ve internettir.

Üretimde robotların insanların yerini aldığı, dijital ağ sistemlerinin sadece iletişimi değil tüm bir yaşam tarzını değiştirmekte olduğu günümüzde siber uzayda yaşanan sınıf ve aktör mücadelesini anlamak önemli bir durum haline gelmiştir. Nick Dyer-Witheford de Marksizmi yorumlayarak bugünün dünyasında Marx"ı ve Marksizmi yeniden anlamaya ve anlamlandırmaya çalışmıştır. Nick Witheford Dyer'ın Marksist bakışında; 21. yüzyıl kapitalist sisteminde enformasyon devriminin internetle birlikte hayatın her alanına girdiğine değinmiştir. Dyer'a göre gündelik hayatımızda kesintisiz bir şekilde hızlanan teknolojik değişiklikler bilgisayardan, telekominikasyona, biyoteknolojiden askeri silah teknolojilerine kadar her alanı etkisi altına almıştır. Enformasyon devriminin bu denli yükselmesi de Marksizm'i daha da geri plana atmıştır. Nick Witheford Dyer'e göre; günümüzde yaşanan enformasyon çağında kullanılan bilgisayar ve Telekomünikasyon gibi özgürlük araçları anti-marksizmi kesin olarak haklı çıkaran ve sınıf çatışması kuramını temelsiz bırakan yani '' var olan sosyalizmin'' sonudur. [128]

Peki, Siber teknoloji çağını Marksist bakışla anlayabilmek için bu tespit ne kadar doğrudur. Yâda yeterli midir? Günümüzde insanlar ve devletler bilgisayar ve Telekomünikasyon gibi teknolojiler sayesinde artık özgür mü? Yoksa daha da mı

[128] Nick Witheford Dyer, "Siber Marx Yüksek Teknoloji Çağında Sınıf Mücadelesi", Çeviren Çakıroğlu, A. Aykırı Yayıncılık, İstanbul, 2004 ss.24-48.

bağımlıdır? Yani dijital verilere gizlice ulaşarak aktaran, işleyen, depolayan ve dağıtan teknolojilerle birlikte siber savaş, siber saldırı, siber terörizm gibi kavramların çıkması aslında bu özgürlüğün var olmasının mı yoksa gerçekleşememesinin mi bir sonucudur? Ya da ideolojik rekabetin yok olmasına karşın, siber rakiplerin artması dünyayı siber savaşa sürükleyecek midir? Beşinci boyutla birlikte varlıklar, hafıza ve bilgisayar zamanı karşılığında emek ürünlerini takas ederek '' bir tür serbest piyasa tarzı içinde'' yaşamlarını sürdürdükleri anarşik bir yapıya dönüşmemiş midir? Ya da aktörler siber uzayda var oluşlarını sürdürmek için ne değer üretmelidir? Siber uzayda başarılı(sız) olana ne olacaktır?

Frankfurt Okulu temsilcilerinden Max Horkheimer, Theodor Adorno ve Herbert Marcuse'nin geliştirdiği ' eleştirel kuramın' temel savu şuydu: bir zamanlar insanlığın yoksulluk ve batıl inançtan kurtuluşu için güçlü bir kaldıraç olan teknolojik akılcılık şimdi baskıcı olmuştur. Aydınlanma döneminde araçlar amaçları kendilerine bağlı kılmış, doğa üzerindeki tahakküm insan üzerine dönüşmüştür. Bu yüzden; Frankfurt Okulu bilim ve teknolojiye eleştiri yöneltmiştir. Bu eleştiriye göre de 1970'ler ve 1980 ler de enformasyon devrimi yoğunluk kazanırken Marksizm güç kaybetmiştir.[129] Marx'ı yeniden keşfetme amacında olanların iddialarına göre; Teknolojik gelişmelerle birlikte emek süreci bilgisayarlaşmıştır. Siber uzayda gerçekleştirilen siber saldırılar vasıtasıyla elde edilen istihbaratlar sonucunda, aktörler diğer aktörlerin harcadığı arge maliyeti ve emeği izinsiz kullanmaktadır. Böylece siber saldırılar sonucu oluşan emek hırsızlığı ile Marx'ın emeğin istismarı fikriyle aynı çatışma ve mücadele gerçekleşmektedir.

1.7.2. Siber Teknoloji Çağının Tarihsel Gelişimi

Tarihçiler tarih öncesi devirleri teknolojiyi kullanma araçlarına göre isimlendirirler. Örneğin; Yontma taş devri, cilalı taş devri ve maden devri gibi. Tarihsel devirleri de dünyanın kaderini ve geleceğini değiştiren ve şekillendiren olaylarla isimlendirmektedirler. İlk çağ yazının bulunması, yeniçağ İstanbul'un fethi, yakınçağ Fransız ihtilali ve 20. yüzyıldan günümüze olan çağ ise İnternet'in bulunmasıyla başlayan bilişim çağıdır.

Alvin ve Heidi Toffler birlikte yazdıkları War and Anti-war, survival at the down of the 21 century adlı kitaplarında; dünyada birbirinden farklı ve aralarında

[129] Dyer N.W. Çeviren Çakıroğlu. a.g.e ss.73

çatışma potansiyeli olan üç medeniyet seviyesi olduğunu belirtiştir. Birinci grup toprağa bağlı olan tarım devriminin ürünü ve hammadde kaynaklarını, ikinci dalga sanayi devrimi makinelerin icadı ve ucuz işçilik, toplu üretimi içine alıyordu. Üçüncü dalga ise ülkeleri bilgi, yenilik, teknoloji, internet gibi değerleri temel almaktadır. [130] Bu son dalgayla birlikte İnternet, zaman ve mekân algısını değiştirmiş ve insanlarda algılama, düşünme, öğrenme ve farkındalık biçimlerini değiştirmiştir. Ayrıca internet birden bire ortaya çıkmış bir icat değildir. Öncesi vardır. İnternet en temel manada bilgisayar ile kullanılan, saklama kapasitesi olan, dünya sınırlarını ortadan kaldıran, hayatın her alanını şekillendiren ve dönüştüren, haber ve medya sektörünü etkileyen, ulusal ve uluslararası savaşları etkileyen ve iletişimin kolay, hızlı ve ucuz olmasını sağlaması amacıyla kurulan bir icattır. [131]

Bu icadın ortaya çıkması ve hızla yayılmasıyla birlikte küresel çapta beş husus değişmiştir.[132]

- ✓ Ülke sınırları ortadan kalkmış
- ✓ Haber ve basın sektörü değişmiş
- ✓ Finans sektörü ve ticari ilişkiler değişmiş
- ✓ Milli ve milletler arası siyaseti etkilemek dönüşmüş
- ✓ Milli güvenlik ve istihbarat kavramı değişmiştir.

Bu değişimler ise yeni sorunları ve bu sorunları ortadan kaldırmaya yönelik yeni strateji ve taktikleri ortaya çıkarmıştır. Bu çerçevede; R.C. Molander ve Andrew S. Riddle tarafından günümüzde aktif olarak yaşandığı belirtilen Stratejik enformasyon savaşı altı başlık altında ele alınmıştır. [133] Bunlar;

- ✓ Bilgi teknolojilerinin maliyetinin düşüklüğü
- ✓ Geleneksel sınırların geçerli olmaması
- ✓ Devlet dışı unsurlarında yeri ve işlevinin olması
- ✓ Yeni bir stratejik istihbarat modeli sunması

[130]Alvin ve Heidi Toffler, "21. yüzyılın Şafağında Savaş ve Savaş Karşıtı Mücadele", Gençlik ve Sabah Kitapları, İstanbul, 1994, ss.47-50.
[131]Tolga Arıcak, "Siber Alemin Avatar Çocukları İnternet ve Gençlik İlişkisinin Bugünü ve Geleceği", Remzi Kitapevi, İstanbul, 2015 ss. 13-30.
[132]Ramazan Kurtoğlu, a.g.e ss.17.
[133] Ümit Özdağ, "İstihbarat Teorisi", Kripto Yayınları, Ankara 2018, ss.207.

- ✓ Taktik ve saldırıların anlaşılmasının zorluğu
- ✓ Tarafların birbirinden bilgi gizlemesinden dolayı ittifak oluşturmanın zorluğu

Peki; İnternet iyi bir şey mi? Yoksa kötü bir şey mi? Diye sorduğumuzda içinde olumsuz etkileri barındırıyor olmasına rağmen günümüzde artık internet yaşamın öyle bir parçası haline gelmiştir ki onsuz bir yaşam sürmek imkânsız hale gelmiştir. Aynı zamanda internetten sonra bilişim sistemlerinin ortaya çıkmasıyla birlikte hissedilen Siber güven(siz)lik tehdit ve riskleri bu yeni alanın oluşmasının en önemli sebebidir. Kısaca bu sebeplerden bahsedersek;

- ✓ Gizli verilerin düşük maliyetle, daha az personelle kısa sürede deşifre edilmesi,
- ✓ Toplumsal yapı ve kimliklere ilişkin algı oluşturması,
- ✓ Ülke ekonomisinin zarar görmesi,
- ✓ Alt yapı sisteminin çökmesi,
- ✓ Çevresel problemlerin ortaya çıkarılması,
- ✓ Uygulama kolaylığı,
- ✓ İleri teknoloji gerektirmemesi,
- ✓ Tespit edilebilme ve kimlik ayırt edile bilinmesinin zorluğu,
- ✓ Muhtemel hedeflerin sayısı ve çeşidinin çokluğu,
- ✓ Uzaktan yapılabilme imkânı sağlaması,
- ✓ Siber saldırıların çekiciliği sebebiyle medyada yer alarak halka ulaşma ve propaganda yapma imkânı bulmaları,
- ✓ İdeolojik bir silah olarak kullanılabilmesi,
- ✓ Yanlış bilgilendirme ile kamuoyunu yanıltma,
- ✓ Kritik alt yapılara gerçekleştirilecek bir saldırı sonrasında maddi ve manevi ciddi kayıplar verdirebilme gücü,
- ✓ İstihbarat faaliyetiyle bilgi çalımı ve verilerin değiştirilmesi
- ✓ İnternete bu kadar bağımlı dünyada ona erişimi kaybetme korkusu
- ✓ Soğuk Savaş iki siyasi ideoloji arasındaki ittifak anlaşmaları ve güvenlik ikilemlerini içeriyordu. Siber savaş ise kamu, özel, devlet, kurum ayrımı yapmaksızın tüm dünyayı içine almaktadır.

- ✓ Ağın boyutu fayda ile doğru orantılı iken ağ güvenliği ile genellikle ters orantılıdır. Diğer bir deyişle ağ ne kadar büyük olursa, daha fazla fayda olurken daha fazla güvenlik sorunu oluşturması vb.dir.

1.7.3. Siber Uzayda Çatışmanın Evreleri[134]

Uluslararası ilişkilerin doğasındaki çatışma olgusu ve bunun beraberinde getirdiği güvenlik çalışmaları tarihin her döneminde dönemin teknolojik koşullarıyla birlikte yeniden şekillenmiştir. Bu sebeple her çalışma çatışmanın evrelerini farklı şekilde örneklendirebilir. Bu tezin asıl konusunun siber uzay olması sebebiyle bu çalışmada çatışmanın evreleri siber uzayın geçmişten günümüze gelen ve günümüzde aktif olarak kullanılan güvenlik alanlarını kapsayacak şekilde oluşturulmuştur. Ayrıca, siber dönemi evrelere ayırırken; internetin, bilgisayarın ve dijitalleşmenin yayılmasıyla birlikte gerçekleşen siber kavramlarla oluşan çatışmalar, rekabetler ve güç mücadelelerine odaklanılmıştır. Bu doğrultuda günümüzde yaşanan bu yeni sürece gelene kadar internet erişimi ve içerik düzenlemesini kapsayan siber uzay yönetmeliğinin 4 aşaması bulunmaktadır.

- **Aşama 1: Açık Müşterekler (1960'lar - 2000)**

Siber uzayın bu dönemi açık ortaklıklar dönemidir. Bu ilk dönem ağın gelişimi ve düzenlemesi ile ilgili baskın teorilerin geliştiği dönemdir. Ayrıca bu dönem; internet'in kendisinin ayrı bir alan olarak görüldüğü "siber" kavramın ortaya çıkışını simgeler. Açık müşterekler sürecini ayrıntılı bir şekilde incelediğimizde şu hususları belirtmemiz gerekmektedir.

2. Dünya Savaşı sonrasında uluslararası sistemde oluşan gerginlik, korku, tehdit ve çatışma süreci iki kutuplu bir yapı olan Soğuk Savaş dönemi olarak yaşanmıştır. "Yalta'dan Malta'ya" mottosu ile özdeşleşen bu dönemi 1990'lardan sonra Soğuk Savaş'ın bitmesi, SSCB'nin dağılması, Berlin Duvarının yıkılması gibi uluslararası sistemde yaşanan köklü siyasal değişimler ile birlikte küreselleşme ve serbest piyasa ekonomisinin yayılması gibi ekonomik değişimler izlemiştir. Bu dönemde teknolojideki yaşanan hızlı gelişmeler ise modern dönemde yeni tehditlerin ortaya çıkmasına, mevcut tehditlerin de şekil değiştirmesine yol açtı. Bunun yanında

[134] Ronald Deibert, John Palfrey, Rafal Rohozinski, ve Jonathan Zittrain, "Access Contested: Security, Identity, and Resistance in Asian Cyberspace", The MIT Press, Cambridge, 2012, ss.5.

uluslararası sisteme devlet dışı aktörler ve askerî olmayan tehditlerin de dâhil olmasıyla güvenlik ihtiyacı çok boyutlu bir hâl almıştır. [135] İnternetin ortaya çıkmasıda bu çok boyutlu yapıyı daha da güçlendirmiştir. İnternetin kuruluşunda en önemli dönüm noktası ise arpanetle gerçekleşmiştir.

ARPANET'in kurulmasıyla birlikte dünya çapında ağ(World wide web-www) oluşumuna giden bilgisayarların birbirine bağlanması süreci hızlanmış ve 1981'de ilk internet protokolü kurulmuştur. 1989'da ise www kavramı ortaya konmuştur. 1990'da gerçek anlamda internet hiper metin transfer protokülü (hyper-text transfer protocol-http), İnternet Explorer ve Netscape kurulmuştur.

Bu kadar büyük miktarda verinin organizasyonu konu haline geldiğinde ise alan adı sistemi(Domain Name System- DNS) gibi teknik çözümler geliştirildi. Güvenlik sorunlarının oluşmasıysa savunma veri ağı(defense data network ve network information center) kurulmasına yol açmıştır. 1992'de savunma dışında halkın erişiminin açılmasıyla birlikte ABD savunma bakanlığı internete desteğini çekmiştir. Böylece DARPA (Defense Advanced Research Projects Agency – İleri Savunma Araştırma Projeleri Ajansı) tarafından geliştirilen internet, 1990 yılların başında ticari amaçlı kullanılmaya başlayarak hızlıca tüm dünyada kullanılmaya başlamıştır.

İlk başlarda sadece insanların birbirleriyle iletişim kurması ve bilgi paylaşması amacına sahip olan internet, takip eden yıllarda finans, bankacılık, ticaret, eğitim, sağlık, enerji… gibi pek çok alanda kullanılmaya başlamıştır. Bu yeni oluşum; bilişim sistemleriyle insanların sürekli etkileşimde oldukları sanal bir ortam oluşturmuştur. Böylece özelde insanların genelde ise devletlerin vazgeçilmez alışkanlıklarından biri olarak tarihteki yerini almıştır. Bu gelişim süreci, donanım sektörünü, yazılım sektörünü, elektronik cihaz üreticilerini geliştirip büyütmüştür. Böylece sanal dünya olarak adlandırılan yeni bir dünya ortaya çıkmıştır. [136]

Bu yenidünya 5. Boyut olarak konumlandırdığımız siber uzay boyutunun oluşmasının en büyük sebebidir. Bu ortam her ne kadar sanal olarak adlandırılsa da sonuçları fiziksel olabilmekte ve insanları farkında olarak ya da olmayarak etkileyebilmektedir. Yani siber uzay coğrafyası, toplumun tüm katmanlarını etkileyerek her alanda her şeyi etkileyebilmektedir. Çünkü siber uzay ve siber uzayı

[135] Mehmet Eren. a.g.e ss.20-30
[136]Ahmet Naci Ünal, "Siber Güvenlik ve Elektronik Bileşenleri", Nobel Yayınları, Ankara, 2015

oluşturan katmanlar birey, toplum ve hatta devletlerin güvenlik sınırlarını zorlayabilmektedir. Bu sebeple; 1991 yılından itibaren ticari olarak kullanılmaya başlayan internet birinci evreyi oluşturarak yeni tehditlerin dönüşümünü sağlayan en önemli unsur olmuştur. Her ortamda ve her alanda yaşanan değişim ve dönüşüm süreci sonunda kara, deniz, hava ve uzay boyutlarına ilave olarak "siber uzay" olarak adlandırdığımız beşinci bir boyut oluşmuştur.

Birinci evrede ortaya çıkan internet ile çatışmalarda yaşanan değişimin ilk basamağı oluşmuştur. İnternet kavramının gelişmesiyle birlikte, zaman ve mekân algısı değişmiş ve insanlarda algılama, düşünme, öğrenme ve farkındalık biçimleri yeniden şekillenmiştir. Bu bağlamda her ne kadar internetin ortaya çıkmasını çatışma değişiminin ilk evresi olarak belirtsek de internet birden bire ortaya çıkmış bir icat değildir. Öncesi vardır. Fakat bu dönemle birlikte internet; dünya sınırlarını ortadan kaldırmış, hayatın her alanını şekillendirmiş ve dönüştürmüş, haber ve medya sektörünü etkilemiş, ulusal ve uluslararası savaşları etkilemiş ve iletişimin kolay, hızlı ve ucuz olmasını sağlayarak önemini ve kullanılır lığını arttırmıştır. [137]

Sonuç olarak; yapının ve sistemin işleyişini internetin güçlü yükselişi etkilemiş ve dönüştürmüştür. Böylece; internet'in etki gücü artarak aktörlere görünmezlik yaratmıştır. Ayrıca, güçsüz devletlere güç kazanma imkânı sağlaması, çok kutuplu yapıyı sürdürmesi, ekonomik ve enerji krizleri yaratarak ülkelere risk ve fırsatları bir arada sunması vb. gibi bu yeni durumların ortaya çıkması çatışma kavramının değişmesindeki ilk evrimi ortaya çıkarmıştır.

- **Aşama 2: Erişim Reddedildi (2000-2005)**

2000-2005 arasındaki internet geliştirmenin ikinci aşamasına "Erişim reddedildi" dönemi denir. Bu ikinci dönemde, hükümetler internete laissez-faire yaklaşımıyla yaklaşarak çevrimiçi etkinlikler ve ifadeler geliştirdi.

11Eylül 2001 tarihinde Amerika'da Pentagon ve Dünya Ticaret Örgütü binalarına gerçekleştirilen asimetrik saldırı sadece ABD için değil aynı zamanda küresel sistem için ikinci evreyi fiilen başlatmıştır. Bu olayı başlangıç olarak kabul etmemizin birkaç sebebi vardır. Örneğin; bu tarihe kadar ABD; Nükleer/konvansiyonel en büyük askeri güce sahip, 20. yüzyıl boyunca hep süper

[137] Tolga Arıcak, a.g.e , ss. 13-30.

güç olan ve Soğuk Savaş sonrasında dünyayı kendi idealleriyle şekillendiren bir ülkeydi. Her iki dünya savaşında bile kendi topraklarında böyle bir saldırı görmemiş hegemon bir güçtü. Bu derecede önemli avantajlara sahip güçlü bir aktörün hiç beklemediği bir anda ve sivil bir aracı kendisine silah olarak kullanan küçük bir gruba karşı yaşadığı hezimet büyük bir dev devlet karşısında küçük bir grubun nasıl başarılı olabileceğini herkese göstermiştir. Bu sebeple uluslararası sistemin içinde bulunduğu değişim/dönüşümü bütünsel olarak yansıtabilmemiz için bu olayla hem ABD dış politikası hem de dünya politikası açısından yeni bir dönem başladığını kabul etmemiz gerekmektedir. Bu yeni dönemle birlikte artık terör, ülke ve sınır ayrımı yapmadan her türlü aracı silah olarak kullanabileceğini göstermiş bu durum ise tüm aktörleri tehdit altına alan anarşik yapıyı kuvvetlendirmiştir. Dolayısıyla, 11Eylül saldırısı klasik ulusal güvenlik anlayışının demode olduğunu, güvenlik ve tehdit parametrelerinin değişmesi gerektiğini tüm dünyaya göstermiştir.[138] Aynı zamanda; 11 Eylül devlet dışı aktörlerin devletler kadar güçlü olabileceğini göstermiş ve tehdit kavramını genişletmiştir.[139]

Sonuç olarak; bu evre ile birlikte güvenlik algısı realist bakıştaki gibi sırf askeri olmaktan çıkmış ve küresel politikada gerilimlerin ve uyuşmazlıkların işbirliği ile çözülmesi yönünde alternatif fikirler gelişmiştir. Bu doğrultuda; dünya ekonomisi küreselleşirken paradoksal bir şekilde küçük aktörlerin önemi artmış ve yerelleşme başlamıştır. Aynı zamanda asimetrik ve dengesiz bir şekilde büyüyen ve gelişen küreselleşme süreci bir yandan teknolojik olarak olumlu fırsatlar sağlarken bir yandan da bazı sosyal ve kültürel çatışmalar yaratmıştır. Bu sebeple insanlar küreselleşme rüzgârının kendi öz değerlerinde değişiklik yaratacağı korkusuyla kendilerini tehdit altında görmeye başlamış ve yerelleşme ihtiyacı hissetmiştir.[140]

- **Aşama 3: Erişim Kontrollü (2005-2010)**

2005'ten 2010'a kadar olan dönem "erişim kontrollü" şeklinde gelişen üçüncü aşamadır. Erişim kontrollü evresinden kastımız filtreler, bloklar veya düzenleyici yaklaşımlarla devletlerin etkilerinin arttığı bir dönemi karakterize etmektedir. Bu

[138]Ramazan Gözen, "Uluslararası İlişkiler Sonrası Çoğulculuk, Küreselleşme ve 11 Eylül", Alfa Yayınları, İstanbul, 2004, ss. 161-163.
[139] Andrew Heywood, "Global Politics", Palgrave Macmillan Foundation, Newyork, 2011, ss:19-21.
[140] John Naisbitt, "Global Paradox,Büyüyen Dünya Ekonomisinin Güçlenen Küçük Oyuncuları", Çev, Gül, S. Sabah Kitapları, İstanbul, 1994.

aşamanın en önemli özelliği, geniş bir dizi çeşitli kontrol noktalarındaki mekanizmaların (teknolojik olmayanlar dahil) bilgi ve bilgiye erişimi sınırlamak ve şekillendirmek için kullanılmasıdır. Aynı zamanda bilgisayar ağ saldırıları ve casusluk faaliyetleri ile devletlerin stratejik çıkarlarına uygun çatışmalar bu dönemde gelişmeye başlamıştır.

Ayrıca bu dönemde; otonom bölgelerdeki etnik ayaklanmaları durdurmak için politik açıdan hassas anlarda içerik ve hizmetleri engelleyen filtreleme mekanizmaları hükümetler tarafından aktif olarak kullanılmaktadır. Örneğin; 2009 yılında Çin'in Sincan bölgesinde veya 2011 yılında Mısır rejiminde mübarek rejiminin sonunu getiren ayaklanmalarda hükümetler kayıt, lisans ve kimlik gereksinimlerini kontrol etmek ve oto sansür uygulamak için İnternet'i kapattı[141] Bir diğer olaysa İran'la alakalıdır. 2009'da İran'daki cumhurbaşkanlığı seçimlerini Mahmud Ahmedinejad kazanmıştır. Fakat seçim sonuçlarına isyan eden muhalefet yanlıları cumhurbaşkanlığı seçimlerine şaibe karıştırıldığına yönelik suçlamalar sonrasında 'oyum nerede?' sloganıyla başlayan yeşil devrim kitlesel seferberlik hareketleriyle hızlandı. Protestocuların Tahran ve diğer kent merkezlerinin sokaklarına dökülmesi küresel sosyal ağ siteleri üzerinden ve dünya çapında sivil toplum grupları tarafından yeni teknolojilerle desteklendi. Buna karşılık; Yeşil Devrim sırasında İran siber ordusu muhalefet Web sitelerine ve devrim destekçilerine saldırmaya başladı. [142] Son örnek ise 2007 yılında halk arasında başlayan ve 2010 da tekrar alevlenen Burma'daki "Safran Devrimi" olaylarıdır. İnsan hakları örgütleri tarafından sürekli olarak dünyada insan hakları ihlalinin en fazla yapıldığı baskıcı rejimlerin başında gösterilen Burma'da, ifade özgürlüğü ve evrensel insan hakları sistematik olarak reddedilmektedir. İktidardaki askeri cunta, ülkede yaşanan silahlı çatışmalar hakkında bilgi iletişim teknolojilerini kullanarak muhalefet gruplarının mesajlarını dünyaya yayması ve hükümete meydan okumasını engellemek için siber alan ve sistemi filtreleyerek sansürlemiştir.[143]

---

[141] Rebekah Heacock, "China shuts down Internet in Xinjiang region after riots", OpenNet Initiative Blog, 06.06.2009, http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots , ET. 23.01.2020.

[142] Hamid Tehrani, "Iran: Cyber Islamic Militarism on the March", Global Voices, 19.02.2010, http://globalvoicesonline.org/2010/02/19/iran-cyber-islamic-militarism-on-the-march ET.23.01.2020.

[143] Committee to Protect Journalists, "Burma ' s Exile Media Hit by Cyber-attacks", 27 Eylül 2010, http://cpj.org/2010/09/burmas-exile-media-hit-by-cyber-attacks.php .ET.23.01.2020.

Sonuç olarak bu vakalar ülkelerin iç çatışmasında, siber uzayın hem bir araç hem de devletlerarasında kontrol, maniple etme, kargaşa çıkarma vb. amaçlarla bir çatışma alanı haline geldiğini gösteriyor. İç çatışmalarda gerçekleştirilen mücadelede muhalefet kurtuluş için hükümet ise bastırmak için siber teknolojiyi bir silah aracı olarak kullanmıştır.

- **Aşama 4: Erişim Yarışması (2010 ve Ötesi)**

2010 sonrası dönemde hükümetlerin iç hukuklarında siber alandaki gücü kullanmaları meşrulaşırken, uluslararası hukukta bu yönde düzenleme girişimleri başlasa da sonuçlanamamıştır. Aynı zamanda devletler uluslararası arenadaki mücadelelerde güçlerini terör örgütleri ve gruplar eliyle yürütmeye başlamıştır. Bunu yapmalarının sebebiyse siber alanda çatışmaların meşru olmamasından kaynaklanmaktadır. Devletlerarasında siber alanda savaşma meşru değildir. Fakat siber ortamda devletler kendi içlerinde siber birimler oluşturmakta veya bu alanda eğitimli profesyonel kişileri yetiştirmek için yarışmalar gerçekleştirmekte olsa da bu faaliyetleri resmi boyuta taşınamamaktadır. Böylece mücadeleler hep suç, terör ve casusluk boyutunda devam etmektedir.

Dördüncü dönemin ana hatlarıyla birlikte ortaya çıkan siber güvenliği sağlama mücadelesinde savunma görevi üstlenecek askerlerin yetiştirilmesi görevi birçok ülkede olduğu gibi ülkemizde de başlamıştır. Bu kapsamda ülkeler kendi içindeki nitelikli, donanımlı ve zeki gençleri ülke savunmasında aktif olarak görevlendirebilmek için ülkemizde de düzenlendiği gibi siber yarışmalar gerçekleştirerek seçmektedir. Böylece siber ortamdaki rekabet ortamında bu seçilen nitelikli personel sayesinde ulusal siber güvenliklerini sağlamaktadır.

Bir diğer yandan son dönemde yaşanan teknolojik gelişmeler sonucunda sürekli gelişen ve genişleyen iletişim ekosistemi ile geniş sosyal veri paylaşımı artmıştır. Ayrıca, nesnelerin internetiyle birden fazla platformdan mobil ağ oluşturularak araç çeşitliliği oluşmuş, yapay zeka ile stratejik kararlar verilir olmuş ve verilerin artmasıyla birlikte "bulutlara" olan güven artmıştır. Siber uzayın gelişimide devletlerin siber kontrol stratejileri oluşturmalarını zorunlu hale getirmiştir. Artık tüm devletler siber uzaya on yıl önce olduğundan çok daha farklı bir şekilde yaklaşmaktadır. Bu yüzden Türkiye'nin de siber alana gereken önemi vermesi gerekmektedir.

Nasıl yirminci yüzyılda Avrupa'da Almanya'nın ortaya çıkışı sisteme karşı bir meydan okuma yaratmışsa, yirmi birinci yüzyılda da internet, bilgi teknolojileri, nesnelerin interneti, yapay zekâ ve bulut bilişim gibi kavramların ortaya çıkışı uluslararası sistemde yeni meydan okumaları, güç mücadelelerini, meşruiyet kavgasını ve rekabeti oluşturmuştur. Asimetrik tehditlerinde etkisiyle birlikte ABD, Çin, Rusya ve İsrail gibi ülkeler "Siber" yoluyla birbirlerine karşı caydırma stratejilerini ve taktiklerini kullanmaya başlamıştır. Çünkü bu son aşama 2. ve 3. evrede gelişen asimetrik tehdit kavramı ile siber uzayın etki güçlerinin birleşmesiyle oluşan yeni siber silah tehditlerine karşı savunma amacıyla oluşmuştur. Aynı zamanda bu son aşamada; asimetrik tehditlerle birlikte siber yöntemlerin birlikte kullanılması çatışmaların yaşamın her alanına damga vurmasına, siber orduların kurulmasına ve çatışma örneklerinin yaşanmasına yol açmıştır. Son olarak dördüncü evrede belirleyici olan bu üç hususu kısaca açıklarsak;

İlk husus çatışmaların yaşamın her alanına damga vurmasıdır.Bu durumla birlikte uluslararası politikanın amaçlarının yanı sıra araçları da sürekli değişmiştir. Realist görüşe göre askeri güç, gerçekten önemli olan tek araçtır. Askeri gücün nihai araçları olan maliyet, güç, etki ve kapsam da tarih boyunca sürekli değişmiştir. Günümüzde güç kavramı hala uluslararası politikada önemli bir araç olsa da tek araç değildir. Karşılıklı ekonomik bağımlılık, iletişim, uluslararası kuruluşlar ve ulus ötesi aktörlerin kullanılması bazen güçten daha büyük rol oynamaktadır. Siber uzayın devletler tarafından beşinci boyut güvenlik alanı görülmesiyle birlikte uluslararası ilişkilerdeki güç parametreleri etkilenmiş, teritoryal sınırlar önemini kaybetmiş, devletlerin yanı sıra çok uluslu şirketler ve bireyler aktör olarak yer almaya başlamıştır.

Günümüzde siber uzay ve teknoloji hayatın her alanında kullanılmakta ve tüm sektörleri bir araya getiren çatı görevi üstlenmektedir. Siber uzayın bu yapısı özellikle realist düşünürlerin önem verdiği askeri güç boyutunu ciddi derecede etkilemektedir. Örneğin; uçakları görünmez kılmanın, güdüm teknolojisi ve güdümlü füzeleri rotadan çıkarmanın veya nükleer tesislerde surfujların hareketlerinin yönlendirilmesi, radar vericilerle gönderilen elektromanyetik işaretlerin, hedeften yansıyarak alıcı antene geri dönmesini önlemek gibi bir dizi faaliyet siber uzay kullanarak gerçekleştirilebilmektedir. Siber uzay kullanılarak gerçekleştirilen bir

diğer önemli yöntem ise siber saldırılar vasıtasıyla sistem içindeki tüm bilgilerin ve komuta merkezinin kontrol edilmesidir. Aynı zamanda; siber saldırıların en temel amaçlarından biri olan karıştırma faaliyeti; haberleşme, radar, füze sistemleri, uçak sistemleri, askeri gemi ve denizaltı sistemlerine karşı kullanılmaktadır. Yâda hava harekâtlarında hedeflerin yanıltılmasında kullanılmaktadır. Elektronik aldatma yapmanın temel amacı, elektronik yöntemler kullanarak sahte hedef işaretleri üretebilmektir. Bu askeri araçlara karşı kullanılmasının yanında sivil gibi görünse de milli güvenlik imkânlarını gerektirecek askeri, emniyet ve istihbarat gibi kurumların internet sitelerine veya elektronik ortamda sakladıkları gizli arşivlere yönelikte gerçekleşebilir. Bunların yanında; siber saldırıların politik bir araç olarak kullanımının artması, uluslararası ilişkilerin tehlikeli araçlarından biri haline gelmesine yol açmıştır. Bu yeni araç zayıf bilgi sistemlerine sahip ulus ve ulus dışı aktörleri hem saldırı hem de savunmayı bir arada kullanmalarını gerektiren bir yapıya sürüklemiştir. Böylece bu yeni araç sayesinde zayıf ve küçük aktörler büyük ve güçlü aktörlere karşı askeri olarak konvansiyonel bir savaş yürütmeden düşmanlarına karşı stratejik bir üstünlük kazanabilir bir hale gelmiştir. Bu yüzden; aktörler tarafından kullanılan bu strateji siber uzayın inter disiplin bir yapıda olması sebebiyle çok amaçlı ve konulu bir şekilde birçok sektörü ilgilendiren bir hale dönüşmesine yol açmıştır.

Dördüncü evrede belirleyici olan ikinci husus siber orduların kurulmasıdır. Siber orduların kurulma sürecinde teknolojinin ve internetin yaygınlaşmasıyla birlikte beşinci boyut alanı olan siber uzayın sınırları içerisinde güvenliklerini sağlamak isteyen devletler; ordular kurmakta, bütçeler oluşturmakta ve faaliyetler yürütmektedir. Günümüz bilgi çağında devletlerin kurdukları bu siber orduların hepsinin potansiyel güçleri, çalışma yapıları, tehditleri ve riskleri farklıdır.

Zaten siber orduların kuruluşu ve siber savaş gücünün ölçümü tüm dünyada hızla yayılan bir durumdur. Siber savaşların etkisinin ve sonuçlarının boyutunu ciddiye alan başta ABD, Çin ve Rusya gibi birçok devlet bireysel internetin kontrolünden sanayi casusluğuna, siber savaştan tüm iletişim ağlarının kontrolüne kadar siber ortamın hâkimiyetini kazanabilmek için siber saldırılara karşı savunma ve saldırı timleri oluşturarak siber ordu birimlerini devreye sokmuşlardır. Aynı zamanda bu ülkeler taşeron hackerlar da kullanarak gerçekleştirdikleri saldırılarda

kimliklerini gizlemeye çalışmaktadır. Böylece günümüzde teknolojinin yeni ürün ve hizmetlerle yayılmasına paralel olarak tehdit parametreleri değişmekte ve aktörler bu alanda yukarıda da görüldüğü gibi ciddi faaliyetler gerçekleştirmektedir. Bu faaliyetler siber güvenlik alanındaki zafiyetleri, saldırı yöntemlerini, tehdit aktörlerini ve geliştirilen güvenlik çözümlerini etkilemektedir.

Ayrıca bu ülkeler dışında siber savaş yeteneğine sahip olan en önemli örgüt NATO olarak gösterilmektedir. NATO gibi askeri örgütlenmeler bu yönde faaliyetler ve stratejiler geliştirmektedir. NATO'nun ortak siber güvenlik kurma çabası olsa da bu yeterli değildir. Çünkü her ülkenin kendi ulusal çıkarlarını sağlama maksadıyla kendi özelinde siber stratejileri vardır. Bu kapsamda; yeni bir savaş türü olarak günümüzde yaşanan çatışmalarda ülkelerin ve örgütün siber güvenlik bütçelerine yaptıkları yatırım çerçeevesinde siber güvenliğe verdikleri önem ortaya çıkmaktadır.

Bu yeni savaş yöntemiyle günümüzde askeri yapılanmalarda kullanılan komuta kontrol sistemleri, silah sistemleri, istihbarat, keşif ve gözetleme sistemleri, muharebe sistemleri gibi sistemlerin çoğu elektronik ortamda ve iletişim altyapısı üzerinde çalışması orduların siber tehditlere bağımlılığını arttırmıştır. Böylece söz konusu ortam ve altyapının korunması devletler için hayati bir öneme sahip olmuştur. Çünkü nükleer tesisler, bilgisayar sistemleri, elektrik santralleri ve hava sistemlerini kapatma kabiliyetleri ulusal güvenlik için ciddi tehdit haline gelmiştir. Böylece bir devlet, diğer devlete karşı kendini avantajlı duruma getirmek ve karşı tarafa boyun eğdirmek maksadıyla siber uzay alanını kullanmaya başlamıştır. Bu alan sayesinde karşı tarafın bilgilerini çalmayı, sistemlerini belirli bir süre devre dışı bırakmayı veya tamamen bozmayı hedefleyen siber saldırı kullanabilmektedirler. Aynı zamanda uluslararası ilişkilerde siber uzay kavramı "sınır problemi" olarak adlandırılan sorunla birlikte yaşamaktadır. Bu sınır problemini disiplinler arası politik, ekonomik, askeri, kültürel ve diğer insani ilişkileri de kapsayacak şekilde kavrama bütünleyici olarak yaklaşmamıza yol açmaktadır.

Bir başka açıdan bu son dönemin ikinci önemli aşamasını incelediğimizde "Savaşlar neden ortaya çıkar?" sorusu çerçevesinde siber savaş ile savaş kavramı arasındaki bağı ortaya koymamız için bazı hususlar gerekmektedir. Bunlar; metodoloji içermesi, bilimsellik içermesi, tarihsellik içermesi, geleneksel savaş yöntemlerinde kullanılan taktik ve stratejilere benzerlik göstermesi, uluslararası

ilişkilerin ana teorileri olan realist ve idealist akımların iddialarını karşılaması gibi sebeplerdir. Aynı zamanda bugünü anlayıp yaşadıklarımızı savaş olarak adlandırabilmemiz için geçmiş savaşların taktikleri, stratejileri, politik hedefleri, diplomatik yöntemleri, amaçları, fiziki etkilerini incelememiz gerekmektedir. Bakış ve algı değişmelidir. Yani; savaş dediğimizde sadece konvansiyonel ve nükleer silahlarla yapılan bir çatışma aklımıza gelmemesi gerekmektedir. Klasik tanımlar günümüzde ve gelecekte artık revize edilmelidir. Böylece siber uzayda yaşanan çatışmaları savaş temeline kolayca oturtabiliriz.

Bu çatışmaları savaş temeline oturttuğumuzdaysa ülkelerin bu alanda yaptıkları çalışmaları ve güçlerini ölçebilecek kabiliyetlerin geliştirilmesi gerekir. Siber savaşı ölçerken iki boyutlu düşünmemiz gerekmektedir. Eğer siber savaşı ölçerken dikkate alınması gereken tek şey diğer uluslara saldırma yeteneğini ölçebilecek güç faktörü olursa Amerika Birleşik Devletleri diğer uluslara kıyasla hakim güç olması gerekir. Ne yazık ki siber savaş gücünün gerçekçi bir şekilde ölçülmesi için diğer iki önemli faktör olan savunma ve bağımlılığı da kriterlere koymamız gerekir. Bu kriterde bir ulus ne kadar az kablolu olursa, bağımlılık sıralaması da o oranda artar. Bu yüzden ABD siber savaşa dayanma güçsüzlüğü de aynı oranda artmaktadır. Bu bağlamda "Savunma" kabiliyeti ve "bağımlılık eksikliği" ni birlikte düşündüğünüzde, birçok ülke siber bir savaşta hayatta kalma yetenekleri bakımından ABD'den çok daha iyi bir durumdadır. Bu istatistikler tezimizin dördüncü bölümünde ABD'nin incelendiği kısımda ayrıntılarıyla belirtilmiştir.

Savunma ve bağımlılıktan kastımız siber uzayda şu şekildedir; "Savunma" bir ulusun, saldırı altında, saldırıyı engelleyecek veya hafifletecek eylemleri. "Bağımlılık" ise Ulus'un ne ölçüde kablolu olduğu ve bu durumda savunmasız olabilecek ağ ve sistemlerin sayısıdır. Örnek olarak; geniş bantlı evler, kişi başına akıllı telefon sayısı, kritik altyapılar (elektrik, raylar, boru hatları, tedarik zincirleri) vb. Bu üç faktörün (saldırı, savunma ve bağımlılık) bir araya gelmesiyle ülkelerin güç sıralamaları belirlenmektedir. Saldırı kabiliyeti boşluğu kapatmaz. Bağımlılığımızı azaltmak da imkansızdır. Bu nedenle, boşluğu kapatmanın tek yolu, aktörlerin siber savaş gücü puanını artırmaları ve savunmalarını iyileştirmeleridir.

Dördüncü evrede belirleyici olan son husus çatışma örneklerinin yaşanmasıdır. Dördüncü evreyi oluşturan en önemli aşamalardan biri olan bu çatışma örneklerini incelerken siber uzayda gerçekleşen çatışmaların, uluslararası barış ve güvenliği doğrudan ve somut bir şekilde tehdit ettiğini gözden çıkarmamız gerekir. Tüm devletlerin bağımsızlığını, toprak bütünlüğünü, siber alt ve üst yapılarını, bilgilerine erişimini, alt yapılarına zarar vermeye yönelik saldırıları sonlandıracak bir üst yapı organizasyon kurulamaması halinde de bu anarşik yapının etkisi artacaktır.

İKİNCİ BÖLÜM

SİBER GÜVENLİK VE SİBER UZAY KAVRAMI

2.1. Siber Kavramlara İlişkin Tanımlamalar

Uluslararası ilişkilerde yeni bir savaş alanı olarak kullanılan "siber savaş" kavramına ilişkin teorik tartışmaları gerçekleştirebilmemiz için öncelikle, "siber" ve "savaş" kelimelerini ayrı ayrı tanımlamamız gerekmektedir.

2.1.1. Siber nedir?

Siber, bilgisayar ve ağlarını içeren kavram ya da varlıkları tanımlamak için kullanılır. Siber alan (cyber space) kelimesi de birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır. Yalın olarak Türkçe sözlüklerde yer almayan "siber" kelimesi, sibernetik kavramından türetilmiş olup günümüzde bilişim ve iletişim ağlarının şekillendirdiği uzayı ifade etmektedir. Amerikan Savunma Bakanlığı'nın Askeri Terimler Sözlüğüne göre; siber uzay; dijitalleştirilmiş bilgilerin iletildiği kavramsal olarak Bilgisayar Sistemleri, İnternet ve Telekomünikasyon Ağlarını birbirine bağlayan ve bilgi teknolojileri altyapılarını kapsayan bilgi ortamı şeklinde tanımlamaktadır.[144]

Siber uzay kavramı ilk kez, Amerikalı bilim kurgu yazarı William Gibson tarafından 1982 yılında yayınlanan "Burning Chrome" adlı eserinde kullanılmıştır. Siber uzay, internet ile sınırlı bir alan değildir, "her türlü yazılım, donanım ve iletişim altyapısından meydana gelen, birbirlerine bağlı veya birbirlerinden bağımsız bilgi sistemlerinin oluşturduğu ortamdır". Ülkeler, onların istihbarat örgütleri, silahlı kuvvetler, resmi ve özel kurum/kuruluşlar ile bireysel veya grup halindeki suçlular siber uzayda faaliyet gösteren aktörler olarak karşımıza çıkmaktadır.[145]

---

[144] Department of Defense Dictionary of Military and Associated Terms, Cyberspace and Cyber Counterintelligence, USA, 09.06.2004, ss.138 https://www.cia.gov/library/abbottabad-compound/B9/B9875E9C2553D81D1D6E0523563F8D72_DoD_Dictionary_of_Military_Terms.pdf ET.29.01.2020.

[145] Hasan Çifçi, "Her Yönüyle Siber Savaş", Tübitak Popüler Bilim Kitapları, Ankara, 2012, ss.3.

Joseph Nye'a göre siber kavramı elektronik ve bilgisayarlarla ilgili faaliyetlerdir. [146]Bu doğrultuda siber uzay, günümüzde tüm alanları altına alan bir çatı görevi görmektedir. Siber uzayın sınırları olmayan küresel ağ yapısı herhangi bir devletin, dolayısıyla herhangi bir hukuk düzeninin egemenliği altına sokulmasını engellemektedir. Bu engel ise hangi fiillerin siber suç olduğunu tanımlamak konusunda da uluslararası arenada bir fikir birliğine varılmasını güçleştirmektedir.

Siber uzayın yeni bir çatışma ve hukuk alanı olduğu herkesçe kabul edilmektedir. Fakat bu çatışma hukukunun kim tarafından konulacağı ve nasıl uygulanacağı üzerine uzlaşılamamıştır. Siber uzayın uluslararası ilişkiler sisteminde yeni bir savaş alanı olarak kullanıldığını iddia etmemizin sebebide aslından bundan kaynaklanmaktadır. Belirsizlikleri içeren siber uzayın dayanmış olduğu üç katman vardır. [147]Bunlar; Fiziksel katman; coğrafi ve ağ bileşenleridir. Coğrafi bileşenler; mevcut ağlara bağlı olarak çalışan bilgi sistemlerinin bulunduğu ortamdır. Fiziksel ağ bileşenler, kablolu/kablosuz/optik altyapılar ile bu altyapılara erişimi sağlayan her tür teknik bileşendir. Mantıksal katman; mevcut ağların bağlı bulundukları düğüm noktalarını belirtmektedir. Bu noktalar bilgisayarlar, akıllı telefonlar, gibi her tür bilişim sistemidir. Sosyal katman ise hem gerçek hem de sanal bireylerden oluşmaktadır. Siber uzayı oluşturan bu katmanlar göz önüne alındığında; siber teknolojilerin insanların hayat standartlarını artırdığı, e-sağlık, e-ticaret, e-devlet gibi uygulamalarla insanın günlük yaşantısını kolaylaştırdığı ve bununla birlikte bireylerin, toplumun, kuruluşların ve hatta devletlerin güvenlik sınırlarını zorlayabildiği görülmektedir. İşte bu güvenlik algısındaki değişim ülkelerin toplam kabiliyetlerinin bir göstergesi olan "milli güç" olgusunun da siber uzay ile birlikte yeniden belirlenmesine sebep olmaktadır.

2.1.2. Siber Alan

Siber alan, birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır.

---

[146] Nye J. Nuclear Lessons for Cyber Security? A.g.e ss.19.

[147] Can Kasapoğlu, Siber Güvenlik: Beşinci Boyutu Anlamak, EDAM Siber Politikalar Kâğıtları Serisi Haziran 2017 http://edam.org.tr/wp-content/uploads/2017/10/besinciboyut.pdf ET.16.12.2019.

2.1.3. Siber uzay

Siber uzay, internet ile sınırlı bir alan değildir. Siber uzay dediğimizde iletişim altyapısından oluşan her türlü yazılım, donanım ve birbirlerine bağlı veya birbirlerinden bağımsız bilgi sistemlerinin oluşturduğu ortam aklımıza gelmelidir. Ayrıca siber uzay, günümüzde tüm alanları altına alan bir çatı görevi görmektedir.

2.1.4. Siber Saldırı

Siber Saldırı**,** kişi, askeri, siyasi ve ekonomik amaçlarla şirket, kurum, örgütlerin bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırıları ifade eder. Bu kapsamda siber savaşlardan siber saldırıların en büyük farkı devlet veya devletlere yönelik yapılmamasıdır.

2.1.5. Siber Güvenlik

Siber güvenlik**,** siber ortamda; kişilerin, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür.

Siber Güvenliğin günümüzde bu denli önem kazanmasının temeli 1990'lara kadar gitmektedir. 1990'ların başı geldiğinde düşünürler, tarihçiler ve siyasetçiler," Tarihin Sonu" ve "Medeniyetler Çatışması" gibi kavramlarla Uluslararası İlişkiler disiplinini şekillendirmeye çalışıyordu. Günümüzde tüm bu kavram çatışmaları sonrasında demokrasi, insan hakları, serbest piyasa ve liberalizm hâkim güç kavramları olarak kalmıştı. Teknolojik gelişmeler sonucunda internet, bilgi ve bilişim sektörleri doğmuştur. Böylece artık farklılıklar sadece konvansiyonel alanda bir çatışma unsuru hali olmaktan uzaklaşmıştır. Yani 20. yüzyılda oluşan milliyetçi hareketler, ulus- devlet bölünmeleri, dini ayrışmalar konvansiyonel alandan siber uzay boyutuna taşınmıştır. Böylece bilgisayar korsanları ve hackerlar artık bu alanı doldurarak ciddi terör saldırıları, casusluk faaliyetleri ve suç işlemeye başlamıştır. Örneğin; Ortadoğu'da milliyetçi ve dini gelenekleri kullanan terör gruplarından İşid'in hackerları klasik güçle eş güdüm halinde çalışmıştır. Bu bağlamda, nasıl sanayi devrimi' nin yarattığı büyük değişiklikler tüm dünyayı ve 20. yüzyılın savaş alanını dönüştürdüyse, 21. yüzyılın ilk çeyreğinde gerçekleşen bilişim teknolojileri

ve biyoteknolojilerindeki gelişmeler de siber uzay alanı içinde kullanılan siber silahlarla aktörleri yeni bir savaş alanına dönüştürmüştür. Böylece, yaşanan teknolojik devrimler sonucunda yapay zekâ, büyük veri algoritmaları, biyomühendislik konuları, siber çatışma araçları ile görünür kılınmıştır.

2.1.6. Siber Silah

Siber silahların ne olduğunu tanımlayabilmemiz için öncelikle silah kavramına bakmamız gerekir. İlk olarak silahlar, zarar aracıdır. Zamanın başlangıcından beri, insanlar avı ve birbirlerini avlamak için silah kullanmıştır. Silahlar, bütün bir şehri yok etmekten tek bir kişiyi korumaya kadar uzanır.

Bu tezde silah kavramının alt kümesi olarak gösterdiğimiz siber silahların tanımı üzerine net bir fikir birliği olmasa da; siber silahlar yapılara, sistemlere fiziksel, işlevsel veya zihinsel zarar vermek veya tehdit etmek amacıyla kullanılan veya kullanılmak üzere tasarlanmış bilgisayar kodunu veya canlı varlıkları içerir. Kısaca; siber silahlar kod kaynaklı cihazlar ve düşük potansiyel araçlardan spesifik yüksek potansiyel silahlara kadar geniş bir yelpazeyi kapsar. Bu ayrım, siber güvenlik konusunun önemine yönelik bu tezde geliştirdiğimiz hipotezimizi desteklemektedir. Bu sebeple bir siber silahın yıkıcı hedeflerinin potansiyeli artarken riskleri azaltma yönünde uygulamalar geliştirmesi şarttır. Zaten son birkaç yıldır, saldırgan siber silahların uluslararası askeri çabaların bir parçası olarak ön plana çıkması yaşanan çatışmaların savaş olarak tanımlanmasını kolaylaştırmıştır.

Siber silahların geniş bir yelpazeye yayıldığını vurgulayan Thomas Rid ve Peter McBurney'e göre; düşük potansiyel 'siber silahlar' paintball silahlarına benzemektedir. Bu silahlar gerçek silahlarla karıştırılabilir, kolayca ve ticari olarak bulunabilir, birçok kişi tarafından vurmak için kullanılabilir.[148]

2.2. Toplumda ve Endüstride Dijital Dönüşüm Süreci

Değerlerin hızlı sayısallaştırılması, internetin finansal potansiyeli ve kuruluşların dünya çapında dijital teknolojiye olan artan bağımlılığı sonucunda hackerler vasıtasıyla mafya ve terör örgütü gibi grupların bu alana ilgisi arttı. Kırılgan mülkiyet hakları, zayıf devlet, verimsiz polis ve zayıf siber suç yasalarıda

[148] Thomas Rid ve Peter McBurney, "Cyber-Weapons", The RUSI Journal, Cilt.157, No.1, Yıl 2012, ss.6-13.

dijital dünyadaki bu saldırılara verimli bir ortam yaratmıştır. Ayrıca ekonomik fırsatların mevcudiyeti, hedef ağlara yönelik önem ve kritiklik, değerlerin dijitalleşmesiyle savunmadaki zayıf mekanizmaların bu ortama etkiside siber çatışmalara yol açmıştır. Böylece örgütlü suçlar ve internet arasındaki gelişen etkileşimle birlikte dijital dünyanın güvensizliği artmıştır.[149]

Tehdit algısının bu kadar arttığı bir dünyada neoliberal kurumsalcıların belirttiği gibi resmi kuralları uygulayacak meşru ve düzenleyici bir kurum oluşturulmalıdır. Oluşturulacak düzenleyici bu kurum açık düzenleyici süreçlerden oluşmalıdır. Örneğin; (hukukun üstünlüğünün gücü)ne dayalı kural belirleme, izleme ve yaptırım faaliyetleri (yargı tahkiminden yararlanarak daha fazla siber saldırıların ortaya çıkmasıyla) ilişkili süreçleri içermelidir. Çünkü tüm dünyada etkili olan saldırılar ve organize siber suçlar az sayıda ya da hiç yasa bulunmayan ülkelerden başlatılmaktadır. Örneğin, bir Filipinli bilgisayar korsanı 2000 yılında bLove LetterQ virüsünü başlattığında, tahmini olarak ABD'ye 4-15 milyar dolar arasında zarar verdi. Ancak bilgisayar korsanının yargılanması veya zararların giderilmesi için bu tür suçları yasaklayan yasalar olmaması sebebiyle ABD hükümeti bu zarara karşı hiçbir şey yapamadı.[150]

Bir diğer yöntemse milliyetçiliğe ve dine ek olarak bilgisayar korsanlarının çıkarlarının küresel kapitalizme karşı mücadelede aktif rol oynamasıdır. Etnik köken, din, dil ve coğrafyaya dayalı bu tür hackerların büyük çokuluslu şirketlerin ağlarına saldırması muhtemeldir. Çünkü internet, bir kuruluşun pazarının geliştirilmesinde kritik bir rol oynamaktadır. Örneğin; Ağustos 1999'da yurtsever ve milliyetçi Çinli ve Tayvanlı hackerlar arasında gerçekleşen siber savaş sonrasında Tayvanlı web sitelerine yönelik Tayvan'ın her zaman Çin'in bir parçası olduğu yönünde Çinli hackerlar tarafından Web tahrifatı gerçekleştirilmiştir. Aynı zamanda, 1999'da ABD-Çin arasında gerçekleşen siber savaş bir diğer örnektir. Bu savaşta Belgrad'daki Çin Büyükelçiliği'nin yanlışlıkla bombalanmasının ardından Çinli bilgisayar korsanları, Amerika'da yaklaşık 1100 ABD sitesine saldırdı. ABD-Çin siber savaşlarında milliyetçilik ve vatanseverlik baskın koddu. Hindistan – Pakistan ve İsrail – Filistin

[149] Nir Kshetri, "Pattern Of Global Cyber War And Crime: A Conceptual Framework", Journal of International Management, Cilt.11, No.1, 2005, ss.541-562.
[150] Kshetri, a.g.e , ss.541–562.

siber savaşlarında islami eylemciler tarafından yapılan saldırılar da ideolojik siber saldırıların ilginç örneklerinden biridir.

Yukarıda bahsedilen örnek olaylar dijitalleşme ve sosyal mühendislik sonucu sanal dünyada gerçekleşen erişim ve operasyonel verimliliğin boyut değiştirmesine yol açmıştır. Örneğin; yapay zekâ ile birlikte insansız araçlar yaygınlaşacak, savaşlar tamamen siber olacak, hologram ile sonsuz yaşam başlayacak, robotlar siyasi seçimlerde daha etkin olacak, yöneticiler robotlar olacak, hayatımızın büyük bir bölümü sanal ortamda gerçekleşecektir. Bu iddiaların hepsi birçok kişiye gerçekçi gelmeyebilir. Fakat bunların hepsi gerçekleşecektir. Bunun en güzel örneğini; bilgisayar alanında dünyanın en önde gelen firması olan ve 1944'te ilk bilgisayar üretimini yapan IBM in kurucusu Thomas John Watson'ın sözlerinde görebiliriz. 1943 yılında o zamanın koşullarında Thomas Watson "Dünyada belki de en fazla 5 bilgisayara ihtiyaç vardır." şeklinde bir açıklama yapmıştır. Yani o düzeyde akıllı bir girişimci bile kurmuş olduğu bir işletme olduğu halde bilgisayarın bu kadar gelişeceğini tahmin edememiştir.

2.2.1. Endüstri 4.0

Endüstri 4.0 kavramı [151] çerçevesinde Dünya, kendi kendine yetebilen akıllı fabrikaların, yapay zekânın, 3D baskının, akıllı robot otomasyon sistemlerinin, simülasyonun, büyük verinin, bulut bilişimin, zenginleştirilmiş gerçekliğin ve siber ağ güvenliği gibi birçok konuyu içinde barındıran Dördüncü Sanayi Devrimi adı altında internet temelli bilgi teknolojilerini temel alan yeni bir devir içinde büyük ve hızlı bir dönüşüm içerisindedir. Özellikle nesnelerin interneti aracılığıyla tüm verilerin anlık paylaşıldığı ve büyük veriyi oluşturduğu bu yeni çağda her gün kullandığımız sosyal medya hesapları, bloglar, arama motorları ve internet gezintileri sırasında arkamızda bıraktığımız her iz devasa bir veri yığını oluşturmaktadır. Ancak bu bilgiler uygun şekilde analiz edilerek yorumlandığında çok önemli kararların doğru şekilde alınmasında, risklerin doğru yönetilmesinde, hatta yeni buluş ve keşiflere imza atılmasında çok önemli katkı sağlamaktadır.

[151] **Endüstri 4.0** bilişim teknolojileri ile tüm yaşamsal mekanizmaları bir arayı getirmeyi amaçlayan bir sistemin genel nitelendirilmesidir ve üçayaklı bir organizasyonu ifade eder. Bunlar; nesnelerin interneti, hizmetlerin interneti ve siber-fiziksel sistemlerdir. Türkiye'nin Endüstri 4.0 Platformu, Endüstri Tarihine Kısa Bir Yolculuk, https://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/ ET.24.11.2020.

Thomas H. Davenport'a göre büyük veri; "Tek bir sunucuya sığamayacak ölçü de büyük (100 terabayttan daha büyük ölçekte), satır ve sütun seklinde yapılandırılmamış, veya durgun bir veri ambarına sığamayacak şekilde sürekli akan veri" dir.[152] Nesnelerin internetinin önümüzdeki yıllarda aktif olarak kullanılması sonucunda tarayıcılar, radarlar, sensörler ve diğer alıcıların üreteceği veri setinin kısa sürede çözümlenmesi ve yanıtlanması büyük verinin bir başka çözüm gerektiren zorluğunu ortaya çıkaracaktır. Bu zorlukların yanında "Endüstri 4.0" kavramından sonra "Toplum 5.0" kavramı ile birlikte insanlar, robotlar ve yapay zekâ bir güç birliğine girmiştir. Uluslararası ilişkilerde yaşanan bu yeni devrim neticesinde gelecekte genetiği değiştirilmiş insanlar ve yöneticiler, robotların vatandaşlık hakları, yapay zekâya devredilmiş ordular, yönetiminde insanın olmadığı ülkelerin oluşması gibi kavramlar konuşulmaya başlamış ve bu kavramlar geleceğe dönük köklü değişimleri içinde barındıran bir bilinç aktarımını doğurmuştur. Bu durum ise dünyada güvenlik denildiğinde siber alanın köklü bir değişiklik ve yenilik yaratacağını göstermektedir.

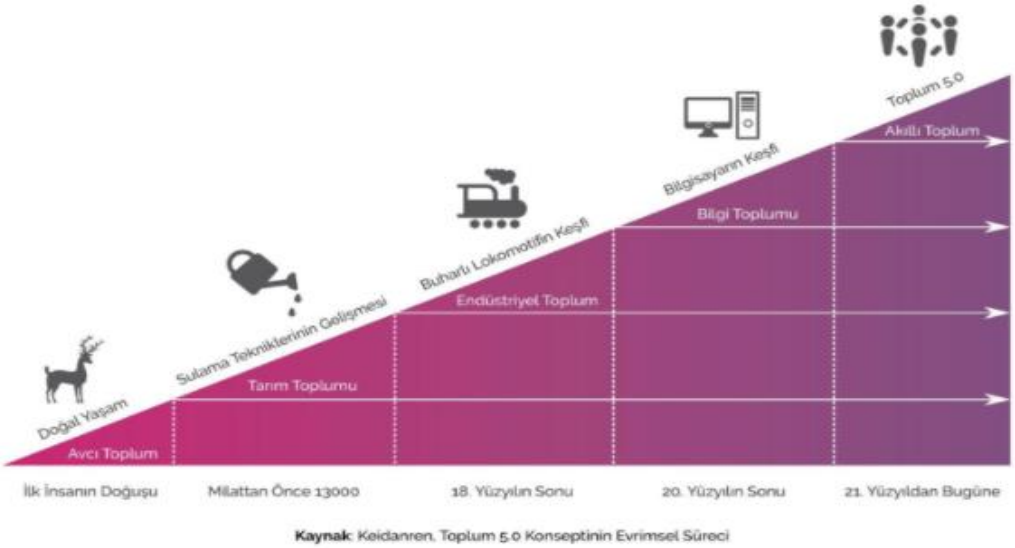
Dördüncü Sanayi devrimi olarak görülen Endüstri 4.0 üretim ve otomasyonu bilişim ve iletişim teknolojilerinin bir fonksiyonu haline getiren, iş süreçlerinde yatay entegrasyonu, veri kullanımında buluta değin dikey veri alış-veriş modellerini kullanmayı öngören yeni bir endüstri modelidir. Bu modelle birlikte verimlilik, istikrar, nitelik, yüksek yaşam standartları, akıllı tasarım, büyük veri, nesnelerin interneti gibi anahtar sözcükleri önem kazanmıştır. Aynı zamanda; 4.Sanayi Devrimi ile yaşanan siber çağının bilgiyi üreten, kullanan ve bilgi ile gelişen bir yapıda olması insanlığın daha önceden yaşamış olduğu hiçbir döneme benzememektedir. Çünkü inanılmaz büyüklükteki veri, robotik sistemler, 3D yazıcılar ve nano teknolojiler sayesinde yaşam biçimimiz inanılmaz derecede değişmiştir. Bilişim teknolojilerinin üretimi ve yaygınlaştırılması konusunda dünya hızına bakıldığında Türkiye olarak yavaş kaldığımız söylenebilir. Bu yüzden Türkiye'de kamu, siyaset, üniversiteler ve büyük sanayiciler gibi bütün sektörler bu adaptasyon sürecine hızlıca dâhil olmalıdır.

[152] Thomas H. Davenport, Paul Barth ve Randy Bean, "How 'Big Data' Is Different", Mitsloan Management Review, Cilt. 54, No. 1, 2012, ss.22-24.

Bu adaptasyon sürecinde Endüstri 4.0'dan Toplum 5.0'a geçişi anlamamız gerekmektedir.

2.2.2. Toplum 5.0

"Süper Akıllı Toplum" olarak da isimlendirilen "Toplum 5.0"[153] kavramı aslında "Endüstri 4.0" başlığı altında oluşan ve bilgi devrimi ile ortaya çıkan tüm güvenlik risklerinin ve tehdit unsurlarının ortaya çıkmasına neden olduğu teknolojik dönüşümün insan yararına nasıl kullanılabileceği üzerine arayışlarla ortaya çıkmıştır. Bu arayış içerisinde devletler akıllı fabrikaların ötesine geçerek, akıllı bir toplum oluşturmak için endüstriyel teknolojiler kullanmaya başlamıştır. Bu bağlamda; "Toplum 5.0" konsepti altında, toplum yararı için bilim ve teknolojinin yönlendirmesinin desteklenerek siber uzay kavramıyla önemi artan Endüstri 4.0 Devriminin gerçekleşmeden önceki tüm süreçlerinin dönüşümünü aşağıdaki tabloda kısaca incelersek;



Kaynak: Keidanren, Toplum 5.0 Konseptinin Evrimsel Süreci

Şekil 1 Endüstri 4.0 ve Toplum 5.0'la Birlikte Teknolojik Gücü Doğru Yönetecek Akıllı Topluma Geçiş [154]

[153] **Toplum 5.0** kavramı İlk kez Ocak 2016'da Japon hükümeti tarafından kullanılmış olup siber alan ve fiziksel alanın (gerçek toplumun) yüksek seviyede entegre olduğu "süper akıllı toplum" olarak tanımlanmaktadır. Türkiye'nin Endüstri 4.0 Platformu, Endüstri Tarihine Kısa Bir Yolculuk, https://www.endustri40.com/endustri-4-0dan-toplum-5-0a/#:~:text=Toplum%205.0%20terimi%20ilk%20kez,s%C3%BCper%20ak%C4%B1ll%C4%B1%20toplum%E2%80%9D%20olarak%20tan%C4%B1mlan%C4%B1yor., ET.24.11.2020.

[154]Keidanren Japan Busşness Federation, Society 5.0: Smart Social Philosophy That Will Manage Technological Power Correctly,https://www.keidanren.or.jp/en/profile/pro001.html ET.30.12.2019.

Sonuç olarak yukarıdaki şekilde de belirtildiği üzere Endüstri 4.0 sürecine herkesin bildiği 1., 2. ve 3. Devrim süreçlerinden geçilerek gelinmiştir.

- ***1.0 Üretimin Makineleşmesi:*** 1760-1820 arasında ilk buharla çalışan makinenin Sanayide kullanılmasıyla başladı.
- ***2.0 Üretimin Serileşmesi:*** 1820-1970 arasında elektrik enerjisinin yardımıyla imalatta iş bölümü ve seri üretimin sanayide kullanılmasıyla başladı.
- ***3.0 Üretim Otomosyonu:*** 1970-2011 arasında üretimi daha da otomatikleştiren bilgisayarlar ve diğer dijital elektronik teknoloji ürünlerinin sanayide kullanılmasıyla başladı.
- ***4.0 Üretimin Dijitalleşmesi:*** 2011 yılında Hannover Sanayi fuarında ortaya konulan geleceğin akıllı üretim ekonomisi siber fiziksel sistemlerin kullanılmaya başlamasına dayanır. Ayrıca; Endüstri 4.0 insanların aracılığı olmaksızın(ya da sınırlı müdahalesiyle) makinaların birbiriyle kontak kurabilmesidir. Siber güvenlik, Bulut, akıllı robot, nesnelerin interneti, büyük veri ve analiz, eklemeli üretim 3D, zenginleştirilmiş gerçeklik, yatay dikey yazılı entegrasyon ve similasyon gibi birçok konuyu kapsar.

Bu dönemlerin oluşumuna kadarki Toplumsal dönemleri de incelememiz gerekir. Toplumsal gelişmeler ise 5 düzlemde açıklanmaktadır.

- ***Avcı toplum(Toplum 1.0):*** İlk insanın doğuşuyla başlayan doğal yaşamdır.
- ***Tarım Toplumu (Toplum 2.0):*** milatdan önce 13.000 yıllarında Sulama tekniklerinin gelişmesi ile başlar.
- ***Endüstri toplum(Toplum 3.0):*** 18. yy sonunda Buharlı Lokomotifin Keşfi ile başlar.
- ***Bilgi Toplumu(Toplum 4.0):***20. yy sonunda Bilgisayarın Keşfi ile başlar.
- ***Akıllı toplum(Toplum 5.0):*** Teknolojik gücü doğru yönetecek akıllı toplum felsefesi olarak düşünülen Toplum 5.0 kavramı ilk kez 2016 yılında Japonya'da sonrasında ise 2017 yılında Almanya'da kullanılmış ve bugün hala devam eden bir süreçtir.

İçinde bulunduğumuz bu Toplum 5.0 felsefesinin asıl amacı teknolojik gelişmeleri(yapay zeka, büyük veri, robotlaşma, siber güvenlik vb) insanlık yararına

kullanabilmek için süper akıllı topluma geçmektir. Akıllı topluma erişmek için ise şu beş husus gereklidir.

- Yargı sistemindeki engeller kalkmalı
- Dijital araçlardaki bilimsel boşluklar doldurulmalı
- Yetişmiş personel eksikliği giderilmeli
- Sosyo-politik önyargılar giderilmeli
- Toplumsal direnç kaldırılmalı

Bu ortam sağlandıktan sonra ise şu sorunlar çözülmelidir;

- Yaşlanan dünya nüfusu ile ilgili çözüm üretilmeli
- Sanal dünya ile gerçek dünyanın birlikte işlemesi sağlanmalı
- Nesnelerin dijitalleşmesi toplumun çıkarları ile birleştirilmeli
- Siber silahlarla ortaya çıkabilecek tehditlerin önüne geçilmelidir.

Yukarıda Toplum 5.0 ve Endüstri 4.0 hakkında belirtilen tüm bu gelişmeler siber güvenliğin etkileştirici rolünü ortaya çıkarmıştır. Özellikle Dördüncü Sanayi Devrimi (Endüstri 4.0) siber güvenlik ihtiyacını ortaya çıkarmakta ve ayrıca siber dayanıklılığı güçlendirme çabalarını vurgulamaktadır. Bu özellikle bulut bilişim, yapay zekâ, ve nesnelerin interneti (IoT) ile daha da önem kazanmıştır. Çünkü ilgili tehditlerin potansiyel etkisi sadece siber alanı değil fiziksel güvenliği de tehlikeye atmaktadır. Örneğin; üretim sürecinin aksaması, ürünlerin zarar görmesi, ekipmanların hasar görmesi ve hatta finansal ve siyasi itibar kayıplarına kadar her alanı kapsamaktadır.

Günümüz sistemi sadece klasik yöntemlerle güvenliği tehdit eden unsurların ortadan kaldırılmasıyla sağlanmaz. Bu anarşik yapı içerisinde siber güvenliğe yönelik uluslararası anlaşma olmadan tehdit ortadan kalkmaz. Şu anda devletler tarafından aleni olarak küresel bir savaş çıkmamasının tek nedeni "bana saldırırsan seni vururum" tehdidir. Bu siber tehdidin etkisinin ne kadar büyük olabileceğinin şuan için ölçülememesi ise aleni savaş ilanını durdurmaktadır. Bankacılıktan enerjiye çok geniş bir alanda ortak bir şekilde kullanılan internet temelli teknolojik araçlardan dolayı her ülke kendine avantaj oluşturmak istemeye devam edecektir. Bu yüzden büyük sistemlerin hepsinde siber güvenliğin sağlanmasına yönelik kurallar koyulmalı ve bu kuralları uygulayacak kurumlar oluşturulmalıdır.

Endüstri 4.0 ile gelen bağlantı ve iletişim protokolleri ile birlikte artan siber tehditlere karşı kritik sistemlerin ve üretim hatlarının güvenliği çok önemli bir hal almıştır. Siber güvenlik sağlanırken makinelerin ve kullanıcıların; erişim yönetimleri, gelişmiş kimlik güvenlikleri ve haberleşme sistemleri gibi birçok konu sürece dahil olmuştur.[155]Çünkü Endüstri 4.0 ile milyonlarca makina ve eşya internete bağlanmıştır. Bu yüzden siber güvenliğe yönelik kapsamlı bir yapı sunulmalıdır.

Eğer nesnelerin interneti (IoT) ile birlikte ortaya çıkan güvenlik açıklarına yönelik tehditler önlenemezse, siber suç inovasyonu, ulus-devlet aktörleri yükselen ddos saldırıları ile saniyeler altında saldırı tehdidiyle baş başa kalabilir. Saldırganlar akıllı ev sensörlerinden akıllı telefonlara, yönlendiricilere ve hatta assle yazılımlarına kadar her şeyden yararlandığından, savunmasız hizmetlerin hızla silahlandırılması gerekmektedir. Ayrıca, güvenlik duvarlarının arkasındaki IoT cihazlarını hedefleyen, saldırı riski azaltılmalıdır. Örneğin; 2018'un son yarısında dünya çapında yaklaşık 4 milyon DDoS saldırısı oldu ve bu saldırı sıklığı 2019'un ilk yarısında yüzde 39 büyüdü. Aynı zamanda Netscout Asert ekibi, IoT kötü amaçlı yazılımlara ilişkin bu artan saldırılarda yaklaşık ayda 20.000'e yakın benzersiz örnek tespit etti. [156]

Günümüzde IoT (Internet of Things – Nesnelerin İnterneti) cihazların kullanımındaki artış beraberinde yüksek yoğunluklu ve farklı çeşitte verilerin oluşmasına sebep olmaktadır. Bu verilerin alınması, işlenmesi, saklanması ve görselleştirilmesindeki zorluklar ise büyük veri sistemi bileşenlerinin kullanılmasını zorunlu hale getirmiştir. Yani kısaca bu süreci açıklarsak; veri alımı katmanında yüksek yoğunluklu verinin alınması, alınan verilerin saklanmasını, saklanan verilerin işlenmesi, tespit edilen anomaliler ve ham verin saklanmasını, son olarak da bu verilerden çıkarılan sonuçlarda yakın gerçeklerin görselleştirilmesinde kullanılmaktadır. Böylece büyük veri ekosisteminde bahsi geçen tüm aşamalar ayrı ayrı bileşenlerde mevcuttur. Açık kaynaklı bu bileşenlerin her aşamasında ise farklı problemlere çözüm üretmek gerekmektedir.

Sonuç olarak; bu süreci uluslararasındaki rekabetlerde incelersek; aktörlerin dış politika süreçlerindeki karar alma mekanizmalarında veri geçmişinin doğru ve

---

[155] Michael Rüßmann, Markus Lorenz, Philiss Gerbert, Manuela Waldner, Jan Justus, Pascal Engel, ve Michael Harnisch, "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries", Boston Consulting Group, Nisan 2015, ss.3-6.

[156] Hardik Modi, "Threat Intelligence Report", Netscout Asert Asert Team, 05.08.2019, https://www.netscout.com/blog/asert/netscout-threat-intelligence-report, ET:24.01.2020.

adil bir şekilde oluşturulması çok önemlidir. Bulutla saklanan bu veriler ile hemen her sektörde kullanımı artan ve makine öğrenmesine dayanan yapay zekâ teknolojilerinin gelişmesi bu anarşik sistemdeki ilişkilerin geleceğine yön verecektir. Böylece dünyanın dijital olarak gelişmiş ekonomileri, bilgi ve iletişim teknolojisine büyük yatırım yaparak sürekli olarak ilerlemelerini sürdürecektir. Geniş bant, veri merkezleri, bulut, büyük veri ve nesnelerin Interneti (IoT) gibi beş farklı teknolojiyi destekleyen ve kırk benzersiz göstergeyi temel alan Küresel Bağlantı Endeksi (GCI) de ülkelerin dijital dönüşümlerindeki başarı düzeyini ortaya koymaktadır.

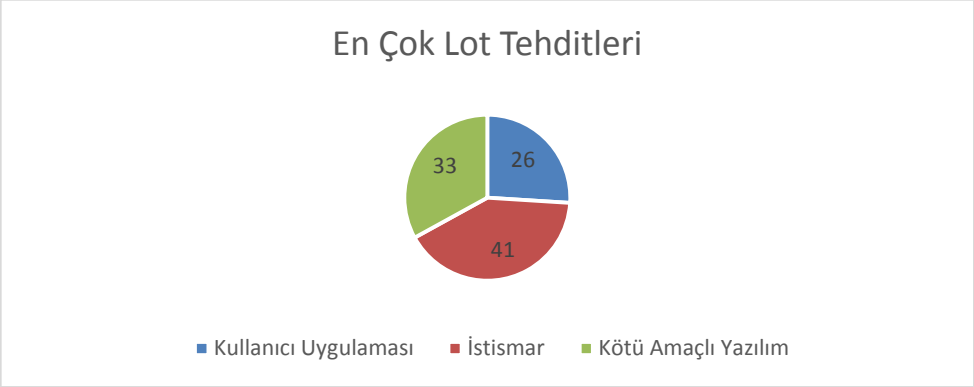
2.3. Büyük Veri ve Nesnelerin İnterneti

Günümüzde yaşanan siber anarşik yapıda yaşanan temel mücadele bilgiyi koruma üzerinedir. Çatışmalarda aslında bu minvalde gerçekleşmektedir. Bilgi den bahsettiğimizdeyse büyük veri kavramı ortaya çıkmaktadır. "Büyük veri" terimi tüm verilerin toplanmasını ve çok çeşitli alanlarda ondan faydalanma becerisini ifade eder. Bilgisayarlardan ve veri tabanlarından önce de veri kullanılmaktaydı. Yani verinin kendisi yeni bir buluş değildir. Sadece depolamanın, işlemenin, erişmenin ve düzenlemenin bilgisayarlar sayesinde kolaylaşmasıyla birlikte verinin yaratabileceği fırsatlar ortaya çıkmış böylece büyük veri daha önemli bir hale gelmiştir. Yani büyük veriyi diğerlerinden ayıran içinde barındırdığı hız, hacim, çeşitlilik ve doğruluktur.

Büyük veri esas olarak bugün, birkaç yıl önce mümkün olmayan şekillerde veri toplayabildiğimiz ve analiz edebildiğimiz gerçeğini, makine öğrenmesini ile birlikte yapay zekâyı loT üzerinde çalıştırmamızı sağlamıştır.[157] Bu derece büyük fırsat yaratan büyük veri bu tezde üzerinde durduğumuz siber çatışmaların ve siber güvenlik gereksinimlerinin temelini ortaya çıkarır. Ayrıca büyük verilerin bu kadar önem kazanması "Nesnelerin İnterneti"(loT) kavramını geliştirmiştir. Lot kısaca internet üzerinden veri toplayan ve ileten cihazları ifade eder ve saat, telefon, televizyon ve buzdolabımıza kadar her şeyi içine alır. Akıllı cihazlar dünyamızı, otomobillerimizi, evlerimizi, şirketlerimizi, toplumlarımızı, devletlerimizi kısaca herşeyi dönüştürüyor. 2020 sonu itibariyle 50 ila 70 milyar arası cihazın internete bağlanacağı tahmin edilmektedir. Böylece bağlantılı cihazlar sadece interneti değil,

[157] Bernard Marr, Çeviren Gündüz, B. "Büyük Veri İş Başında 45 Yıldız Şirket Büyük Veriyi Nasıl Kullandı?" Mediacat, İstanbul, 2016, ss.11.

birbirlerine de bağlanarak bilgi paylaşacaklardır.[158] Makineden makineye olan bağlantıların artması ise yakın gelecekte siber güvenliğin önemini daha da arttıracaktır. Çünkü IoT odaklı siber saldırılar, endüstrileri ve temel iş operasyonlarını korumak için IoT cihazlarıyla ilişkili riskleri tanımayı ve yönetmeyi zorunlu kılmaktadır. Özellikle kritik alt yapılara yönelik endüstriler inanılmaz derecede beklenmedik bir riske maruz kalmaktadır. Aynı zamanda bazı IoT güvenlik açıkları hayati tehlike oluşturabilirken, bazıları kritik kurumsal işlevlere saldırır veya gizli verileri dışarı aktarır. Bu çerçevede IoT cihazlarının% 59'ı orta veya yüksek önem dereceli saldırılara karşı savunmasızdır ve bu da IoT'ı saldırganlar için düşük maliyetli hale getirir.IoT cihazlarını etkileyen en çok tehditler şunlardır;



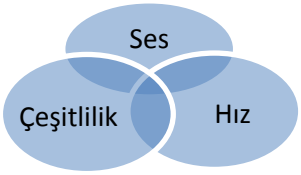
Şekil 2 En Çok IoT Tehditleri

Kaynak: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Üç ana hatta ayrılan bu Iot tehditleri yapay zekâyının gelişimini etkilemiştir. Böylece farklı veri türleri daha kolay analiz edilebilecek ve veriler tehditlere karşı daha iyi karar alınabilmesi için kullanılacaktır. Bu kapsamda; teknoloji ve internetin gelişmesi sonucunda bilginin üretilme ve yayılma hızının inanılmaz derecede artışı günümüzün stratejik karar verme süreçlerini milyonlarca veriyle beslenen bir yığına dönüştürmüştür. Çalışma tablolarından veri tabanlarına, sunuculardan bulut servislere kadar her türlü veriyi kapsayan Big Data (Büyük Veri) günümüzde veri tabanı uzmanlarının ilişkisel veri tabanlarında yapısal biçimde sınıflandırmaya başladığı, aktörlerin kullanabileceği ve yöneticilerinin raporlama sistemleri üzerinden karar almasını destekleyen sistemlere evrilmiş durumdadır.

[158] Bernard Marr, "Veri Stratejisi Büyük Veri ve Nesnelerin İnterneti Nasıl Kar Getirir?" Media Cat, İstanbul, ss.10-15.

2000'li yıllarda büyük veri kavramına ilişkin en önemli açıklamalardan birini sunan Doug Laney, " Büyük Veri (Big Data) Analitiği"ni 3V olarak tanımlamıştır.



Şekil 3 Büyük Veri Analitiği

Kaynak: https://bigdataldn.com/intelligence/big-data-the-3-vs-explained/

3V, İngilizce volume (hacim), velocity (hız) ve variety (çeşitlilik) kelimelerinden meydana gelmektedir. Bir diğer yandan Big Data; sosyal medya, arama motorları, bilgi belge arşivleri, log dosyaları, makine dataları gibi farklı kaynakların oluşturduğu bilgi yığınlarını işleyerek anlamlı verilere dönüştürmek için ar-ge faaliyetleri yapan yazılım şirketleri tarafından ortaya atılmış bir olgudur. Bu olgudan yola çıkarak büyük veri ne kadar bilgi sahibi olunduğundan ziyade onunla ne yapılacağı üzerine yoğunlaşmaktadır. Herhangi bir kaynaktan veri alıp onları para ve zaman tasarrufu sağlamak, yeni proje gelişimi ve optimize edilmiş önerileri sunmak, aynı zamanda da akıllı karar verilmesini sağlamak için kullanılır. Bu kapsamda; büyük veri güçlü analizlerle birleştiğinde doğabilecek tehditlerin önceden belirlenerek bertaraf edilmesini sağlayabilir. Yâda siber casusluk yoluyla elde edilen verilerle düşmana karşı nerden saldırılması gerektiği, en zayıf halkanın neresi olduğu gibi politikaların oluşturulmasını tetikleyebilir. Veri deposundaki bu süreç veri madenciliğine olan ihtiyacı ortaya çıkarmıştır.

Bu süreci daha da açarsak; yapay zekâ ile birlikte verilerin kullanımı konusunda ciddi bir güç kazanılmıştır. Hayatın her alanının internetle entegre olmasıyla birlikte teknolojik düzlemde gerçekleşen tüm hareketler bir bilgi niteliği kazanmıştır. Böylece bu bilgilerin kapasitesinin her geçen gün artmasıyla birlikte bulut dediğimiz depolama ihtiyaçları ortaya çıkmıştır. Veri ambarında depolanan bu veriler sonrasında ise yapay zekâ sayesinde veri madenciliğine dönüştürülmektedir. Aynı zamanda, veri analizi için veri ambarı ve stratejik iş kararları vermek şarttır. Bu bağlamda; bir veri ambarı için üç tür uygulama vardır. İlk olarak, temel istatistiksel

analizler sorgulanmalı ve raporlanmalıdır. İkincisi, İlk aşamada gerçekleştirilen raporlama sonucunda elde edilen veriler detaylandırılır. Üçüncü olarak, detaylandırılan veriler veri madenciliği sayesinde gizli kalıplar ile ilişkilendirilerek sonuçlar görselleştirilir. Bu doğrultuda veri ambarının bu üç tür uygulamasının beş temel özelliği aşağıdaki gibidir. [159]

1. **Veri Temizleme:** Bir veri ambarındaki veriler konu odaklı bir şekilde ana konulara odaklanılarak geçersiz veriler kaldırılır..

2. **Veri Entegrasyonu:** Birden çok kaynaktan gelen veriler entegre edilerek oluşturulur

3. **Veri Dönüşümü:** Geçmişten gelen veriler özet veya toplama şeklinde dönüştürülerek saklanır.

4.Veri madenciliği: Saklanan kalıpları ayıklamak için akıllı yöntemler uygulanır.

5. Değerlendirme ve Sunum: Akıllı yöntemlerin uygulanması sonucunda elde edilen sunumlar görselleştirilerek gelecek perspektifi oluşturulur.

Sonuç olarak; Endüstri 4.0 ve Toplum 5.0 sürecinde büyük veri, nesnelerin interneti ve yapay zekâ gibi günümüz dijital dünyasında telaffuz edilen kavramlarla yaşantımıza giren ve gelişmekte olan ileri teknolojiler iş yapış biçimlerimizi muazzam bir şekilde değiştirmektedir. Dijital dünyadaki bu değişim birçok alanda olduğundan daha hızlı gerçekleşmektedir. Bu değişimin takip edilmesi ise sadece bu hıza ayak uydurmakla mümkün olabilecektir. Çünkü avantajlarının yanında ciddi oranda dezavantajları da vardır. Bu durum da ülkelerin her alandaki kritik yapılarında siber güvenlik ihtiyacını karşılamalarının zorunluluğunu ortaya çıkarmaktadır. Eğer siber güvenlik sağlanırsa, işleyiş etkilenmeden önce ortaya çıkabilecek yanlış davranışlar tespit edilerek güvenlik sağlanabilecektir.

2.4. Siber Uzayın Uluslararası İlişkiler ’de Beşinci Boyut Olarak Doğuşu

Tezin bu bölümünde güvensizliğin ve belirsizliğin yeni cephesi siber uzay kavramının ortaya çıkması sonucunda söz konusu bu yeni alanın Uluslararası İlişkiler Teorileri kapsamında teknoloji felsefesiyle birlikte ortaya çıkan dijital dönüşüm kavramların da etkisiyle çerçevesinin çizilmesi, kavramsal çözümlemeler yapılması, siber tehdit altyapısı ve siber güvenlik araçlarının ortaya konması

[159] Singhal Anoop, “Data Warehousing and Data Mining Techniques for Cyber Security”, Springer, United States of America, 2007, ss.20-33.

hedeflenmektedir. Bu kapsamda; dünyada internet tarihi'nin gelişimi ve uygulanmasını teşvik etme çabaları insanlığın sürekli olarak farklı dönemlerde farklı araçlar ve bu araçlar sayesinde farklı yaşamlar sürmesi geleneğinin bir parçasıdır. Yaşanan değişimler ekonomiden, kültüre, sosyal hayattan askeri yaşama kadar her alanı değiştirip dönüştürmüştür. Telgrafın, telefonun, radyonun ve bilgisayarın icadı mevcut imkanların eşi benzeri olmayan bir şekilde entegre edilmesinde bir aşamadır. İnternet ise iletişimi daha önce olmadığı şekilde devrimleştirmiştir. İnternetin gelişimi teknolojik olmaktan ziyade interdisiplin bir değişimdir. İnternetin tarihçesi aslında 1837'de Samuel Morse'un telgraf verici ve alıcılarını icadıyla başlayan kitle iletişimin tarihçesinin bir parçasıdır. Sonrasında bu süreç devletlerin telgraf ile ilgili birim kurmaları ile devam etmiştir. [160]

20'nci yüzyıla kadar tüm faaliyetlerini kara ve deniz olmak üzere iki boyutta gerçekleştiren uluslararası sistem 20'nci yüzyılın başında havacılık boyutu, 1957 yılında dünyanın yörüngesine yerleştirilen ilk insan yapımı uydu olan "Sputnik" ile birlikte kara, deniz ve hava boyutuna ilave olarak dördüncü boyut olan " uzay " boyutunu uluslararası sisteme eklemiştir. Beşinci boyut olan "siber uzay" kavramı dünyadaki tüm bilgisayar ağları ve onların bağlı oldukları ve kontrol ettikleri her şeydir. Sadece internet demek değildir. Çünkü İnternete bağlı olmasa bile teknolojik araçlar kontrol edilebilmektedir. Kısaca internetin bu gelişim sürecini açıklarsak;

1950'lerde transistörlerin kullanımı ile micro işlemciler gelişerek bilişim çağı denilen süreci başlatmıştır. 1958'i takip eden yıllarda elektronik bilimin gelişmesi, özellikle DARPA tarafından geliştirilen ve kullanılmaya başlanan internet yapısı ile bilgisayarın gelişmesi süreci sağlanmıştır. Bunun üzerine daha 'İnternet' kelimesi icat edilmeden önce 1962'de yurtiçinde, telefon hatları üzerinden veri iletişimi için kullanılan AT T ile serüven başlamıştır. İlk başta Amerika'da ortaya çıkan ve sonrasında Avrupa'ya yayılan internet, J.C.R. Licklider'in 1969 yılında ARPA'yı kurmasının ardından ortaya çıkmıştır. Fakat, internet ortaya çıktığı 1960'lı yıllarda ABD savunma bakanlığı tarafından olası bir savaş durumunda askeri iletişimin zarar görmeden kullanılmaya devam etmesi için bilgisayarlardaki verilerin başka bilgisayarlara aktarabilmesi amacıyla kullanılmaktaydı. ARPA ile başlayan bu yaklaşım Dünya çapında ağ(World wide web-www) oluşumuna giden bilgisayarların

[160] Taner Altınok ve Haydar Çakmak, a.g.e ss. 60-88.

birbirine bağlanması sürecini hızlandırmış ve 1981'de ilk internet protokolünün imzalanmasına yol açmıştır. 1980 lerin başına geldiğimizde İnternet kavramı askeri ve bilimsel arge çalışmalarında bilgi paylaşımı için kullanılmaya başlamıştır. [161] Böylece internetin zaman içinde gelişmesi bilgisayar uzmanlığının ve biliminin gelişmesine de yol açmıştır.

Aslında 1980'lerin başında ARPANET'in ortaya çıkmasıyla bugünkü internetinde temellerinin de atılmaya başlandığı söylenebilir. Bugünkü internetin ilk temellerinin atıldığı bu süreç ise şu şekilde gelişmiştir; ARPA ilk başta 4 ayrı üniversitedeki ana bilgisayarlarla bağlantı halindeydi. ARPA projesiyle başlayan girişimler sonucu 1980'lerde NSF beş tane süper bilgisayar merkezi kurmuştur. Bu merkezleri sadece savaş üreticisi firmalar ve dev araştırma firmaları kullanmaktaydı. Bu merkezleri bağlamak için ARPANET'in teknolojisi kullanılmıştır. Ardından araştırmalar üniversitelerde yapıldığı ve üniversitelerdeki araştırmacıların bu merkezlere bağlanmasıyla artan maliyetten dolayı bölgesel şebeke zincirlerinin yaratılması ihtiyacı ortaya çıkmıştır.[162]

Bu ihtiyaç doğrultusunda 1989 yılında Tim Berners ve ekibi tarafından www(World wide web) geliştirilmiştir. World wide web'in ortaya çıkmasının ardından 1990'da gerçek anlamda internet hiper metin transfer protokülü (hyper-text transfer protocol-http), İnternet Explorer ve Netscape kurularak süreç hızlanmıştır. Bu gelişmeyle birlikte ARPANET'in 1990 yılında kullanımdan kaldırıldmasıyla sonucunda 1993 yılı itibariyle internet kullanımı da artış göstermiştir. Özellikle Microsoft'un Windows 95 ve sonrasında 98 i çıkarması ile internet artık sıradan kullanıcıların kullanımına açılmaya başlamıştır. Böylece İnternet'in 1990'larda kamu malı olarak gelmesinden bu yana, İnternet ve BİT insan toplumunun tüm yönleriyle tamamen bütünleşerek kullanıcı sayısı inanılmaz düzeyde artmıştır. [163] Bu gelişimi aşağıdaki istatistiklerde de açıkça görebiliriz.

---

[161] Atalay Keleştemur, a.g.e ss.130-132.

[162]İrfan Erdoğan, "Uluslararası Bilgisayar Şebekesi İnternet ve İletişimin Emperyalist Kontrolü" , Bilim ve Ütopya Dergisi, Cilt.13 , Sayı. 7, Yıl. 1995, http://www.irfanerdogan.com/makaleler1/internet.htm, E.T.31.01.2020 .

[163] Lıeutenant Colonel ve Scott W. Beıdleman, "Defınıng And Deterrıng Cyber War", U.S. Army War College Strategy Research Project, 2009.

Tablo 2 İnternet Kullanıcılarının En Yüksek Sayısına Sahip 20 Ülke[164]

İnternet Kullanıcılarının En Yüksek Sayısına Sahip 20 Ülke – 30.06.2019						
#	Ülke	Nüfus	Nüfus	Internet Kullanıcısı	Internet Kullanıcısı	Internet Büyümesi
		2019	2000	30.06.2019	31.12.2000	2000 - 2019
1	Çin	1,420,062,022	1,283,198,970	854,000,000	22,500,000	3,70%
2	Hindistan	1,368,737,513	1,053,050,912	560,000,000	5,000,000	11,10%
3	ABD	329,093,110	281,982,778	292,892,868	95,354,000	207%
4	Endonezya	269,536,482	211,540,429	171,260,000	2,000,000	8,46%
5	Brezilya	212,392,717	175,287,587	149,057,635	5,000,000	2,88%
6	Nijerya	200,962,417	122,352,009	123,486,615	200	61,64%
7	Japonya	126,854,745	127,533,934	118,626,672	47,080,000	152%
8	Rusya	143,895,551	146,396,514	116,353,942	3,100,000	3,65%
9	Bangladeş	168,065,920	131,581,243	96,199,000	100	96,10%
10	Meksika	132,328,035	101,719,673	88,000,000	2,712,400	3,14%
11	Almanya	82,438,639	81,487,757	79,127,551	24,000,000	229%
12	Filipinler	108,106,310	77,991,569	79,000,000	2,000,000	3,85%
13	Türkiye	82,961,805	63,240,121	69,107,183	2,000,000	3,36%
14	Vietnam	97,429,061	80,285,562	68,541,344	200	34,17%
15	İngiltere	66,959,016	58,950,848	63,544,160	15,400,000	312%
16	İran	82,503,583	66,131,854	62,702,731	250	24,98%
17	Fransa	65,480,710	59,608,201	60,421,689	8,500,000	610%
18	Thayland	69,306,160	62,958,021	57,000,000	2,300,000	2,38%
19	Italya	59,216,525	57,293,721	54,798,299	13,200,000	315%
20	Mısır	101,168,745	69,905,988	49,231,493	450	10,84%
İlk 20 Ülke		5,187,499,066	4,312,497,691	3,213,351,128	251,346,400	1,18%
Dünyanın Geri Kalanı		2,528,724,143	1,832,509,298	1,322,897,680	109,639,092	1,11%
Toplam		7,716,223,209	6,145,006,989	4,536,248,808	360,985,492	1,16%

Tablo 3 Kıtalara Göre İnternet Kullanımı

DÜNYA İNTERNET KULLANIMI VE NÜFUS İSTATİSTİKLERİ 2019 Yıl Ortası Tahminleri						
Dünya Bölgeleri	Nüfus (2019 Tahmini)	Dünya nüfusunun % 'si	İnternet Kullanıcıları (30.06.2019)	Penetrasyon Oranı (% Pop.)	Büyüme 2000-2019	İnternet Dünyası %
Afrika	1320038716	17,10%	522809480	39,60%	11,48%	11,50%
Asya	4241972790	% 55.0	2300469859	54,20%	1,91%	50,70%
Avrupa	829173007	10,70%	727559682	87,70%	592%	% 16.0
Latin Amerika / Karayipler	658345826	% 8.5	453702292	68,90%	2,41%	10,00%
Orta Doğu	258356867	3,30%	175502589	67,90%	5243%	3,90%
Kuzey Amerika	366496802	4,70%	327568628	89,40%	203%	7,20%
Okyanusya / Avustralya	41839201	0,50%	28636278	68,40%	276%	0,60%
DÜNYA TOPLAMI	7716223209	% 100.0	4536248808	58,80%	1,16%	100%

Kaynak: Internet World Stats, www.internetworldstats.com/stats.htm.

[164] Internet World Stats, "İnternet users in the Top 20 Countries in 30.06.2019", http://www.internetworldstats.com/top20.htm , ET:17.01.2020.

Bu sayılar çerçevesinde siber hakkında düşünürsek; siberin yüz binlerce birbirine bağlı bilgisayardan oluştuğu, kritik altyapılarımızı yapan sunucular, yönlendiriciler, anahtarlar ve fiber optik kabloları içerdiği unutulmamalıdır. Bu kadar büyük miktarda verinin organizasyonu konu haline geldiğinde de alan adı sistemi(Domain Name System- DNS) gibi teknik çözümler geliştirilmeye başlamıştır. Güvenlik sorunlarının oluşmasıda savunma veri ağı(defense data network ve network information center) kurulmasına yol açmıştır. 1992'de savunma dışında halkın erişiminin açılmasıyla birlikte ABD savunma bakanlığı internete desteğini çekmiştir. Böylece DARPA (Defense Advanced Research Projects Agency – İleri Savunma Araştırma Projeleri Ajansı) tarafından geliştirilen İnternet'in, 1990'lı yılların başında ticari amaçlı olarak tüm dünyada kullanımı hızla yaygınlaşmıştır. 1992 yılına gelindiğinde; zaman çizelgesi sona ermiş, internetteki sunucu sayısı bir milyona ulaşmış, ARPANET varlığını sonlandırmış, bilgisayar dokuz kat daha hızlı hale gelmiş ve ağ bant genişliği yirmi milyon kat daha fazla olmuş bir hale gelmiştir.[165] İnternetin hızlı bir şekilde artan önemi ve kullanılır lığının bu şekilde artması sonucunda zamanla ülkelerin denetleyici kontrol ve veri toplama (SCADA) sistemleri ile ülke güvenliğinin kritik altyapıları BİT'e son derece bağımlı hale geldi. Yani bir benzetme yaparsak siber alan kısaca dünyanın sinir sistemi haline gelmiş; modern toplumun kontrol sistemini yönetmeye başlamış ve son olarak korunması zorunluluk olan uluslararası varoluşsal bir kaygı haline dönüşmüştür. Böylece 2000 li yıllarla birlikte artık internet asıl kullanım amacını terk ederek siber tehditler ve güvenlik risklerini oluşturmaya başlamıştır. Bu yeni süreç sonucunda da sahtekârlık, dolandırıcılık, terör faaliyetleri, casusluk, savaş ve saldırılar bu alana geçmeye başlamıştır. Bu yüzden devletlerin internetin doğuşuyla birlikte siber çatışma döneminin bir parçası olduğunu rahatça söyleyebiliriz.

Bir diğer yandan ilk başlarda sadece insanların birbirleriyle iletişim kurması ve bilgi paylaşması amacına sahip olan internet, takip eden yıllarda tüm alanlarda kullanılmaya başlamıştır. Böylece bilişim sistemlerini içeren sanal bir ortam oluşmuştur. Bu yeni ortamdaki artan etkileşim özelde insanların genelde ise devletlerin vazgeçilmez alışkanlıklarından biri olarak tarihteki yerini almıştır. Bu gelişim süreci, donanım sektörünü, yazılım sektörünü, elektronik cihaz üreticilerini

[165]Computer History Museum, A History of the Internet 1962-1992, https://www.computerhistory.org/internethistory/ , ET.17.01.2020.

geliştirip büyütmüştür. Böylece sanal dünya olarak adlandırılan yeni bir dünya ortaya çıkmıştır. [166]

Bu yenidünya ortamı 5. Boyut olarak konumlandırdığımız siber uzay boyutunun oluşmasının da en büyük sebebidir. Bu ortam her ne kadar sanal olarak adlandırılsa da sonuçları fiziksel olabilmekte ve insanları farkında olarak ya da olmayarak etkileyebilmektedir. Yani siber uzay coğrafyası, toplumun tüm katmanlarını etkileyerek her alanda her şeyi etkileyebilmektedir. Çünkü siber uzay ve siber uzayı oluşturan katmanlar birey, toplum ve hatta devletlerin güvenlik sınırlarını zorlayabilmektedir. Bu teknolojik altyapı sadece internet ile kısıtlı kalmayıp; bankacılık sisteminden, sulama sistemlerine, enerji üretiminden, ulaşım sistemlerine, finans sistemlerinden sağlık sistemlerine, haberleşme sistemlerinden ulusal savunma sistemlerine kadar pek çok farklı alanda etkili bir şekilde kullanılmakta ve güvenlik olgusu açısından da büyük önem taşımaktadır. Her alanda artan bu önem güvenlik problemini ortaya çıkarmış ve bu yönde strateji geliştirilmesini zorunlu hale getirmiştir. Çünkü binlerce yılın birikimiyle gerçekleştirilen radikal teknolojik yenilikler yâda taktiksel ve stratejik doktrinler nasıl tarih boyunca sürekli kökünden değiştirdiyse ve dönüştürmüşse günümüzde de beşinci boyutla birlikte güvenlik ihtiyacı siber alana kaymıştır. Bu durum ise mevcut teknolojilerde milli yazılımların geliştirilip birleştirilmesi sonucunu ortaya çıkarmıştır. Böylece siber uzay 1980'lerde varsayımsal bir terim iken, günümüzde bilgisayarların boyutları küçüldükçe, maliyetler düştükçe, iletim ve aktarım hızları arttıkça, kapasiteleri ve yetkinlikleri genişledikçe hayatın her alanında tüm aktörler için kullanılan stratejik açıdan vazgeçilemez bir terim haline dönüşmüştür. Bunu siber öncesine bakarak daha iyi anlayabiliriz.

Siber çağdan önce ulusların kapasitesi insan gücü, donanım, coğrafya, ekonomi ve moral karışımı üzerinden değerlendiriliyordu. Savaş ve barış dönemleri arasında kesin bir ayrım vardı. İnternet teknolojisi stratejiyi de doktrini de gerisinde bıraktı. Siber saldırıda bulunmanın korunmadan daha kolay olması karmaşıklığı daha da ağırlaştırdı. Bir dizüstü bilgisayar ile küresel boyutta etkisi olabilecek sonuçlar yaratılabilir hale geldi. Bir ülkenin fiziksel topraklarının tamamen dışında yürütülen eylemlerle elektrik şebekeleri vurulabilir ve enerji tesisleri devreden çıkarılabilir hale

[166]Ahmet Naci Ünal, a.g.e , ss. 20-30.

geldi. Bu etki boyutunun yanında siber çağın bu kadar önemli bir hale gelmesini Henry Kissinger'ın Dünya Düzeni adlı kitabındaki yaklaşımıyla daha iyi anlayabiliriz. Henry Kissinger bu kitabında uluslararası düzenin evrimini 4 döneme ayırmaktadır. Bunlar; Vestfalya barışı (çoğulcu uluslararası düzen), viyana kongresi (Avrupa güç dengesi sistemi), nükleer çağda dünya düzeni ve son olarak siber teknoloji dünya düzenidir.[167]

Aynı zamanda; yazara göre dünya Vestfalya'dan beri bir düzene ve fikir birliğine sahip değildir. Bu yüzden gerilim artmakta ve siber güvenlik riskleri ön plana çıkmaktadır. Kitle imha silahlarının artması, nükleer santrallerin yayılması, çatışmaların insan anlayışının ötesine taşınması tehdidi ile teknolojik gelişmeler küresel düzeyden siber uzaya taşınmıştır. Örneğin; Sanayi ve teknolojide meydana gelen değişiklikler büyük güç dengelerinde ortaya çıkan değişiklikleri, iletişim alt yapısındaki değişimleri, mali etkenleri, askeri silahları, ulaşım ve enerji faaliyetlerini etkilemekte böylece savaş yöntem ve çeşidi de değiştirmektedir. Her yüzyılda değişimler yeni savaşları ve yeni güçleri ortaya çıkarmış ve bu sürekli devam etmiştir. Örneğin sanayi devrimi bir çırpıda oldu diyemeyiz. 1776, 1789 ve 1917 devrimleriyle kıyaslandığında sanayi devrimi kademeli ve ağır gelişen bir süreçtir. Sanayi devrimiyle birlikte canlı güç kaynaklarının yerine cansız güç kaynakları almıştır. Günümüz bilgi devrimiylede artık cansız güç kaynakları sanayi üretimi yani imalat sanayi yerine siber uzayı ön plana çıkarmıştır.[168] Bu durumda harp malzemelerindeki değişimi yaratarak siber silahların kullanımını arttırmıştır. Kullanılan bu yeni siber silahlarla birlikte bilginin üretimi, toplanması, aktarımı ve dağıtımının bilgisayarlar ve ağlar ile gerçekleştirilmesi de güvenlik yaklaşımlarını geliştirmiştir.

Özetle; siber uzay'ın uluslararası ilişkilerdeki gelişini anlayabilmemiz için kısaca internet'in yerel ağ ve uluslararası ağ üzerindeki izlediği gelişme sürecini açıklamalıyız. Bu süreci kısaca açıklarsak şunlara değinmemiz gerekir. En az iki bilgisayarın birbirlerine bağlanıp, bilgi alışverişinde bulunmasına bilgisayar ağı (Network) denir. Bilgisayar ağları, kullanıcılara bilgisayarlar arası bilgi paylaşımı yapabilecekleri bir ortam sağlar. Bilgisayar ağına bağlı kullanıcıların, ağın kaynaklarına ulaşması ve diğer kullanıcılarla iletişimde bulunması ağ kullanımının

[167] Kissinger. D.D, a.g.e. ss. 372-379.
[168] Paul Kennedy, B.G.YveÇ. a.g.e, ss.185-187.

temel amacıdır. Bu da zaman ve para tasarrufu sağlar. Aynı ortamlarda bulunan bilgisayarların oluşturduğu ağlarada yerel bilgisayar ağları (LAN, Local Area Network) denir. [169] Bir ofiste bulunan birkaç bilgisayarın ve bir yazıcının birbirine bağlanması yerel bilgisayar ağına örnektir. Farklı mekânlarda bulunan ya da birbirlerinden uzak bilgisayarların oluşturduğu ağlara ise geniş bölge ağları (WAN, Wide Area Network) adı verilir. Geniş bölge ağları, yerel bölge ağlarını birbirine bağlar. Böylece içinde bulunduğumuz küresel ağ sistemi içinde tüm dünya birbirine hızlıca bağlanarak geniş bölge ağını oluşturmaktadır. Milyonlarca bilgisayardan oluşan, binlerce bilgisayar ağını birbirine bağlayan global ağa ise Internet denir. Bu ağın bir yöneticisi yoktur. Zaten uluslararası sistemin anarşik yapısına benzerlik oluşturarak bu yapıyı tetikleyip dış politikada aktif olarak kullanılmasının da sebebi bu yüzdendir.

Ayrıca Internet kullanıcıları birbirleri ile haberleşmek için her cihazda sayılardan oluşan IP adresleriyle ortak bir anlaşma dili kullanılır. Bu adreslere bilgiler en kestirme yoldan ulaşır. Burada IP adreslerinin değiştirilmesi veya izinsiz kullanılması gibi durumlarla kendilerine ait olmayan bilgi paketlerini diğer yerlere aktarmalarıyla birlikte suç, terör ve savaş üçgeni ortaya çıkmaktadır. Çünkü siber uzay, içerisinde bilginin çevrim içi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağlarının (ve arkalarındaki kullanıcıların)âlemidir. Siber uzay, ilk başta yaratılan, saklanan ve her şeyden önce paylaşılan dijital verilerden oluşan bilgi ortamıdır. Siber uzay sırf sanal değildir. Hücresel teknolojileri, fiber optik kabloları ve uzay tabanlı iletişim araçlarını da kapsar. Siber uzayın anahtar özelliklerinden biri sistem ve teknolojilerinin insan yapımı olmasıdır. Siber uzay küreseldir ve yaşam gibi sürekli evrim geçirmektedir. Doğal olarak siber uzaydan beklentilerde evrim geçirmektedir. Siber uzayı(interneti) telgraf ve telefondan ayıran devre değişim yerine paket değişimini içermektedir. Paketler küçük dijital veri zarfıdır. Böylelikle hızlı ve daha çok bilgi saklama ve paylaşma imkânı sağlamaktadır. [170]

Siber uzay ile ilgili bir diğer önemli nokta 1990'lardan itibaren internetin hızla gelişmesine paralel olarak siber suç, siber terörizm, siber saldırı, siber casusluk ve siber savaş gibi kavramların ortaya çıkmasıdır. Yani; bireylerin ve devletlerin yaptıkları saldırgan eylemler geleneksel düzenden sanal ortama taşınmıştır. Bu

[169] Anonim, Network, http://www.egitim.com, ET. 10.12.2019.
[170] P.W Sınger, ve Allan Fıedman, S.G ve S.S. a.g.e, ss. 29-33.

sorunların çözülememesindeki en önemli sorun da uluslararası işbirliği eksikliği, bu alanı düzenleyen bir hukuk kuralının olmaması ve uluslararası bir kurumun bulunmamasıdır. Böyle bir yapı içerisinde siber uzayın kullanımı arttıkça iç ve dış hukuk boyutundaki eksiklikler daha da artacaktır. Çünkü iç hukukta siber suçların ifade edilmesi 1960'lar, düzenleme yapılması ise 1970'lere kadar gitmekteyken uluslararası bir hukuk yapısı hala kurulamamıştır. Bu durumda ölçemiyorsan yönetemezsin özdeyişiyle siber veriyi toplayıp, işleyen, analiz eden ve geleceğe yönelik strateji üreten devletlerin bu yeni boyutta yaşanacak çatışmalarda ön plana çıkacağını göstermektedir. Bunun en güzel örneğini de dördüncü bölümde ayrıntılarıyla açıklayacağımız çatışma örneklerinde görebiliriz. Sonuç olarak, son zamanların en büyük buluşu olan internet, hayatın her alanını etkileyerek önemi her geçen gün artmaktadır.

2.5. Siber Saldırı Teknik ve Yöntemlerinin Sorunsala Dönüşmesi

Uluslararası ilişkilerin temel güvenlik kavram tartışmaları çerçevesinde siber kavramların sorunsala dönüşmesi, siber uzay ve teknolojinin günümüzde her alanda kullanılması ve tüm sektörleri bir araya getiren çatı görevini üstlenmesinden kaynaklanmaktadır.

Uluslararası anarşik yapıda kullanılan siber saldırılar vasıtasıyla sistem içine ulaşılarak tüm bilgilerin ve komuta merkezi kontrol edilebilmektedir. Siber saldırıların en temel amaçlarından biri olan karıştırma faaliyeti; haberleşme, radar, füze sistemleri, uçak sistemleri, askeri gemi ve denizaltı sistemleri gibi birçok alanda kullanılmaktadır. Yâda hava harekâtlarında hedeflerin yanıltılmasında kullanılabilir. Elektronik aldatma yapmanın temel amacı, elektronik yöntemler kullanarak sahte hedef işaretleri üretebilmektir. Bu yöntem askeri araçlara karşı kullanılmasının yanında sivil gibi görünse de milli güvenlik imkânlarını gerektirecek askeri, emniyet ve istihbarat gibi kurumların internet sitelerine veya elektronik ortamda sakladıkları gizli arşivlere ulaşarak önemli bilgilere erişilmesi içinde kullanılmaktadır.

Bu bağlamda siber dönüşüm kavramlarının uluslararası ilişkilerin temel kavramları üzerinde yarattığı sorunsalları belirli başlıklar altında inceleyebiliriz. Kısaca bu sorunsallar şunlardır;

➢ Hegemon Sorunu

Anarşik uluslararası yapı hiçbir zaman değişmemiştir. Fakat tarih boyunca hegemon bir güç olarak adlandırılan aktörlere her zaman askeri açıdan bakılmıştır. Dünyanın en büyük imparatorluğu kabul edilen Roma İmparatorluğu, Dünyaya "Pax Britanica" yı getiren Kraliçe Victoria Britanya'sı, sonrasında Dünya'nın tek kutuplu olduğunu iddia eden ABD Pax-Americanası iddia edilmiştir. [171] Bu hegemon güçler bir döneme etki etmiş olsa da dünya anarşik sistemi hiç değişmemiştir. Dünya tarihinde hegemon güçlerin yerleri, coğrafyaları, anayasaları, nüfusları, kültürleri, kullandıkları teknolojileri, savaş araçları, savaşta ve barışta güvenlik anlayışları her zaman askeri nitelikli olmakla birlikte birbirlerinden hep farklı olmuş ve anarşide devam etmiştir. Günümüzde de teknolojinin gelişmesiyle birlikte internetin hayatımıza girmesi sonucunda "bilgi devrimi" gerçekleşmiş ve güvenlik bakışı salt askeri olmaktan çıkarak siber yöntemlerle askeri sonuçlar elde edilebilme imkânını ortaya çıkarmıştır.

Günümüz küresel durumu teknoloji liderliğinin erozyona uğradığı ve her devletin artık siber alanda saldırı ve savunma konusunda aktif olmak zorunda olduğu bir yapıya dönüşmüştür. Dünya imalat ve ticaretindeki paylar, küresel banka mevduatları, küresel yatırım akışı, uluslararası teknoloji transferi, nükleer silahların yayılması ve küresel markalar sayesinde "çok kutuplu" bir uluslararası sistem anarşik siber uzaya giden süreci hızlandırmıştır. Anarşik bu yeni süreçte tüm aktörlerin kaçınmak zorunda olduğu husus nükleer savaş gibi yıkıcı sonuçlara yol açabilecek küresel siber savaşın olma olasılığını önlemektir. Özellikle bu yapı içerisinde hegemon bir güç bulunmaması ve devletlerin rakiplerine karşı iz bırakmadan siber silahları kullanabilmesi fırsatından dolayı bu ortamı kullanması ciddi bir sorun yaratmaktadır.

➢ Güç Paradoksu, Gücün Kaynağı, Güç Dengesi ve İttifak Sorunu

"Güç" insanlık tarihinden beri en önemli kavramdır. Bugüne kadar yaşanan tüm mücadeleler gücü elde etmek için yaşanmıştır. Fakat "Güç" kavramının oluşmasını sağlayan araçlar teknoloji nedeniyle sürekli değişmiştir. "siber uzay" geçmişten günümüze kadar kabul edilen tüm güç unsurlarını içine alan ve etkileme

[171]Burak Semih Gülboy, "Pax Britannica'dan Pax Americana'ya", Academia, https://www.academia.edu/5416592/Pax_Britannica_dan_Pax_Americana_ya ET.14/12/2019.

gücüne sahip olan yeni bir güç alanı oluşturmuştur. Geçmişten günümüze kullanılan bu güç alanlarından bazıları şunlardır;

Askeri; İlk başlarda ok ve yay etkiliyken, sonrasında barutun icadıyla tabancalar kullanılmıştır. 1. Dünya Savaşında makineli tüfek ve tankların gelişmesiyle sonucunda savaş daha kanlı hale gelmiştir. İkinci Dünya Savaş yıllarının sonlarına doğru nükleer çağın başlaması ise Soğuk Savaş süresince nükleer ve biyolojik silahların güç ve tehdit unsuru olarak ortaya çıkmasına yol açmıştır. siber uzayın tehlikeli hale dönüşmesinin sebebi ise tehlikesi baştan kabul edilen nükleer ve biyolojik silahlara dışarıdan müdahale edilme riskidir.

Nükleer Enerji; 19. yüzyılda uranyum güç kaynağı değildi. Fakat günümüzde uranyumun zenginleştirilmesi çok önemli bir güç kaynağı haline gelmiştir. Soğuk Savaş'ın başlangıcından günümüze kadar geçen süreçte uluslararası sistemde gerçekleştirilen temel mücadelelerin başında rakip güçlerin nükleer bir güce sahip olmasını engellemek vardı. Bu strateji günümüzde de siber uzay aracılığıyla gerçekleştirilmektedir. Bunun en güzel örneğini İran'ın yüz yüze kaldığı stuxnet olayında görmekteyiz.

Ulaşım; 19. yüzyılda savaş unsurlarının hızlı bir şekilde savaş alanına sevk edilmesi için demiryolları sistemi kullanılmakta ve sanayi önemli bir unsur olarak ön plana çıkmaktaydı. Örneğin; 1860'larda Bismarck Almanya'sı ile birlikte bu araçlar aktif olarak kullanılmaya başlanmıştır. 20. yüzyılda Rusya'nın batısında demiryolunun gelişmesi ise Almanya'ya korku salmıştır. Günümüzde bilgi devrimi sonucunda internetin hayatımıza girmesi tüm ulaşım sistemlerini (havacılık, karayolları, demiryolları vb.) birbiriyle entegre haline getirmiştir. Entegre olan bu sistemlere karşı gerçekleştirilebilecek bir siber saldırı ise tüm ülkenin ulaşım sistemini çökertebilme riskini içinde barındırmaktadır. Bu iddianın en güzel örneklerini ise Estonya Krizi, Gürcistan ve Ukrayna Müdahalesinde görebiliriz.

Sonuç olarak; David Hume güç dengesini temkinli politikaların sürekli hâkimiyeti olarak ifade eder. Çok kutuplu bir sistem olarak güç dengesi, ittifaklar kavramıyla da yakından ilişkilidir.[172] Siber uzay alanında güç dengesi ve ittifak sistemini oluşturma yönündeki ilk atılımlarıda Estonya krizi sonrasında görmekteyiz.

[172] Joseph S. Nye ve David A. Welch, K.Ç. ve İ.A. a.g.e , ss.108-118.

Estonya krizi sonrasında NATO tarafından oluşturulan merkezle devletlerin kendi siber güvenliklerini sağlamaları yönündeki ilk ittifak eğilimi örnekleri görülmüştür. Fakat Siber uzayın sahip olduğu dinamiklerden dolayı ittifak kurulma ihtimali çok zordur. Bu sebeple Soğuk Savaş dönemi nasıl aynı zamanda kriz istikrarı getirdiği için istikrarlı bir dönem olarak görülüyorsa aynı şekilde günümüz siber savaş dönemi de bu sahte istikrar yapısını içinde barındırmaktadır. Nasıl nükleer savaşın etkisi korku yaratmış ve ülkeleri frenlemişse, siber savaşın aleni olarak uygulanmasının etkisinin büyüklüğü de devletlerin bu saldırıları aleni bir şekilde yürütmelerini engellemektedir. Bunu bir örnekle açıklarsak; 20. yüzyılda Soğuk Savaş'ın hâkim olduğu yıllarda ABD, Vietnam'a komünizmin domino etkisi gibi yayılacağını düşündüğü için girmişti. Eğer girmeseydi komünist tehlikenin yayılacağından korkuyordu. Bugün siber savaşların aleni uygulanmamasındaki sebepte bu domino etkisidir. Bir sistemin bozulması diğer hayati sektörleri de etkileyecek böylece insanoğlunun geçmişten günümüze tüm kazanımları yok olabilecektir.

- **Evrensel Siber Uluslararası Hukuk Kuralı ve Üst Otorite Yoksunluğu Sorunu**

Uluslararası sistemin içerdiği anarşik yapı siber uzay alanında da devam etmektedir. Bu yüzden devletler ulusal çıkarlarını sağlayabilmek için siber faaliyetlerini gizli olarak yürütmektedir. Aynı zamanda coğrafi konum ve yakınlık, jeopolitik gelenek gibi konularda öngörüleri ortadan kaldıran siber uzay tamamen sınırı olmayan ve herkesin herkese kolaylıkla saldırabileceği bir yapı sunmuştur. Buda ülkelerin kendi siber güvenlik duvarlarını oluşturmalarını zorunlu kılmıştır. Aynı zamanda; bu bölümde vurgulanması gereken asıl husus uluslararası kurumların realistlerin varsaydığı anarşinin etkisini hafiflettiğidir. Bu sebeple siber uzayda gerçekleşen sorunlardan sorumlu bir uluslararası örgütün oluşturulması şarttır. Siber uzay hakkında tam anlamıyla yetkiye sahip bir şekilde oluşturulacak bu örgüt uluslararası hukuk kuralları çerçevesinde sistemde bir güç dengesi ve istikrar yaratacaktır. Aksi takdirde sistemin içinde barındırdığı anarşi artarak devam edecektir.

Öngörülen bu çatışma sürecinde liberal barış perspektifiyle uluslararası barışın inşasının sağlanabilmesi için uluslararası hukuk kuralları ve bu kuralları uygulayacak kurumsalcı bakıştaki kurumların oluşturulmasıyla birlikte sağlanacak

bir kapsamlı yönetişim şarttır. Liberal kurumların yokluğu ve / veya zayıflığı ise siber silah kullanılarak gerçekleşen çatışmalara yol açan güvensizliğin ana nedenidir. Bu iddiamızı destekleyecek en güzel örnek Soğuk Savaş döneminde yaşanmıştır. Soğuk Savaş sırasında Birleşmiş Milletler'in (BM) güvenlik işlevleri olmasına rağmen, Doğu-Batı çatışmasındaki güvenlik politika sorunları kurumlar tarafından sağlandı. [173] Günümüzde de güvensiz zamanlarda yaşıyoruz. Bu yüzden küresel güvenlik politikasının güvensizliği ele alması gerekmektedir. Bu da aynı Soğuk Savaş dönemindeki gibi devletlerin ve kurumların birlikteliğiyle sağlanabilir. Bu birlikteliğin sağlanması ise Uluslararası Hukuk kurallarının oluşturulmasına bağlıdır.

Geleneksel olarak güvenlik politikaları, bir yabancı tarafından yapılan bir saldırıyı püskürtmek için tasarlanmış askeri güçleri ifade eder. Günümüzde de siber çatışmalarda Gürcistan-Rusya savaşında ABD'nin Gürcistan siber güvenliğine yönelik desteği, Estonya Saldırısından sonra NATO'nun verdiği destek bu doğrultuda gerçekleşmiştir. Aynı zamanda AB'nin üye ülkeleri için oluşturduğu uygulayıcı polis gücü ve hukuki sözleşmelerdeki belirlediği hukukun üstünlüğü ilkesi de bu amaçla gerçekleştirilmiş örneklerdir.

- **Özgürlük Sorunu**

Otoritenin bireylerin duyguları, arzuları ve seçimlerine yansıyan özgür insan iradesinden kaynaklandığını savunan Liberaller, insanların özgürlüğünü en önemli değer olarak kabul eder ve yüceltir. Özgürlüklerini koruması için ise insanlar bu hakkı leviathana devretmiştir. Günümüzde devletler siber uzay alanında verecekleri kararları ve uygulayacakları yöntemleri yapay zeka ve bulut bilişim sistemlerine bırakmaya başlamıştır. Artık insanların beyin ve beden hareketleri bilimsel anlamda ölçülüp, incelenip takip edilmektedir. Böylece " özgür irade" fikri ve özgür iradeye sahiplik hissi yok olmaya başlamaktadır. Hareket ve konuşmaların dışarıdan izlenmesi ve iç deneyimlerin kaybedilmesi yönetim sistemlerini doğuran bir gözetim rejimine dönüştürmektedir. Bu çerçevede yukarıda ayrıntılarıyla bahsettiğimiz hususlar iki konuda içinde büyük bir risk barındırmaktadır. Bunlardan birincisi; yapay zekâ sayesinde gerçekleştirilen algoritmalar çerçevesinde vatandaşlar daha iyi tanındıkça otoriter hükümetlerde vatandaşlar üzerinde mutlak bir kontrol elde etme

[173] Mary Kaldor ve Iavor Rangelov, "The Handbook of Global Security Policy", Wiley Blackwell Journal, 2014, ss.1-29.

imkânı kazanmaktadır. Bir diğer tehlikeli husus siber güvenlik zafiyeti sonucunda gerçekleştirilecek bir siber saldırı sonrasında ülkedeki vatandaşlara yönelik tüm kritik verilerin düşmanların eline geçme ihtimalidir. Bu yüzden tehlike şurada yatmaktadır. Tüm aktörler vakitlerini yapay zekâ geliştirmek, bulut bilişimi oluşturmak, siber uzay alanında çalışmalar gerçekleştirmek üzerine kurgularsa; önümüzdeki yıllarda tüm dünyanın sahip olduğu özgürlükleri derinden sarsacak büyük bir yıkımın gerçekleşme ihtimali açık bir şekilde ortada durmaktadır.

- **Yetki Sorunu**

Nesnelerin interneti ve yapay zekâ gibi uygulamaların hayatın her alanında kullanılmaya başlamasıyla birlikte kanunların ve kararların vericisi ve uygulayıcısı bilgisayarlar ve robotlar olmaya başlamıştır. İlerleyen süreçte artık savaşı robotlar yapacaksa veya savaş kararını robotlar verecekse bu robotların kime ve nasıl hizmet edeceği fiilen kanıtlanabilmiş değildir. Örneğin; yapay zekâ insanların hayatlarıyla, hangi okula gideceğinden, nerede çalışacağından, kimle evleneceğine yönelik her türlü karar verme yetkisini ellerinden almaktadır. Artık aktörler yerine yapay zekâ düşünüp karar vermektedir. Bu durum sosyal, kültürel veya ekonomik kararlarla sınırlı değildir. Siyasi ve askeri kararlarda da benzer süreçler kullanılmaktadır. Peki, gelecekte yapay zeka ile yanlış karar verirlerse durum ne olacak? Şuan bu sorunun cevabı belli değildir. Askeri ve siyasi süreçte bir diğer önemli durum ise siber savaş ilan etme yetkisinin bir devlette kimde olması gerektiğidir. Siyasi irade de mi? Yoksa orduların içinde oluşturulan siber orduların komutanlarında mı? Bu tarz yetki kararları hala net değildir.

- **Eşitlik ve Mülkiyet Sorunu**

Eski zamanlarda en kıymetli şey topraktı. Günümüzde ise en kıymetli husus "internet" ve "veri" dir. Veriyi elinde tutan geleceği de elinde tutmaktadır. Eskiden devletlerin askeri ve siyasi amaçları toprakları kontrol etme mücadelesi iken günümüz siber dünyasında verilere erişmek için mücadeleler yaşanmaktadır. Artık tüm aktörlerin en değerli varlığı olan kişisel ve hayati verileri elektronik ortamda bir başkası tarafından ulaşılıp, kontrol edilip ve izlenme tehlikesine sahiptir. Bu yüzden tüm insanlar, makinalar, sektörler ve sistemler birbiriyle iç içe geçmiş bir sistem içindedir. O zaman asıl soru şudur? Verinin mülkiyeti nasıl düzenlenir? İnternet

kullanımını yasaklama hakkı var mıdır? Varsa bu hak kime aittir? Sorusu cevaplanamazsa günümüz liberal eşitlikçi düzeni bu krizi taşıyamayacaktır.

Günümüzde yaklaşık olarak iki yüz civarında olan bağımsız devlet diplomatik ve uluslararası hukuk konusunda Birleşmiş Milletler çatısı altında içlerinde farklılıklar bulunsa da uzlaşılmış gözükmektedir. Peki, siber uzayın sınırı konusunda devletler neden bir çizgi çizememektedir?

21. yüzyıl ile insanlık tarihinden beri süregelen orantısız toplum yapıları ve sınıflar arası orantısızlık daha da derinleşmiştir. İşin ilginç tarafıysa küreselleşmeyle birlikte teknolojik gelişmeler sonucunda oluşan bu makasın, siber uzay tarafından gözler önüne serildiği halde artarak devam etmesidir. Tabii malvarlığı uzun süreli eşitsizliklerin önkoşuldur ve eşitsizlik taş devrine kadar uzanmaktadır. Fakat internetin hayatımıza girmiş olmadığı hiçbir zamanda bu kadar aleni bir şekilde herkes tarafından görülen bir hiyerarşi oluşmamıştır.

- **İnternetin Durduğu Gün ve " World Wide Web War-1 " Riskini Kabul Etmeme Sorunu**

Teknolojinin hayatımızdaki yeri arttıkça bundan istifade etmek isteyen, devlet, örgüt, kişi sayısı da artmaktadır. İnternetin tamamen durma ihtimaline karşı birkaç senaryo bulunmaktadır. Bu saldırılardan en önemlisi "kök alan sunucularını" hizmet dışı bırakacak saldırılardır. Böylece internet sitelerine ulaşım ve IP'lere erişim sağlanamayacaktır.[174] Şu ana kadar siber uzayda yaşananların başlangıç noktasında olmasından dolayı gerçekleşebilecek riskler henüz tam olarak bilenememektedir. En önemli risk ise oluşabilecek bir küresel siber savaş tehdidinin bir kıyamet senaryosuna yol açma ihtimalidir.

2. Dünya Savaşının bitmesinden sonra dünya tarihinin en barış dolu dönemi yaşanmıştır. Teknolojideki gelişmeler sayesinde savaş araçlarındaki değişim bu savaşın geleneksel ve nükleer bir savaşa dönüşmesini engellemiş ve devletler, siber savaş denilen bir başka alana güçlerini kaydırmıştır. Günümüzde artık sadece askeri güç veya "sert güç" işe yaramamaktadır. Örneğin; ABD'nin Irak ve Afganistan'da yaşadığı fiyasko, İsrail'in 1967 savaşı hariç hiçbir savaşta büyük kazanç elde etmemesi, yükselen güç Çin'in 1979 Vietnam çıkarması sonrası ekonomi temelli

[174] Alper Başaran, "Yaklaşan Felaketin Habercileri Siber Kıyamet", Arion Yayınevi, İstanbul, 2017 ss.11-14.

faktörlere dayanarak gelişim göstermeye mecbur kalması vb. Bu yüzden artık büyük devletlerin küçük devletlere karşı bile her türlü silahlı saldırıdan ziyade ekonomik, siyasi ve siber yöntemleri kullanmaya başlamıştır. Bunun en güzel örneği ise; 21. yüzyılda bu alanı en başarılı kullanan ülkelerin başında olan Rusya tarafından Gürcistan savaşı ve Ukrayna da Kırım'ın işgal edilmesi aşamalarında görülmüştür. Böylece; Rusya fazla savaşmasına gerek kalmadan stratejik öneme sahip bir bölgeyi ele geçirdi. Rusya'nın son yıllarda eski Sovyet coğrafyasına yönelik gerçekleştirdiği bu saldırgan hamleler, yeni bir dünya savaşına giden süreçte yeni bir alan olan "siber uzay" konusundaki açıkları kapatma çabası gibidir. Bunu da NATO üyesi Estonya'ya karşı gerçekleştirdiği siber saldırılarda görebiliriz.

Sonuç olarak eğer ülkeler savaşın kaçınılmaz olduğunu düşünürse, siber silahlarla geliştirilmiş geleneksel veya nükleer bir savaş dünyaya çok ciddi zararlar verebilir. Bu durumda herkes için bir felaket olabilir.

- **Güvenlik Sorunu ve Güvenlik İkilemi**

Günümüzde artık her alan bilişim sistemleri üzerinden yürütülmekle birlikte ihtiyaç duyulan her şeyde bir başkasının uzmanlığına ihtiyaç duymaktayız. Böylece işbirliği ve bağımlılık her geçen gün artmakta bu da siber uzay yöntemiyle bunlara erişilebilme riskini ortaya çıkarmaktadır. Bu sebeple günümüzde her alanda uzmanlaşıldığından Taş Devri'nde yaşayan insandan daha fazla şey bildiğimizi düşünsekte aslında kendi başımıza daha az bilgiye sahibizdir. Kurumsal hafıza sebebiyle başkasının kafasındaki bilgileri kendi bilgilerimiz gibi kullanmamız ve bu bilgileri bulutlar sayesinde siber alanda muhafaza etmemiz "siber saldırıları" ortaya çıkarmakta ve hem bireylerin hem de devletlerin ne kadar güçsüz ve çaresiz bir durumda olduğunu göstermektedir.

Aynı zamanda saklanması gereken büyük sırlar siber uzay vasıtasıyla artık ifşa edilerek devlet başkanlarını veya önemli liderleri baskı altına almaktadır. Bu sebeple, bireyler veya önemli liderler, teknolojik cihazlar, ekonomik eğilimler ve dünyayı şekillendiren siyasi dinamikler sebebiyle korunmasızdır. Böylece teknoloji insanları ve dolayısıyla diğer aktörleri yönlendirip kontrol etmektedir. Bu yönlendirmeler ise devlet kademesinde krizleri ve görevden almaları doğurmaktadır. Bu durum 7/24 savunma yapmamız gerektiği bir güvenlik riskini ortaya çıkarmaktadır.

Son olarak ülkeler kritik alt yapı hizmetlerini“ network“ adı verilen bilgi ağları üzerinden kontrol etmekte ve bu da sanal saldırıların çıkış noktasını oluşturmaktadır. Siber uzayla birlikte artık ulusal sınırları korumak güvenlik ihtiyaçlarını karşılamamaktadır. Telekominikasyon, bankacılık, finans, elektrik enerjisi, petrol ve doğalgaz dağıtımı, su temini, nakliye, acil hizmetler ve devlet hizmetleri gibi ortak kritik alt yapılar siber saldırılar sayesinde müdahale edilebilecek kritik ulusal güvenlik alt yapılarını oluşturmaktadır. Bu yapı içerisinde aktörlerin her birinin siber alana yatırım yapıp elde ettikleri teknolojik kazanımlarla siber silahlar üretmesi bir diğerinde güvenlik ikilemi yaratmaktadır.

- **Değişimi Kabullenmeme Sorunu**

Yüzyıllar önceki dönemde yaşayan medeniyetler bugünkü dünya düzenini hayal bile edemezdi. Aynı şekilde günümüzde yaşanan siber çatışmaların gelişerek gelecekte siber savaşın yaşanacağını iddia etmemizde birçok kişi tarafından kabul edilmeyecektir. Bu yüzden; gelecekteki dünyanın nasıl olacağını şuan kestiremezken teknolojinin bu kadar geliştiği ve dönüştürdüğü dünyada güvenlik yaklaşımlarının oluşturulmasında teknoloji kaynaklı siber güvenliğe daha çok önem verilmesi gerekmektedir.

Değişim kaçınılmaz bir gerçektir. Beden değişir, hayat değişir, zihin değişir, bireyler değişir, devletler değişir ve dünya değişir. O halde hayatı bir arada tutan şey tüm bu değişimin içindeki bilinmezliklerdir. Siber saldırılar ve siber istihbarat vasıtasıyla bilgiler toplanır, yapay zekâ sayesinde ön görüler ve tahminler yapılabilir böylece bilinmezlikler siber istihbarat ve siber saldırı sayesinde yok olabilir.

Artık bilginin inanılmaz miktarda yoğun olması ve bilgiye erişimin kolaylığı geçmişten günümüzü tamamen ayırmaktadır. Günümüzde Big Data, Bulut Bilişim ve Yapay Zekâ sayesinde stratejik bilgi sistemlerine siber saldırılar vasıtasıyla sızarak ulaşılan bilgiler işlenip en doğru plan belirlenmektedir. Bu durumu kabul etmemek çağın gerisinde kalmak ve başarısızlığı baştan kabul etmek demektir. Tüm bu gelişmeleri uluslararası ilişkilerde yaşanan çatışmalardan ayrı değerlendiremeyiz.

- **Eğitim Sorunu**

Sanayi devrimi ile birlikte uluslararası arenada devletler güçlü olabilmek için sömürge ve pazar arayışına girerek savaşlar yapmıştır. İçeride ise devletler sanayi

devrimi seri üretim bandı kavramı üzerine bir eğitim kuramı geliştirerek bu alanda uzmanlar yetiştirmişlerdir. Aynı şekilde günümüzde de siber uzayın önemini fark eden devletler; normal eğitim müfredatı sisteminin yanında çocuklara diferansiyel denklem çözme, bilgisayar kodu yazma, yazılım geliştirme, bir test kupüründeki kimyasalları tespit etme gibi yetenekleri çocuklara yerleştirmeye çalışmaktadır.

Değişim hızı arttıkça sadece askeri, ekonomik, sosyal ve kültürel hayat değişmemekte, insanlar da değişmektedir. Dolayısıyla üst otorite olarak devlette dönüşmekte ve tüm hizmetler e-devlet'e kaymaktadır. Sistemi, Devletleri ve hatta bireyleri hacklemek kavramı bu sebeple bu alanda eğitim almamış yöneticiler tarafından kontrol edilirse bu yönetimler ciddi güvenlik risklerinin oluşmasına yol açabilir. Çünkü elektronik taarruza karşı en etkili tedbir, iyi tasarlanmış bir sistem kadar, iyi eğitilmiş bir operatör yani iyi eğitimli bir insan yetiştirmekten geçmektedir. Ne yazık ki günümüzde bu bilinç tam anlamıyla oturmamıştır.

- **Dış Politika Stratejilerinin Belirlenmesinde Diplomatik Müdahale Sorunu**

Uluslararası politikayı var eden, devletlerin izledikleri dış politikalardır. Her ülkenin dış politikası çap ve büyüklüğüne göre değişmektedir. Doğal olarak güvenlik algısı da aynı şekildedir. Bir devletin dış dünyadan etkilenme düzeyi ne kadar düşük, dış dünyayı etkileme düzeyi ne kadar yüksekse, o devletin dış politikasının diğer devletler üzerindeki etkisi de o kadar güçlü olur.[175] Siber savaşlarda ve siber uzayda da bu durum böyledir. Devletler var oluşlarını sürdürebilmek ve uluslararası politikada daha nüfuslu olabilmek için günümüzde siber güvenlik stratejileri geliştirmek zorundadır. Siyasi, askeri, ekonomik, teknolojik ve kültürel araç bakımından bir devletin zenginliği, o devletin siber güvenliğinde de risk potansiyelini etkilemektedir. Örneğin; ABD'nin sahip olduğu yumuşak güç kapasitesi; ters orantılı olarak siber güvenlik riskine onun daha açık bir durumda olduğunu göstermektedir. Dolayısıyla, siber uzay ile birlikte ulusal güç kavramları da değişim göstermiştir.

Dış ilişkiler geçmişinde acı tecrübeler yaşamış bir devlet; o tecrübelerden bağımsız bir politika geliştiremez. Günümüzde NATO ülkeleri Soğuk Savaş

[175] Gültekin Sümer, Dış Politika Stratejileri, İkinci Adam Yayınları, 2013.

korkuları ile bağlantılı olarak günümüz çatışmalarında Rusya ve NATO/ABD arasındaki gerilimlerde bu durumun devam ettiğini Estonya örneğinde görmekteyiz.

Ayrıca siber dış politika stratejilerinin belirlenmesinde asıl olan kazanım, başarı, bilgi, birikim, gelişme ve özellikle güvenliği sağlamaktır. Siber stratejiler ile asıl hedeflenen amaçlar güvenlik, statükoyu sağlama, caydırıcılık oluşturma, büyük güç olma, rakibi saf dışı etme, rakipler üzerinde nüfus kazanma, inşa etme, ittifak/koalisyon oluşturma vb. dir. Barış dönemi stratejisi olarak gözüken günümüz siber dış politika stratejilerinin temel güvenlik hedefleri bir devletin en temel dış politika hedeflerini içeren bağımsızlık, toprak bütünlüğü, egemenlik gibi bir devleti devlet yapan en temel öğe ve değerlerin siber uzayda sağlanmasına dayanır.

Aynı zamanda; dış politika stratejilerinin siber güvenliği sağlama çerçevesinde uygulanması ekonomi, siyaset ve diplomasi gibi pek çok alanı içine alır. Zaten; Fiziki güvenliğin olmadığı yerde siber güvenlikten bahsedemeyiz. Bu yüzden günümüzde güvenlikten bahsetmemiz için geleneksel ve siber alanı birbirinden ayırmamalıyız. Dünyanın en iyi en güçlü ordusuna da sahip olsanız da eğer bilişim açıklarınız varsa daha güçsüz bir rakip size büyük zararlar verebilir. Bu durum çatışma kavramının geleneksel alandan bilişim alanına kaydığını göstermektedir. Örneğin; Türkiye açısından S-400 Hava Savunma Sistemlerinin satın alınması ve yeni nesil F-35 savaş uçaklarının Türkiye'ye teslimi konusunda günümüzde yaşanan sıkıntılar dış politika stratejilerinin siber güvenlik özelinde tartışıldığının en temel göstergesidir. Bu konuya siber güvenliği gerçekleştirme temelinde yaklaşırsak; Türkiye tarafından S-400 Hava Savunma Sistemlerinin satın alması NATO Güvenlik sistemlerine ilişkin Rusya tarafından sistemlere sızılması riskini ortaya koymaktadır. Bu yüzden de ABD uzun bir süredir ambargo koyarak yeni nesil F-35 savaş uçaklarını Türkiye'ye teslim etmeyeceğini belirtmektedir. Konuya stratejik açısından yaklaşırsak; Türkiye Rusya'dan S-400 Hava Savunma Sistemlerini satın almayarak Patriot hava savunma sistemini alsa da bu sorunu yaşamaya devam edecektir. Yani sorunun asıl temeli Diplomatik Müdahale Sorunudur.

Özetle; bir ülke için istediğini istediği yerden satın alarak alternatifleri arttırması onun uluslararası alanda bağımsızlığının, alternatif güç kaynaklarına sahip olma isteğinin, millileştirme ve kendi yazılımını kullanarak kendi güvenliğini

sağlama ve bağımlılığını azaltmaya yönelik stratejik bir bakışıdır. Geçmişte ülkemizde yaşanan diplomatik krizler sonrasında alınan Kabotaj kanunu ve kapitilasyonların reddi gibi kararlar aslında günümüzdeki S-400 mücadelesinin arkasındaki milli duruş ve bağımsızlık zihniyetiyle aynıdır. Farklı olan tek şey dış politika stratejileri belirlenirken teknolojinin değişmesi sonucu bilgisayar, internet ve yazılım temelli bir askeri güvenlik yapısının oluşmasıdır. Bu sorunsallar çerçevesinde siber güvenlik tehditlerine karşı kritik alt yapıların korunması ve uygulanacak politikalardaki risk yönetimi çok önemli bir hal almıştır.

2.5.1. Duygusal Etkiler ve Algı Faktörleri Çerçevesinde Psikolojik Bakış

Siber dönüm kavramlarının yarattığı sorunsalları incelerken ilk olarak duygusal ve algı faktörleri çerçevesindeki gelişimi ve psikolojik olarak etki boyutunu incelememiz gerekmektedir. İnternet ve internet ticareti her geçen gün gelişen teknoloji yaşantımızın vazgeçilmez bir parçası olmuştur. Özellikle bilgisayar ve cep telefonlarının dışında arabalardan, buzdolaplarına ve hatta akıllı ev sistemlerine kadar hayatın her alanı internetle çalışır hale gelmiştir. Barajlardaki pompalayıcı sistemlerden, elektrik santrallerine, enerji sistemlerinden ulaşım ve haberleşme yapısına, finans ve bankacılık sisteminden tüm hasta kayıtlarının işlemlerinin yürütüldüğü sağlık sistemine, e-devletten e-arşive kadar hayat tamamen internete hem psikolojik hem de fiiliyatta bağımlı hale gelmiştir. Örneğin; ABD seçimlerinde veya Gürcistan-Rusya Savaşı'nda da görüldüğü gibi siber uzayın bilgi sistemlerine yönelik etkileri halk üzerinde ciddi derecede psikolojik bir etki unsuru haline gelmiştir. Çünkü kişisel özelliklerinin bilinmesi tüm davranışları etkileyip manuple edebilir, psikolojiyi bozabilir, motivasyonu yok edebilir ve prestij kaybına yol açabilir.

İnsan davranışlarının nasıl şekillendiğini anlamak için yardımcı bir yaklaşım insan ihtiyaçlarının bir tipoloji içinde belirtilmesi ve organizasyonu olmuştur. İnsan motivasyonunu sınıflandırmanın ve tüketici davranışlarını açıklamanın en popüler yöntemlerinden birisi de Maslow'un İhtiyaçlar Hiyerarşisi dir. Abraham Maslow'un ihtiyaçlar hiyerarşisi beş basamaktan oluşmaktadır. Bunlar temel fizyolojik ihtiyaçlar, güvenlik ihtiyaçları, sosyal ihtiyaçlar, saygınlık gereksinimi ve kendini geliştirme ihtiyaçlarıdır. İhtiyaçlar, yemek, sevgi, kendine güven gibi şeylerin eksik

olmasıyla harekete geçen güçlerdir. Maslow'un hiyerarşisi bir kişinin hiyerarşi tablosundaki ilk basamağı tamamlamadan sonraki basamağa geçilemeyeceğini gösterir. Günümüzde internet bütün basamakların tamamlanmasında en etkin intiyaç olarak ortaya çıkmıştır. Web siteleri, e-postalar, oyunlar, iletişim(cep telefonu/uydu vb.), elektrik sistemleri gibi insanların anlık olarak kullandıkları yaşamın her parçasına internet hakimdir. Bu alanların dışında da bir çok sektör ve hizmette gereksinimlerin hepsi doğrudan veya dolaylı olarak günümüzde internete birşekilde bağımlıdır.

Bu yeni teknolojilerle insanlık modern çağda artık gerçek ve sanalın bir arada olduğu dünyada kendilerini yeniden konumlandırmaya ve fizyolojik ihtiyaçlarını da değişime uğratmaktadır. Öncelikle yapay zeka, bilgi entegrasyonu, otomasyon, robotizasyon, insan hayal gücü ve yaratıcılık gücüyle birleştiğinde Maslow'un ihtiyaçlar piramidi bu çerçevede yeniden mercek altına alınabilir.

2.5.2. Donanım ve Yazılım Güvenliğinin Rolü

Anarşik uluslararası sistemde, sadece geleneksel düzeyde değil aynı zamanda bilişim alanında da aktörler tehdit edilmektedir. Bu tehditlere karşı elektromanyetik sistemler ve siber uzay yoluyla çeşitli teknikler kullanılarak gelen saldırılar bertaraf edilmeye çalışılmaktadır. Burada kullanılan asıl önemli sistem dost sistemleri koruma sorunudur.

Hem siber uzayda hem de elektro manyetik alanda güvenliği sağlayabilmek için gerekli sistemler ve yazılımlar oluşturulurken dost ve düşman olarak sistemin algılayacağı formüller kullanılmakta ve bunlara yönelik personel, tesis, elektronik ekipman ve sistem oluşturulmaktadır. Böylece; bilişim dünyasında kullanılan bu sistemlerin dışında kalan her şey elektronik ortamda düşman olarak görülmektedir. Bu durum elektronik ortamda korumayı yani siber güvenliğe olan ihtiyacı ortaya çıkarmaktadır. Bu yüzden elektronik korumada dikkat edilmesi gereken önemli hususlar bulunmaktadır. Bunlar; radar tasarımı, verici düzenekleri, frekans seçimi ve kullanımı, radar güç yönetimi, alıcı düzenekleri, otomatik kazanç kontrol sistemleri, değişik yapıda alıcı ve özel alıcı devreler, gelişmiş izleme teknikleri, radar karıştırıcı, karıştırma işaretlerinin kullanımı vb.dir.[176] Siber güvenliği sağlamak için kullanılacak

[176]Ahmet Naci Ünal, a.g.e, ss. 99-101.

bu yöntem ve taktikler geleneksel yöntemlerden tamamen farklı olmamakla birlikte bu dost sistemlere olan sızmaları engelleme amacıyla bir arada yürütülmelidir.

Aynı zamanda; uluslararası bir çatışma aracı olarak siber savaş hem sivil hem de askeri alanda kullanılan kritik derecede sofistike elektroniklere, uydu iletişimine, ve bilgisayar yazılımı türü sistemlere müdahale etme yeteneğini sağlayan siber silahlarla saldırı gerçekleştirilmesine bağlıdır. Bu yüzden siber silahlar tehlikelidir. Siber silahların kapsayıcı ve bütünleştirici bir şekilde kullanılmasıyla oluşabilecek siber savaşı mümkün kılan üç şeyden en önemlisi ise yazılım ve donanımdaki kusurlardır. Örneğin; İnternet birçok donanımda kullanılabilir. Fakat tüm cihazlar (bilgisayar terminalleri ve dizüstü bilgisayarlar, yönlendiriciler ve anahtarlar, e-posta ve web sayfası sunucuları, veri dosyaları) çok sayıda şirket tarafından yapılır. Farklı şirketler tarafından üretilen tüm bu cihazları çalıştıran şey ise yazılımdır.[177] Örneğin; ABD'de donanım ve yazılım pazarında, çoğu dizüstü bilgisayar Dell, HP ve Assle tarafından üretilmektedir. HP, Dell, IBM ve diğer pek çok ürünün çalıştıkları yazılım esas olarak Microsoft, Oracle, IBM ve Assle tarafından yazılır. Fakat Çinli bir şirket olan Lenovo'nın IBM'in dizüstü bilgisayarını satın alması ve BT ve ağ konusunda dünya lideri olan Cisco ve Juniper'in de Çinli Huawei şirketi tarafından üretilmeye başlamasıyla birlikte iki ülke arasındaki rekabetin ilk sinyalleri verilmeye başlamıştır. Aynı zamanda, ABD şirketleri olmasına rağmen, makineler üzerinde çalışan kodların başka yerden gelmesi de güvenlik risklerinin tehdit boyutunu arttıracağı bir sürece sistemi götürmüştür. Bu yüzden siber güvenli toplum için hem donanımların hem de yazılımların güvenliğinin sağlanması gerekmektedir.

İlk olarak siber güvenlik açısından donanımların güvenliğinin sağlanmasına yönelik geliştirilen hedefler incelendiğinde, cihazların her zaman sınırlı olacak bir siber risk oluşturacağı bilinmelidir. Aynı zamanda güvenli bir cihaz, güvenli bir mimari ve sistem tasarımı yaklaşımı gerektirir. Güvenlik özelliklerine sahip bir cihazın güçlendirilmesi, her zaman siber güvenlik açıklarını bırakacak bir durdurma boşluğu yaratacaktır. [178]

[177]Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books ss.60-80.
[178] Erik Halthen, "The Role of Hardware Security to Meet Industry 4.0 Aspirations", Analog Devices, ss.1-3https://www.analog.com/media/en/technical-documentation/tech-articles/The-Role-of-Hardware-Security-to-Meet-Industry-4.0-Aspirations.pdf ET.28.02.2020.

Bu boşlukları doldurarak siber güvenlik açıklarının azaltılması ve daha güvenli yapıların oluşturula bilinmesi için üç önemli adım geçilmelidir. İlk büyük adım siber ortama yönelik endüstri standartlarını ve en iyi uygulamaları karşılamak için bir siber güvenlik çözümü stratejisinin uygulanmasına olanak tanıyan bir organizasyon oluşturmaktır. İkincisi; siber güvenlik yaklaşımında gerçek dünyadan gelen girdileri kabul edebilen, güvenilirliğini değerlendirebilen ve bağımsız hareket edebilen bir siber güvenli sistem aracılığıyla sağlanan gerçek zamanlı kararlar verilebilmesinin sağlanmasıdır. Son sorun, yalnızca buluta bağlı değil, aynı zamanda bulut hizmetleri aracılığıyla diğer sistemlerle senkronize olarak çalışan bir yapı geliştirmektir.

Sonuç olarak bu üç önemli adımı başarılı geçebilmemiz için siber uzayı insan vücudunu oluşturan hücre, doku, organ ve sistem gibi düşünmeliyiz. Hepsi benzer yapıda ve bir arada vücudu çalıştırdığı gibi siber savaşlarda diğer tüm yöntemlerle bir arada kullanılan bir çatı görevindedir. Bu sebeple siber uzayda siber güvenliği sağlamak için milli imkânlarla oluşturulacak siber kümelenmelerin oluşturulması şarttır.

2.5.3. Kritik Alt Yapılara Yönelik Risk Yönetimi

Siber güvenlik tehdit türleri genel olarak finans, askeri, enerji, sağlık ve bilişim gibi tüm kategorilerde bozma, engelleme, casusluk faaliyetleri ile gizli bilgilere erişme vb. teknikleri kapsamaktadır.

Tehdit edilen potansiyel kritik alt yapı hedeflerden bazıları şunlardır;

Tablo 4 Siber Güvenlik Tehdit Alanları

Kritik alt yapı tesisleri, akaryakıt ve enerji merkezleri	Su sistemleri, barajlar ve arıtma tesisleri	Acil hizmetler, sağlık sistemleri ve merkezleri
Bilgi ve Telekominikasyon	Bankacılık, Finans merkezleri ve ticaret sistemleri	Hükümet
Dijital alan ve Sosyal Medya Platformları	Posta, nakliye ve lojistik merkezler	Tarım ve gıda
Savunma sanayii	Stratejik askeri ve siyasi hedefler	Kimyasal materyaller
Kamu düzeni ve güvenlik	Ulaşım sistemleri ve ulaştırma tesisleri (Hava üsleri, limanlar, karayolları, demiryolları vb.)	Gaz
Sivil havacılık	Elektrik	Nükleer santraller ve fabrikalar

Bu sebeple ulusal güvenliğin korunması ve ulusal çıkarların sağlanması içinde tehdit ve fırsatları barındıran daha karmaşık ve zorlu bir hal almıştır. Bu durum beşinci savaş ortamı olarak görülen siber uzayda başarı için amaç ve araç uyumunun olmasını zorunlu hale getirmiştir. Bu uyum tam anlamıyla sağlandığı takdirde, ülke destekli siber saldırılara karşı milli güvenlik sağlanarak kritik bilgi altyapıları korunabilir. Fakat bu koruma asla %100 güvenliği sağlamamaktadır. Bu sebeple siber tehditler herkes tarafından çok önem verilmesi gereken bir tehdit türüdür. Aynı zamanda buradaki en önemli tehditlerin başında çatışmaların sadece suç ve teröre indirgenmesi ve savaş boyutunun önemsenmemesidir. Bir başka ifadeyle siber terörizm ve siber suçla mücadele için yasalar var olsa da Kritik Altyapı Korumasının önemi hala tam olarak anlaşılamamıştır.

Modern bir toplumda birbirine bağlı altyapılar ve temellerin varlığı komut ve kontrol işlemlerinin sanal ağa yönelik bağımlılığını, savunmasızlığını ve tehlike altında kalmasını tetiklemektedir. Toplumun altyapısını oluşturan bu sistemler ve ağlardan sadece biri için bir kesinti diğer sektörlerde korkunç sonuçlar doğurabilir.

Bu yüzden başlıca donanım ve yazılım platformlarındaki güvenlik sorunlarıyla yüzleşmek için ülkeler kendi içlerinde Bilgisayar Acil Müdahale Ekibi (CERT-In) oluşturarak siberliği artırmak için reaktif ve proaktif hizmetler sunmak zorundadır. Oluşturulan bu Bilgisayar Acil Müdahale Ekibi (CERT-In)in raporlama ve analiz olmak üzere iki ana fonksiyonu bulunmalıdır. Bu raporlama ve analizler sonucunda siber uzay saldırısı söz konusu olduğunda güvenlik bakışının nasıl olması gerektiği yönünde aşağıdaki tavsiyelerin bir benzeri sunulmalıdır. [179]

a. Hükümetler siber suç ve siber savaş arasındaki ilişki konusunda açık bir ayrım yapmalı

b. Gerçek güvenlik açıkları tanımlanmalı

c. Ulusal hükümetler ve özel sistemler tanımlanarak saldırılardan izole olmaları sağlanmalı

d. Savunmanın da suç içerdiği anlaşılmalı

e. Çevrimiçi savaş araçlarının olup olmadığı belirlemek için Ar-Ge ye öncelik verilmeli

f. Açık bir yanıt doktrini geliştirmeli

[179] Lopamudra Bandyopadhyay, a.g.e. ss.1-14.

g, Altyapısına yönelik gerçekleşen saldırılara karşı tek taraflı olarak yanıt verme hakkını saklı tutmalı

h. Siber tehditler, siber savaş ve CIP gerçeğine yönelik mevcut iç hukuk oluşturulmalı

Bilgisayar Acil Müdahale Ekibi (CERT-In) tarafından oluşturulması beklenen yukarıdaki bu tavsiyeler dış politika stratejilerinin ve güvenlik yaklaşımlarının oluşturulması açısından çok önemlidir. Çünkü sosyal ve politik hedeflerinden dolayı devlet desteğini arkalarına alan bireyler ve gruplar siber terörizm bahanesiyle herhangi bir devletin bel kemiği olan altyapılarına saldırılar gerçekleştirmektedir. Kısacası şuanda devletler siber saldırıları direk kendi ordu birimleri vasıtasıyla gerçekleştirmek yerine terör örgütleri veya milliyetçi hacker grupları tarafından suç işleme maksadıyla gerçekleştirilen saldırı süsü vermektedirler. Günümüzde yaşanan bu çatışma süreci ile ilgili Nikolai Kuryanovich şunları söylemiştir;

Nikolai Kuryanovich'a göre; "Yakın gelecekte, açık savaş alanında pek çok çatışma olmayacak, daha çok bilgi askerlerinin yardımıyla Internet'teki alanlarda savaşacak. Bu, korsanların küçük bir kuvvetinin mevcut silahlı kuvvetlerin binlerce kuvvetinden daha güçlü olduğu anlamına geliyor.[180] Nikolai Kuryanovich belirttiği gibi siber uzay çatışmalarının aktif olarak yaşandığı bu yeni boyut Uluslararası İlişkiler sisteminin bir parçası olmaya devam edecektir. Çünkü günümüzde her alanda bilgisayar sistemleri ve bilgi sistemleri kullanılmaktadır. Bu nedenle siber saldırılara karşı korunma ve güvenliği sağlama önemlidir.

Siber saldırılara karşı güvenliği sağlamanın ve riskleri azaltmanın en etkili yollarından biriyse iletim sırasında gizlilik ve veri bütünlüğünün şifreleme sistemiyle sağlanmasıdır. Siber terörist saldırılara karşı modern kuantum bilgi teknolojilerinin sistemleştirilmesi ve sınıflandırılmasına yönelik oluşturulan güvenlik protokolleri doğrultusunda Kuantum anahtar dağılımı (QKD) protokolleri iki kullanıcı arasındaki bu şifrelemeyi sağlamaktadır.[181]

Kuantum anahtar dağılımı (QKD) protokollerinin avantajları:

---

[180] Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks", The Washington Post,16Ekim2008,http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?nav=rss_blog ET. 07.01.2020.

[181] Oleksandr Korchenko , Yevhen Vasiliu ve Sergiy Gnatyuk, "Modern Quantum Technologies Of İnformation Security Against Cyber- Terrorist Attacks", Aviation, Cilt.14, No.2, Yıl. 2010, ss.58-69.

1. Bu protokoller her zaman gizlice dinlemeye izin verir
2. Vernam ile QKD protokollerinin içerdiği şifreli (tek seferlik pad), karmaşık olmayan, koşullu, güvenli ve kimlik doğrulamalı düzenler tamamen güvenli bilgi aktarım sistemini sağlar.

Kuantum anahtar dağılımı (QKD) protokollerinin dezavantajları

1. Sadece QKD protokollerine dayanan bir sistem komple bir çözüm olarak hizmet verememesi
2. Kuantum özellikleri kaybolmadan kuantum kanal uzunluğunu sınırlaması
3. Tek yerine zayıf darbe kullanma ihtiyacı
4. Veri aktarım hızının kanal uzunluğundaki artışla ters orantılı olması
5. Foton kayıt problemi uygulamasıyla anahtar oranının düşmesi
6. Yüksek fiyat

Sonuç olarak; teknoloji patentlerinin çoğu ABD'de olan Kuantum Güvenli Doğrudan İletişim Protokollerinin (QSDC) ana özelliği hiçbir kriptografik dönüşüm olmaması sebebiyle anahtar dağıtım sorununun olmamasıdır. Bu protokollerde, gizli bir mesaj kubitlerin (quadits) kuantumuyla kodlanır ve bu kanal yoluyla gönderilir. Yani bilgi aktarmadan önce kanal oluşur. Böylece de sır elde edilemez. Ancak bu tür kübit bloklarını saklamak için büyük miktarda kuantum hafızaya ihtiyaç olması sebebiyle kuantum bellek teknolojisi aktif olarak kullanılamamaktadır. Bu doğrultuda günümüzün en gelişmiş kuantum kriptografisi olan QKD protokolleri bile komple bir çözüm olarak hizmet vermemektedir. Bu anarşik yapıda dezavantajlar riskleri, riskler ise tehditleri arttırmaktadır. Bu tehditleri kullanmayı seçip siber uzayda saldırı gerçekleştirmek isteyen aktörlerde siber güvenliğe önem vermeyen aktörlere ciddi zararlar verebilmektedir. Bu yüzden bilgi güvenliği yöntemi kuantum teknolojilerinin (içinde araştırma enstitüleri, laboratuvarlar ve merkezler, kuantum gizli anahtar dağıtımı için kriptografik sistemler ve uzak meşru kullanıcılarca) güvenli kullanımlarıdır.

2.5.4. Siber Uzayın Üstünlükleri ve Zayıflıkları

Soğuk Savaş'ın bitmesiyle birlikte dünya pazarını disipline etme savaşı bazen askeri engelleme ve tehdit, bazen ekonomik ambargo ve ticaret savaşı şeklinde

yürütülse de asıl geri planda siber çatışmalar devam etmektedir. Küresel alanda bu üstünlük arayışı ve beka mücadelesi için bilgi çok önemli olmuşken bilginin güvenliği ise siber güvenlik stratejilerinin gelişmesine yol açmıştır. Aynı zamanda; ekonomik ve siyasi bağımlılık askeri mücadeleden ayrı düşünülemez. Bu bağlamda siber silahlar bu rekabet içerisinde tartışmasız bir öneme sahiptir. Küreselleşmeyle birlikte kapitalist yaşamın etkisi derinleşme, ittifak ve işbirliklerinin krizleri fırsata dönüştürme mücadelesine yol açmıştır. Böylece internet gelişmiş Sovyet komünizmi gücünü kaybetmiştir. İnternet dengeleri değiştiren bir rol üstlenirken tüm dünyayı siber uzayın komutası altına alıp günümüzde yaşanan savaşların ana çerçevesini oluşturmuştur. Bu durumda devletler bütün ilişkilerini, kurumlarını, hizmetlerini ve hatta savaşlarını siber uzay çerçevesinde yürütmesine yol açmaktadır. "siber uzay" kavramının ağlarının her geçen gün artması sebebiyle de önemi artmaya devam edecektir. Nasıl geçmiş zamanlarda telgraf, demiryolu ve buharlı gemiler kullanılmışsa günümüzde de internet kullanılan en önemli iletişim aracıdır. Siber uzay kavramıyla birlikte artık dünya pazar ağı oluşmuş bu ağ ise tüm devletleri birbirine bağımlı hale getirmiştir. Bu ortak ağ sonucunda günümüzde enformasyon teknolojileri ile gelişen ortak dijital dil sayesinde teknolojik sistemler birleşmekte bu durum ise içinde avantajı ve kaosu bir arada barındırmaktadır.

Son olarak avantajı ve kaosu bir arada barındıran internet, geleneksel tehditlerle kıyaslandığında düşmanlara karşı belirlenen stratejilere ulaşma, zaman, mekân, maliyet, iletişim, vb. gibi konularda üstün ve zayıf yönleri içermektedir. Her bir aktör kendi güvenlik risklerine uygun güvenlik ve savunma faaliyetlerini gerçekleştirmelidir. Aksi halde oluşturulacak stratejilerden, alınacak kararlardan, uygulanacak dış politika faaliyetlerinden olumlu bir sonuç elde edilemez.

Dünyada her geçen gün kaynakların azalması ve üretim hacminin artmasıyla birlikte maliyetler artmaktadır. Bunun sonucunda yenilik beklentileri oluşarak gittikçe şiddetlenen küresel rekabet gelişmektedir. Bu sebeple devletler uluslararası politikada etkili olmak için dijitalleşmeninde etkisiyle daha hızlı, esnek ve verimli bir şekilde ilerlemelerine fayda sağlayacak araçlar kullanmaya başlamıştır. Siyasi, ekonomik, finansal, sosyal, hukuki, kültürel, dini, vb her alanda yaşanan bu değişimden en çok etkilenen güvenlik ihtiyacı olmuştur. Bu doğrultuda güvenlik algısına yönelik risk ve tehditlerde gerçekleşen dönüşüm sonucunda tehditleri fırsata,

dezavantajları avantaja dönüştürebilmek için siber güvenlik faaliyetlerini oluşturmak zorunluluk olmuştur. Ayrıca siber uzay stratejisinin geliştirilmesindeki iş modelinin ve swot analizinin yapılabilmesi için fırsat ve tehditler ile güçlü ve zayıf yönlerin ortaya konulması gerekir.

- **Siber Uzayın Üstün Yönleri**

İnternetin hayatımıza bu denli hızlı girmesi nedeniyle internet kullanımına olan talep artmıştır. Bu talep artışının temel sebebi güvenlik, sağlık, sosyal, enerji, kamu düzeni, finans, bankacılık vb. her alanda hem kurumların hizmetlerini kolay verebilmesi ve takip edebilmesi hem de insanların hayatlarını daha kaliteli, hızlı ve kolay yaşayabilmesidir. Bu durum devletlerin kendi aralarında yürüttükleri siber savaş, bireylerin ise birbirlerine veya kurum/devletlere karşı yürüttükleri siber saldırı, siber suç, siber terör ve siber casusluk gibi kötü yolların kullanılmasına yol açmıştır. Bu kavramların oluşmasındaki üstün yönler ise şu şekilde sıralanabilir.

- ✓ **Yer ve Zaman Bazında Gösterim**

Siber uzayın içinde barındırdığı belirsizlik, tahmin edilemezlik ve iz bırakmazlık gibi özellikler gerçekleşen saldırıların ne zaman, nerede, hangi hedef kitleye hitap edeceğini bilmeyi zorlaştırmaktadır. Bu durum ise geleneksel güvenlik yaklaşımlarının bırakılarak yerine asimetrik olarak tanımlanan tehditlere karşı ulusal yada uluslararası düzeyde savunma stratejilerinin oluşturulmasını zorunlu kılmıştır. Tüm aktörlerin siber uzaya olan bağımlılığının ve çalışma koşullarının farklı olmasıysa oluşturulacak güvenlik yazılımlarının milli olması gerekliliğini ortaya çıkarmıştır. Coğrafi bölgeler açısından da özellikle Estonya örneği sonrasında NATO siber saldırılara karşı oluşabilecek tehditlerin yer ve zamanının önceden tespit edilebilmesi ve önlem alınabilmesi için Mükemmeliyet Merkezi oluşturmuştur. Bu sebeple geleneksel güvenlik yaklaşımlarının aksine 7/24 hedef kitleye hitap edebilecek saldırı ve savunmayı içinde barındıran ve sürekli kendini ve sistemlerini değiştirmeye, yenilemeye ve güncellemeye hazır bir şekilde tutmak zorundadır.

- ✓ **Hızlı Sunum ve Yayınlanma**

Teknolojinin gelişmesiyle birlikte bireyler için en önemli şey zamanla yarışmaktır. Zamanın bireyler açısından bu denli önemli olması nedeniyle internet

sosyal hayatta çok daha hızlı ve etkili olmuştur. İnternet'in hızlı yayınlanması ise hem bireylerin bağlı oldukları devletlerin kendi vatandaşları üstünde özgürlüklerini ellerinden alarak güç elde etmelerinde hem de rakip devletlerin diğer ülkenin vatandaşları üzerinde proboganda yürütmelerine yol açmıştır.

Geleneksel yöntemlerle sunulan askeri güvenlik yöntemlerinde sınırlara askerler, tanklar, savaş araçları yığmak yeterli gözükebilir. Ya da nükleer bir silah geliştirerek rakibe karşı bir caydırıcılık yaratılarak bu süreç tamamlanabilir. Saldırmak istendiğindeyse günümüz şartlarında sadece geleneksel yöntemler düşünülürse kara, hava, deniz ve uzay faaliyetleri yürütülebilir. Bu süreçlerin hepsi günler sürebilir. Fakat siber uzay üzerinden gerçekleştirilen saldırılar sanal ortamda bir anda çok geniş bir alana yayılarak etkili olabilir.

- ✓ **Düşük Maliyet**

Günümüzde ordu beslemek ve silah satın almak çok maliyetli bir iştir. Devletler düşmanlarıyla bir savaşa giriştiklerinde bunun her iki taraf içinde ciddi derecede maliyetli olacağını bilmektedir. Siber uzay ise devletlere amaçladıkları politikalara en düşük maliyetle en hızlı şekilde ulaşma imkânı tanımıştır. Bu sebeple bilgi devrimi sonrasında gelişen teknoloji ve internet sayesinde savaşlarda bu alana kaymış, devletler ordular kurmuş ve bütçeler oluşturmuştur. Günümüzde oluşturulan bu siber orduların geleneksel yöntemlere göre çok düşük bütçelerde yürütülüyor olması gelecekte de böyle olacağını göstermemektedir. Siber uzay'ın kullanıldığı alanlar arttıkça en az maliyetler maksimum fayda sağlama imkânı sebebiyle bu durum tersine dönecektir.

Siber uzayın saldırı ve savaşlarda sağladığı düşük maliyet ve maksimum fayda bakışı istihbarat faaliyetleri içinde geçerlidir. Siber casusluk ile devletler istihbarat birimlerini de bu alana kaydırarak faaliyetlerini internet, bilişim, yazılım, donanım, cihaz vb. üstünden gerçekleştirmeye başlamıştır. Özellikle kaynak kısıdı nedeni ile araştırmaya fazla bütçe ayıramayan küçük devletler Internet sayesinde hem hızlı hem de düşük maliyetli bir güç kazanmıştır.

- ✓ **Etkileşim**

Küreselleşmeyle birlikte teknolojinin gelişmesi ve bilgi devriminin etkisiyle uluslararası anarşik sistemde tüm aktörler arasında bağımlılık ve etkileşim artmıştır.

Bu bağımlılık ve etkileşimde bazı gruplar ittifak oluşturarak caydırıcılık yaratmayı seçmiş, bazıları ise hegemon olma amacıyla güç kapasitelerini arttırma yolunu seçmiştir. Fakat tüm bu gelişmeler sonucunda güvenlik ikilemi ortaya çıkmıştır. Güvenlik ikileminin bu denli artmasında özellikle internet sayesinde dünyanın küresel bir köy haline gelmesi önemli bir etken olmuştur. Bu sayede internet tüm aktörler üzerinde dost ve düşman demeden çift yönlü bir etkileşim olanağı sağlamıştır.

Böylelikle internet'in interaktif olma özelliği hem devletlere hem de devlet dışı aktörlere benzersiz kolaylıklar sağlama ve caydırıcılık yaratma noktasında önemli üstünlükler yaratmaktadır. Bu yüzden uluslararası anarşik yapıda siber uzayın kullanılır lığını ve etkinliğini her geçen gün arttırarak uluslararası ilişkileri domine eden hâkim savaş alanlarından biri haline dönüşmüştür. Bu durumun oluşmasının en önemli sebep ise bilginin en önemli güç haline gelmesidir. Bilginin bu denli önemli bir zenginlik haline gelmesi yüzyıllardır en zengin şirketler olarak gösterilen enerji şirketlerinin üstünlüğünün yerini bilişim şirketlerinin almasında görebiliriz. Bugün Assle, Microsoft, Google, Facebook, Yahoo gibi şirketler dünyanın en güçlü ve zengin aktörleri haline gelmiştir. E-ticaret alanı olarak da işlev gören internet, müşteri ve üreticileri biraya getirerek sağladığı hızlı ve etkin iletişim ile birlikte tüm dünya uluslarının aralarında daha güçlü ve sürekli bir ilişki kurmalarını sağlamıştır.

- ✓ **Ölçülebilirlik**

Geleneksel güç kapasitelerini siber güç kapasitesinden ayıran temel özellik bunun net olarak ölçülememesidir. Fakat devletlerin içinde internet kullananlarının oranı, internete bağımlı alanların sayısı, e-ticarete olan bağımlılıkları, finans sistemlerinin ve iletişim yapılarının elektronik ortamda kullanılır lığı gibi rakamlar üzerinden ölçümleme yapılabilir. Çünkü internet ortamının elektronik bir ortam olması sebebiyle kullanıcı ve katılımcıların oranları kolayca hesaplanabilmektedir. Devletler açısından konvansiyonel gücün tam tersi şekilde eğer siber alanda kullanım oranı fazlaysa içinde bulunulan risk ve tehdit oranı da aynı oranda yüksektir. Yani ABD'de internetin ilk icat edilmesi ve hayatın her alanında kullanılması aslında ABD'yi en riskli ülkelerden biri haline getirmektedir. Buda küçük ülkelere karşı bir avantaj sağlamaktadır.

- ✓ **Etkinlik**

Siber saldırıların etkinliğini gösteren en güzel örnek; bir aktörün düşmana karşı diplomasiyle gerçekleştiremediği veya silah kullanırsa kayıplarının ağır olacağı bir savaşa girmek yerine istediklerini siber uzayı kullanarak elde etmesinde görebiliriz. Bu durumu ABD'nin İran'a karşı uranyum zenginleştirmesini engellemek istediği fakat bunu askeri bir müdahale gerçekleştirmeden stuxnet silahıyla elde etmesinde görebiliriz.

Siber uzayın içinde belirsizliği, görünmezliği ve bilinmezliği barındıran yapısı ABD gibi büyük süper bir gücün bile kendinden görece küçük bir aktöre yönelik etkinliği sebebiyle bu silahı kullanmasına yol açmıştır. Ayrıca siber silahların hedefe özel hazırlandığında ne kadar avantaj sağladığını stuxnet olayı göstermiştir. Bu sebeple siber güvenliğin sağlanması ve etkinliğinin arttırılması için siber uzayda yazılımların milli olması, farkındalığın yaratılması, eğitimlerin verilmesi, kuralların koyulması ve kurumların oluşturulması gibi etkinliklerin gerçekleştirilmesi son derece önemlidir. Eğer bunlar tam anlamıyla gerçekleştirilirse dış politika stratejileri bütünlükçü bir yapıda siber güç kullanılarak daha etkin bir şekilde yürütülebilir.

- ✓ **Doğal Hayat**

Uluslararası anarşik yapının temeli insan doğasının kötü olmasına dayanır. Siber güvenlik içerisinde her ne kadar elektronik cihazları, yazılımları ve sistemleri barındırsa da en önemli halka bireydir. Bireylerin birbirlerine güvenmemesi, çıkarlarının uyuşmaması ve hep daha fazlasını istemesi ise birbirlerine karşı güvensizlik hissetmeleri ve korku duymalarına yol açmaktadır. Duyulan korku tehdit hissini perçinlemekte, tehdit hissi ise güvenlik riskini oluşturmaktadır. Bu süreç internete de aynı şekilde geçmiştir. İnternet ilk başta sadece iletişim ve haberleşme için üretilmişti. Fakat günümüzde çevreye zarar verebilmekte ve doğal hayatı olumsuz etkileyebilmektedir.

- ➢ **Siber Uzayın Zayıf Yönleri**

Internet üzerinden gerçekleştirilen tüm faaliyetlerin bireyler, toplumlar, devletler ve örgütler üzerinde olumlu ve içinde fırsatları barındıran güçlü yönleri olduğu kadar bazı zayıf yönleri de bulunmaktadır.

- ✓ **Tüm Topluma Ulaşamaması**

Dünyada, internet erişimine sahip olmayan hala devletlerin olması siber uzayın hak ettiği öneme ve etkinliğe ulaşmasını engellemektedir.

- ✓ **Dikkat Çekememe**

Güvenlik anlayışından bahsedildiğinde hala konvansiyonel silahların, balistik ve kıtalararası füzelerin ve nükleer silahların konuşuluyor olması siber silahların konuşulmasını engellemektedir. Siber ortam üzerinden gerçekleştirilecek saldırılar sayesinde aslında tüm bu yukarıda saydığımız geleneksel silahlar dışarıdan kontrol edilebilir, yönlendirilebilir, çalışamaz hale getirilebilir veya bozulabilir. Bu durum siber silahların amacının, gücünün ve hedef kitlesinin tam olarak anlaşılamadığını göstermektedir.

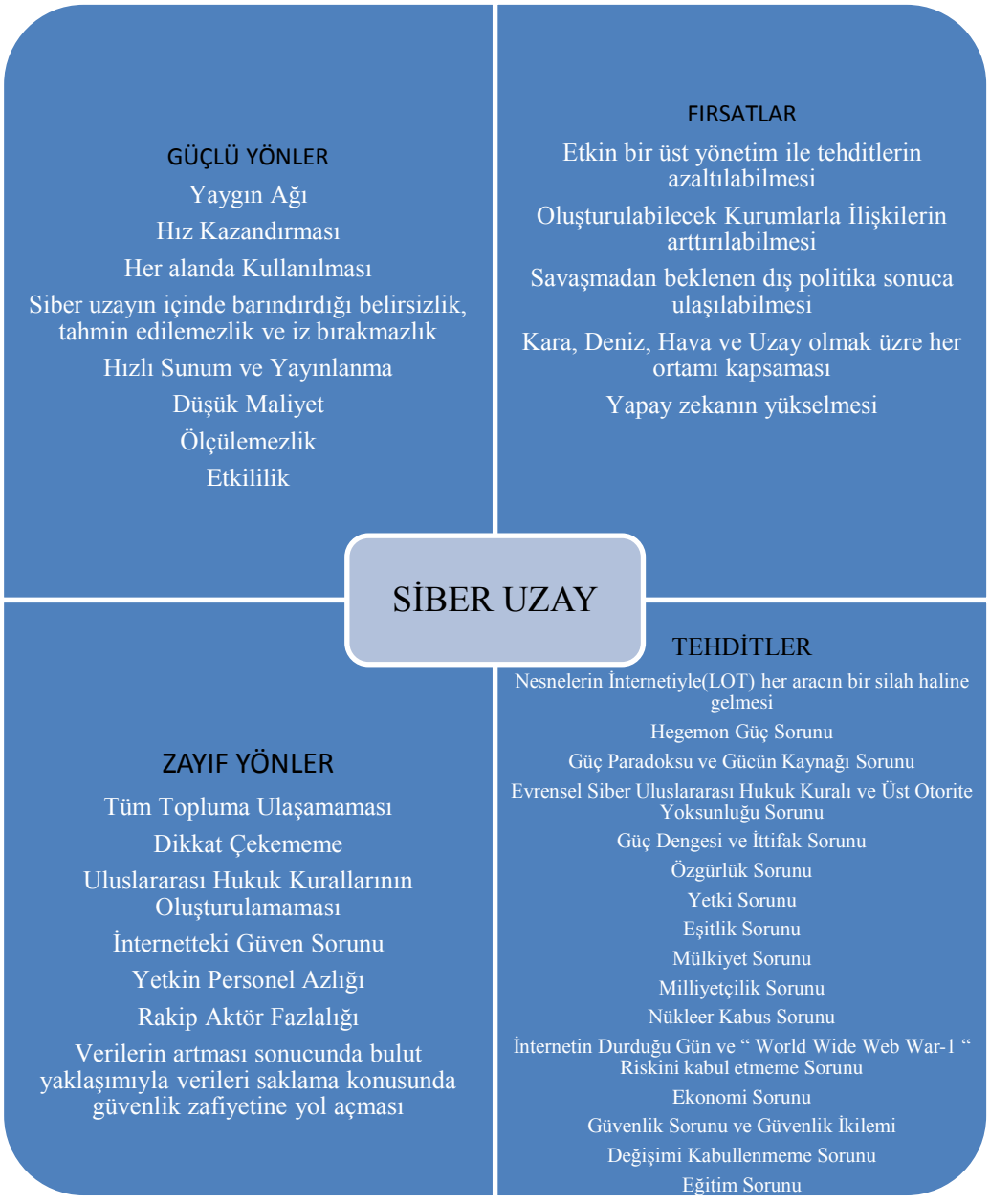
- ✓ **Uluslararası Hukuk Kurallarının Oluşturulamaması**

Siber uzayda gerçekleştirilecek tüm faaliyetlere yönelik uluslararası sistemde tüm aktörlerin izleyecekleri kurallar ve genel ilkeler, henüz tam anlamıyla yerleşmiş değildir. Bu olgu, ciddi bir siber saldırı, siber suç, siber terör, siber casusluk ve siber savaş kirliliği yaratmakta ve aktörlerin birbirlerine olan güvenlerini ortadan kaldırmaktadır. Amacı iyi belirlenmeyen her siber faaliyet hem işbirliğine hem de bağımlılık modeline önemli ölçüde zarar vermekte bu durum ise güvensizliği arttırmaktadır. Eğer amaçları iyi belirlenmiş uluslararası kurallar ve bu kuralları uygulayacak devletler üstü kurumlar oluşturulursa çatışma modeli işbirliğine dönülebilir. Aksi taktirde bu durum zayıflık olarak görülmeye devam edecektir.

- ✓ **İnternetteki Güven Sorunu**

Internet etiği kapsamında tartışılan ve zayıflık olarak gösterilen bir diğer önemli konu siber uzayda karşının görülmemesidir. Dark Web denilen internetin karanlık yüzü sayesinde hiçbir şey görüldüğü gibi değildir. Bu sebeple de insan ilişkileri arasında veya devletlerarasında kurulabilecek ilişkilere göre güven sağlanması çok zordur. Hiçbir aktör siber uzayda kendi bilgilerini karşıyla paylaşmak istemeyecektir. Bu durum ise günümüzün en değerli metası olan bilgi

kirliliğini ve dolaylı yoldan güven sorununu ortaya çıkaracaktır. Siber saldırılar günümüzde en çok prestij kaybı amacıyla kullanılmasıdır. Bu sebeple etik kuralların uygulanması şarttır.



Şekil 4. Siber Uzayın Güçlü/Zayıf Yönler İle Fırsat/Tehditleri İçeren Swot Analizi

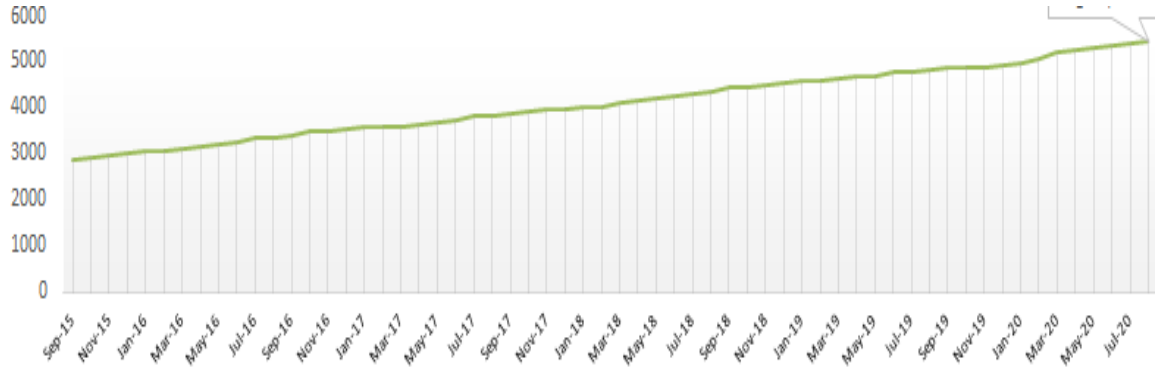
Sonuç olarak; internetin ortaya çıkmasından beri geçen süreçte internet kendi içinde sürekli bir ilerleme ve değişim geçirmiştir. 1982 yılında 1G, 1992 yılında 2G, 2001 yılında 3G, 2009 yılında 4G ve son olarak günümüzde konuşulan 5G bu süreci en kısa ve öz şekilde tanımlayabilir. Fakat 5G ile olan geçiş bütün diğer geçişlerden farklı yaşanmaktadır. Çünkü 1G den 4Gye geçiş aslında sadece internetin hızını arttırmaya yarayan süreçti. Fakat dünyanın 5G ye geçmesiyle birlikte bu durum tamamen farklı bir hal alacaktır. Yapay zekâdan ultra hızlı internete, uzaktan cerrahi müdahaleden evimizdeki her şeyin internetle yönetilmesine kadar gidecek bir süreçtir. Akıllı evler, akıllı şehirler, sürücüsüz araçlar ve daha da fazlası hatta bilim kurgu olarak görülen çoğu şey 5G teknolojisiyle hayatın gerçeği haline gelecektir. 5G diğerlerinden farklı olarak sadece hız değil aynı zamanda daha az gecikme de sağlayacaktır. Fakat bu durum avantajlar kadar dezavantaj da sağlayacaktır.

Hem olumlu hem de olumsuz yönlerine bakarak siber uzayda yaşanan bu yeni 5G dönüşümü bir fırsat mı yoksa tehdit mi bunu nasıl daha iyi anlayabiliriz? Daha az gecikme, akıllı yollar ya da sağlık sisteminde davinci robotunun çalışabilmesi bütün bunlar avantaj olarak görülebilir. Bu değişim ve dönüşüm aynı şekilde siyaset, istihbarat ve savaşlarda da aynı şekildedir.

Nesnelerin internetiyle hayatın her alanı internetle bütünleşip yapay zekâyla yönetilecektir. 5G bu avantajların yanında içinde bilinmezlikleri barındırması sebebiyle büyük bir tehdit de olabilir. Normal sosyal yaşamda karşımıza çıkabilecek bu risk örneklerini kısaca incelersek; 5G'nin yüksek hız düşük gecikme sağlamasından dolayı çevreye salacağı daha yüksek radyasyon ve bu artan radyasyon sonucu oluşabilecek hastalıklardaki artışlar, frekans sayısında artış sağlamak için daha fazla baz istasyonunun konulması ihtiyacı ve daha fazla enerji tüketimidir. Bu dezavantajlardan daha önemlisiyse bu tezinde asıl konusunu oluşturan siber güvenlikle alakalı olan kısmıdır. Siber uzayın sunduğu bu yeni 5G yapısı özellikle Türkiye gibi gelişmekte olan ülkelerde bu alanda yazılım, frekans, modem, baz istasyonu vb. ihtiyaçlarının gelişmiş diğer ülkelerden satın alma ihtiyacını doğurur. Bu durumda siber alanda ciddi bir milli güvenlik riski yaratacaktır. Böylece 5G ile bugüne kadar gerçekleştirilen tüm teknolojik yenilikler, gelişmeler ve çabalar yok olacaktır. Bu yüzden millileşme çabalarının boşa gitmemesi için siber gelişmeler yakından takip edilip en üst düzey güvenlik gereksinimleri karşılanmalıdır.

Ayrıca bu teknolojinin diğer ülkelerden ithal edilmesi güvenlik zafiyetinin dışında ciddi oranda ekonomik dengede de negatif yansıma yaratacaktır. Çünkü 5G sistemi ile hayatın bütün alanları etkileneceğine göre bütün bu alanlarda kullanılmasını sağlayacak araçların ithal edilmesi de aynı zamanda istihbarat anlamında güvenlik zafiyeti oluşacaktır. Böylece nesnelerin interneti ile bildiğimiz her şeyin internetle yönetilebilecek olması sonucu siber güvenlik riski boyut değiştirecek ve siber saldırılar artış gösterecektir. Dünya Ekonomik Forumu da zaten siber güvenliği bu gelecekteki gücünden dolayı en büyük risklerden biri olarak göstermiştir. Dünya Ekonomik Forumu'nun bu iddiasını en güzel örneklendirecek şey ise şudur; günümüzde yaklaşık 11milyar civarında cihaz internete bağlı durumdayken bile ciddi oranda risk faktörü oluşmakta bu durumda siber güvenlik zafiyeti yaratmaktadır. 5G ile birlikte önümüzdeki birkaç yıl içinde 50 milyar cihazın internete bağlanacağı düşünüldüğünde mevcut yapıyı uluslararası ilişkilerdeki anarşik yapı asla yürütemez. Yani 5G insanlığın en büyük fırsatı da olabilir insanlığın sonu da olabilir. Aşağıdaki tabloda belirtilen Siber Güvenlik Endeksinin en son halini incelediğimizde ise bu artan riskin yükselişini net olarak görmekteyiz.

Tablo 5 Siber Güvenlik Endeksi Yıllara Göre Risk Artış Grafiği [182]



2.5.5. Siber Saldırıların Motivasyonu

Siber silahların türlerinin farklı olması saldırılarında çeşitli olmasına yol açar. Farklı saldırı türleri ise farklı tür hedefleri içerir. Hedeflerin ve araçların farklı olduğu bu saldırılarda motivasyon kombinasyonlarını etkiler. Bu kapsamda; hedefli ve fırsatçı olmak üzere siber saldırılar iki türe ayrılmaktadır. Hedefli saldırılar, belirli

[182]Tandoon School Of Engineering, The Index of Cybersecurity, ICS Value, February 2020 = 5046 (Base = 1000, March 2011), WordPress, https://wp.nyu.edu/awm1/ ET.13.03.2020.

siber hedeflere karşı özel araçlar kullanır. Fırsatçı saldırılar ise gelişigüzel bir şekilde yayılan solucanları ve virüsleri içerir. Bu noktada, hedefli saldırıların fırsatçı saldırılara göre daha tehlikeli olduğu vurgulanabilir. Bu yüzden ciddi hasarlar yapmak için uzmanlığa sahip yetenekli bilgisayar korsanları tarafından gerçekleştirilen hedefli siber saldırıların oranı her geçen gün artmaktadır. Her geçen gün artan bu hedefli saldırılar; teröristler, rakip şirketler, ideolojik hackerlar veya devlet kurumları tarafından başlatılabilir. Hedefli saldırıların bir bölümü finansal kazançlarla motive olurken bir bölümü siyasi kazanç, prestij veya kritik tesislerdeki çalışmalarının aksaması yönünde sosyal motivasyon etkilerine odaklanmaktadır. [183]

Yukarıda da belirttiğimiz üzere önemli saldırı türü olan bu hedefli saldırılardaki motivasyonların kombinasyonu tıpkı fiziksel dünyada olduğu gibi, web üzerindeki savaşlar da maddi amaçlar için onur, hakimiyet ve prestij gibi somut olmayan hedefleri içerir. Zamana göre değişse de birçok durumda, insan davranışı içsel ve dışsal olarak çoklu motivasyonlar tarafından yönlendirilir. Böylece, para kazanmak veya eğlenmek isteyenler muhtemelen ekonomik ödül veren fırsatları seçebilir. Seçilen bu fırsatlar ise suç, terör, casusluk ve savaş gibi kavramların oluşmasına yol açar.

Bu bağlamda hedefli saldırı türlerinin motivasyonunu belirleyen kriterlerden bazıları şunlardır;

- ✓ **Sembolik Önem ve Kritiklik**

6 Ağustos 1945 tarihinde Japonya'da gerçekleşen atom bombası saldırısı ve daha sonrasında 11 Eylül 2001 tarihinde İkiz Kuleler ve Pentagon'a karşı gerçekleştirilen saldırılar hem Amerika'nın hem de dünyadaki tüm aktörlerin dış politikasındaki güvenlik gidişatının değişmesine yol açmıştır. 11 Eylül 2001 teröristleri için ideal hedefler Dünya Ticaret Merkezi'ni oluşturan ikiz kuleler, Beyaz Saray ve Pentagondu. Bu saldırı sonrasında asimetrik tehditlerin sembolik alanlara yönelik kullanım riskleri önem kazanmıştır. Örneğin; günümüzde sembolik olarak önemi olan ve dünyadaki tek uluslar üstü topluluk olan Avrupa Birliği üzerine gerçekleştirilecek bir siber saldırı üye ülkelere ciddi zararlar verebilir. Bu örneği daha da açarsak; Avrupa Komisyonu bünyesindeki Ortak Araştırma Merkezi (JRC)

[183] Kshetri, a.g.e. , ss. 541–562.

AB politikalarının temelini oluşturacak fikirlerin üretilmesi, bu politikaların geliştirilmesi, uygulanması ve izlenmesi süreçlerine yönelik olarak müşteri odaklı bilimsel ve teknik destek hizmetleri sunan bir kurumdur. Avrupa Komisyonu'nun bir birimi olarak JRC, bilim ve teknoloji alanında Birliğin tümü için bir referans noktası görevi üstelenmiştir. Politika tespit sürecinin yakınında olması münasebetiyle Merkez, özel ya da ulusal çıkarlara değil Birliğin ortak menfaatlerine hizmet etmektedir. [184] Böyle sembolik bir öneme sahip olan bir yer ciddi bir hedef olabilir. Ya da günümüzde muazzam derecede sembolik öneme sahip olan Telekomünikasyon, Gaz, Petrol ve Yakıt Tedariki gibi belirleyici ve kritik altyapı sistemleri hackerlar için ideal hedeflerden bazılarıdır.

- ✓ **Değerin Sayısallaştırılması**

Bilgisayar ağlarına saldırma motivasyonları kurumsal ve ekonomik faktörlerle doğrudan bağlantılıdır. Büyük şirketlerin, örgütlerin veya devletlerin daha fazla hedef sunan daha büyük ağlara sahip olması bilgisayar korsanları tarafından gerçekleşen saldırı hedeflerinin bireylerden, küçük şirketlerden, örgütlerden veya küçük devletlerden ziyade daha büyük ses getireceklere yönelmesine yol açmıştır. Örneğin; uluslararası faaliyet gösteren büyük şirketler siber saldırılara karşı daha güçlü savunma mekanizmaları ortaya koyduğundan, küçük ve orta ölçekli işletmelerin (KOBİ) siber saldırıya uğrama olasılığı daha yüksektir. Dolayısıyla, KOBİ'leri hedefleyen toplam siber suçların oranı artacaktır. Bu yüzden devletler iç hukukta bu yönde düzenleme yaparken uluslararası arenada bunları korumaya yönelik bir uygulama da geliştirilmelidir. Yani dijitale yüksek bağımlılığı olan işletmeler çevrimiçi kumarhaneler, bankalar, finans şirketleri, enerji tesisleri ve e-ticaret merkezleri dâhil olmak üzere teknolojiler, dışsal motivasyonlu bilgisayar korsanlarının hedefi haline gelmektedir.

- ✓ **Savunma Mekanizmalarının Zayıflığı**

Çoğu bilgisayar ağının savunma mekanizmalarının zayıflığı bu ağların siber suç hedefi olma olasılığını arttırmaktadır. Yani savunma mekanizmasının zayıflığı, bir saldırı olasılığı ile doğru orantılı bir şekilde değişmektedir. Bu doğrultuda dijital dünyada, bilgisayar korsanlarının hedefleri de bu zayıflıkları kullanarak düzeltilmemiş yazılım deliklerinden yararlanmaya dayanmaktadır.

[184]The European Commission's science and knowledge service, The JRC in Seville, 07.07.2016, https://ec.europa.eu/jrc/en/about/jrc-site/seville, ET.03.02.2020.

Bu süreci kısaca özetlememiz gerekirse; bilgisayar korsanlarının motivasyonlarının, kaynak özelliklerinin ve hedef ülke özelliklerinin farklı olması saldırılarında farklı olmasına yol açar. Saldıran birimin hedefe yönelik seçim ölçütleri sembolik önem ve kritikliği olan organizasyonlara yöneliktir. Örneğin; hükümet web siteleri ve kritik altyapılar ulusal sembol olarak algılanır. Ayrıca değerlerin sayısallaştırma derecesinin artmasıyla birlikte ekonomik olarak fırsatları değerlendirmek en önemli stratejik hedeflerin başında yer almaktadır. Bu yüzden küresel siber çatışmalar hedefli saldırılara doğru ilerlemektedir. Aynı zamanda uluslararası arenada tüm kuruluşlar eşit değildir. Bu yüzden siber hedefleri özünde motive olmuş hackerların hedefine dayanmaktadır. İkinci olarak bir ağın sembolik önemi ve kritikliği büyük işletmeler ve yüksek bağımlılığı dijital teknolojiler için çalışan bilgisayar korsanlarının en kazançlı hedeflerdir. Bu nedenle devletlerin güçlerini yayma aracı olarak kullandıkları uluslararası şirket ağlarının siber suç hedefi olma riskleri artmaktadır. Bu yüzden devletleri gerçekleşen bir siber saldırıda zan altında bırakmamak için savunma mekanizmaları küçükten büyüğe savunmayı içeren bir yapıyla tüm dünyayı kapsayacak şekilde bir üst otorite altında geliştirilmesi yönünde bir motivasyon oluşturulmalıdır.

Sonuç olarak; hedefli saldırı motivasyonları ve bu saldırılara karşı gerçekleştirilecek güvenlik reflekslerinin sağlıklı olarak uygulanabilmesi için bu bölümde kısaca şu politik sonuçlara varılmaktadır. İlk olarak, ulusal hükümetler, bilgisayar suç yetkilileri ve işletmeler güvenlikle ilgili teknolojileri içeren sorunlarda ve siber saldırılarla mücadelede kritik öneme sahiptir. İkinci olarak, ulusal hükümetlerin birbirleriyle ve uluslararası örgütlerle birlikte kurumlar için uygun politikalar tanımlayarak dijital dünyanın güvenliğini daha hızlı ve düşük maliyetle sağlaması gerekir. Üçüncüsü, siber güvenliğin artırılmasında kritik öneme sahip olan şey cezanın kesinliğidir. Dördüncüsü, birçok küçük ve yoksul ülkeyi de siber suçları araştıracak kaynakları oluşturması yönünde oluşturulacak bu uluslararası düzenlemenin içine entegre edilmesi gerekir. Çünkü sistem anarşiktir. İçinde bulunduğumuz çağın özellikleri veya düzensizlik eğilimi nedeniyle dünya değişim süreçlerinden geçmektedir. Bu yüzden ülkeler ve kurumlar siber güvenliğin sağlanması yönünde kalıcılık, dayanıklılık ve kararlılık gibi bileşenlere sahip olmalıdır. Aynı zamanda daha önce tanımlanmadığı halde yeni ortaya çıkan siber

tehditleri en aza indirmek için yeni yasalar (düzenleyici kurumlarda değişiklik) ve bilgisayar korsanlarını etkileyen sosyal normlar (normatif kurumlarda değişiklik) güncellenmelidir.

2.6. Siber Silahlar ve Oluşturulan Saldırı Tespit Sistemleri

Siber silahların ne olduğunu tanımlayabilmemiz için öncelikle silah kavramına bakmamız gerekir. İlk olarak silahlar, zarar aracıdır. Zamanın başlangıcından beri, insanlar avı ve birbirlerini avlamak için silah kullanmıştır. Silahlar, bütün bir şehri yok etmekten tek bir kişiyi korumaya kadar uzanır. Bu tezde silah kavramının alt kümesi olarak gösterdiğimiz siber silahların tanımı üzerine net bir fikir birliği olmasa da; siber silahlar yapılara, sistemlere fiziksel, işlevsel veya zihinsel zarar vermek veya tehdit etmek amacıyla kullanılan veya kullanılmak üzere tasarlanmış bilgisayar kodunu veya canlı varlıkları içerir. Kısaca; siber silahlar kod kaynaklı cihazlar ve düşük potansiyel araçlardan spesifik yüksek potansiyel silahlara kadar geniş bir yelpazeyi kapsar. Bu ayrım, siber güvenlik konusunun önemine yönelik bu tezde geliştirdiğimiz hipotezimizi desteklemektedir. Bu sebeple bir siber silahın yıkıcı hedeflerinin potansiyeli artarken riskleri azaltma yönünde uygulamalar geliştirmesi şarttır. Zaten son birkaç yıldır, saldırgan siber silahların uluslararası askeri çabaların bir parçası olarak ön plana çıkması da bunun göstergesidir.[185] Bu yüzden saldırgan siber silahların askeri oluşumunu ve önemini anlamak uluslararası anarşik sistemde gerçekleşen çatışmaları azaltmak için çok önemlidir.

Siber silahların önemini ortaya koymak ve riskleri ortadan kaldırmak için gerçekleştirilecek çalışmaların belirlenmesinde ABD Savunma Bakan Yardımcısı William J Lynn'ın Eylül 2011'de terörist bir grubun yıkıcı siber silahlar elde etmesi yönündeki riskleri ortaya koyduğu sözleri etkili olmuştur. Bu görüşlerin ardından 2 Ocak 2012'de Savunma Bakanlığı, Amerika'nın 'Kara, hava, denizcilik, uzay ve siber uzay gibi tüm alanları kapsayan bütünleşik bir silahlı kuvvetler kurulması yönünde çalışmaları başlatmıştır. Bu çalışmalar sonucunda siber uzayı kapsayan bütünleşik bir ordu sistemi kurulsa da tam olarak güvenlik sağlanamamıştır. Çünkü siber silahlar geniş bir yelpazeye yayılmaktadır.

[185]Conner Forrest, *Understanding The Military Buildup Of Offensive Cyberweapons*, ZDNet, September1,2016,https://www.zdnet.com/article/understanding-the-military-buildup-of-offensive-cyberweapons/ ET.28.02.2020

Aynı zamanda; geniş yelpazeye dayanan bu siber silahların kullanıldığı uluslararası anarşik yapı içerisinde gerçekleşen çatışmalarda bir tehdit unsuru ve savaş aracı olarak siber silahların kullanılmasının önemini anlayabilmemiz için üç husus çok önemlidir. Bunlar, siber silahların kavramsal olarak neyi ifade ettiği, ampirik vakaların siber saldırı araçlarını sınıflandırmadaki rolü ve değişen çatışma yöntemleri üzerindeki etkili rollerinin nasıl ortaya koyulacağıdır. Eğer bu hususlar ayrıntılı bir şekilde ortaya konabilirse siber silahların savaş kavramı içerisindeki önemi daha kolay anlaşılabilir.

Tezimizin üçüncü bölümünde ayrıntılı olarak incelediğimiz siber savaş kavramı birçok yazar tarafından son derece sorunlu, hatta tehlikeli bir kavram olarak gösterilse de yukarıda bahsedilen siber silah terimi siber savaş kavramında daha geniş anlamda kullanılmaktadır. Bir savaş eylemi, ister siber alanda olsun ya da olmasın, araçsal, politik ve potansiyel olarak ölümcül olmalıdır. Bu yüzden günümüzde ülkeler arasında yaşanan çatışmaları açıklamak için tek başına siber suç kavramı yeterli olmamaktadır. Bunu bir başka şekilde ifade edersek; savaş kavramı üzerindeki tartışmaları bir yana bırakırsak günümüzde yaşananlar tek başına siber suç ve terör kavramlarıyla birlikte açıklanamaz. Bu yüzden günümüzde siber silahlar kullanılarak gerçekleştirilen aktif bir siber çatışma dönemi içerisinde olduğumuz bu tezin asıl vurgusudur.

Silahlar elbette sadece savaşta kullanılmamaktadır. Silahlar tehdit, savunma, caydırma, saldırı, koruma vb. çok çeşitli amaçlar için kullanılmaktadır. Aynı şekilde siber silahlar için de bu durum geçerlidir. Bu sebeple siber savaş kavramına odaklanarak konunun önemini kaçırmak yerine siber silahlar kullanılarak gerçekleştirilen çatışmalar hakkında örnek vakaları inceleyerek gelecekte ortaya çıkabilecek risk ve tehditlerin önlenmesi için bu tezde üretken ve açıklayıcı çözümler ortaya koyulmaya çalışılmıştır.

Herhangi bir tehdit, suçlunun başarılı bir saldırıyı tekrarlama güvenilirliğine dayanır. Yani güçlü bir siber silah bir kez başarılı bir şekilde kullanılsa bile, siyasi bir hedefe ulaşmak için tekrarlanıp tekrarlanamayacağı bilinemez. Bu kapsamda siber silahların kullanılması karşı tarafı tehdit etme veya bir hedefe zarar verme niyetinin gösterilerek endişe yaratma şeklinde psikolojik bir etki gücüne sahiptir. Aynı zamanda siber silahların defansif veya saldırgan bir amaçlarla kullanılıp

kullanılmayacağı da bilinemez. Bu doğrultuda siber alanda güç kullanımı ile ilgili temel sorular hala cevaplanmamış olsa da siber silahlar tehdit olarak kullanılırsa veya kullanımı açıklanırsa veya tahmin edilirse, ikinci bir psikolojik tehdit boyutunun devreye girdiği birçok çatışma örneğinde görülmüştür. Günümüzde yaşanan bu siber çatışma örnekleri doğrultusunda aktif olarak bir siber savaş döneminin yaşandığını belirtmemizin son derece sorunlu ve iddialı bir kavram olduğu açıktır. Bu yüzden bu sorunu çözebilmemiz için öncelikle siber silah ve siber silah olmayan silahlar(konvansiyonel veya nükleer) arasındaki çizgiyi güvenlik kavramıyla ortaya koymamız gerekmektedir. Ayrıca silahsız bir saldırı silahlı olandan siyasi olarak daha az patlayıcı olduğundan dolayı bu çizgiyi çizmenin politik sonuçları vardır.

Bir silahın bir veya daha fazlasına zarar verme potansiyeli o silahın tehlike derecesini ortaya çıkarmaktadır. Tehlikeleri ortadan kaldırma mücadelesinin de yasal sonuçları vardır: bir şeyi silah olarak tanımlamak, en azından prensipte, yasadışı ilan edilebileceği ve gelişimi, bulundurulması veya kullanımının cezalandırılabileceği anlamına gelir. Sonuç olarak, silah ve silah olmayanlar arasındaki çizgi kavramsal olarak çok önemlidir. Bu sebeple kavramsal olarak bir şeyi silah olarak tanımlayabilmemiz için internet ağlarının mesafeleri yakınlaştırarak bilginin dolaşımını kolaylaştırmasını kriterler içine almalıyız.

Ulusal ve uluslararası düzenlemelerdeki eksiklikler, siber tehditlere ilişkin farkındalığın yetersizliği, kullanılan uygulamaların tasarım aşamalarında güvenlik boyutunun düşünülmemiş oluşu gibi sebepler tehditlerin etki alanını genişletmiştir. Bu bağlamda; dünya genelinde sıkça karşılaşılan ve yaygın kullanılan siber tehdit araçları ile elde edilen bilgiler iç işlerine karışma, probaganda yürütme, lobicilik, diplomasi yürütme ve caydırma gibi faaliyetlerde kullanılmaktadır. [186] Bu yüzden; siber silahların rolü; nükleer silahlar gibi aktörler üzerinde caydırıcılık yaratmaktadır. Belirli bir zamanı ve veriyi yok etme veya yeniden yazma amacıyla yazılıma zarar vermek üzere caydırıcı bir unsur olarak kullanılan mantık bombaları ve bilgisayar virüslerini içeren siber silah türlerinden bazıları şunlardır;[187]

1. Bilgisayar Virüsleri
2. Truva Atları
3. Solucanlar

[186] Mehmet Eren, a.g.e. ss.50-60.
[187] Lopamudra Bandyopadhyay, a.g.e. ss.1-14.

4. İnsanlar
5. Elektro-Manyetik Nabız Silahları
6. Zombi

Bu virüs tehditleriyle ilgili uluslararası sistemde yaşanan gelişmelere bakarsak; Siber silahlar kullanılarak gerçekleştirilen siber saldırıların en yaygın ve muhtemelen en maliyetli şekli casusluk yapmayı amaçlayan Ekim 2011'in başlarındaki 'Duqu' dur. Duqu'nun misyonu, muhtemelen ilgili kontrol sistemlerini kullanarak üçüncü bir tarafa karşı gelecekteki bir siber saldırıya olanak sağlamak için endüstriyel kontrol sistemlerinden istihbarat toplamaktı. Duqu'nun bir bileşeninin Stuxnet ile neredeyse aynı olması yüzünden ikisinin de yaratıcısının aynı olduğu düşünülmektedir. Ancak tehditlerden stuxnet zarar verme amacıyla kullanıldığından bir silahken Dugu gösterilmemektedir. Dugu gibi saldırılar, bilgi çağı ile birlikte suçun baskın bir nitelik kazandığını göstermektedir. Stuxnet silahı ise güvenli hedeflere saldırmak için muhtemel bir devletin kaynak veya desteğinin gerekliliğini göstermektedir. Bu yüzden siber silahların ve tehditlerinin farkını ortaya koyabilmek için bu silah örnekleri çok önemlidir. 2010 yılında tüm İran endüstriyel yapısını etkilemek için yaratılan *Stuxnet,* 2011 yılında stuxnetin kardeşi olarak görülen bilgi toplama hedefini içeren zararlı yazılım *Dugu*, 2012 yılında kaspersky lab tarafından bulunan ve stuxnet ile bağlantılı bir silah olarak kendini sürekli güncellediği tespit edilen *Flame ve*, 2012 yılında bu sefer endüstriyel yapı yerine finansal bilgileri hedef alan ve Ortadoğu ülkeleri üzerinde faaliyet gösteren *Gauss* isimli bir diğer yazılım siber saldırıların asla bitmeyeceğinin kanıtıdır.

Tüm bu örneklerde de görüldüğü üzere internet ile birlikte bilgisayar sistemleri birbirine bağlanmakta ve tüm dünyada sürekli gelişen bir iletişim, bilgiyi saklama, paylaşma ve kolayca ulaştırma gibi çatışma mücadeleleri gerçekleşmektedir. Bu mücadelelerde internetin kısa tarihinde de görüldüğü üzere, bireyler, şirketler, örgütler ve devletler gibi tüm aktörleri içermektedir. Aynı zamanda; bireysel bilgisayar korsanları, istihbarat servisleri ve suç gruplarının siber alanda en büyük tehlikeyi oluşturmalarından dolayı hükümetler siber uzayda çıkarlarını korumakta

zorlanmaktadır. Ancak siber yetenekleri savaşta kullanma kavramının yavaşça gelişmesi Rus-Gürcistan savaşı gibi örneklerle süreci farklı boyuta taşımıştır.[188]

Bir diğer önemli silah olan Slammer Solucanı ile Ohio Nuke Tesis ağı çökmüştür. Kısaca bu süreci incelersek; Davis-Besse tesisi, Ohio'da faaliyet gösteren Ohio kamu hizmeti şirketi FirstEnergy Corp. tarafından işletilmekteydi. Slammer solucanı, Ohio'daki Davis-Besse nükleer santralinde özel bir bilgisayar ağına girdi ve tesis personelinin ağın bir güvenlik duvarı tarafından korunduğuna inanmasına rağmen, yaklaşık beş saat boyunca bir güvenlik izleme sistemini devre dışı bıraktı. Böylece slammer saldırıları yıllarca süren uyarıları dikkate almamanın sonrasında ortaya çıkan güvenlik açığının santralleri veya elektrik dağıtım sistemlerini nasıl etkileyebileceğini göstermiştir. Şu anda hala, ABD nükleer santralleri genellikle kritik tesis operasyonlarını izleyen, fakat onları kontrol etmeyen dijital sistemlere sahiptir. Eğer bir davetsiz misafir müdahale edebilirse bu kaza riskini arttırabilir. "Slammer" bilgisayar solucanı 2003 yılında beş saat boyunca Ohio'da elektrik santralini etkiledi ve nükleer güvenlik izleme sistemini bozdu. Yani burada yaşanan deneyim Stuxnete giden sürece katkı sağlamıştır.[189]

Tanımlı siber yazılım tehditlerin en çok kullanılan siber silah türleri ise şunlardır;

- ✓ Hedef aygıtta veya ağda verileri bozmaya veya sistemi ele geçirmeye yarayan "Malware(kötücül yazılım)"
- ✓ E-posta kaynaklı gizli bilgileri ifşa etmeye veya E-posta mesajdaki bir köprüye tıklayarak kötü amaçlı yazılım indirmesi için kandıran "Phishing(oltalama"
- ✓ Birçok cihazı devralabilen veya hedef sistemi aşırı bir talep ile çökertebilen "Hizmet Reddi saldırısı veya Dağıtılmış Hizmet Reddi Saldırısı (DDoS)"
- ✓ Gönderen ve alıcının, doğrudan birbirleriyle iletişim kurduğuna inandırılarak verilerin değiştirilmesini sağlayan "Ortadaki Adam" (MitM) saldırısı
- ✓ İnternette isimsizlik yaratarak serbestçe ifadeyi simgeleyen "Tor" [190]

[188] Derek S .Reveron, "Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World", Georgetown University Press, Washington, 2012.
[189] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Nework", Security Focus, 19.08.2003, http://www.securityfocus.com/news/6767 ET.17.01.2020.
[190] Singer ve Fıedman a.g.e., ss. 151.

- ✓ Bilgisayar korsanları tarafından büyük kitleler için kullanılan koordineli sistem saldırıları "Botnet"
- ✓ Standart bir yazılım parçası gibi hedef sisteme girerek ana bilgisayar sistemine kötü amaçlı kodu veren "Trojan"

Kötü amaçlı bu yazılımlar Derek S .Reveron tarafından Paintball silahlarına benzetilmektedir. Paintball silahlarına benzetilen bu silahlar bir sistemi dışarıdan etkileyebilen ancak teknik olarak sisteme nüfuz edemeyen ve doğrudan zarar yaratamayan silah türleridir. Bu saldırı türündeki hizmet reddi (DoS) saldırılarının montajı kolaydır, savunması nispeten kolaydır, etkileri görünürdür. Aynı zamanda; Smart akıllı bombalara benzeyen bu silah türleri, yüksek potansiyel ucunda, korumalı ve fiziksel olarak izole edilmiş sistemlere bile nüfuz edebilen ve doğrudan işlemek için çıktı süreçlerini bağımsız olarak etkileyebilen akıllı bir ajan olarak hareket edebilen kötü amaçlı yazılımlardır. Bu silahların yarattığı hasarlar, siber silahlardan kaynaklanan doğrudan hasar değil, ikinci dereceden etkilerdir. Bu duruma en güzel örnek ise 2007 de gerçekleşen Estonya saldırısı gösterilmektedir.[191]

Siber silahların ortaya çıkardığı tüm bu siber tehditler ekonomik, politik ve askeri her alana ait motivasyonlarda gelecekteki konumlarını ve önemlerini arttırmaktadır. Bu sebeple bu siber silah tehditlerini caydırmak, bertaraf etmek veya bu tehditlerden korunmak için alınması gereken siber savunma önlemlerinden bazıları şunlardır; [192]

- ✓ Güvenilir Uygulamalar Kullanılması,
- ✓ Güncellemelerin ve Doğru Konfigürasyonların Yapılması,
- ✓ Saldırıya Maruz Kalınabilecek Alanların Azaltılması,
- ✓ Savunulabilir Bir Ortam Kurulması,
- ✓ Yetkilendirme Yönetiminin Uygulanması,
- ✓ Güvenli Uzaktan Erişim Uygulamalarının Kullanılması,
- ✓ İzleme ve Müdafaa Uygulamalarına Başvurulması,

[191]Derek S .Reveron, "Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World", Georgetown University Press, Washington, 2012.
[192]Nurullah Aydın, "Türkiye'nin İç ve Dış Tehditlerine Stratejik Bakış", Paralo Yayınları, İstanbul, 2014, ss. 137-152.

- ✓ Nitelikli ve eğitimli personel yetiştirmesi,
- ✓ Ülke içinde sektörler arasında kümelenme gerçekleştirmesi,
- ✓ Konuyla ilgili teknik ve milli donanımlara sahip olunması,
- ✓ Siber tehditlerin tespit ve analiz edilmesi,
- ✓ Gerekli önlemlerin alınması,
- ✓ Siber tehditlerin gerçek zamanlı olarak izlenmesi,
- ✓ Siber tehditlerin haritalanması,
- ✓ Elde edilen tüm verilerin devletlerin ilgili kurumlarıyla paylaşılması,
- ✓ Güvenlik değerlendirmesinin yapılması,
- ✓ Olay inceleme ekiplerinin oluşturulması,
- ✓ Zararlı yazılımların ve veri hırsızlığının tespit edilmesi ve önlenmesi,
- ✓ Bilgi ve iletişim alt yapılarının fiziksel saldırılara karşı dayanıklı hale getirilmesi,
- ✓ Siber uzay içindeki tüm zafiyetlerin takip edilmesi,
- ✓ Siber, elektronik ve enerji saldırılarına karşı önlemlerin alınması,
- ✓ Antivürüs programları gibi internet güvenlik paketlerinin, uç nokta güvenlik sistemlerinin, içerik filtreleme sistemlerinin ve son olarak güvenlik duvarlarının aktif ve güncel olarak kullanılması,

Her ne kadar bu savunma süreçleri uygulanılsa da siber silahlar kullanılarak ağ ve sistem güvenliğini tehdit edecek saldırılara maruz kalınmasına karşı saldırı tespit sistemlerinin geliştirilmesi şarttır. Çünkü veri deposundan veri madenciliğine geçilen günümüzde bilgisayar güvenliği bankacılık, finans, enerji, sağlık, askeri vb. endüstrilerden çok uluslu şirketlere, uzaydan istihbarat topluluğuna kadar bir çok alan için veri çok önemli olmuştur. Bu doğrultuda silahlara karşı iyi bir güvenlik çözümünün temelinde kimlik doğrulama, yetkilendirme, kullanılabilirlik ve denetim şarttır.[193]

Bilgisayar güvenliği gizlilik, bütünlük ve bilgi işlem kaynaklarının kullanılabilirliğine dayanır. Bilgisayar güvenliğinin kaynakları olan donanım, yazılım, ağ ve veri gibi bileşenlerin hepsinin güvenlik açıkları vardır ve insanlar bu güvenlik açıklarından yararlanmak için bu kaynaklara karşı saldırılar

[193] Singhal Anoop, a.g.e , ss,41-51.

gerçekleştirirler. Güvenlik için bir başka zorluk da cep telefonları, kişisel dijital asistanlar, bilgisayarlar ve diğer tüketici cihazlar gibi her cihazda kullanılan ağların yaygın olmasıdır. Bu bileşenlerin güvenliklerini tehdit eden tüm bu tehditler önemsenmelidir. Başta tehlikesiz olarak görülebilen bir olay aslında sinsi bir saldırı hedefleyen bir silah olabilir. Çünkü virüslerin saldırı aşamaları 4 evrede gerçekleşmektedir. Bunlar; hareketsiz aşama, yayılma aşaması, tetikleme aşaması ve son olarak yürütme aşamasıdır. Aynı zamanda; içinde mobil kod ve web hizmetlerinin geleceğinde önemli olacak uzaktan güncellemeler ve yamalarda ağlardaki en önemli risklerdir. Bu sebeple ağlardaki tehditlere yönelik geliştirilebilecek Saldırı Tespit Sistemleri ve Güvenlik duvarları ağları korumak için popüler ürünler haline gelmeye devam edecektir.

Saldırı Tespit Sistemleri ve güvenlik duvarları aslında siber saldırıların tespitinde kullanılabilecek son teknolojilere genel bir bakış sunmaktadır. Saldırı tespit sistemleri dediğimizde aklımıza yazılım / donanım bileşenleri gelir. Bu bileşenlerden oluşan saldırı tespit sistemlerinin asıl amacı sistemleri izlemek ve izinsiz giriş olaylarını analiz etmektir. Bilgi işleme ve internet erişilebilirliğinin maliyeti düştükçe kullanım artmakta bu da kritik alanlara karşı gelecek siber saldırılara karşı sistemleri savunmasız hale getirmektedir. Aynı zamanda Saldırı Tespit Sistemleri (IDS) modern ağa sahip herhangi bir güvenlik paketinin ayrılmaz bir parçasıdır. Bu sebeple saldırılar gerçekleşmeden önlem alabilmek için saldırı tespit sistemlerinin oluşturulması bir zorunluluktur. Fakat bu zorunluluğun ticari bir meta haline dönüşmüş olması ve bu imkanları satan aktörler tarafından sistemlerin ele geçirilebilme riskinin de saklı olması sebebiyle bu sistemlerin milli imkanlarla gerçekleştirilmesi şarttır. Geçtiğimiz birkaç yıl içinde, izinsiz giriş tespiti ve diğer güvenlik şifreleme, kimlik doğrulama ve güvenlik duvarları gibi teknolojiler giderek önem kazanmaktadır. Bu bağlamda Saldırı Tespit Sistemleri üç fonksiyonel açıdan tanımlanabilir. İlk olarak **k**ullanılan veri kaynakları incelenerek izinsiz giriş oluşumu belirlenir. Sonrasında bu izin girişlerdeki yaklaşımlar ve yanlış kullanımlar tespit edilir. Yani analiz edilir. Son olarak yanıt verilir. Yanıt işlemi ise şu şekilde gerçekleştirilir. Bir saldırı tespit edildiğinde eylem kümesi aktif olarak

gruplandırılarak aktif eylemlere karşı otomatik bir müdahale gerçekleşir, pasif bir eylem için ise IDS uyarıları mekanizması sistem sahibine bilgi verir.[194]

Bir diğer yandan yukarıda ayrıntılarıyla bahsettiğimiz veri madenciliği süreci Saldırı Tespit Sistemlerinin saldırıları tespit etmesi için kullanılır. Çünkü veri deposu sayesinde geleneksel saldırıların tespit edilmesi kolaylaşmakta böylece saldırı stratejileri oluşturularak hasarları azaltacak stratejiler geliştirilerek izinsiz girişlerin analizi yapılabilmektedir. Bu yüzden Saldırı Tespit Sistemlerinin (IDS) performansını ve kullanılabilirliğini iyileştirmek için siber uzayda uyarı korelasyon tekniklerinin oluşturulması şarttır.

2.7. Siber Silahsızlanma ve Siber Silahların Yayılmasını Önleme

Siber silah uygulamalarının arka planına bakabilmemiz için şu tanımlamaları açıklamamız gerekmektedir. Saldıran bilgisayarlara "botnet", temel olarak önceden programlanmış ağları çökertmek veya sıkışmak için tasarlanmış internet trafiği seline "ddos", uzaktan kumandalı bilgisayarlar sahiplerinin bilgisi olmadan talimatları izlemesine ise "zombi" denir. Bu tanımlar çerçevesinde bilgisayarların ne zaman zombiye dönüştüğünü ya da bir DDOS ile meşgul olduğunu söyleyebilmek çok zordur. Bir kullanıcı şunu fark edebilir: dizüstü bilgisayar biraz yavaş çalışıyor veya web sayfalarına erişim normalden biraz daha uzun sürüyor, ancak bu tek göstergedir. Kötü amaçlı etkinliğin tümü arka planda gerçekleşir ve kullanıcı üzerinde görünmez.

Siber silah uygulamalarının arka planındaki karmaşıklığı bu silahların kullanıldığı örnekler üzerinden anlattığımızda süreci daha kolay açıklayabiliriz. "solucan" olarak bilinen enfeksiyon bir bilgisayardan geçerek sadece birkaç saat içinde tüm dünyaya yayılabilir. Stuxnet süreci de aslında tam böyle bir ilerleme yaşamıştır. Aynı zamanda Estonya'daki DDOS saldırısıda şimdiye kadar görülen en büyük oyundur. Her biri farklı olan birkaç farklı botnet ve uyuyan on binlerce virüslü makine ile gerçekleştirilmiştir.

Suriyeliler, Iraklılar, İranlılar, Estonyalılar ve Gürcüler arasında yaşanan siber olayların hepsi siber saldırıları içeren ulus-devlet çatışmasının başladığını göstermektedir. Siber alanda tanımlanan bu çatışmalarda ilkel siber silahlar kullanıldığından dünya üzerinde etkileri çok ciddi olmadı. Fakat gelişmiş modern siber silahlar modern bir ulusa çok ciddi zarar verebilir. Tüm bu silahlar ve

[194] Singhal,D.W.D.M.T.F.C.S. a.g.e. ss53-68

gerçekleşen olaylar siber çatışmaların başladığı ve ulusların yeni bir savaş alanına hazırlandığını göstermektedir. Örneğin**;** Rusya, Çin ve ABD gibi ülkelerin askerleri ve istihbarat örgütleri tarafından internet hem "mantık bombası" şeklinde silah hem de savaş alanı olarak kullanılmaktadır. Yürütülen bu yeni alandaki siber çatışmalarla, barış zamanında diğer ülkelere sanal patlayıcılar yerleştirerek "tuzağa düşürmek" temel hedef olmuştur. Siber uzayın doğası göz önüne alındığında olası hedefler ilk olarak sivildir. Bu yönden nükleer savaşı engelleyen caydırıcı güç, siber savaşta aynı sonucu vermez.[195]Ama farklı sonuçlar yaratır.

Siber savaş, nükleer strateji ve casusluk konusundaki geçmişe göre şekillenmektedir. Siber savaş, kucaklamamız gereken kurbansız, temiz, yeni bir savaş türü değildir. Yeni tip çatışmalarda kullanılan bir tür silahtır. Bu silahı kullanan ülkeler bu silahı bir avantaj olarak görse de şuana kadar ciddi derecede uluslara büyük bir tehlike yaratmamıştır. Bu doğrultuda; siber savaşın ne olduğunu anlamak, nasıl ve neden çalıştığını öğrenmek, risklerini analiz etmek, hazırlanmak ve kontrol etmek bu tezin ulaşmaya çalıştığı noktaların başında gelmektedir. Bu tezde "siber savaş" terimi kullanıldığında, bir ulus-devletin, başka bir ülkenin bilgisayarlarına veya ağlarına hasara veya bozulmaya neden olan saldırıları vurgulanmaktadır. Yani savaştan kastımız konvansiyonale veya nükleer bir savaş değildir.

Bu bambaşka savaş türünde günümüzde askerlerin kullandığı hava savunması, drone, iha/siha ve radar gibi sistemlerinin doğası gereği siber silahlardan gelebilecek saldırılara en açık alanlardır. Bunun en güzel örnekleri İsrailliler tarafından İsrail-Suriye savaşı sırasında Suriye hava savunma ağının kandırılmasında görülmüştür. Ya da 1990'da Amerika Birleşik Devletleri Irak ile ilk kez savaşa hazırlanırken, erken dönem ABD'li siber savaşçıların Irak hava savunma radarına yönelik gerçekleştirdikleri sanal savaş operasyonlarında görülebilir. ABD ve İsrail'in siber faaliyetleri ise daha konvansiyonel bir savaş türüne yardımcı olmak için hacklemeyi bir araç olarak kullanan ordu örneğidir.

Siber silahların tüm bu durumlarından dolayı kontrol edilmesi gerekmektedir. Bu kontrolün gerçekleştirilmesi içinde öncelikle bu silahların sınırlandırılması

[195] Clarke ve Knake, Cyber War The Next Threat to National Security and What to Do About It, a.g.e.,ss.1-20.

gerekmektedir. Bu kapsamda; bu tezde belirttiğimiz siber silahların sınırlandırılmasının gerekliliğini sorgulayanlar ve değişime karşı duran muhafazakarlarda muhakkak olacaktır. Fakat burada politikanın bir aracı olan savaş kavramının en önemli unsuru silahlarda yola çıkarak siyasal olanı yeniden düşünmemizin iyi bir politika olacağını vurgulamaktayız.

Siber silahların politik bir araç olarak kullanıldığından yola çıkarsak bu silahların kontrolü hakkında üç önemli konu vardır. Bunlardan birincisi bu silahlar hakkında ne düşünüldüğü, ikincisi etkisinin neler olabileceği, sonuncusu ise kullanımının sınırlandırılması ve kontrolü hakkında neler yapıldığıdır. [196] Örneğin; 2. Dünya Savaşı'ndan önce ülkeler sahip olabileceği savaş gemilerinin sayısını donanma gücünün ülkeleri tekrar savaşa sürüklemesinden dolayı sınırlandırdı ve Milletler Cemiyetini yarattı. 2. Dünya Savaşından sonrada yeni bir savaşın ortaya çıkmasını önlemek için Birleşmiş Milletleri yaratarak 1960'ların başında başlayan ABD ile Rusya arasındaki Soğuk Savaş sırasında nükleer silahın üretilmesi, kullanılması (SALT, START)vb. hususların sınırlandırılması amacıyla çok taraflı anlaşmaların yapılmasına yol açtılar. Fakat Soğuk Savaş sonrasında gerçekleşen Endüstri 4.0 ve Toplum 5.0 gelişmeleriyle ortaya çıkan yeni dijital dönüşüm silahlarına yönelik bu yönde hala bir çalışma yapılmamaktadır. Bunun üzerinde durmamızın sebebide geçmişte yaşanan bu deneyimlerin, siber silahların kontrolü hakkında düşünme şeklimizi şekillendirmesidir.

Bu şekillendirme sonucunda günümüzde ülkelerin artan bir hızda her geçen gün ordularında siber birimleri kurmaları ve bu orduların kullanacağı silahları geliştirmeleri siber tehdit ve riskleri önlemeye yönelik girişimleri ve silahsızlanma çabalarını zorunlu bir hale getirmektedir. Günümüze kadar yaşanan tüm siber çatışma vakaları siber silahların gerektiğinde politik, ekonomik, sosyal ve askeri hedefleri gerçekleştirmek için tüm kritik alt yapı veya tesislere yönelik ne kadar tehlikeli olabileceğini gözler önüne sermektedir. Bu durumda siber silahların kontrol edilmesi gerektiği sonucuna ulaşılmaktadır. Bu kontrolün gerçekleştirilmesi içinde öncelikle bu silahların sınırlandırılması gerekmektedir. Çünkü silah kontrolü iyi çalışırsa belirsizliği azalır ve daha öngörülebilir bir güvenlik ortamı oluşur. Silah kontrol anlaşmaları sayesinde bazı uygulamalar yasa dışı gösterilebilir, bazı silahlar

[196] Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books, ss.80-110.

ihlal olarak tesis edilerek ulusların niyetleri ortaya konabilir ve kullanımı sınırlandırabilir. Böylece belirli silah ve uygulamaların yasaklanması ve silahların kontrolü ile belirsizlikler azalırken aynı zamanda diğer ulusların da aynısını yapması korkusu ortadan kalkar. Böylece bu yönde yapılan harcamalarda azalır.

Bu azalmanın en güzel örneğini ABD ve diğer dünya güçleri arasında nükleer, biyolojik ve kimyasal silahların yanı sıra tankların ve diğer topçu silahlarının konuşlandırılmasını ve kullanımını sınırlayan silah kontrol önlemleri konusunda imzalanan anlaşmalarda görebiliriz. Fakat siber silah kullanımı için geçerli bir silah kontrol önlemi yok? Sorun şu ki, hükümetler "siber silah" ı neyin oluşturduğuna ve "siber savaş" ın neye benzeyebileceğine dair çok çeşitli fikirlere sahipler. Bu konuyu daha da açarsak; gelişmiş endüstriyel demokrasiler bir siber saldırıyı bilgisayar altyapısına Güç, Telekomünikasyon, Ulaşım ve Finansal sistemlerin altında yatan bir saldırı olarak görmektedir. Ancak gelişmekte olan birçok ülke siber savaşı politik olarak görmektedir. Örneğin; Siber silah kontrol anlaşmasının önde gelen savunucusu olan Rus hükümeti, bir hükümetin interneti kullanarak başka bir ülkenin siyasi sistemine meydan okunması sürecini açıklarken "bilgi savaşı" terimini tercih ediyor ve siber çatışmayı bir fikir savaşı gibi seslendiriyor. Aynı zamanda; 2008 yılında, Rusya Savunma Bakanlığı Sergei Korotkov bir tercüman aracılığıyla, "Bir devlet veya birkaç devlet tarafından başka bir devlete karşı yürütülen herhangi bir bilgi operasyonunu, iç işlere müdahale olarak nitelendirilebileceği yönündeki sözleri de Rusya'nın bu silahların kullanımının sınırlandırılması hakkındaki niyetine güzel bir örnektir.[197]Dolayısıyla, demokrasinin geliştirilmesi gibi herhangi bir iyi neden, siber silah kullanımı için gerekçe olarak kullanılamaz.

ABD internet iletişimini sınırlama, bilgiyi ve içeriği kontrol etme gibi çabalara sürekli olarak karşı çıksa da, Ruslar yabancı hükümetleri istikrarsızlaştırmak için "bilgi" tehdidinin kullanılabileceği üzerine birçok açıklama gerçekleştirmiştir. Örneğin; 2008 yılında Rusya ve Çin gibi ülkelerin de yer aldığı Şanghay İşbirliği Örgütü'nün zirvesinde siber silahsızlanma teklifi yenilenerek sonuç anlaşmasında, "bilgi savaşını" kısmen, bir devletin bir başkasının "siyasi, ekonomik ve sosyal sistemlerini" baltalama ve devletlerin ruhsal, ahlaki ve kültürel alanlarına zarar

[197]Tom Gjelten, "Seeing the Internet as an " Information Weapon, National Public Radio", 23 Eylül2010, https://www.npr.org/templates/story/story.php?storyId=130052701 ET:23.01.2020.

vererek kitlesel psikolojilerini bozma çabası olarak gösterilmiştir.[198] Sonrasında; internet yönetişimi ve siber silahların kontrolü konusundaki tartışmalara bu alanda yönlendirici bir görev üstlenmek isteyen Uluslararası Telekomünikasyon Birliği de katılmıştır. Dönemin ITU genel sekreteri Hamadoun Toure, "Siber" kavramının, tüm kritik sistemlerin var olduğu fiziksel ve kavramsal alemi simgelediğini belirterek "siber savaş"'ın genel olarak siber alanda yapılan bir savaş olarak anlaşılabileceği bu yüzden de ITU'nün silahsızlanma anlaşmasını "gerçekleştirerek siber ortamda barışı sağlayabileceğine inandığını belirtmiştir.[199]

Aslına bakılırsa bu tezde üzerinde durduğumuz siber uzayın askerileştirilmesi süreci siber araçların bir silah şeklinde kullanılmasıyla doğrudan bağlantılıdır. Bu yapıda hem hükümetler hem de diğerleri saldırgan siber silah yetenekleri geliştirmek için sahada gizlice ve hızlı bir şekilde yarışmaktadır. Bu yüzden silah kavramlarına yönelik ulusal politikaları belirlemek, siber savaş aktivitelerinin kontrolü veya sınırlamaları gerçekleştirmek için, siber uzayda kullanılan silahlarının kontrolü ve sınırlandırma deneyimi için sürecin ne kadar olgunlaşacağı tespit edilmelidir. Bunu da uluslararası kurallar ve bu kuralları uygulayacak kurumlarla gerçekleştirebiliriz. Örneğin; Geçmişte kurumlar oluşturularak silahsızlanma girişimleri olmuştur. 1957 Uluslararası Atom Enerjisi Kurumu Kuruldu. Ardından sırasıyla, 1968 Nükleer Silahların Yayılmasını Önleme Anlaşması(NPT)[200], 1970'lerde kimyasal ve biyolojik silahların geliştirilmesi ve üretilmesinin yasaklanması, SALT-1 ve SALT-2(Stratejik Silahların Sınırlandırılması Görüşmeleri), 1980'lerde Nükleer Silahlardan Arındırılmış Bölge(NSAB) ve START-1 (Stratejik Nükleer Silahların İndirimi Anlaşması), 1990'larda START-2 ve 2000'lerde START-3 şeklinde devam etti. [201] Tüm bu gelişmeler nükleer silahların yıkıcılığına verilen önemden kaynaklı devletler tarafından uygulanan tehlikeyi azaltmaya yönelik girişimlerdi. Bu girişimler sonucundaki düşüş aşağıdaki şekilde açıkça görülmektedir.

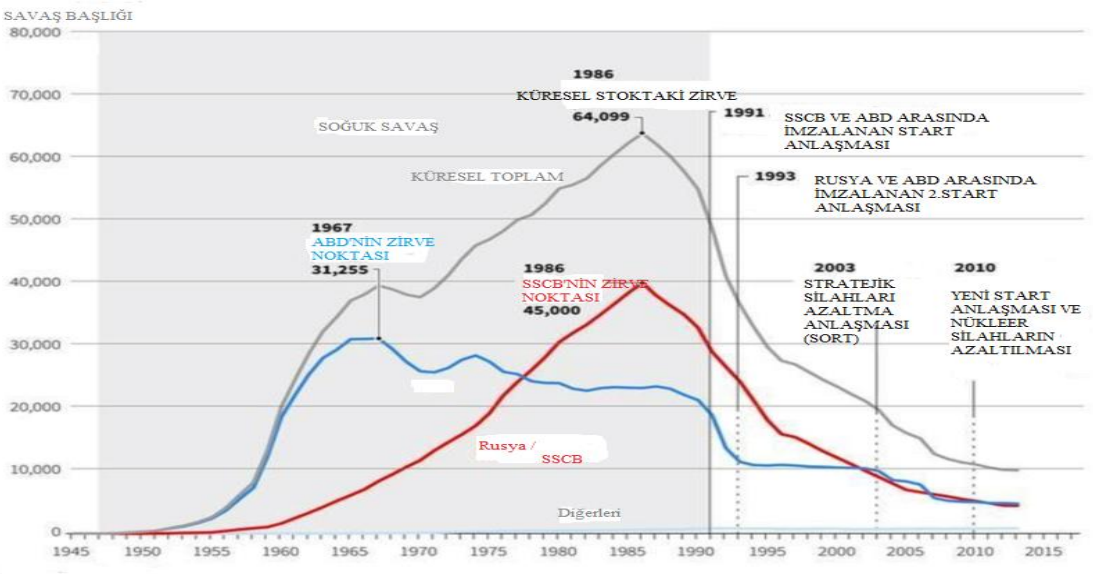
---

[198]Agreement Between The Governments Of The Member States Of The Shanghai Cooperation Organization On Cooperation İn The Field Of İnternational İnformation Security, 61st Plenary Meeting, 02.12.2008, ss.202-213https://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf ET.15.07.2020.

[199]Hamadoun I. Touré, The Quest For Cyber Peace, International Telecommunication Union, January 2011,ss7-16https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf ET.19.02.2020.

[200] Lawrence Scheinman, The Non-Proliferation Treaty: Ont He Road To 1995,Special Reports, IAEA Bulletin, Ocak 1992, ss.33-40.

[201] Beril Dedeoğlu, 2014, Uluslararası Güvenlik ve Strateji, Yeni yüzyıl Yayınları ss.147.



Şekil 5 Dünya'da Nükleer Savaş Başlığı Stoğundaki Düşüş [202]

Peki, internetin hayatımızda bu kadar büyük bir öneme sahip olmasıyla birlikte ortaya çıkan siber silahlar hakkında neden bir fikir birliği yoktur? Savaş evrenseldir. Çözümü de evrensel olmak zorundadır. Örneğin; ABD'nin siber kontrollü sistemlere bağımlılığı, potansiyel rakiplerinin hiçbirinin onun kadar özel şirketler tarafından sahip olunan ve işletilen ulusal sistemlere sahip olmaması, başka hiçbir sanayileşmiş ve teknolojik olarak gelişmiş ulusun onun kadar lobicilik faaliyetleriyle kolayca yönlendirilmemesi ve son olarak da ABD ordusunun siber saldırılara karşı oldukça savunmasız olmasından dolayı Dünyanın en büyük gücü ABD ufak bir ülke yada grup tarafından siber silahlarla zarara uğrayabilir. Bunun en güzel örneğini ABD- Irak savaşında Irak'taki isyancıların yirmi altı dolarlık yazılım kullanarak ABD kuvvetlerinin dronlarının veri tabanlarına ve bilgilerine erişim sağlayarak milyonlarca dolarlık araştırma ve geliştirme sonucunda üretilmiş dronların kontrolünü ele geçirmesinde görebiliriz. Sonuç olarak bu 4 asimetri birlikte ele alındığında, dünyanın en büyük gücü ABD ile potansiyel bir düşman arasında gerçekleşebilecek sınırsız siber savaş da, ABD kendisinin düşmana uğratabileceği bir zarardan çok daha fazlasını kendisi yaşayabilir. Bu yüzden Richard A. Clarke ve Robert K. Knake'a göre siber savaşın bazı yönlerini sınırlayan uluslararası bir

[202]Reuters. "Threats To The Cybersecurity Of Nuclear Weapons", World Econic Forum, 11.02.2018, https://www.weforum.org/agenda/2018/02/nuclear-weapons-and-cybersecurity-threats-vulnerabilities-and-consequences , ET.30.01.2020.

anlaşmanın yapılması tüm ülkelerin faydasına olduğu gibi ABD için daha da faydalı olabilir.[203]Bu örnekte de görüldüğü gibi aktif olarak günümüz uluslararası anarşik yapısında gerçekleşen çatışmalarda kullanılan siber silahlar tehlikelidir. Önlem alınması da zorunludur.

Sonuç olarak anarşik yapıda siber silahsızlanmayı gerçekleştirmek ve siber silahların (nükleer, kimyasal, biyolojik, kıtalararası, siber vb.) yayılmasını önleme ancak büyük güçlerin bir faydalar ve yaptırımlar sistemi uygulamasıyla gerçekleşir. Günümüzde siber silahların yayılması yavaş ama emin adımlarla gerçekleşmektedir. Bu süreçte siber silahsızlanmanın sağlanabilmesi için siber silahların yayılmasının önlenmesi fikrine ülkeler ikna edilirse bu durum ülkeler tarafından daha çok benimsenir ve silahsızlanma konusu daha güçlü bir hale gelebilir.[204] Peki, siber silahların yayılmasının önlenmesi veya silahsızlanma ifadeleriyle bu tezde tam olarak ne kastetmekteyiz?

Siber silahların yayılmasının önlenmesinde, devletlerin siber silah ediniminin önlenmesi yer alırken, silahsızlanma ise bir devletin gerçek siber silahlardan tamamen vazgeçmesi anlamına gelir. Günümüzde ülkelerin artan bir hızda her geçen gün ordularında siber birimleri kurmaları ve bu orduların kullanacağı silahları geliştirmeleri bu önleme ve silahsızlanma çabalarını zorunlu bir hale getirmektedir. Günümüze kadar yaşanan tüm siber çatışma vakaları da bu silahların gerektiğinde politik, ekonomik, sosyal ve askeri hedefleri gerçekleştirmek için tüm kritik alt yapı veya tesislere yönelik ne kadar tehlikeli olabileceğini gözler önüne sermektedir.

Siber silahların kullanımında gözler önüne çıkan bir diğer önemli hususta devletlerin bu silahların kullanımında öne çıkmayıp, gerçekleşen tüm çatışmalarda faaliyeti gerçekleştiren birey(hacker) veya örgütlere konuyu atfederek süreci suç ve terör bağlamında tutmalarıdır. Devletler, uluslararası hukuktaki cezai maddelerin eksikliğinden faydalanarak kendilerini arka planda tutmakta ve rakiplerine karşı gerçekleştirecekleri saldırılarda terör örgütlerini kullanmaktadır. Böylece Terör Örgütleri, Ulusötesi Gruplar, Şirketler ve Bireyler tarafından siber silahlar kullanılarak devletlere karşı gerçekleştirilen saldırılar, siyasete şantaj yaparak

[203]Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books, ss.108-110.
[204] Mary Kaldor and Iavor Rangelov, "The Handbook of Global Security Policy", Wiley Blackwell Journal, 2014, ss.115-126.

siyaseti etkileme amacı güden bir şiddet türünü oluşturmaktadır. Bu asimetrik şiddet türü ile sivillere yönelik şiddet doğrudan kullanılarak toplumun gözü korkutulmakta ve siyaset etkilenerek otorite istikrarsızlaştırılmaktadır.

Siber silahların bu istikrarsızlaştırıcı rolü ile küreselleşme ve teknolojik gelişmelerdeki yoğunlaşma nedeniyle hayatın her alanında kullanılan teknolojik araçlardan bireylerin veya toplumların izole edilemeyecek veya göz ardı edilemeyecek olmasından dolayı siber çatışmadan etkilenen her alan, tehdit olarak değerlendirilen bir kaos bölgesidir. Bu araçlara bağımlık derecesi ise siber silahların etki alanıyla doğrudan etkilidir. Aynı zamanda; siber silahlarla birlikte zayıf ve başarısız devletler, gelişmiş ve güçlü devletlerin savaş tehditlerinde birincil güvenlik sorunu olarak ortaya çıkmıştır. Bu doğrultuda; devletin internet kullanımına bağımlılığı ve siber ortamdaki gücü ile zayıflığı, kırılganlığı ve güvenlik tehdidi altında olması tamamen ters orantılıdır. Bu güvensizliğin ortadan kaldırılması için ise hangi silahlara izin verileceğine yönelik kurallar belirlenmelidir. Bu kurallarda kısaca şu hususlara dikkat edilmelidir;

- İzin verilen siber silahlar hakkında kurallar siberin kendi karakteristik özelliklerine göre belirlenmelidir. Siber işlemler bilgi sistemlerini bozar. Bu yüzden kullanılacak siber silahlar kesinti oluşturmamalı, fiziksel hasar oluşturmamalı veya istenmeyen etkilere neden olmamalıdır.
- Siber operasyonlar şiddet ve doğrudan yaralanma veya acıya neden olmaz. Böylece siber işlemler siber çatışma hukukunda yeni bir bilgi işlem biçimi olarak görünmelidir. Örneğin ölümcül olmayan stuxnet kuvvet kullanımı ile ilgili uluslararası hukuk kapsamında neyi temsil ettiği konusunda bir fikir birliği yoktur. Bu bağlamda savaşın "beşinci boyutu" olarak, siber alan Silahlı Çatışma Hukukunun yeni bir boyutunu temsil etmektedir. Daha önce olduğu gibi de, yeni bir savaş boyutu olan siber uzay tasarlanan kuralların önünde yarışmaktadır. Bu yüzden kurallar belirlenerek bu tersine döndürülmelidir.
- Siber silahlarla birlikte savaş ve dış politika bakışı asimetrik bir nitelik kazanmıştır. Bu sebepten ötürü güvenlik çalışmaları alanı bir dönüm noktasında olabilir. Hangi silahlar kullanılabilir, hangileri ise yasaklanmalıdır? Buna karar verilmelidir.

ÜÇÜNCÜ BÖLÜM

SİBER SAVAŞ

3.1. Siber Savaş Kavramları

Uluslararası ilişkilerde yeni bir savaş alanı olarak kullanılan "siber savaş" kavramına ilişkin teorik tartışmaları gerçekleştirebilmemiz için öncelikle, "siber" ve "savaş" kelimelerini ayrı ayrı tanımlamamız gerekmektedir.

3.1.1. Kültürel Olgu Olarak "Savaş" Kavramı ve Siber Savaş

Tarihsel olgulardan bahsedilirken değinilecek en önemli vakaların başında savaş gelmektedir. İnsanlık tarihi kadar eski olan savaşlar tarihini incelediğimizde, devletlerin, ulusal çıkarlarını korumak ve hayat alanlarını genişletmek amacıyla düzenli ordular kurdukları görülmektedir. İktidarda iktidarını pekiştirmek ve güçlendirmek amacıyla bu ordular aracılığıyla silahlı güç kullanılması yöntemine tarih boyunca sürekli başvurmuştur. Aynı zamanda; uluslararası sistemde yer alan aktörler arasında savaş ve çatışma içerikli çift yönlü ilişki her zaman var olmakla birlikte tarih boyunca hayatın her alanında meydana gelen değişimlerden de bu çift yönlü ilişki doğal olarak etkilenmiştir.[205] Bu yüzden; savaşın tanımlanması hukuksal, ideolojik, felsefi, siyasal, ekonomik, sosyolojik ve psikolojik boyutlarıyla yakından ilgilidir.

Uluslararası hukukta savaşın herkes tarafından kabul edilmiş bir tanımı bulunmamaktadır. Bunun sebebi, bir silahlı çatışmanın veya eylemin savaş sayılıp sayılmayacağı hususunda uluslararası hukukta objektif bir ölçütün benimsenememiş olmasıdır. Bu doğrultuda; herhangi bir silahlı çatışma eyleminin savaş sayılıp sayılmayacağı hususundaki temel ölçüt ilgili devletlerin amacı olarak değerlendirilmektedir. Bu sebeple, savaşan taraflardan herhangi birisinin savaş amacıyla hareket etmesi durumunda, söz konusu silahlı çatışmaların savaş olarak değerlendirilmesi gerektiği genel olarak kabul görmüş bir kuraldır.

Savaş; "bir toplumun, bir ulusun veya devletler topluluğunun isteklerini diğer bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştikleri bir mücadele" şeklinde tanımlanmasının yanında, "uluslararası hukuk kurallarına uygun

[205]Fatih Dedemen, a.g.e. , ss.141-176.

şekilde devletlerarasında yürütülen silahlı bir çatışma, bir çekişmedir" şeklinde de tanımlanmaktadır. Yani savaş kavramına yönelik geçmişten günümüze birçok askeri teorisyen savaşı hep değişik şekilde açıklamıştır. Fakat Sun tzu'dan Clausewitze genel olarak orta noktalarını bulmaya çalışırsak; hedeflerin, olanakların, sınırlamaların sıralanması ve bu bilgiler ışığında en az kayıpla başarılı olmanın hedeflendiği açıktır.[206] Örneğin; savaşı ayrıntılı olarak inceleyen Napolyon'a karşı savaşmış Prusyalı General Carl Von Clausewitz'e göre savaş genişletilmiş bir düellodur ve savaş "düşmanlarımıza isteklerimizi şiddet kullanarak zorla kabul ettirme eylemidir. Savaş sanatı ve stratejisi bağlamında savaş, politik gücün şiddet yoluyla ifadesidir. Clausewitz'in (1780-1831)"savaşın politikanın başka araçlarla devamı" yönündeki görüşü, savaş olgusunun devletler açısından işlevsel anlamını ifade etmek bakımından önemlidir. [207]

Ülkelerin kendi aralarındaki anlaşmazlıkların çözümü için bir araç olarak kullandıkları savaş, teknolojik gelişmelere bağlı olarak zaman içinde değişerek, günümüzdeki tahribatı çok büyük boyutlara ulaşabilecek çatışma haline dönüşmüştür. Günümüzde savaşlar, sadece düzenli orduların kullandıkları dış politika aracı olmaktan çıkarak, gayri nizami gruplar tarafından asimetrik tehdit boyutuyla güçlü devletleri bile işbirliğine ihtiyaç duyar hale getirmiştir. Bunun en güzel örneği; silah sistemleri teknolojisinin, savaşın operatif ve taktik bütün safhalarını ilgilendirmesidir. Ulaşım ve haberleşmedeki gelişmeler savaşın etkisini küresel düzeyde şiddetlendirmiştir. Bu sebeple günümüzde siber uzay savaşlarda kullanılan operatif ve taktik safhalar ile ulaşım ve haberleşmeyi sağlayan en temel araçtır. Aynı zamanda savaşın maliyetinin oldukça ağır olması düşük yoğunlukta olan çatışmaları da siber alana yönlendirmiştir.

Savaş kavramında asıl amaç beslenme, üreme, kendini karşıya kabullendirme ve yaşama alanını genişletmektir. Bu hedeflere ulaşmak için gerçekleştirilen savaşların boyutlarının büyük maddi ve manevi zarar vermesinden dolayı uluslararası ilişkilerde diplomasi kavramı gelişmiştir. Zaman içinde siyasi, sosyolojik, psikolojik ve teknolojik anlayıştaki değişim savaş olgusunun da eskisi kadar sık yaşanmamasına yol açmıştır.[208] Bu sebeple teknolojik gelişmeler neticesinde

[206] Knake ve Clarke, "Siber Savaş", a.g.e. , ss.79.
[207]Carl Von Clausewitz, "Savaş Üzerine", Çeviren Koçak, S. Doruk Yayınları, 2015.
[208]Haldun Yalçınkaya, Savaş Farklı Disiplinlerde Yeni Yaklaşımlar, Siyasal Kitapevi, Ankara, 2010.

alternatif olarak "siber" alan etkili bir savaş alanı olarak kullanılmaya başlanmıştır. Örneğin; Liddell Hart, savaşın bütün prensiplerini kuvvet toplama deyimine indirgemiştir. Burada değindiği temel prensip gerçek kuvvet toplamanın, hesaplı bir dağılmanın meyvesi olduğudur. Liddell Hart'a göre planlar mevcut şartlara göre uydurulurken daima amaç araçlara göre ayarlanmalıdır. En az umulan hareket tarzı seçilmeli ve en az direnilen yerden saldırılmalıdır. [209] Günümüzde siber uzay bu en hassas noktadır.

Günümüzde aktif olarak kullanıldığını iddia ettiğimiz siber savaş döneminin olmadığı yâda ne zaman başladığı yönünde tezimize yönelik geliştirilebilecek olumsuz görüşlere verilebilecek en güzel cevap şu şekildedir. İnsanların bencilliği ve saldırganlığı insanlık tarihinden beri tartışılan bir konudur. Savaş, insan doğası için vazgeçilmez bir durum ise barış dönemleri nasıl açıklanabilir? Savaşın olmadığı dönem barış olarak nitelendirilebilir mi? O zaman Soğuk Savaş barış dönemi midir? Ticaret savaşları yaşandığını iddia edenler neyi kastetmektedir? Ya da siber savaş yaşandığını iddia etmemiz ne kadar bilimseldir? Tüm bu sorulara gerçekçi olarak verilecek en önemli cevap; ülkelerin harbe hazırlanması, kendi iradelerini başkalarına zorla kabul ettirmesi, maruz kalacakları dayatma ve baskılara boyun eğmemek için milli kaynaklarının önemli bir bölümünün silahlı kuvvetler için ayırmasından anlayabiliriz. Yani savaş; bir toplumun başka bir topluma, istediğini benimsetme amacıyla tüm olanakları ve güçleriyle yaptıkları düzenli saldırı olarak görmeliyiz. Clausewitz'in savaş'ın çok genişletilmiş bir düello olarak tanımlaması aslında fayda sağlamaktadır. Çünkü zaferin kazanılması, toplum, ordu ve hükümetin uyumuna dayanmaktadır. Siber ortamda bu uyumun tam ortasındadır.

Peter Paret, Clausewitz'in "Savaş siyasetin başka araçlarla devamıdır." ünlü sözünü bugünün savaş ve barış kavramları ile bağını şu şekilde kurmuştur. Paret'e göre Clausewtiz bu sözü söylediğinde muhtemelen bu ayrım daha netken bugün savaş ve barış arasındaki ayrım şüphelidir. Bu sebeple geçmişteki deneyimler bugünün Endüstri 4.0 ve Toplum 5.0 kavramları sonucunda oluşan teknolojik çağını tam olarak açıklayamaz ama anlamamıza yardımcı olur. Bu yüzden modern

[209]B.H. Liddell Hart, Strateji Dolaylı Tutum, Çev. Koçak, S. Doruk Yayıncılık, 2015, ss.464-465.

teknolojiye göre bu kavramların güncellenmesi gerekmektedir.[210]Siber savaşlarda modern teknolojinin en yeni saldırı şeklidir.

Beril Dedeoğlu'na göre savaş; diğer yöntemlerle çözülememesi, devlet tekelinde kullanılması, geçmişi ve geleceği olması, genel mantığı olarak ekonomik kaynakları ve stratejik olanakları ele geçirerek genişleme hedefi içermesi, silahların organize kullanılması, şiddet içermesi, hasma kendi iradesini kabul ettirmesi, diplomasinin tıkandığı yerde çözüm olarak görülmesidir.[211]

Sonuç olarak tüm bu tanımlamalar savaşın geçmişten gelen stratejik bir kültüre sahip olduğu ve zamanın şartlarına göre araçlarının ve yöntemlerinin sürekli değiştiği ve dönüştüğünü göstermektedir.

3.1.2. Genel Anlam Bakımından "Siber savaş" Terimi nedir?

Siber savaş, uluslararası ilişkilerde bilgisayar ve iletişim teknolojisini saldırı ve savunma amaçlı kullanarak devletler veya devlet benzeri aktörler tarafından gerçekleştirilen, kritik ulusal altyapıları, askeri sistemleri veya ülke için önemli endüstriyel yapıyı tehdit eden, simetrik veya asimetrik, saldırı veya savunma maksatlı dijital ağ faaliyetleri şeklinde kısaca tanımlanabilir.

Diğer bir siber savaş tanımı "ülkelerin ulusal güçlerinin tamamını veya bir kısmını kullanarak siber ortamda gerçekleştirdikleri mücadele" olarak yapılabilir. Burada gözden kaçırılmaması gereken nokta, mücadele siber ortamda gerçekleştirilse de sonuçlarının siber ortamda olduğu kadar fiziksel ortamda da görülebilecek olmasıdır. Bu çerçevede siber savaşlar stratejik, operatif ve taktik olmak üzere her seviyede uygulanabilir olma özelliğini içinde barındırır. Teknoloji geliştikçe ve bilgisayar kullanım alanı ve kullanıcı sayısı arttıkça siber taarruzun hedef kitlesi ve alanı da doğru orantılı bir şekilde artmaya devam edecektir.[212]

Dilbilgisi Bakımından "Siber Savaş" kavramını incelediğimizde; Türk Dil Kurumu Büyük Türkçe Sözlüğü 'ne bakıldığında siber savaş tanımlanmamıştır.[213]

---

[210] Peter Paret, "Modern Strateji Machiavelli'den Nükleer Çağa", Çev. Koçak, C. DorukYayınları, 2015, ss.1033-1042.
[211] Beril Dedeoğlu, "Uluslararası Güvenlik ve Strateji", a.g.e, ss-25-30.
[212]Gökhan Bayraktar, "Siber Savaş ve Ulusal Güvenlik Stratejisi", Yeni yüzyıl yayınları, İstanbul, 2015, ss.48-50.
[213]Siber Savaş, Türk Dil Kurumu Sözlükleri, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5cbd798e8c87c4.76321916 , ET.30.01.2020.

Birleşmiş Milletler Terimler sözlüğünde, siber barış, şiddetin yokluğuna dayanan evrensel bir siber alan olarak tanımlanmıştır. Siber savaş (cyber war) ve bilgi savaşı (information warfare) kavramları birlikte benzer anlama gelecek şekilde "bilgisayar sistemlerinin düşman sistemlerine zarar vermesi veya yok etmesi amacıyla kullanılan savaş tipi" şeklinde tanımlanmıştır.[214]

Aynı zamanda, siber savaş, karşıt çıkarları olan ulusların, birbirlerine bilişim ağ ve sistemlerini kullanarak savunma ve taarruz amaçlı olacak şekilde bilgi ve iletişim sistemlerinin yok edilmesi, zarara uğratılması ya da manipüle edilmesi şeklinde özetlenebilecek bir olgudur. Bu yüzden siber savaş günümüzde genel olarak dikkat dağıtma teknolojisi ve psikolojik saldırı yöntemi olarak kullanılmaktadır. Uygulanan bu siber saldırıların yöntemleriyse çeşitlidir. Öncelikli olarak kullanılan yöntem, elbette internet üzerinden saldırmaktır. Bunun için kullanılan en basit yöntem, DDoS adı verilen saldırı türüdür. Bu yöntemle belirli bir siteye ya da sunucuya, yanıt veremeyeceği kadar sahte erişim isteği yollanır. Bunun sonucunda, site sunucusu talepleri karşılayamaz hale getirerek kendisini kapatması sağlanır. Kullanılan bu yöntem siber silahlar kullanılarak gerçekleştirilen siber savaşın sadece bir çeşididir. Teknolojinin ilerlemesiyle birlikte, savaş yöntemleride artmıştır. Böylece siber çatışmalarda açıktan savaş ilan etmeye gerek olmamakla birlikte barış dönemlerinde bile başvurulan bir yöntem şeklini almıştır. Yani makineli tüfeklerin yerini rahatlıkla bilgisayarların almış olduğunu söyleyebiliriz.[215]

Siber silahlar kullanılarak gerçekleşen siber savaşta, saldırı zamanı ile bu saldırının karşı tarafta yaratacağı etki neredeyse aynı anda gerçekleşmektedir. Bu durum aynı zamanda kriz yöneticilerinin karar alma süreçlerini ve ellerinde bulundurdukları zamanı önemli ölçüde zora sokmaktadır. Ayrıca siber ortamın yapısı ve kullanılan tekniklerin karmaşıklığı, herhangi bir siber çatışma durumunun kolaylıkla küresel hale gelebileceğini ve birçok devleti bu savaşın içerisine çekebileceğini göstermektedir. Bu yüzden siber savaşın tanımlanması konusundaki en önemli problem savaş konusu sayılabilecek saldırıların neler olduğunun belirlenmemesi ve saldırı kaynağının tespitinin siber ortamda zor olmasıdır.

[214]Cyber War, UNTerm Portal, https://unterm.un.org/unterm/search?urlQuery=cyber+war ET.30.01.2020.
[215]Aydın, a.g.e. ss. 137-152.

Siber savaş gerçektir ve şuanda uygulanmaktadır. Geleneksel savaş gibi çift taraflıdır. Siber savaşta gerçekleşecek saldırılar bir ülkeyi derinden sarsacak bir güce sahiptir. Şuana kadar yöntemleri net olarak ortaya konmamıştır. Işık hızında gerçekleşmektedir. Küreseldir. Geleneksel savaş alanından önce kullanılır. Henüz resmi olarak devletler tarafından ilan edilmemiştir. Bu yüzden kimin kazanacağı, sonuçlarının ne olacağı, etkisinin nerelere varabileceği ve gelecekteki boyutunun ne olacağı bilinememektedir. Günümüzde daha çok istihbaratçılar siber uzayda faaliyet yürütmektedir. Bu faaliyetlerde güvenlik riski yaratmakla birlikte hem saldırı hem de savunma alanında güçlü olmayı zorunlu kılmaktadır.[216]

Siber savaşın ilgi alanı siber uzaydır. İçinde istihbarat, psikolojik unsur, ordu birimi, asker(hacker grubu), komuta grubu olan bu savaş türü hem ekonomik hem de elektronik bir savaş şeklidir. Siber savaş doğrudan bilgi sistemlerini hedeflemektedir. Siber savaş gerçekte geleneksel savaşla elde edilebilecek sonuçları sanal dünyada gerçekleştirmeyi hedeflemektedir. Bunu yaparken de savaşın diğer boyutlarını kullanıp farklı araçlarla aynı amaca ulaşmaya çalışır. Çünkü klasik hayatta olduğu gibi günümüz siber dünyasında da iyi ve kötü birlikte bulunmaktadır. Uluslararası anarşik bu yapı içerisinde üst çatı ve kurallarda belirlenememiştir. Bunun en güzel örneğini stuxnette görebiliriz. İran dışında birçok ülkeyi de alarma geçirerek önlem almalarına yol açan Stuxnet solucanının arkasında kim olduğu yönünde İran bir grup hackerı suçlamak yerine İsrail ve Amerika Birleşik Devletlerini sorumlu tutsa da bu ülkeler bu iddiaları asla kabul etmemiştir. Faillerde resmi olarak kanıtlanamamıştır. Bu bilinmezlik ortamındaysa siber saldırılara karşı önlem almak bir zorunluluk haline gelmiştir.

Bu bağlamda alınan önlemler açısından "Siber Savaş" kavramına baktığımızdaysa; siber silahlardan gelebilecek saldırılara karşı aktörler tarafından alınan önlemler siber savaş ve klasik savaş arasında strateji, taktik, diplomasi, uluslararası hukuk ve silah sistemleri açısından kıyaslama yapmamızı kolaylaştırır. Bu kolaylaştırma için özellikle iki önemli aktör olan devletler ve uluslararası aktörler açısından alınan siber savaş önlemleri belirleyici bir rol üstlenmektedir.

İlk olarak devletler açısından alınan önlemleri incelediğimizde,siber silahların kullanılmasının henüz çok yeni bir durum olmasından kaynaklı devletlerin gerçek

[216]Knake, ve Clarke, a.g.e. , ss. 23-29.

siber yetenekleri ve sahip oldukları siber silahların gerçek kapasiteleri tam olarak ölçülememektedir. Bu yüzden; ABD, Rusya, Çin ve diğer aktörlerin sahip oldukları gerçek yetenekler tam anlamıyla kullanıldığında bu saldırıların bir ulusun sonunu getirip getiremeyeceği henüz bilinememektedir.

Ayrıca siber alanda kullanılan yazılım, araç ve yeteneklerin satın alınabilir olması devletlerin üzerinde durdukları en önemli husustur. Devletler rakiplerine karşı avantajlı konuma geçmek için yapacakları saldırıları bu işten para ve güç kazanan gruplar üzerinden gerçekleştirmektedir. Bu durum terör grupları ve bilişim şirketleri tarafından gerçekleştirilen siber suç, siber casusluk, siber terörizm, siber saldırı gibi faaliyetlerin ve kavramların gelişmesinde önemli bir rol oynamaktadır. Bu şirketler veya gruplar devletlerin veya devlet dışı grupların kullanacakları siber yeteneklere yönelik alternatif stratejiler geliştirerek açıklar bulmaya çalışmaktadır. Bu durumda uluslararası anarşik sistemin içinde ana aktör olarak kabul ettiğimiz devletleri ciddi bir risk tehdidi içine bırakmaktadır.

Aynı zamanda; uluslararası düzende belirleyici kurallar olmaması yüzünden devletler siber güvenliklerini sağlayabilmek için özellikle iç hukuk sistemlerinde çıkardıkları kanun, yönetmelik ve yönergeler doğrultusunda oluşturdukları kurum, kuruluş ve birimler çerçevesinde çeşitli projeler geliştirerek rakiplerden gelebilecek tehditlere karşı caydırıcılık oluşturmaya çalışmaktadır.

Diğer önemli aktör olan uluslararası aktörler açısından alınan önlemleri incelediğimizde, siber güvenlik faaliyetleri gerçekleştirilirken savunan açısından dijital ağlar ve altyapılar arasında yüksek seviyede birbirine bağımlılık, saldırgan açısından ise teknolojik yeterlilik en öncelikli konular arasındadır. Bu sebeple alınan önlemleri özellikle NATO örnekleminde incelediğimizde, siber savaş kavramının ortaya çıkmasıyla birlikte doktrinini değiştirerek konunun teknik ve hukuki boyutunu tartışmak üzere çalışmalara başlamıştır. Bu süreci kronolojik olarak kısaca vurguladığımızda ise önemli dönüm noktaları şu şekilde gerçekleşmiştir.

11 Eylül saldırısı gerçekleştikten sonra NATO, Kasım 2002'de kabul edilen "Prag Yetenek Taahhütleri"nin bir parçası olarak yeteneklerin siber saldırılara karşı koruyabilecek şekilde İttifak öncelikli olarak askeri kanadın talep ettiği pasif koruma önlemlerinin uygulanmasına odaklanmıştır. 2007 yılında Estonya'nın maruz kaldığı siber saldırı ise hazırlık boyutunu farklı bir boyuta taşıyarak resmi bir "NATO Siber

Savunma Politikasının" hazırlanmasına yol açmıştır. 2008 yılında Bükreş Zirvesi ile NATO'nun, savaş kavramında yaşanan değişikliğe cevap verecek yeniden yapılanmaya dönüşmesine yönelik Strateji Belgesi oluşturulmuştur. Bu çerçevede Zirve Bildirgesi'nin 46. maddesinde, NATO'nun bu değişimin sağlanması için gereken kaynağı temin edeceği belirtilmiştir. Bükreş Zirvesi sonrasında siber güvenlik alanında ise iki önemli gelişme yaşanmıştır. Bunlar; Brüksel Merkezli NATO Siber Savunma Yönetimi Otoritesi ve Estonya Tallinn merkezli bir NATO Siber Savunma İşbirliği Mükemmeliyet Merkezi'nin kurulmasıdır. 2010 yılındaki Lizbon zirvesinde ise siber savunmanın sürekli olarak NATO gündeminde bulunması yönünde temel bir karar alınmıştır. 2011 yılındada NATO Siber Savunma Politikası ve Siber Savunma Eylem Planı'nın detayları kabul edilmiştir. Bu politika, ittifaklara yönelik siber savunma konusunda gerçekleştirilecek olan topluluk bazındaki çabaları içermektedir. Aynı zamanda; Siber Savunma Politikasındaki siber tehditler, yeni Stratejik Kavram doğrultusunda 5. maddede ifade edilen toplu savunma görevini yerine getirmesi için potansiyel kaynak olarak tanımlanmaktadır. Bu yüzden 2012 yılında NATO Bilgisayar Olayları Karşılama Kapasitesi'nin (NATO Cyber Incident Response Capability - NCIRC) tamamen operasyonel hale gelebilmesi için 58 milyon Avroluk bir kontrat imzalanmıştır.[217]

Günümüzde de NATO üyesi ülkelerden birisinin kritik altyapısına karşı gerçekleştirilecek bir siber saldırının diğer ülkeleri de ilgilendiren sonuçları olabileceği, bu nedenle üye ülkelerin siber savunma imkân ve kabiliyetlerinin artırılmasının önemi vurgulanmaktadır. NATO siber güvenlik konusunda önemli mesafe almış olmakla birlikte, konuyla ilgili temel sorun ortak savunma koşulunu kapsayan 5. maddenin siber saldırıyı kapsayıp kapsamayacağıdır. Yani üye ülkelerden birinin silahlı saldırı yerine siber saldırıya uğraması halinde, anlaşmanın bu maddesinin geçerli olup olmayacağının belli olmamasıdır. Bu belirsizlik aynı şekilde uluslararası ortamda da devam etmektedir. Silahlı çatışma hukuku kuralları ve savaş hukukuna ilişkin uluslararası hukuk kurallarının siber savaşta uygulanıp uygulanamayacağı hala tartışılmaktadır. Tartışmalar devam etse de siber alanda yaşanan saldırı/savunma yönündeki gelişmeler Siber Savaş'ın gerçek olduğunu

[217]Neil Robinson, "Başarılı Bir Siber Savunma İçin Harcama Yapmak", NATO Dergisi, 2017 https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html , E.T 29.01.2020.

göstermektedir. NATO özelinde gerçekleşen çatışma örneklerine kısaca bakarsak, NATO'nun Kosova müdahalesinde Sırbistan tarafından kaynaklandığı düşünülen NATO'nun Brüksel'deki ağ sunucunu bozma yönünde NATO'ya yönelik saldırılar gerçekleşmiştir. Yâda 1992'de NATO'nun yanlışlıkla Belgrat'taki Çin büyükelçiliğini bombalaması sonrasında Çinli hackerler tarafından ABD'deki hükümet siteleri hacklenmiştir. [218]

3.1.3. Hukuki Bir Terim Olarak "Siber Savaş"

En genel ifadeyle "siber savaş", "bilgi teknolojilerini korumak için bilgisayar ve iletişim teknolojisini kullanarak siber alanda savunma yapmak veya saldırmak ya da kritik altyapılarına yapılan planlı saldırıları engellemek için yapılan faaliyetlerin tümü" olarak tanımlanabilir.

Siber savaş kavramını tartışmadan önce, siber savaş terimini hukuksal bir terim olarak açıklamamız gerekmektedir. Şu ana kadar, siber savaş teriminin anlamı ve bu savaşı düzen altına alacak ulusal ve uluslararası kural ve stratejilerin ne olacağını konusunda uluslararası arenada bir fikir birliğine varılamamıştır.[219] Bunun en önemli sebebi; Siber alandaki hangi saldırıların kuvvet kullanımı olarak algılanacağının henüz netlik kazanmamasıdır. Aynı zamanda, gerçekleştirilen bir siber saldırıya karşı nasıl bir karşılık verileceği konusunda da ciddi boşluklar bulunmaktadır. İç hukukta ise durum farklıdır. Devletler kendi sorumluluk sahaları içerisinde gerçekleşen siber olaylarda bunu suç kabul edip yasalarla koruma altına almış ve bu korumayı sağlıklı gerçekleştirebilmek için kendi emniyet, istihbarat ve ordu birimleri içerisinde siber birimler oluşturmuştur.

Sonuç olarak; gerçekleştirilen düzenlemeler sonucunda hukuki ve etimolojik bakış açılarıyla siber savaş var diyebiliriz. Her ne kadar uluslararası arenada bir fikir birliğine varılamamış olsa da siber güvenlik kavramının gelişmesi, siber tehditlerin etkilerinin kapsamının genişlemesi ve sınırlar üstü bir savunma zafiyeti haline gelmesi siber savaş hukuku alanında hem iç hukukta hem de uluslararası hukukta çalışılmasını zorunlu kılmıştır. Bu zorunlulukları kısaca açıklarsak;

---

[218]Taner Altınok ve Haydar Çakmak, a.g.e ss. 92

[219]Mehmet Yayla, "Hukuki Bir Terim Olarak Siber Savaş", TBB Dergisi Cilt.104, Yıl. 2013, ss.184-185. http://portal.ubap.org.tr/Ass_Themes/Dergi/2013-104-1247.pdf ET.14.12.2019.

- **Uluslararası Hukuk Kuralları, Uluslararası Kaideler ve Anlaşma Standartları Çerçevesinde Siber Savaş**

Devletler, güvenliğin kendi kendine yardım sistemi olduğu anarşik bir dünyada yaşamlarını sürdürmektedir. Bu anarşik sistem içerisinde devletler meşru şiddet üzerindeki tekellerini kullanarak düzen ve güvenliği sürdürmektedir. Meşruiyet ise uluslararası yasalar, normlar ve savaş ile ilgili tanımlardan gelir. Benzer şekilde, siber savaş tanımları ve ilgili normlar, tanımlar ve şartlar da devletlerin siber alanda nasıl davranacağını yönlendirir. Siber yeteneklerin kapsamını ve kullanımı belirleyip, sınırlayıp, bazı yasaklamalar oluşturulmazsa anarşik yapı içerisinde siber alanda çatışmaların artması da kaçınılmaz olacaktır. Bu yüzden siber savaşta ortak bir anlayış, devletlerin oluşturacağı siber saldırıları caydırabilir.

Siber alanda savaş çok geniş bir tanımdır. Siber savaş normal anlamda bir savaş kavramının eşanlamlısı değildir. Bilişim alanındaki süregiden çatışma mücadelesinin bir alt kümesidir. Çünkü psikolojik harekat, askeri aldatma, harekat güvenliği, elektronik harp ve bilgisayar ağ operasyonları gibi birçok bilgi ve bilgisayarlara ek olarak personele, tesislere veya ekipmana saldırmayı da içinde barındırır. Fakat uluslararası hukukun mevcut rejimi bu siber yeteneklerin hiçbirini öngörmemiştir.

Örneğin; Birleşmiş Milletler (BM) Sözleşmesi, Lahey ve Cenevre Sözleşmeleri ve ilgili antlaşmalar devletler arasındaki "kuvvet kullanımının hukuki sonucu", "güç kullanımı", saldırganlık ve savaş eylemlerini değerlendirmenin tek temelidir. BM Sözleşmesinde Madde 2 (7)'deki Birleşmiş Milletler tarafından iç işlere müdahale edilmemesi maddesi ve Madde 2 (4)'deki uluslararası ilişkilerde tehdit veya güç kullanımı yasağı maddeleri çok önemlidir.[220]

BM Sözleşmesinde Madde 2 (7)'deki Birleşmiş Milletler tarafından iç işlere müdahale edilmemesi maddesi; Birleşmiş Milletler 'in ve dolayısıyla Güvenlik Konseyinin temel amaçlarından birinin "eşit haklar ilkesi ve halkların kendi kaderini tayin" ilkesine saygılı dost uluslararası ilişkiler geliştirmek olduğunu tespit eder. Güvenlik Konseyi bu maddeyle halkların bağımsızlık, özerklik, referandum,

[220]United Nations Charter, Purposes and Principles of the United Nations Article 2(4), https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter, ET:17.01.2020.

seçimlerle ilgili olabilecek kendi hükümetlerine karar verme hakkını verir ve dış müdahaleyi yasaklar. Bu tezde siber saldırılarda kullanılan vaka çalışmaları özelinde, 2016 yılında gerçekleşen Amerikan Seçimlerine yönelik sabotaj iddiaları siber alanın hükümetlerin meşruiyeti ve ülkelerin mili egemenliklerine yönelik bir saldırı ortaya koyduğu yönünde bir sonuç çıkarmaktadır.

BM Sözleşmesinde Madde 2 (4) , tehdidi veya güç kullanımını yasaklar ve tüm Üyeleri diğer Devletlerin egemenliğine, toprak bütünlüğüne ve siyasi bağımsızlığına saygı duymaya çağırır. Bu tezde ayrıntılarıyla ortaya koyduğumuz siber vakaların hemen hemen hepsinde ülkelerin sanal topraklarına yani sınırlarına veya siyasi bağımsızlıklarına yönelik müdahale mevcuttur. Yani BM Şartı'nın 2 (4) maddesi ihlal edilmektedir.

BM Genel Kurulunun 3314 sayılı Kararının "Silahlı kuvvetlerin kullanımı" egemenlik, toprak bütünlüğü veya bir başkasının siyasi bağımsızlığına karşı bir devletin doğası gereği kendini savunma hakkını tetikleyen…" yasal olanı tanımlar. Bu yasal alan içinde siber savaşın anlaşılmasında kilit konu silahlı saldırı kavramını içermesidir. Fakat, BM Şartı silahlı saldırı için bir tanım sunmamaktadır. Bu durum da kullanımında diğerlerine fiziki olarak yada Gürcistan ve Estonya'daki gibi ekonomik ve psikolojik olarak zarar veren siber silahlar konusunda bir boşluk ortaya çıkarmaktadır.

Kuvvet kullanmanın dinamik yapısı göz önünde bulundurulduğunda, yapısı itibariyle fiziki gücü içermeyen ancak silahlı saldırı ile aynı derecede somut zararlara sebep olabilen siber saldırılar, kuvvet kullanmaya eşdeğer olabilirler. Örneğin; kimyasal, biyolojik ve radyolojik silahlar da yapısı itibariyle silahlı saldırılar gibi yıkıcı olmamasına rağmen kuvvet kullanımı kapsamında değerlendirilmektedir. Siber saldırılar bağlamında yukarıda ele aldığımız 2010 İran'ın nükleer kapasitesine yönelik yapılan Stuxnet virüs saldırısı, bunun açık örneğini teşkil etmektedir. Dolayısıyla, siber saldırılar açık bir şekilde doğrudan fiziki zararlara yol açabilme eşiğini geçmiş ve ciddi zararlar verebilme kapasitesine ulaşmıştır.[221]

[221]Ramazan Güreşçi, Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi, Savunma Bilimleri Dergisi, Cilt. 18, Sayı. 1, Mayıs 2019, ss.87.

Yukarıda da belirttiğimiz gibi siber suçların ulus ötesi karakterini ele almak küresel bir çaba gerektir.[222] Bu yüzden BM tarafından ortaya konacak yaptırımlar veya cezai eylemler, siber saldırganlar için güçlü bir caydırıcılık yaratacaktır. Bu yaptırım ve cezai eylemlere ilişkin kullanılabilecek en güzel temel ise Avrupa Konseyi'nin (CoE) Siber Suç Sözleşmesidir. Antlaşma, siber alanda suçla mücadelede uluslararası işbirliğini teşvik ederek "ortak bir ceza politikası oluşturma" amacıyla siber suçlar olarak işlenen suçlardan caydırma ve "suçluların kaçınabileceği ülke sayısını azaltmayı amaçlayan bir model sunmaktadır. Ancak, tek başına bu sözleşme, siber savaşa genişletilemez.

Bu doğrultuda savaş kuralları ve uluslararası kaideler günümüz tehditlerini tam olarak kapsamamaktadır. Bu yüzden bu kuralların siber savaş kriterlerini içine alacak şekilde revize edilmesi gerekmektedir. Örneğin; internet, bilgi ağlarına bağımlı toplumlar için gerçek riskler oluşturmaktadır. Bilgisayar saldırılarının sadece diğer bilgisayarları değil, daha büyük altyapıları da tehdit ediyor olması bu virüsleri füzeler kadar tehlikeli hale getirmektedir. Aynı zamanda, siber saldırılar ölüm riskini ve çatışma maliyetlerini en aza indirme potansiyeline sahiptir. Yani siber saldırılar, bir elektrik şebekesini yıkmak yerine, geçici olarak devre dışı bırakma seçeneği sunmaktadır. Özellikle Estonya olayı siber güvenliği NATO'nun hızla gündemine almasına yol açtı. Bu olay sonrasında NATO'nun en önemli ülkesi olan ABD'nin o dönemki Başkanı Bush da, ABD sistemlerinin siber saldırılara karşı savunmasızlığını ve hükümetin bunlara karşı savunma geliştirme ihtiyacını kabul etmiştir.[223] Ancak ülkeler ve örgütler, siber alanı yeni bir savaş alanı olarak tanımlasa da bu yeterli değildir. Silahlar ne zaman ve nasıl konuşlanmalıdır? ve Siber savaşın kuralları nelerdir? Gibi ayrıntılarında oluşturulması gerekmektedir.

Yüzyılı aşkın bir süre önce uluslar, çatışmalardan ve savaştan kaçındığında veya insan acısını en aza indirmek istediklerinde Cenevre Sözleşmesi gibi uluslararası hukuk kurallarını geliştirdiler. Aynı zamanda yeni teknolojiler ortaya çıktıkça, ülkeler biyolojik, kimyasal ve lazer silahlarını kısıtlayan antlaşmalar doğrultusunda yeni kuralları koyup koymayacaklarını tartıştılar. Bununla birlikte,

[222]Kristin Archick, "Cybercrime: The Council of Europe Convention", CRS Report for Congress RS21208, 28 Eylül 2006.
[223]Duncan B. Hollis, "Rules of Cyberwar?", Los Angeles Times, 8 Eylül 2007, https://www.latimes.com/archives/la-xpm-2007-oct-08-oe-hollis8-story.html ET.17.01.2020.

geleneksel bilgelik, sahip olduğumuz yasaların benzer şekilde siber alanı kapsayacak şekilde genişlemesi gerektiğini göstermektedir.

Mevcut savaş yasaları öncelikle ülkeler arasındaki çatışmalara odaklanmaktadır. Ancak 11 Eylül ile birlikte Irak ve Afganistan'da devam eden asimetrik savaş, bu yaklaşımın ne kadar yetersiz olduğunu göstermektedir. Örneğin, BM Şartı devletlerin kendini savunma veya BM yetkisi dışında güç kullanmasını açıkça yasaklamaktadır. Peki bu Rusya'yı Estonya'ya yapılan bilgisayar saldırılarından yasaklıyor mu? Yoksa hedef sadece fiziksel zarar görmüşse "güç kullanımı" mıdır? Ya da sadece ölüm ve yıkıma yol açarsa? Veya hedef ne zaman bir ülkenin güvenliği için kritik olursa? Benzer belirsizlikler tarafsızlık ve sivil ayrımcılıkla ilgili kuralları da çevrelemektedir. Devletler, neye izin verildiğini bilmiyorlarsa, bu saldırılarda kullanılacak silahlar tahmin edilenden daha fazla zarar verebilir.

Siber uzay teknolojisinin ucuz olması, kullanımının kolay olması ve her yerden uygulanabilir olması siber suç ve siber terör kavramlarını arttırarak El Kaide gibi grupları içine çekmiştir. Aynı zamanda Rusya-Estonya, İran-İsrail ve Çin-ABD vakalarının gösterdiği gibi, bir siber saldırının kökenlerini bireysel hackerlardan ziyade bir ülkeye sabitlemenin zor olması da devlet destekli terör gruplarının bu alanı kullanmalarını arttıracaktır. Bununla birlikte, yeni kurallarla, ülkeler egemenlik kaygılarından feragat etmeyi ve teröristlerin tüm ulusların engellenmesini isteyebilecekleri siber saldırılar gibi belirli durumlarda doğrudan müdahaleye izin verecekleri kuralları oluşturmalıdır. Bu durum ülkelerin milli siber ordularında görev yapan askeri komutanların siber alanda daha büyük bir kesinlik ile çalışabilmeleri ve çatışmaların azalması için yeni uluslararası hukuk kurallarının güncellenmesine ihtiyaç olduğunu göstermektedir. Çünkü savaş bilgi çağına girmiştir.

Bilgi çağındaki güvenlik konuları, risk yönetimi yöntemiyle ele alınır, ardından tipik saldırı stratejileri ve savunma ilkeleri gözden geçirilerek takip edilir. Bu süreçte bazı etik sorunlar vardır. Örneğin, iyi tasarlanmamış güvenlik mekanizmaları, saldırganlara istenmeyen hassas bilgilerin sızdırılması gibi yan etkiler, asimetrilerin ve dışsallıkların birçok güvenlik sorununun merkezinde yer

alması gibi pratikte benimsenen çözümsüzlükler etkili bir etik sorundur.[224] Bu etik sorunlar içindeki savaş kuralları, uluslararası kaideler, anlaşma standartları gibi hususlar siber savaş içinde henüz bulunmamaktadır. Etikten bahsedemediğimiz her nokta etik dışı büyük tehdit ve risklerin varlığı ihtimalini ortaya çıkarmaktadır. Savaş kuralları uzun yıllardır vardır. Fakat siber saldırıda ne kadar ilerlenebileceği, ne zaman durulması gerektiği bilinmemektedir. Bu sebeple, Stratejide ve askeri operasyonlarda kullandığımız bütün terimler siber dünyaya adapte edilmelidir. Aksi takdirde bu bir gün kargaşa yaratacaktır. Bir ulusun bir siber silahı nasıl, ne kadar, ne zaman, hangi koşullarda kullanabileceği veya üretebileceği ve bu süreci denetleyecek uluslararası bir rejim kurulma ihtimali ise şuan için zor gözükmektedir. Siber uzayın bu denetim edilemez yapısı güvenliğin sağlanması için tüm stratejik karar verme süreçlerini 7/24 aktif tutulması zorunluluğunu ortaya çıkarmaktadır. Böylece her devlet kendi ulusal güvenliğine odaklanmakta ve bir orta yol kabul etmemektedir.

Yukarıda ayrıntılarıyla açıkladığım savaş kuralları ve uluslararası kaidelerin revize edilmesini iddia etmemizin altında yatan asıl sebep siber savaşların mümkün olduğunu vurgulamamızdır. Peki siber savaş nasıl ve neden mümkündür?

Siber uzay sadece internet demek değildir. Siber dünyadaki tüm bilgisayar ağları ve bağladıkları ve kontrol ettikleri her şeydir. İnternet açık bir ağ ağıdır. Bu sayede herhangi bir ağda, herhangi bir bilgisayara bağlı herhangi bir bilgisayar ile iletişim kurabilmemizi sağlar. Bazı ağlar, makinelerin diğer makinelerle(para akışları, borsa işlemleri, kredi kartı hakkında veri gönderme, pompalar, asansörler ve jeneratörlerle konuşan kontrol panelleri gibi.) konuşmasına izin veren kontrol sistemleridir. Bu doğrultuda ağları askerlerin savaşabileceği bir yer yapan nedir?

En geniş anlamda, siber savaşçılar bu ağlara girebilir ve onları kontrol edebilir veya kilitleyebilir. Eğer bir ağı ele geçirirlerse, siber savaşçılar veriler silmek, tüm bilgilerini çalmak veya para taşımak, petrol dökmek, gaz boşaltmak, jeneratörleri havaya uçurmak, trenleri raydan çıkarmak, uçakları çarpıştırmak, bir uyduyu yörüngeden döndürmek, pusuya bir müfreze göndermek veya füzenin patlamasına neden olmak gibi yanlış talimatlar gönderebilir. Bunlar varsayımsal

[224] Markus Christen, Bert Gordijn ve Michele Loi, The Ethics of Cybersecurity, Springer Open, The International Library of Ethics, Law and Technology 21, Switzerland, 2020 ss.11.

değildir. Bunun gibi şeyler zaten oldu, bazen deneysel olarak, bazen yanlışlıkla ve bazen de siber suç veya siber savaşın bir sonucu olarak. Bu yüzden bilgisayar ağları tarafından yönetilen kamu hizmetleri, ulaşım, bankacılık ve iletişim saniyeler içinde yararlanılabilir veya saldırıya uğrayabilir. Öyleyse güvenlik önlemleri yok mu?

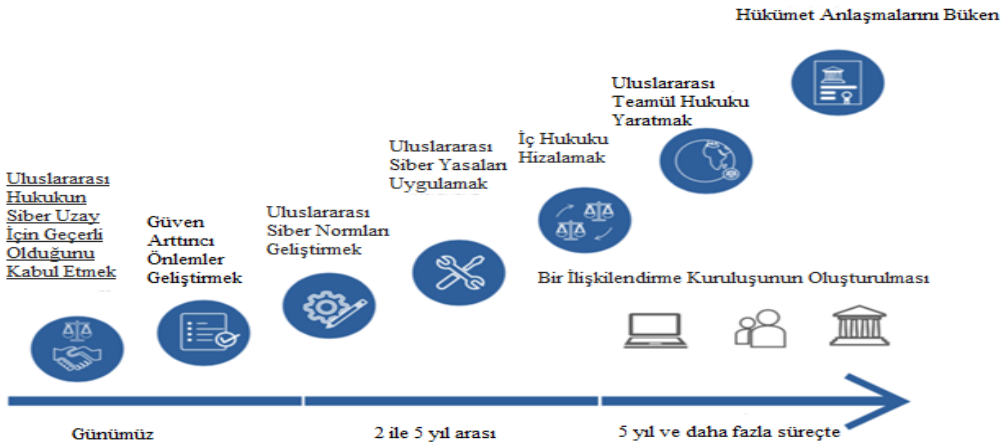
Bilgisayar ağlarının tasarımı, onları çalıştıran yazılım ve donanımlar ve bunların nasıl tasarlandıkları gibi güvenlik savunmalarının hepsi için binlerce yol vardır. İnsanlar hata yapar. Doğal olarak insanların yaptığı yazılımlarda fırsat yaratır. Bu yüzden siber savaşın nasıl olabileceğini günlük yaşantılarda meydana gelen dijital dönüşüm ve değişimlere bakarak açıklayabiliriz. Eğer bu değişimlere bakarsak siber savaşı üç kritik husus mümkün kılmaktadır. Bunlar; internet tasarımındaki kusurlar; donanımdaki kusurlar ve yazılım; ve daha fazla kritik sistemi çevrimiçi duruma getirme hamlesidir.[225]

Siber savaşı mümkün kılan bu üç kriter hakkında genel bir kabul olsa da uluslararası hukukta siber güvenliğin sağlanmasına yönelik geliştirilmiş bir fikir birliği ne yazık ki bulunmamaktadır. İnternet'in artık hayatın her alanını kapsamasından dolayı siber tehditlerin uluslararası hukuktaki yeri vazgeçilmezdir. Bu yüzden oluşacak tehditlerle mücadele edilebilmesi için "siber suç" ve "siber suçlu" gibi kavramlara yönelik Birleşmiş Milletler gibi bir üst otorite tarafından hukuksal düzenlemelerinin yapılması şarttır. Fakat ABD ve Rusya gibi ülkeler böyle bir uluslararası anlaşmanın imzalanmasının, anlaşmaya uyulmasının, denetlenmesinin ve devletler tarafından uygulanmasının imkânsızlığı gerekçesiyle böyle bir düzenlemeyi istememektedir. Bu itirazın asıl altında yatan asıl sebep siber saldırıların devletlere sağladığı güç avantajını kullanmaya devam etme isteğidir. Örneğin; Uluslararası Anarşik Sistem üzerinde devletlerarasında meydana gelebilecek herhangi bir saldırıda başvurulacak temel kurum Birleşmiş Milletlerdir. BM Sözleşmesi'nde 51. maddede; klasik/fiili anlamda bir çatışmadan bahsedildiği görülmektedir. Bu ifadede herhangi bir şekilde siber saldırı ifadesi yer almamaktadır.[226] Ama yine de uluslararası alanda gerçekleşen savaşları önlemeye yönelik siber güvenlikle ilgili ufakta olsa kıpırdanmalar gözükmektedir.

[225]Clarke ve Knake, a.g.e. ss.60-80.
[226]Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, Birleşmiş Milletler Sözleşmeleri, http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/bm_yeni.html, ET.29.01.2020.

Siber güvenlik kapsamında yapılan uluslararası seviyede ilk çalışma NATO Siber savunma mükemmeliyet merkezi ve uluslararası bağımsız uzmanlar grubu tarafından hazırlanan "siber savaşta uygulanacak hukuk hakkında talinn el kitabı"dır. Cambridge Üniversitesi tarafından 2013 yılının Mart ayında yayınlanan bu el kitabı, uzman grubu görüşlerinden oluşmaktadır. " Talinn El Kitabı" NATO destekçi ülkelerinin görüşlerini ya da resmi bir NATO görüşünü temsil etmemektedir.[227]

Bir diğer çalışma ise Avrupa Birliği özelinde gerçekleşmektedir. Avrupa Konseyi bünyesinde siber suçlarla ilgili hazırlanan ilk resmi belge olma özelliği taşıyan Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi, 23.11.2001 tarihinde Macaristan'da imzalanarak 01.07.2004 tarihinde yürürlüğe girmiştir. Türkiye'de ise Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi 10.11.2010 tarihinde imzalanmasına rağmen, 02.05.2014 tarihli ve 28988 sayılı resmi gazetede yayınlanan "6533 sayılı uygun bulma yasası" ile yürürlüğe girmiştir.[228] Bu bağlamda siber uzaya yönelik küresel olarak hukuksal düzenlemeler artmaktadır. Bu durumu aşağıdaki tabloda daha net olarak görebiliriz.



Şekil 6 Siber Uzayla İlgili Görüşülecek Küresel Yasalar [229]

[227]Milli Güvenlik Kurulu Genel Sekreterliği, "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı", Uluslararası Siber Güvenlik Hukuku, https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku ET.29.01.2020.

[228]Bakanlar Kurulu, "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun BulunduğunaDairKanun",ResmiGazete,22.04.2014,http://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm ET.29.01.2020.

[229]Reuters, "Why We Urgently Need A Digital Geneva Convention", Weforum, 29.11.2017, https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention ET.30.01.2020.

- İç hukukta siber savaşın kavramlaştırılması sürecini incelediğimizdeyse şu noktalara değinmemiz gerekmektedir. Günümüzde bilginin geliştirilmesi, aktarılması ve ele geçirilmesinde bir araç olarak kullanılan siber silahlar ülkeler arasında gerçekleştirilen saldırı ve savunmalar, yasa dışı kanunsuz yöntemlerde kullanılmaktadır. Siber uzay ve bilgi teknolojilerine olan bağımlılığın her geçen gün artması istihbarat, suç, terör ve savaş gibi geleneksel kavramların da dönüşmesine yol açmıştır. Bu yüzden de devletler en azından kendi içlerinde bu suçları engellemek için yasalar, yönergeler ve yönetmelikler vasıtasıyla iç hukuklarını düzenlemektedir.[230]

Türk hukukunda uluslararası adlaşmaların iç hukuka nasıl aktarıldığına baktığımızda; milletlerarası sözleşmelerin iç hukuktaki yerini Monist görüş çerçevesinde ortaya koymalıyız.

Monist görüş taraftarlarına göre, dünyada var olan hukuk düzeni tek bir düzendir. Milletlerarası hukuk ve iç hukuk düzenleri bu bütünün parçalarıdır. Gerek milletlerarası hukukun gerekse iç hukukun nihai sujeleri aynıdır. Bu da fertlerdir. Aynı sahaya ve aynı şahıslara uygulanan iki hukuk düzeni arasında farktan söz edilemez. Bu iki hukuk düzeni ya "tabilik" ya da "eşitlik" ilişkisi içindedir. Bu ilişki içerisinde milletlerarası hukuk iç hukuktan üstündür. Bu durumda niteliği ne olursa olsun (anayasa, yasa vs.) bir iç hukuk kuralı ile bir milletlerarası hukuk kuralının çatışması halinde, milletlerarası hukuk kuralı kendisiyle çatışan iç hukuk kuralını ipso facto tadil eder veya ortadan kaldırır. [231]

Genel anlamda normlar hiyerarşisi hukukun yazılı kaynakları arasında bulunan astlık üstlük ilişkileridir. Normlar hiyerarşisi, hiyerarşik sıradaki hukuk kurallarından altta bulunan kuralın kendi üstündeki kurala aykırı olmamasıdır. Bu yüzden devletler "siber uzayın kullanılması sebebiyle temel hak ve özgürlüklere ilişkin" ortaya çıkabilecek tehditlere karşı oluşturulacak kuralları kabul etmek ve uygulamak zorundadır. Bu çerçevede; siber uzaya yönelik belirlenecek uluslararası kurallar normlar hiyerarşi olgusu çerçevesinde tüm devletler tarafından uygulanmak zorunda olduğu gibi Türkiye tarafından da uygulacaktır.

---

[230]Atalay Keleştemur, a.g.e , ss.417

[231]Hasan Tunç, "Milletlerarası Sözleşmelerin Türk İç Hukukuna Etkisi ve Avrupa İnsan Hakları Mahkemesinin Türkiye İle İlgili Örnek Karar İncelemesi", Anayasa Yargı Sempozyumu, 2000, ss.174-193.

Türk hukukunda siber adlaşmaların hukuki değerini normlar hiyerarşisi çerçevesinde açıklarsak; normlar hiyerarşisi, hukuk normlarının derece ve kuvvetini belirlemekte ve bir hukuk düzeninde var olan normların çokluğu anlamına gelmektedir. Hukuk düzeni bir piramide benzetilecek olursa bu piramit anayasa, yasa, tüzük, yönetmelik ve adsız düzenleyici işlemlerden oluşan birden çok normun varlığını ifade etmektedir. Anayasa'nın 90.maddesine 2004 yılında "temel hak ve özgürlüklere ilişkin milletlerarası antlaşmalarla yasaların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası anlaşma hükümleri esas alınır" tümcesinin eklenmesi, Milletlerarası Sözleşmelerin Türk Hukukundaki hiyerarşik yerini doğrudan doğruya düzenlemiştir. [232]

3.1.4. Siber Uzayın Terörist Kullanımı ve Siber Savaşlar

Geleneksel terörizm, hükümet politikalarını manipüle etmeyi, küresel düzeyde insanları olumsuz etkilemeyi ve altyapılara yönelik fiziksel zarar vermeyi hedefler. Günümüzde yaşanan siber süreçteyse teknolojideki ilerlemelerinde etkisiyle yazılım ve donanım kullanımı kolaylaşarak yaygınlaşmıştır. Bu bağlamda; terörizm grupları, siber araçlara ve yeteneklere adapte olmaya ve bunlardan yararlanmaya başlamış buda bilgisayarlar ve internet de saldırıları arttırmıştır. Böylece toplumun karşı karşıya olduğu terör tehdidinin niteliği son 20 yılda önemli ölçüde değişerek siber alana kaymıştır. Zaten bilgi ve iletişim teknolojilerinin terörizm eylemlerini teşvik etmek, desteklemek, kolaylaştırmak için kullanılması siber terörizmin çoktan ortaya çıktığı ve siber terör çağında "yaşadığımız" anlamına gelmektedir.[233]

Siber terörizm terimi, solucanlar, virüsler, kimlik avı etkinlikleri ve çeşitli diğer kötü amaçlı yazılımlar ve programlama komut dosyaları gibi çeşitli araçlar kullanılarak bilgisayar ağlarının kasıtlı olarak bozulması, ciddi bedensel zarar verilmesi, bilgi çalmak veya saklamak yoluyla bir avantaj elde etme veya ölümle sonuçlanan tehdit ve şiddet eylemlerini içerir. Aynı zamanda; siber terörizm eylemleri genellikle yıldırma, korku ve tehdit yoluyla siyasi veya ideolojik avantajlar elde etmeyi amaçlamaktadır.

---

[232]Rona Aybay, "Uluslararası Antlaşmaların Türk Hukukundaki Yeri", TBB Dergisi, Cilt.70, Sıra 1, Yıl 2007, ss.187-213.

[233]Serge Krasavin, What is Cyber-terrorism?, Computer Crime Research Center, 2001-2002, http://www.crime-research.org/library/Cyber-terrorism.htm, ET.09.09.2020.

Dorothy Denning'a göre siber terörizm, terörizmin ve siber uzayın birleşerek politik veya sosyal hedeflere ulaşmak için bir hükümeti veya halkını sindirmek veya zorlamak için yapıldığında bilgisayarlara, ağlara ve burada depolanan bilgilere yönelik yasa dışı saldırılar ve saldırı tehditleri anlamına gelmektedir.[234] Ayrıca D. Denning'in Activism, Hactivism and Cyberterrorism adlı çalışmasında tanımdaki belirsizliğin eylemde belirsizlik getirdiğinden bahsetmektedir.[235] Bunu bir başka şekilde ifade edersek bir e-posta bombası kimileri tarafından hacktivizm, kimileri tarafından siber-terörizm olarak kabul edilebilir. Kısaca özetlemek gerekirse siber terörizm terimi, internetin terörist amaçlarla kullanılmasıdır.

Siber terörizm açısından varsayımsal senaryolar oluşturulduğunda Havacılık, Nükleer enerji santralleri ve Nükleer Silah Sistemleri en tehlikeli olanlar olarak ortaya çıkmaktadır. Eğer siber saldırılar vasıtasıyla teröristlerin eline kitle imha silahlarına ulaşma fırsatı geçerse tüm dünya bundan ciddi bir şekilde etkilenebilir, şehirler yok olabilir ve milyonlarca insan ölebilir. Dolayısıyla, günümüz terörizmi büyük ölçüde geleneksel yöntemler içerse de geleceğin nükleer, siber ya da biyolojik terörizmi çok daha büyük tehlike yaratacaktır. Bu yüzden devletler tarafından ortak bir irade ile radikal grupların gözlem altında tutulması ve kitle imha silahlarının kontrolü ele geçirmelerinin engellenmesine yönelik siber güvenlik yönünde önlemler alınmalıdır. Örneğin; 11 Eylül saldırısı askeri olmayan araçlarla terör gruplarının devletlere karşı çok ciddi zarar verebileceğini göstermesinin yanında böyle ufak bir olayın 1. ve 2. Dünya Savaşlarında da olduğu gibi nasıl küresel bir çatışmayı doğurabileceğini göstermiştir. Çünkü bu olay sonrasında Afganistan, Irak ve Suriye gibi birçok alanda ABD tarafından önleyici savaş doktrini çerçevesinde savaş ilan edilmiştir. Günümüzde de siber, nükleer ve biyolojik tehditlerin ne gibi sonuçları doğurabileceğini kimse tahmin edemez.

Büyük güçler arasında artan gerilim beraberinde küresel sorunları (1914 ve 1939 daki gibi) getirerek dünyayı küresel bir savaşın içine çekmiştir. Nükleer

---

[234]Dorothy E. Denning, "Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services", Georgetown University, USA, 23.05.2000https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm, ET.09.09.2020.

[235]Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, Networks and Netwars: The Future of Terror, Crime, and Militancy", ss.239-288
https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf
ET.09.09.2020.

tesislere gerçekleştirilecek siber saldırılar yoluyla radyoaktif patlamalar gerçekleşebilir. Bu durum ise Çernobil yaşanma riskini içinde barındırır. Bunun en güzel örneği siber silah olarak kullanılan stuxnettir.2009-2010 yıllarında İran nükleer programlarını hedef alan binlerce santrifüjün imhası milyonlarca dolar kayba yol açmıştır. Böylece siber savaş ve siber silah kullanımı konuşulmaya başlanmış ve tehlike boyutu gözler önüne çıkmıştır.

Soğuk Savaş yıllarının hâkim olduğu yıllarda 1964 Küba Krizi nükleer imha tehdidini gözle görülür bir şekilde herkese göstermişti. Günümüz siber dünyasındaysa nükleer güce sahip devletlerin nükleer güç sistemlerini elektronik ortamda muhafaza etmesi, kontrol etmesi ve geliştirmesi rakip veya düşman bir aktör tarafından yapılabilecek bir saldırı ihtimalini kuvvetle ortada tutmaktadır. Çünkü siber saldırılar saldıranın kimliğini saklamasına fırsat vermektedir. Dolayısıyla siyasi, ahlaki, askeri, ekonomik veya kültürel hangi alanda olursa olsun bu konu küçümsenecek bir konu değildir. Nükleer Tesislerin sistemlerine verilebilecek bir zarar çok ciddi sonuçlar doğurabilir. Bu tehditte Soğuk Savaş'taki Küba Krizinde Soğuk Savaş'ın sıcak savaşa dönüşerek aleni olarak iki tarafın birbirine savaş açmasını engellemiştir. Aynı şekilde siber silahların etki gücü de siber savaşların resmi olarak ilan edilmesini engellemektedir. Bu yüzden; nasıl nükleer silahların nasıl denetleneceği yönündeki krizler üst otorite anlaşmalarını(SALT, START vb.) ortaya çıkardıysa siber silahlara yönelikte bu çerçevede bir üst otorite anlaşması oluşturulmalıdır. Böylece siber saldırı, çatışma ve savaşların bir silah olarak kullanılması kaygısı azalacaktır.

Aksi halde nükleer santral ve nükleer silahlara sahip olan devletlerin kendi iradeleri dışında uzaktan erişim ile başka aktörler tarafından kullanılıp imha edilebilme riski insanlık doğasında çok ciddi bir riski ortaya çıkaracaktır. Bunun yanında yapay zekâ, biyomühendislik, bulut bilişim ve siber saldırılar artık güç kavramının etkisini çok ileri boyutlara taşımıştır. Yani teknoloji hiçbir milletin tek başına çözemeyeceği çapta varoluşsal tehditler yaratarak her şeyi değiştirmiştir. Bu yüzden artık günümüzde iki önemli düşman vardır. Bunlardan biri nükleer savaş, bir diğeri ise içinde yapay zekâ ve bulut bilişim kavramlarını barındıran siber savaş oluşma ihtimalidir.

Bu bağlamda; siber tehditler herkes tarafından çok önem verilmesi gereken bir tehdit türüdür. Aynı zamanda buradaki en önemli tehditlerin başında çatışmaların sadece suç ve teröre indirgenmesi ve savaş boyutunun önemsenmemesidir. Bir başka ifadeyle siber terörizm ve siber suçla mücadele için yasalar var olsa da Kritik Altyapı Korumasının önemi hala tam olarak anlaşılamamıştır.

Sosyal ve politik hedeflerinden dolayı devlet desteğini arkalarına alan bireyler ve gruplar siber terörizm bahanesiyle herhangi bir devletin bel kemiği olan altyapılarına saldırılar gerçekleştirmektedir. Kısacası şuanda devletler siber saldırıları direk kendi ordu birimleri vasıtasıyla gerçekleştirmek yerine terör örgütleri veya milliyetçi hacker grupları tarafından suç işleme maksadıyla gerçekleştirilen saldırı süsü vermektedirler. Böylece yumuşak güç kullanımının aslında en güzel örneğini oluşturan siber savaşlar uluslararası terörizm faaliyetleri adı altında ülkelere kendilerini gizleme imkânı sunmaktadır. Bu yüzden siber suç ve terörizmle mücadele kavramı modern toplumların korunmasızlığı olduğundan devletlerden ayrı sadece özel sektörü içerecek şekilde tek boyutlu olarak kesinlikle düşünmemeliyiz.

Bunu küresel düzeyde en önemli güç olan ABD'nin siber terörizm üzerindeki algısını inceleyerek daha anlaşılır bir hale getirebiliriz. Örneğin; günümüz siber çağında siber terörizm ve siber saldırıların savunmasız ve karmaşık yapısıyla özellikle ABD'nin tüm sistemlerini ilgilendiren bir tehdit haline gelmiştir.[236] Bu durumda dijital güvenlik tehditlerinin her geçen gün artması tek başına etkili olmamaktadır. O ülke içindeki algı ve psikolojik etkenlerde önemli bir belirleyicidir. Bu durumu en güzel 2016'da Amerikalıların % 73ünün siber terörizmi tehdit olarak gördüğü halde 2018 itibariyle, %81'inin siber terörizmi tehdit olarak görmeye başlamasında görebiliriz.[237]Tüm bu özelliklerinden dolayı siber terörizmin önlenmesi, korunması ve azaltılması gerekmektedir.

3.1.5. Savaş Olgusunun Evrimi ve Siber Savaş'ın Tarihsel Gelişimi

Askeri düşünce, yaptırım ve uygulamaları artık ne Machiavelli'nin zamanındaki gibi konvansiyonel, ne de 2. Dünya Savaşı'nın kapanışı ve Soğuk Savaş

[236]Gary Hart, Dördüncü Güç 21. Yüzyılda Amerikan Büyük Stratejisi, Çev. Karabaşoğlu, İ. Avangard Kitap, İstanbul, 2016, ss.21.
[237]Kedi Cronin, American Security Project, 25.06.2019 https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/ ET:10.01.2020.

dönemi gibi nükleer tehditleri içeren bir çağdır. Günümüzde siber uzayın ortaya çıkışı ile birlikte tehditler evirilmiş böylece üçüncü bir aşamaya geçilmiştir. 1945 yılından günümüze kadar, pek çok seviyede durmadan devam eden bir çatışma dönemi yaşanmaktadır. Fakat günümüzde Soğuk Savaş dönemindeki gibi büyük güçler birbirlerine karşı açık bir şekilde savaş ilan etmekten kaçınmakta ve fırsat buldukça ittifaklar, anlaşmalar, ufak krizler, casusluk mücadelesi ve ambargo uygulama gibi faaliyetler yürütmektedir. Bu durum Clausewitz'in "savaş, siyasetin başka araçlarla yapılan bir devamıdır." cümlesindeki o günün savaş ve barış arasındaki bağlantısına bakışla bugünün savaş ve barış arasındaki bakışında mantıken bir fark bulunmamaktadır. Geçmişten günümüze değişen tek şey savaş ve çatışmalarda kullanılan araç ve boyuttur. Bu dönemleri kısaca tabloda gösterirsek;

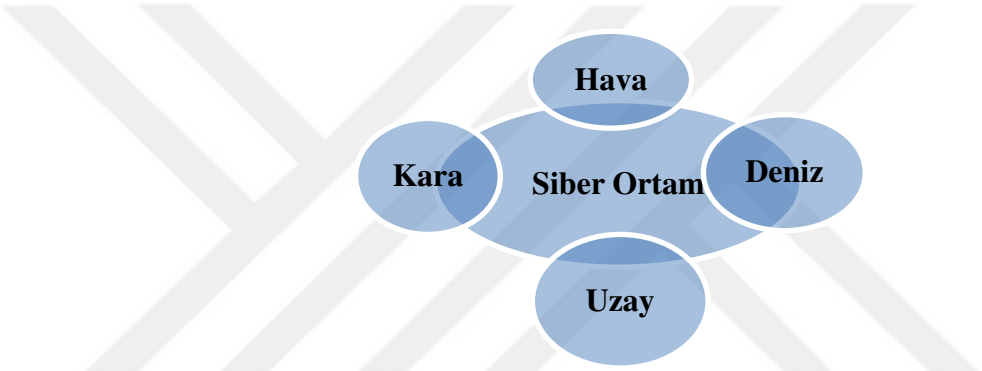
Tablo 6 Stratejik ve Operasyonel Açıdan Tarihten Günümüze Savaş Şekilleri

Stratejik ve Operasyonel Açıdan Tarihten Günümüze Savaş Şekilleri
18. yüzyıla Kadar Kara Savaşları
19. yüzyıl Deniz Savaşları
20. yüzyıl Başları Hava Savaşları
20. yüzyıl Ortaları Nükleer Savaş
20. yüzyıl Sonları Soğuk Savaş
21. yüzyıl Siber Savaş

1990'dan sonra Soğuk Savaş'ın bitmesi bir dönüşümü ortaya koymuştur. Bu dönüşüm siber uzay olarak adlandırdığımız internettir. İnternetin hayatımıza girmesiyle birlikte değişen dünya değerleri çerçevesinde bilgiyi, koruma ve muhafaza etme biçimi de değişiklik göstermiştir. Elektronik ortama entegre olan ülkeler, kurumlar ve örgütler bilgiyi korumak için de elektronik ortam muhafazasına ihtiyaç duymuşlardır. Böylece ülkeler, kurumlar ve örgütler gizli olan bilgileri korumak için yeni bir aşamaya geçmiştir. Bu aşama siber uzay olarak adlandırdığımız elektronik ortamdır. Bilgilerin siber uzay dediğimiz internet alanına girmesiyle birlikte güvenlik tehditleri, saldırılar, çatışmalar ve savaşlarda bu alana geçmiştir. Üzerinde durulması gereken nokta kritik ve gizli bilgilere ulaşmak maksadıyla ülkeler tarafından kullanılan siber saldırıların çoğunun "bir grup milliyetçi hacker" ve benzeri kimliğe sahip gruplar tarafından üstlenilmesi ve terör faaliyeti şeklinde gösterilmesidir. Böylece devletler siber çatışmaları bir savaş

şeklinde resmi olarak ilan etmeyerek çatışmanın boyutunu konvansiyonel ve nükleer savaştan sonra üçüncü aşama olan siber alana resmi olarak geçirmemektedir.

Siber çatışmaların gelişmesiyle birlikte savaş ekonomisi de büyümüştür. Böylece devletler topyekün güvenliklerini sağlayacak olan son teknolojik atılımı sağlamak maksadıyla kendi içlerinde bilim adamları tutmuş ve mühendisler görevlendirmiştir. Bilgisayar, internet ve yazılımların teknolojideki gelişimi ile birlikte yeni bir silah olarak kullanılması eğitimli ve profesyonel ekipler tarafından yürütülen siber ordulara olan ihtiyacı gündeme getirmiştir. Modern teknoloji böylece savaş kavramını da değiştirerek üçüncü aşama için dönüştürmüştür. Böylece üçüncü aşama olarak konumlandırdığımız siber uzay tüm boyutları kapsamaktadır.



Şekil 7 Siber Uzayın Tüm Alanları Kapsayan Evrenselliği

2. Dünya Savaşına kadar geçen dönem konvansiyonel ve geleneksel silahların kullanıldığı birinci aşamadır. 2. Dünya Savaşı'nın bitmesiyle birlikte nükleer savaş ve Soğuk Savaş kavramlarının ortaya çıkmasıyla birlikte ikinci aşama oluşmuştur. Bu iki dönemde gerçekleşen örnekler ve uyarılar, üçüncü aşama olan siber uzay(internet) aşamasındaki süreci yorumlamamıza fayda sağlamaktadır. Böylece siber savaş stratejilerinin oluşturulması yönünde savaş ve diplomasi tarihi, ulusların siber politikalarını bu geçmiş hakikatlere dayanarak oluşturmasına yol açmıştır. Son aşamada kullanılan siber harbin en önemli iki avantajı, yarattığı büyük etki ve sorumluluktan kaçma fırsatıdır. Devletler bu aşamada engelleme, karıştırma, yavaşlatma ve bilgi toplamaya yönelik faaliyetler gerçekleştirmekle birlikte oldukça düşük risk ile son derece etkili sonuçlar alabilmektedir.

Aynı zamanda siber savaşta saldırının ne zaman, nasıl ve kim tarafından gerçekleştirildiğinin tespit edilmesi çok zordur. Siber Savaş'ın net tanımı olmadığından siber savaş ve suç arasındaki çizgide belirsizdir. Bu yüzden siber çatışmaların ne olduğunu anlamamız için siber savaşın alt yapısını siber suç, terör ve savaş gibi siber kavramların temel özelliklerini ortaya koymamız bu tezde bir sonuca ulaşmamıza fayda sağlayacaktır.

Tablo 7 Siber Suç, Siber Terör ve Siber Savaşın Karşılaştırmalı Temel Özellikleri[238]

Eylemin	**Siber Suç**	**Siber Terör**	**Siber Savaş**
Niteliği	Doğrudan	Sembolik	Her İkisi
Şiddeti	Az yoğun	Yoğun	En yoğun
Motivasyonu	Kişisel kazanç	Siyasi	Siyasi, doğrudan, casusluk
Failleri	Bireyler, organize örgütler	Terörist örgütler	Kanıtlanmasa da kaynak devlet kabul edilir.
Hedefleri	Kazanç sağlamak	Kritik tesisler, hükümet temsilcilikleri, güvenlik birimleri	Askeri yapılar, hükümet birimleri, kritik tesisler, ekonomik ve endüstriyel altyapılar
Kaynağı	Ülke içinden yâda dışından	Ülke içinden yâda dışından	Ülke dışından

Bu kavramların ortaya çıkması ülkelerin kendi iç işlerinde siber suçlara yönelik bilişim hukukunu oluşturmalarına yol açmıştır. Aynı şekilde; Uluslararası İlişkiler alanında devletlerin işlediği insan hakları ihlalleri, savaş suçu ve soykırım gibi suçlarda genel kabul görmüş uluslararası kararlar bulunmaktadır. Fakat devletlerin birbirlerine karşı aleni olarak uygulayacakları siber saldırılarda suçlu olan devlete uygulanacak ceza hakkında tüm devletler tarafından kabul görmüş uluslararası bir karar yâda gerçekte böyle bir suçun işlenip işlenmediğini denetleyecek bir üst otorite bulunmamaktadır.

Kısaca özetlememiz gerekirse tarih boyunca bilimsel ve teknolojik gelişmeler sürekli olarak savaşlarda kullanılmıştır. "Savaş" kavramı tarih boyunca değişen bir olgudur. Doğal olarak savaşlarda kullanılan strateji, taktik ve silahlar da sürekli olarak değişim içindedir. Küreselleşmeyle birlikte bilgi teknolojilerinin ve internetin dünya çapında yayılması ile uluslararası arenadaki tüm aktörler 5. Boyutta yaşanan

[238]Altınok ve Çakmak, S.T.veS.Ü.S.D.ss.49.

bu yeni savaş yöntemini ve silahlarını kullanmaya başlamıştır. Bu kapsamda günümüz literatüründe kullanılan "Siber Savaş" savaşın günümüzde kullanıldığı alternatif halini göstermektedir. Alternatif olarak kullanılan siber savaşın temelleri teknolojik gelişmelerle birlikte Soğuk Savaş döneminde atılmıştır. 1990'larda oluşan bu yeni nesil savaş kavramı eskiye göre bazı değişiklikler gösterse de Clausewitz'in savaş üzerine ortaya koyduğu kavramsal çerçeve ile büyük ölçüde örtüşmektedir. Soğuk Savaş sonrasındaki gelişmelerle birlikte siber uzay modern yaşamı tanımlayan ve ticaret, finans, girişimcilik, yeni fikirlerin gelişmesi, sosyal ağların genişlemesi ve teknolojik ilerlemeler bakımından kritik bir rol oynayan en önemli unsur olmuştur. Bu bakımdan devletlerin günümüzde savaşları ve çatışmaları yönetebilmek ve çözüm sağlayabilmek adına ortaya koyacakları siyasi ve stratejik amaçlarının günümüzde şekillenen adı siber savaştır.

3.2. Siber Savaşın Uygulama Alanları

Siber uzayın sahip olduğu ana karelerin sınırlarını teller, sabit sürücüler ve ağların oluşturmasından dolayı siber kavramı fizikseldir. Fizikselliği içinde barındırmasından dolayı etkileri de fiziksel olabilmektedir. Bu doğrultuda siber savaş teriminin gerçek/sanal fark etmeksizin ortak kullanımındaki gerçek amaç, aktörler arasında dış politika etkileşimlerindeki çatışmalar oluşturur.Ayrıca siber savaş kavramı genellikle bir devletin siber teknolojileri kullanarak gerçekleştirdiği saldırgan yetenekleri ve siber alandaki yabancı ağları çalışmaz hale getiren eylemlerini içerir.[239] Bu yüzden siber savaş bir hedefe karşı diplomatik veya askeri açıdan avantaj elde etmek için kullanılan özünde rekabet barındıran bir taktikler zinciridir. Siber güvenlik ise devletin siber uzayda savunma (ve bazen de saldırgan) yetenekleridir. Siber saldırılar hizmet reddi saldırıları, web sitesi tahrifatı ve kötü amaçlı yazılım biçimini alır ve siber savaşın en güçlü biçimidir. Yani tüm bu mücadeleler uluslararası ilişkilerdeki rekabetin resmedilmiş halidir.

Siber savaşın uluslararası ilişkilerdeki rekabet üzerine teorik etkisine baktığımızdaysa, rekabet sırasında gerginlikler artar ve bir anlaşmazlık olduğunda çatışma olması muhtemeldir. Bu bağlamda dış politika ilişkilerinde, siber savaşın rekabet ilişkileri üzerindeki etkisi ne olabilir?

[239]Seymour M. Hersh, 'The Online Threat: Should We Be Worried about Cyber War?, New Yorker, Kasım 2010. https://www.newyorker.com/magazine/2010/11/01/the-online-threat ET.11.02.2020.

Bir rekabet sırasında, savaş dahil tüm seçenekler masada olmalıdır. Aynı zamanda bir rekabette savaşa tırmanma genellikle belirli bir yüksekliğin ardından gerçekleşir. Genellikle olaylar bir rekabet ilişkisinde meydana gelir. Rekabetin doğası nedeniyle, siber saldırının nereden geldiğinin bilinememesi sebebiyle siber taktikler sık sık bir dış politika seçeneği olarak kullanılmaktadır. Saldırgan tarafa kazanç sağlaması, düşük işletme maliyeti ve avantajları nedeniyle siber taktikler, rekabet ilişkisinde savaş öncesi bir " ilk atış " olma eğilimindedir. Sanal savaşın geleneksel savaşı tetikleme olasılığı düşüktür, ancak bu operasyonlar önde gelen kaynaklar olabilir.[240]Fakat, siber rekabet gerginliği arttırabilir ve işbirliğinin bozulmasına yol açabilir. Bu yüzden siber savaşın özelliklerini ortaya koymak ve kullanılan hakim unsurları belirlemek gerekir. Bu bağlamda; siber savaşın ne zaman başladığını ve bittiğini bilmek, onu tanımlamaktan daha zordur. İspat etme yöntemi de şuan için imkânsızdır. Örneğin; 2007'deki Estonya'ya düzenlenen Rus kaynaklı siber saldırıların Rusya kaynaklı olduğu herkes tarafından kabul edilmesine rağmen, Estonya'ya saldıran bilgisayarların %25'inin ABD'de konuşlu olması bu kanıtla namazlığın en güzel örneğidir.[241]

Aynı zamanda; siber savaşın çizgileri, izledikleri teknik ve yöntemleri de bulanıktır. Bu savaş yerel bir savaş değil internetin hâkim olduğu, bilgisayar ve elektronik tüm eşyaların bulunduğu, her ülkeyi kapsayan bir küresel etkisi bulunan, cepheleri belli olmayan, 7/24 saldırı ve savunmanın hâkim olduğu, çok cepheli bir savaş türüdür.

Şu ana kadar yaşanan siber savaş türleri üç tiptir. Bu üç tip savaş şekli; sosyopolitik, din ve büyük güçler tarafından nüfuz yayma veya gücünü karşı tarafa kabullendirme şeklindedir.

- **Sosyopolitik Siber Savaşlar:** Küreselleşme veya savaş karşıtı hareketlere mensup militanların internet üzerinden çok hızlı bir biçimde örgütlenerek küresel kurum veya kuruluşların sitelerini ele geçirmeleri sosyopolitik amaçlı siber savaşa örnek verilebilir.

[240]Derek S .Reveron, Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World, Georgetown University Press / Washington, Dc, 2012.
[241]Sınger ve Frıedman, S.G.veS.S. ss.107.

- **Din Merkezli Siber Savaşlar:** Daha çok gerçek ortamlarda yapılan savaşın siber alana taşınması şeklinde ortaya çıkmaktadır. Kosova'daki dini etnisiteler, İsraillilerle Filistinliler, Pakistanlılarla Hindistanlılar, Çinlilerle Tayvanlılar arasındaki gerçekleşen çatışmaların siber ortamda da sürdürülmesi din merkezli siber savaşa örnek gösterilebilir.
- **Büyük Güçler Tarafından Nüfuz Yayma veya Gücünü Kabullendirme:** Özellikle Rusya'nın eski coğrafya ülkeleri üzerinde gerçekleştirdiği siber saldırı faaliyetleri bu alanda değerlendirilebilir. Estonya örneğinde de olduğu gibi bu tip savaşlarda düzenlenen siber saldırının ülkenin tüm alt yapısını hedef almasından dolayı durum "siber savaş" olarak tanımlanmıştır. Yâda Stuxnet ile ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak ve istediğini karşıya zorla uygulatması anlamında siber savaş olarak tanımlanabilir. ABD ve İsrail'in Ortadoğu'daki projelerinde rakip gördüğü ve özellikle Rusya tarafından örtülü bir şekilde desteklenen İran'ın nükleer faaliyetlerini durdurma hedefi doğrultusunda Stuxnet virüsünün yayılması gibi etmenler bu savaşın olduğunu göstermektedir.

Sonuç olarak; büyük güçler tarafından aktif bir savaş aracı olarak kullanılan siber silahların özellikleri ve etki boyutu Birinci ve 2. Dünya Savaşında kullanılan silahlardan farklıdır. Nispeten Soğuk Savaş dinamiklerine benzer nitelikte psikolojik yapı, karşılıklı gerilim, her an saldırı yaşama korkusunu içeren ama teknolojinin gelişmesiyle birlikte bunu konvansiyonel ve nükleer savaş araçları vasıtasıyla değil de siber silahlar yöntemiyle uygulayan bir çatışma türüdür.

3.2.1. Siber Silahların "Elektronik Harp" de Kullanılması

Günümüzde yaşanan modern savaşlar ve gelecekte gerçekleşebilecek savaşlar içerisinde bilgi yönetimi sürecini barındırır. Bu süreç elektronik savaşı, siber ortamda bilgisayar şebekelerinin kullanımını, psikolojik harekatı, askeri aldatmayı ve operasyonel güvenliği içermektedir. Düşmana karşı bilgi üstünlüğünü elinde tutmak isteyen komuta kademesi artık uzaktan savaş alanını komuta etmektedir.[242] Aynı zamanda, küresel medya ve bilgi teknolojileri alt yapısı sayesinde karşı tarafın karar

[242]Terrence Guay ve Robert Callum, "The Transformation And Future Prospects Of Europe's Defennce İndustry", İnternational Affairs, Cilt.78, Sıra.4, Yıl. 2002, ss.757-776.

döngüsü etkilenmektedir. Siber çatışma süreçlerinde de karşı tarafın elektromanyetik komuta kontrol sistemi felç edilebilmektedir. Örneğin, 1967 Arap-İsrail Savaşında İsrail kuvvetleri elektronik karıştırmayı başarılı bir şekilde kullanmıştır. Geçmişte gerçekleşen bu örnekten yola çıkarak gelecek siber uzay düzeninde yaşanacak "Elektronik Harp" de siber silahların kullanılması sürecini açıklamaya çalışacağız.

Tarihten bugüne yaşanan siyasi devrim, savunma sanayi devrimi, ekonomik devrim, bilim ve teknoloji devrimi gibi adlandırılan tüm devrimler dünya sisteminde kullanılan araçların değişim sürecini şekillendirmiştir. 20. yüzyılla birlikte gündeme gelen ve günümüzde önemini giderek arttıran elektronik harp kavramı modern silahlı kuvvetlerde çok önemli bir unsur olarak karşımızda durmaktadır. Etkin kullanılmaya başlandığı 2. Dünya Savaşı'ndan bugüne sürekli gelişmiştir. Eskiden düşmanı aldatmak, birlik ve tesislerin yerini belirlemek, haberleşme olanaklarını köreltmek ve düşmanı komuta, kontrol ve hedef tespit sistemlerini tahrip etmek için kullanılmaktaydı. Günümüzdeyse yukarıda saydığımız bu işlevlerinin yanında artık askeri alan dışında da kullanılmaktadır. Bunun en güzel örneğini enerjiden, ulaşıma, sağlıktan finans yapısına kadar her alanda kullanıldığında görmekteyiz. Bu doğrultuda günümüzde kullanım oranı ve alanı artan siber alanın tezimizde belirttiğimiz gelecekte gerçekleşebilecek bir "World Wide Web War'a" dönüş(üp)meyeceğini görebilmemiz için elektronik harp yönünden geçmiş büyük savaşları da incelememiz gerekmektedir.

İnsanlık tarihinin çok büyük bir bölümünde gerçekleşen küresel geniş kapsamlı "Birinci Dalga " savaşlar toprak elde etmek için yapılmıştır. 19. ve 20. yüzyıl ile birlikte gerçekleşen küresel savaşlar ise ekonomik kapasiteleri kontrol etme amacını taşıyan "ikinci dalga " savaşlardır. 21. yüzyıl ile birlikte teknolojik gelişmeler sonucunda internetin hayatın her alanına girmesiyle birlikte " üçüncü dalga" savaşlar olarak adlandırdığımız siber uzayı bilgi temelli alan olarak kullanan çatışmalar oluşturmuştur.[243] "ikinci dalga " savaşlar olarak belirtilen ve 20. yüzyılda gerçekleşen küresel savaşlarda kullanılan askeri araçları elektronik harp olgusunu içine alacak şekilde incelemek istersek genel olarak 4 bölüme ayırmamız gerekmektedir. Bunlar; tıpkı canlı bir varlık gibi doğum ve çocukluk(1. Dünya Savaşı), çocukluk ve ergenlik geçiş(2. Dünya Savaşı), yetişkinlik (Soğuk Savaş

[243]Alvin Toffler, Üçüncü Dalga Bir Fütürist Ekonomi Analizi Klasiği, Çev. Yeniçeri, S. Koridor Yayıncılık, İstanbul, 2018.

dönemi) ve olgunluk (günümüz siber uzay dünyası ve gelecek) şeklinde geliştiğini belirtebiliriz. "ikinci dalga " savaşlarda Elektronik Harbin kullanım alanlarıda şu şekildedir. [244]

- 1. Dünya Savaşı: telsiz haberleşmelerinin yerinin tespit edilmesi, yayınların önlenmesi, aldatılması şeklinde istihbarat faaliyetlerinde kullanılmıştır.
- 2. Dünya Savaşı: 1935'den sonra kullanılmaya başlanan radar ikaz cihazının kapsamlı olarak kullanılması ve uçak seyrüsefer sistemlerinin aldatılması şeklinde teknoloji elektronik ortamda savaşta bir araç olarak kullanılmıştır. Aynı zamanda bu dönemde "Channel Dash Olayı" olarak ta bilinen ve ilk elektronik karşı tedbir (EKT) uygulaması 1942 yılında üç Alman savaş gemisinin kurtarılması için kullanılmıştır. Aynı zamanda Normandiya Çıkartması'nda ilk kez hareket planlamasında elektronik harp kullanılmıştır.
- Soğuk Savaş Dönemi: Kore Savaşında Kuzey Kore tarafından kullanılan Rus2 radarlarını ABD'nin fark edememesi sebebiyle Kuzey Kore uçak savar aktif olarak kullanılmıştır. Yine aynı şekilde Vietnam Savaşı'nda radarları taklit eden vericilerin yaymış olduğu işaretlerden füze sistemlerini korumak için EA-6B karıştırma uçaklarını kullanılmıştır. Arap-İsrail savaşlarında İsrail tarafından bilgi toplama, bilgiyi yerine ulaştırma, anında değerlendirme, hedefe saldırı unsurları gibi elektronik harp yöntemleri ilk defa kullanılmıştır.

Elektronik Harpte Üçüncü Dalga Savaş olarak yaşanan günümüz siber uzay dünyasıysa şu şekildedir. 2. Dünya Savaşı ve Soğuk Savaş'ta günlük telgraflar, kabine tutanakları, haftalık mektuplar, yayınlanan bültenlere önem veriliyor ve erişilen bilgiler istihbarat olarak paylaşılıyordu. Günümüzde ise e-devlet oluşmasıyla birlikte artık her bilgi siber uzaya kaymıştır. Bu yüzden savaşın sürprizlerle ve gizemlerle dolu hali bu alana kaymıştır. Nasıl Churchill'in savaş anlayışı bir tür resimdir ve stratejiyi oluşturmak da bir tür sanattır. Günümüzde de internet, büyük resmi görebilmemizi sağlayan ve siber uzay vasıtasıyla bunu gerçekleştirmemize imkan tanıyan bir savaş sanatıdır. Günümüz büyük siber stratejisi kaygan bir kavramdır ve devleti savunmanın siyasi, diplomatik, ekonomik, enerji, ulaştırma, din, ordu vb. her alanını kapsar. Artık günümüzde siber silahların gücü sunduğu avantajlarla ölçülmektedir.

[244] Ahmet Naci Ünal, a.g.e , ss. 67-83

Üçüncü Dalgayla birlikte siber silah kavramlarının uluslararası politikadaki kullanım şekilleri artmıştır. Siber saldırıların politik bir araç olarak kullanımının artması, uluslararası ilişkilerin tehlikeli araçlarından biri haline gelmesine yol açmıştır. Bu yeni araç, zayıf bilgi sistemlerine sahip ulus ve ulus dışı aktörleri hem saldırı hem de savunmayı bir arada kullanmaları gereken bir yapıya sürüklemiştir. Böylece askeri olarak geleneksel bir savaş yürütmeden düşmanlarına karşı stratejik bir üstünlük sağlamışlardır. Ayrıca aktörler tarafından kullanılan bu strateji siber uzayın inter disiplin bir yapıda olması sebebiyle çok amaçlı ve konulu bir şekilde birçok sektörü ilgilendiren bir hale dönüşmesine yol açmıştır. Bu yüzden devlet ve devlet dışı aktörler tarafından siber güvenlik risklerine karşı bilinç artmıştır.

Siber dünyada gerçekleşen siber saldırıların bir diğer özelliğide istihbarat sağlama imkânı ile (savaş öncesi, sırası ve sonrası) aktörlere bilgi gücü sağlamasıdır. Özellikle; 19. yüzyılda istihbarat çalışmalarında teknoloji kullanılmaya başlanmış olup telgraf ve demiryolları istihbarat faaliyetlerinde kullanılmaya başlamıştır. 20. yüzyılda teknolojik gelişmeler ve ulaşım sisteminin gelişmesi istihbarat ağını kuvvetlendirmiş ve 21. yüzyılda internetle birlikte doruk noktasına ulaştırmıştır. 21. yüzyılın ilk yıllarında siber saldırılar genellikle servis dışı bırakma, spam, e-posta gönderme, web sitesinin içeriğini değiştirme/ yönlendirme şeklinde yapılmaktaydı. Günümüzde ise siber saldırı teknikleri ile siber casusluk/istihbarat gibi kavramların gelişmesi üçüncü dalgada gerçekleşen savaş yöntemlerini değiştirmiştir.[245]

3.2.2. Siber Silahların Diplomaside Kullanılması

Şu ana kadar yaşanan siber savaş türlerinin üç tip olduğunu biraz önce yukarıda belirtmiştik. Gerçekleşen tüm bu siber savaş türlerinde aktörler tarafından kullanılan siber silahlar rejimlerin kendisini değiştirmesinde bir araç olarak görülmüş ve siber güvenlik konularıyla bu süreçlerin doğrudan ilgili olduğu tespit edilmiştir.

Uluslararası politikada gerçekleşen savaşlarda kullanılan siber silahların dış politikada etki unsuru olarak uygulandığı vakalardan bazıları şunlardır; İnternette serbestçe ifadeyi sağlayarak isimsizlik yaratan "Tor" bir konuşmanın hem kaynak hem de son noktasını gizlemek için bir aracılar ağını kullanır. Bu siber silahın 2009

[245]Atalay Keleştemur, a.g.e , ss. 148-150.

yeşil devrim ve 2011 Arap Baharı'nda kullanıldığı iddia edilmektedir.[246]Böylece; Tor gibi yeni teknolojilerin gelişimi ve dağıtılması geleneksel diplomasinin ötesine geçerek yeni bir diplomatik silah şekline dönüşmüştür. Ayrıca; 2010 yılında ABD ve İsrail tarafından kullanıldığı iddia edilen "Stuxnet"'in İran endüstriyel yapısı üzerinde ciddi etkisi olmuştur. "Stuxnet", muhtemelen tarihteki, fiziksel etkisi doğrudan görülebilen ilk 'ciddi' siber saldırı olarak kayıtlara geçmiştir. 4 adet Windows© güvenlik açığı ve iki çalıntı güvenlik sertifikası ile İran'da bulunan Natanz Uranyum Zenginleştirme Tesisindeki 984 adet SIEMENS marka santrifüjü hedef alan ve işlemez hale getiren bu saldırının, 500 kilobayt büyüklüğünde bir istismar dosyası ile yapılmış olması ise durumun ciddiyetini göstermektedir.[247] 2011 yılında kullanılan "Dugu", stuxnet'in kardeşi olarak görülür. Genellikle siber istihbarat faaliyeti için kullanılan "Dugu" siyasi amaçla bilgi toplamaya yarayan zararlı yazılımdır. 2012 yılında kullanılan "Flame" ise kaspersky lab tarafından bulunan ve kendini sürekli güncelleyen Stuxnet ile bağlantılı bir silah olarak gösterilmektedir. Aynı zamanda, 2012 yılında kullanılan ve Ortadoğu ülkeleri üzerinde faaliyet gösteren "Gauss" isimli bir diğer yazılım ise siber saldırıların asla bitmeyeceğinin kanıtı olarak gösterilmektedir. Çünkü daha önce endüstriyel yapılara yönelik gerçekleştirilen siber saldırıların aksine bu saldırıda finansal bilgiler hedef alınmıştır.

Yukarıda da belirttiğimiz gibi siyasi amaç hedeflenerek birçok siber silah kullanılmıştır. Bu silahlardan en yaygın kullanılanları oltalama(phishing), kötücül yazılım(malware), bot net, hizmeti engelleme(DOS/DDOS) saldırıları ve sosyal mühendislik saldırılarıdır.[248] Ayrıca truva atı, virüs, bot net, ddos, solucan, reklam içerikli ve casusu yazılımlar da siyasi amaçlarla kullanılan kötücül yazılımlar şeklinde devam etmektedir.

Bu silahlara yönelik araştırma ve geliştirme açısından uluslararası savunma sanayi ittifakları da üzerinde durulması gereken kritik konuların başında gelmektedir. Ülkelerin ortak tedarik projesinden geri çekilmesi, politik ve milliyetçi yaklaşımlar, tedarik miktarlarındaki değişim ve ekonomik sıkıntılar uluslararası ittifakların

[246]Singer ve Friedman. A.g.e ss.151.
[247]Oğuz Bozoklu ve Celal Zaim Çil, "Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:1, 2017, ss. 6-26.
[248]Mehmet Eren, a.g.e , ss.60-80.

teknolojik silahlar geliştirmelerinde ciddi sorun yaratabilir. Bunların yanında gerçekleştirilen yazılımların ve iç sistemlerin güvenliği, uzaktan kontrol edilebilme ve tanınma yönünde risklerin varlığı, gizli bilgilerin düşmanlara sızdırılması gibi konular ise bilişim sektöründe ve uluslararası savunma sanayi işbirliklerinde zorunlu olan teknolojik ürünlerin üretilmesinde ve geliştirilmesinde millileştirme gerçekleştirilerek en uygun ve hızlı iç yolun izlenmesi gerekmektedir. [249]Bu sebeple ülkemizde Türkiye Siber Güvenlik Kümelenmesi kurulmuştur.

Sonuç olarak, yüksek teknolojiyle birlikte bilgi devrimi ve internet, savaşların kaba kuvvete dayanan vahşi yüzünü maskelemiş, savaşa uzaktan icra edilen temiz bir bilgisayar oyunu izlenimi kazandırılmıştır. Aynı zamanda teknoloji ne kadar gelişir ve değişirse değişsin, savaşta disiplin, azim ve insan kaynağına olan ihtiyaç devam etmektedir. Belirgin bir cephe hattının olmadığı doğrusal olmayan muharebe sahası "siber uzay" olarak adlandırdığımız internet, bilgisayar, cep telefonu vb. tüm teknolojik araçlar üzerinde kullanılmaktadır. Savaş araçları sayılar ve boyut yerine operasyonel esneklik, yetenek ve tecrübeye dayandığından küçük ve güçsüz bir devlet, güçlü ve büyük devlete karşı ciddi zararlar verebilmektedir. Bu doğrultuda teknolojik gelişmelerin savaşları dönüştürdüğünü kabul ederek gelecekteki savaşlara hazır olmamız gerekmektedir. Çünkü biyoteknoloji ve bilgi teknolojileri insanlığın daha önce karşılaşmadığı kolaylıkların yanında ciddi derecede zorluklarda çıkarmıştır. İnsanlar, bulgular, sayılar, denklemler, görüntüler, bilgiler artık 21. yüzyılın savaş hedefleridir. 20. yüzyılın son döneminde yaşanan faşist, komünist ve kapitalist savaşlar böylece sona ermiştir. Artık şiddet ve baskı fikirlerin ve malların küresel ticarete dönüşmesi, stratejik bilgilerin önemli hale gelmesi, arge çalışmalarının gizliliği gibi konuların elektronik ortama taşınmasıyla birlikte siber güvenlik hayati bir konuma yükselmiştir.[250] Siber güvenliğin bu kadar önemli hale gelmeside siber ordular arasında casusluk faaliyetlerini arttırmıştır. Siber casusluk, 21. yüzyılla birlikte gelişmiş ve genellikle devlet destekli yürütülmektedir. Bilgisayar tabanlı kullanılan siber casusluğun en büyük avantajıda kesin ve doğru bilgiye bilginin kaynağından en düşük maliyetle ulaşma imkânını sağlamasıdır. Uzmanlar dünyanın en büyük ekonomisi olmaya çalışan Çin'in büyümesini korumak için daha

[249]Haldun Yalçınkaya, Savaş Farklı Disiplinlerde Yeni Yaklaşımlar, Siyasal Kitapevi, Ankara, 2010.
[250]Yuval Noah Harari, "21. yüzyıl İçin 21 Ders", Çev. Siral, S. Kolektif Kitap Yayınları, İstanbul, 2018.

fazla siber casusluğa yöneldiğini belirtmektedir. Siber casusluk siyasi sırlara eriştiği için hükümetlerin birbirlerini hırsızlıkta suçladığı bir gerilim ortamı yaratmaktadır. Yani, siber casusluk hem stratejik kazanan hem de kaybeden yaratır. [251]

3.2.3. Siber Savaşın Kritik Altyapılar ve Sistemler Üzerinde Kullanılması

Bir zamanlar internet sadece birinin kafasındaki bir fikirdi. Fakat internetle birlikte her şey ve herkes bağlantılı hale gelmiş, sınırsız veri ve bilgi akışı gerçekleşmiştir. Böylece iletişim, sağlık hizmetleri, ulaşım otomasyonu, askeri silah sistemleri, robot sistemleri ve ticarette eşi benzeri görülmemiş ilerlemeler yaşanmıştır. Fakat yeni sistemde acımasız gerçek şudur: organizasyonunuz ne kadar en yeni siber güvenlik donanımı, yazılımı, eğitimi, bütçesi ve personeli olursa olsun ya da ana sistemini diğerlerinden ne kadar ayrı tutmaya çalışırsa çalışsın sonuç nafiledir. Eğer sistemler dijitalse veya bir şekilde internete bağlanmışsa asla tam anlamıyla güveli hale getirilemez. Bugün dijital bağlantılı sistemler ABD ekonomisinin hemen her sektörüne nüfuz etmiştir. Örneğin; ABD'de 16 alt yapı sektöründen 12'sinde operasyonlar kısmen ya da tamamen dijital kontrol ve güvenlik sistemlerine dayalı olarak yürütülmektedir.[252] Dolayısıyla dijital teknolojiler kritik alanlara yönelik gerçekleştirilebilecek harika yeni beceri ve etkinlikler kazandırdı ama aynı zamanda siber saldırı riskine son derece açık riskler yarattılar. Bu sebeple siber güvenlik meselesini ihmal etmek ister birey, ister şirket, ister kurum, isterse devlet olsun herkesin zararınadır.

Bir ülkede kritiklik kayıp işlerden yasal para cezalarına ve iyileştirme maliyetlerinden veri ihlallerine kadar sonuçları çok geniş olan veri ihlallerinin yıkıcı mali kayıplara neden olabileceğini gösterir. Böylece bir aktörün yıllarca biriktirdiği itibarını bir anda kaybedebileceğini IBM araştırması gözler önüne sermiştir. Ponemon Institute tarafından yürütülen ve IBM Security tarafından desteklenen "2019 Veri İhlali Maliyeti Raporu", 16 coğrafya ve 17 sektörde 507 kuruluş tarafından rapor edilen veri ihlali maliyetlerinin ne kadar büyük olduğunu ve bu

[251]Sınger ve Frıedman, a.g.e. ss.31-133.
[252]Çiğdem Zeynep Aydın, "Dijital Dönüşüm Siber Güvenlik", Optimist Yayınları, İstanbul, 2020, ss.7-18.

oranın her geçen gün nasıl arttığını göstermiştir.[253] Aynı zamanda; Cisco da siber saldırıya hedef olanların ciddi gelir, müşteri, iş olanağı vb. kayıplara uğradığını gözler önüne sermiştir.[254] Ayrıca, devletlerin dünyanın farklı bölgelerine bilgisayar temelli ürün ihraç ederek casusluk faaliyetlerine girişmesiyle tüm veriler siber güvenliğin ticaret politikasının anahtar konusuna dönüşmüştür.

Her ne kadar ABD-Çin ve ABD-Rusya arasındaki ticari ihtilaflar basının ve gündemin daha çok ilgisini çekiyor olsa da, siber güvenlik bağlantılı ticari, siyasi, askeri, sosyal ve kültürel çatışmalar gerçek bir küresel olgudur. Yakın zamanda yapay zekâ becerileri çoğaldıkça kritik noktalara yönelik daha ileri otomatikleşmiş ve hassaslaşmış sosyal mühendislik saldırıları görmeye başlayacağız. Böylece yapay zekâ güdümlü siber saldırıların artması, ağlara sızma ve kişisel veri hırsızlığında patlamaya yol açarak akıllı bilgisayar virüslerinin salgın bir virüs gibi veya bir silahlanma yarışı gibi yayılmasına neden olacaktır. Aynı zamanda süper akıllı yapay zekâ sistemlerinde oluşabilecek tek bir başarısızlık tüm insanlığa küresel ölçekte zarar verebilme potansiyeli taşıyan bir risk doğurabilir. Bu yüzden yapay zekâ siber güvenliğin geleceğidir.

Ayrıca geleneksel ordulara kıyasla askerlerin silah taşımaması, üniforma giymemesi, yaralanma veya ölme ihtimali bulunmaması gibi sebeplerden dolayı sanal ordulara asker bulmak ve siber savaş çıkarmak çok kolaylaşmıştır. Aynı zamanda, siber teknolojinin bilgi paylaşımını ve haberleşmeyi kolaylaştırması, kaynaklarının belli olmaması, sınır tanımaması, düşük maliyetli olması, saldırı yapanların genelde tespit edilememesi, küresel ölçekte uygulanabilir olması ve ülke içi ya da dışından yapılabilmesi gibi nedenlerden dolayı klasik savaş unsurlarına göre çok kolaydır. Bunun yanında siber güç kapasitesi ile artık savaş cephede yaşanmamaktadır. Siber uzay olarak adlandırdığımız 5. Boyutta yaşanan 7/24 saldırı ve savunma içeren mücadelenin cephesi yoktur. Bu da siber çatışmaların gerçekleşmesini kolaylaştırmıştır. Bu kadar kolay gerçekleşen siber çatışmalar ise "Siber Güvenlik" konusunda çaba verilmesini önemli kılmıştır. Bu çabalardan en önemli olanı elektronik ortamda milli sınırları ve kritik alt yapıları korumaktır.

[253]IBM ve Ponemon Enstitüsü, 2019 Cost of Data Breach", Study by Ponemon, https://www.ibm.com/security/data-breach ET.30.03.2020

[254] Cisco, Cisco 2018 Annual Cybersecurity Report, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf ET.30.03.2020

Çünkü kritik altyapıların günümüzde neredeyse tamamı bilgisayar sistemleri tarafından yönetilmektedir. Bu sebeple, siber savaş alanı olarak kullanılan bu kritik alt yapılar aynı zamanda geleneksel savaş dönemlerinde de kritik rol oynayan alanlardır. Kısaca bu alanlardan bazıları şunlardır;

Tablo 8 Kritik Alt Yapılar

Enerji	Su	Sağlık
Bilgi ve Telekominikasyon	Bankacılık ve Finans	Hükümet
Posta ve nakliye	Lojistik	Tarım ve gıda
Savunma sanayii	Acil hizmetler	Kimyasal materyaller
Kamu düzeni ve güvenlik	Ulaşım	Gaz
Sivil havacılık	Elektrik	Nükleer santraller ve fabri

Yukarıda belirtilen tüm bu kritik altyapılara yönelik önlemler alınmalı ve savunma yöntemleri geliştirilmelidir.

Bunun en önemli sebebi internet ağlarının mesafeleri yakınlaştırarak bilginin dolaşımını kolaylaştırmış olmasıdır. Böylece askeri ve sivil güçler için tüm bu kritik alt yapılar ciddi tehlike ve tehdit unsuru haline gelerek internet ağları, toplumlarda ve devletlerde korku paranoyası oluşturmuştur. Meydana gelen gelişmelerle birlikte finans, sağlık, eğitim, nüfus, ticaret, ulaşım, haberleşme, enerji ve basın gibi alanlarda birçok hizmet internet ortamına taşınmış, bu da siber ortamın güvenliğini gündemin önemli konularından biri haline getirmiştir. Bu yüzden, yeni stratejik önlemler almak artık bir zorunluluk haline gelmiştir.

Ayrıca ulusal ve uluslararası düzenlemelerdeki eksiklikler, tehditlere ilişkin farkındalığın yetersizliği kullanılan uygulamaların tasarım aşamalarında güvenlik boyutunun düşünülmemiş oluşu, tehditlerin etki alanını genişletmiştir. Etki alanı genişleyen bu siber tehditlerin belirlenmesinde anarşik yapının yanında aktörler arasındaki "rekabet edebilme gücü", "bilgiyi koruma" ve "karşılaştırmalı üstünlükler" gibi perspektifler kullanılmaktadır.

Siber uzay sisteminde hiçbir ülkenin %100 güvenli olmaması, siber güvenlik stratejilerinin oluşturulmasında güvenli olma, farkında olma ve dirençli olmaya yönelik üç temel unsura odaklanılması gerektiğini ortaya çıkarmaktadır. Bu odaklanma siber riski bitirmemekle birlikte sadece siber tehditlerin etkisini

azaltmaktadır. Böyle anarşik bir ortamda internet sisteminin kullanıldığı her yerde risk tehdidi mevcuttur. Bu yüzden devletler güvenliklerini sağlayabilmek için ulusal bilgi güvenliği stratejisi oluşturarak kritik altyapıların korunması ve buna ilişkin kamu-özel işbirliği modeli geliştirilmelidir. Bu stratejiyi uygulama yönünde tarafların kimler olduğu sorusuna verilebilecek en güzel cevap ise internete bağımlı olan birey, kurum ve devlettir. Aynı zamanda siber tehditler sahip olduğu ekonomik, politik ve askeri motivasyonlar sayesinde gelecekteki konumunu arttırarak devam edecek gibi durmaktadır.

3.3. Siber Savaş Stratejileri

Siber stratejilerin belirlenmesinde davranışsal beklentiler ve rekabet ilişkileri önemli bir etkendir. Örneğin; hangi rakiplerin siber yeteneklerinin var olduğunu bilmek ve bu ölçüde incelemek savaş taktiklerini, diplomasiyi ve askeri ilişkileri içeren karar verme kriterlerini değiştirmektedir. Bu yüzden modern çağda, önce gerçek siber yeteneklerin durumu incelenmelidir. Bir diğer etken ise siber yeteneklerin rekabet ilişkileri üzerindeki etkisini ortaya koyabilmektir. Eğer bir devletin rakibi hedef almakla görevlendirilmiş bir siber birimi varsa, bu işlem aslında devletler arası ilişkileri etkilemektedir. Bundan dolayı politika yapıcılar öncelikle karşı devlete karşı uygulayacakları kararlardan önce siber güvenlik ihtiyacını veya siber savaş tehlikesini tartışabilmelidir. Böylece siber teknolojilerin çatışmalarda kullanılması bir analiz gerektiren çalışmanın sonrasında gerçekleşmiş olur.

Siber stratejilerin belirlenme sürecine torik olarak baktığımızdaysa şu noktalara dikkat etmemiz gerekir. Siber taktikler komutanı yok edebilir, ordudaki yapıların kontrolünü sağlayabilir, bir devletin medya aygıtını yok edebilir, finansal belleği silebilir, ekonomisini çökertebilir, sağlık endüstrisini işlemez hale getirebilir ya da iç güvenlik birimlerinin vatandaşları koruma yeteneğini ortadan kaldırabilir. Tüm bu etkilerin tamamen spekülatif olduğu düşünülebilir. Ancak, düşmandaki kaosun bir değeri olduğunu Estonya ve Gürcistan örneklerinden biliyoruz. Özellikle bu örneklerde de gördüğümüz üzere uluslararası ilişkilerde özellikle rakip üzerinde oluşturulan algı, başarıya giden süreci hızlandırmaktadır.

3.3.1. Siber Savaş'ın Doğası ve Stratejileri

Siber saldırılar bir ülke ekonomisini, elektrik, su, enerji, ulaştırma, iletişim ve hatta polis ve yangından korunma işlemlerini çökertebilir. Bunların hepsi aynı anda da gerçekleşebilir. Neyse ki Estonya siber savaşında bu gerçekleşmemiş olsa da Estonya parlamentosunun o dönemki başkanı Ene Ergma yaptığı açıklamada; "Nükleer bir patlamalara ve Mayıs ayında ülkemizde meydana gelen patlamaya baktığımda aynı şeyi görüyorum."[255] bakışı siber silahların etkisine yönelik algıyı ortaya çıkarmaktadır. Eğer bu saldırı birçok alanı içine alan kapsamlı bir saldırı olsaydı ülkenin bilgi altyapısının çoğu yok edilirdi. Bu korku da nükleer silahtaki yıkıma benzer şekilde kıyamet günü şeklinde bir siber terör saldırı korkusu yaratırdı.[256] Çünkü nükleer radyasyonda olduğu gibi, siber savaş modemi de bir durumu kan almadan yok edebilir. Kısaca siber silahlar geleneksel silahlarla yapılan fiziksel saldırılar gibi öldürücü bir etkiye sahiptir. Bu güce sahip olan dijital istilacılar, Estonya'da olduğu gibi, saldırılarını uzak konumlardan yönlendirerek kökenlerini kasten maskelemektedir. Çünkü siber saldırıda hiçbir bayrak veya tank ve faillerin kimliği yoktur. [257]

Bu doğrultuda siber savaşın doğasını belli yasalar çerçevesinde açıklayabilmemiz için bazı sorulara cevap bulmamız gerekmektedir. Teorik olarak egemenliği çevreleyen endişeler siber alanı etkiler mi? Siber saldırı BM Şartı'nın 2 (4) Maddesi ile tanımlanan "kuvvet kullanımını"? kapsar mı ? Uluslararası hukuk genel olarak ve uluslararası insani yardım yasası ("IHL") veya uluslararası insan hakları hukuku ("IHRL") siber saldırıları sınırlayabilir mi? "Adil" bir bilgi savaşını oluşturan nedir? Gibi sorular çerçevesinde siber uzayda adil bir bilgi savaşı oluşturulabilmesi için siber saldırıların tehdidinin tanımlanması şarttır. Aynı zamanda eğer Estonya Nisan 2007 saldırılarının arkasında Rusya'nın olduğunu kanıtlansaydı Estonya'nın yasal olarak cevap verip veremeyeceği önemli bir sorudur. Çünkü Estonya'da görüldüğü gibi, küçük ölçekli bir saldırı egzersizi bile "ciddi hasar verme veya bozma" potansiyeline sahiptir.

---

[255]Kevin Poulsen, "Cyberwar and Estonia's Panic Attack, Wired", 22 Ağustos 2007, http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html. ET.07.02.2020.

[256]Doomsday Fears of Terror Cyber-Attacks, BBC News, 11 Ekim 2001, http://news.bbc.co.uk/2/hi/science/nature/1593018.stm. ET.07.02.2020.

[257]Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", Berkeley Journal of International Law, Cilt.27, sayı 1, 2009. ss.192-251.

Siber saldırıların bu etkilerine karşı kendini savunma kriterlerinin belirlenmesi gerekir. Bu doğrultuda eğer saldırı gerçekse veya tehdit yakındaysa, bir siber saldırının kurban durumu, herhangi bir alternatif yol olmadan, makul savunmayı haklı çıkarmak için kendini savunmayı haklı kılabilir. Bunun içinde BM Şartı'nın Madde 2 (4) Uyarınca güvenliği sağlamak için gerekli ve orantılı önlemler belirtilmiştir. BM Şartı'nın bu bölümü uluslararası barış ve güvenliği sağlamaya çalışmaktadır. İstikrarsızlaşan güç kullanımları barışın 2 (4) 'ün kapsamına girmesi ve kuvvet tehdidini arttırır. Bu bağlamda BM Sözleşmesi gereğince baskı silahlı kuvveti kapsamazsa Madde 2 (4) 'ü ihlal etmez.

Siber saldırı klasik bir silahlı saldırıdan farklıdır. Bu yüzden Madde 2 (4), siber silahları da içine alacak şekilde yükseltilmesi gerekir. Çünkü hem silahlı kuvvetler kendi içlerinde artık siber ordu birimleri oluşturmakta hem de siber saldırılar geleneksel askeri güçlerin saldırısıyla aynı etkiye sahip olabilmektedir. Bu tip kuralların oluşturulabilmesi için günümüzdeki en güzel örnek ise Siber Suçlar Sözleşmesidir. Avrupa Konseyi'nin 1 Temmuz 2004'ten beri yürürlükte olan Siber Suçlar Sözleşmesi, devletle siber suç yasalarını uyumlu hale getirmek için başka bir araç sağlamıştır.[258]

Eğer yukarıda bahsettiğimiz gibi vekalet yükümlülüğü oluşturulur, bir üst otoriteyle birlikte uluslararası hukuk kuralları ortaya konur ve böylece geçerli bir kendini savunma uygulaması oluşturulursa saldırganlığın reddedilemez kanıtı ortaya çıkacaktır. Böylece her devlet üzerine düşen sorumluluğu yerine getirmek zorunda kalacaktır. Aynı zamanda bu zorunluluk aktörlerin her türlü misilleme gerçekleştirmesine de katkı sağlayacaktır. Bu durumu daha da açarsak her devlet önleyici veya öngörülen siber saldırılara ve yaklaşmakta olan tehlikelere karşı kendini savunma hakkına sahiptir. Peki bu hakka sahip olunduğu nasıl anlaşılabilir?

Uluslararası toplum Birleşmiş Milletler 'in (BM) kuruluşuna kadar tarih boyunca birçok savaş ve çatışma yaşamış olsa da uluslararası arenada kuvvet kullanımını yasaklayamamıştır. Her ne kadar BM tarafından uluslararası ilişkilerde güç kullanımı yasaklanmış olsa da çatışma ve savaşlar tamamen sonlanmamıştır. Ayrıca, uluslararası ilişkilerde kuvvet kullanımı yasaklansa da ortaya çıkacak

[258]Council of Europe, Convention on Cybercrime, European Treaty Series - No. 18, Budapest, 23.11.2001,https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, ET:20.01.2020.

savaş/ların ve çatışma/ların sınırlarını belirlemek de Silahlı Çatışma Hukukunda önemli bir görev üstlenmektedir.[259]

Tüm bu yasalar çerçevesinde mevcut literatürde, gerçek veya siber çatışma arasındaki ilişki hakkında farklı görüşler bulunmaktadır. Fakat gerçek şudur ki rekabet ve çatışma alanı haline gelen siber güvenliğin politika alanı, şimdi her zamankinden daha fazla siber çatışma tehdidini içermektedir. Bu tehditlerdeki artış bir yana şuana kadar yaşanan deneyimler siber teknolojilerin ölümcül olmayan silahlara benzediğini göstermektedir. Bu yüzden siber silahlara yönelik stratejik bakış ve savaş stratejimizde savunmanın rolünü belirleyebilmemiz için Sun Tzu'dan von Clausewitz'e kadar askeri kuramcıların teknolojik gelişmeler çerçevesindeki askeri strateji tanımlamasına değinmeliyiz.

Tüm bu kuramcılar çerçevesinde oluşturulan tanımlamalara bakarsak strateji, ne yapmak istediğimiz ve genel olarak bunu nasıl yapmayı planladığımızla ilgili entegre bir teoridir. Ulusal Güvenlik Stratejisi ve Ulusal Askeri Strateji içinde hedeflerin, araçların (geniş tanımlanmış), sınırların (belki de) ve muhtemelen dizilimin açıklanmasının yapılmasıyla birlikte kamuya açık entegre bir siber savaş stratejisinin var olması buna teorik açıdan yaklaşmayı zorunlu kılmaktadır. Ayrıca jeopolitik sınırların ötesinde gerçekleşen operasyonların ve kritik altyapıları içeren sivil hedeflerin varlığı konuya stratejik açıdan yaklaşmayı zorunlu kılmaktadır. Bu yüzden strateji de ki asıl amaç rakibin siber alanda kendisine saldırmasını beklemeden siber güvenlik önlemlerinin alınacağı ciddi savunma mekanizmalarının geliştirilmesini sağlamaktır.

Bir diğer yandan aktörler dış politika stratejilerini oluştururken düşmanlarına karşı gerçekleştirdikleri siber saldırılarda iz bırakması halinde olabilecek karşı etkileri düşündüğünden kendi içlerinde bir caydırıcılık stratejisine uğrayarak saldırılarının aleni olmasını engellerler.[260] Son olarak siber çatışmalarda ABD gibi büyük ülkeler Kuzey Kore gibi küçük devletlerden daha fazla risk altında ve çok daha savunmasız durumdadır. Bu durumu değiştirmek için büyük ülkeler ordu birimleri ve iç hukuk düzenlemeleri kurarak önlem almaya çalışsa da yeterli değildir.

[259]Mehmet Emin Erendor, "Silahlı Çatışma Hukuku İlkelerinin Değerlendirilmesi: Askeri Gereklilik, Gereksiz Acı ve Istırabın Önlenmesi ve Onur", Manas Sosyal Araştırmalar Dergisi, Cilt.8, No.2, Yıl. 2019, ss. 1991-2009.

[260]Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books ss.20-30.

Bu bağlamda siber saldırıya karşı kırılganlığın azaltılması gerekir. Çünkü başkalarının neler yapabileceğini bilmek, kullanmakta isteksiz olduğumuz bir caydırma durumu yaratabilir. Hayati sistemlerimizin siber savaşa karşı çok savunmasız olması da kriz istikrarsızlığını arttırmaktadır. Ayrıca ekonomik ve askeri sistemlerimizin savunmasız olması rakiplerin gerginlik döneminde bu alanlara yönelik siber saldırı gerçekleştirmelerini teşvik edecektir. Bu mevcut koşullar, stratejik dengesizliği azaltmak için hızla ülkelerin siber savaş yeteneklerini ortaya çıkarma çabasına yol açacaktır.

Bu doğrultuda her devlet için ülkesini bir siber saldırılardan korumak, bir siber savaş stratejisinin ilk hedefi olmalıdır. İkinci ulusal güvenlik stratejilerinin temel amacı ise ülkenin savunulması olmalıdır. Bu strateji de asıl önemli olan en iyi savunmanın saldırı olduğu ve sadece koruyarak savunmanın ne kadar zor olabileceğine dair algıdır. [261] Bu sebeple siber alana yönelik geniş kapsamlı hedefler (bankalar, enerji şirketleri, demiryolları ve havayolları vb.) belirlenmelidir. Siber uzayın çatışmanın gerçekleştiği bir "alan" olduğu algısı, ülkelerin bu alanların hepsinde güvenliklerini sağlama çabaları, siber operasyonlar için oluşturulan askeri kararlar hep bir stratejik üstünlüğe sahip olma çabasıdır. Bu çabada savunma için şarttır.

3.3.2. Asimetrik Bir Güç Unsuru Olarak Siber Savaş

Geleneksel suçların siber varyasyonlarının arka planını "Net bağlantılar" dan "karşılıklı bağımlılık" a geçiş oluşturmaktadır. Web 1.0 aşamasında, İnternet ticari organlar ve portallardı; bireyler çevrimiçi bilgi alıcısıydı. Web 2.0 aşamasında, çevrimiçi etkinliklere katılım ile birlikte internet insan yaşamının temel platformu haline geldi. Böylece gerçek hayattaki bire bir yaralanma, siber alanla birlikte bire çok yaralanmaya dönüştü. Dolayısıyla internetin evrimi yarattığı asimetrik bu güç sayesinde geleneksel suçların siber varyantlarının altında yatan en önemli sebep olmuştur. Aynı zamanda internetin geçirdiği bu evrim sonucunda internetin sanal doğası gittikçe göreli hale gelmiş ve çevrimiçi davranışlar tamamen sanal olmayı bırakarak toplumsal bir önem kazanmıştır. Bu yüzden internet kullanıcıları ister birey

[261]Jamil N. Jaffer, "The Best (Cyber) Defense Is a Good (Cyber) Offense", Opinion, Newsweek, 14Eylül2020, https://www.newsweek.com/best-cyber-defense-good-cyber-offense-opinion-1531606, ET.16.09.2020.

ister devlet olsun çevrimiçi söyledikleri ve yaptıklarıyla ilgili yasal sorumluluk almak zorundadır. [262]

Çevrimiçi söylenen veya yapılanlarla ilgili yasal sorumluluk alınması gerektiği halde günümüzde yaşanan bilgi çağında, geleneksel suçların siber varyantları konusunda uygulanacak ceza hukuku teorisi, mevzuat ve ceza adaletinde karmaşık bir yapı bulunmaktadır. Bu yüzden siber uzay, geleneksel suçların siber varyantlarını şekillendiren güçlü bir asimetrik güç haline gelmiştir. Bu kapsamda geleneksel suçlarla ilişkili siber uzay varyantlarının somut örneklerini kısaca incelediğimizde şu hususları belirtmemiz gerekir.

Yargı perspektifinden bakıldığında, gerçek alanda işlenen bir suçu mevcut yasalar çerçevesinde atamak kolayken siber alanda aynı suç işlendiğinde, atamak genellikle zordur. Fakat bu zorluğu hafifletmenin bir yolu vardır. Bu yol internetin özünde bir bilgi ortamı olması sebebiyle siber alanda sanal mülkiyet kavramını ortaya çıkarmış olmasıdır. Sanal Mülkiyetin doğası bilgisayar sahiplerinin bilgisayar sahipliğinden ziyade bilgisayar kullanıcılarının kullanım haklarını etkilemektedir. Bu kullanım haklarının kötüye kullanılması ve suç işlenmesinin en güzel örneği internetin karanlık yüzünü gösteren Botnetler ve Microsoft "Siyah Ekran" sayesinde yazılım tekniklerinin kötüye kullanılması sonucunda bir tür "kullanım hırsızlığının" gerçekleşmesidir. Yani siber uzay, içinde barındırdığı asimetrik güç sayesinde suç için yeni bir platform görevi üstlenmiştir. Bu yüzden botnet kullanımı ile ilgili getirilebilecek bir hukuki düzenleme geleneksel suçlardaki siber uzay değişikliklerinin neden olduğu sorunlara bir çözüm getirebilir. Fakat burada ciddi bir sorun vardır. Buda suçun sonuçlarındaki siber farklılıklardır.

Bu farklılığın arka planını sosyal bilimlerin en çok bilinen ve uluslararası ilişkilerde de en çok kullanılan strateji oyunlarında biri olan tutsak ikilemi ve güvenlik ikilemi çerçevesinde açıklamaya çalışalım.

Tutsak ikilemi oyunun amacı suçu ispatlanamayan ve herhangi bir kanıt bulunmayan mahkumları ikilemde bırakıp kendileri için doğru olan kararı vermemelerini sağlamaktır. Siber ortamda da durum benzerdir. İnternetin kullanılmasını sağlayan sayısız birbirine bağlı bilgi sistemlerini oluşturan ve aynı zamanda birbirlerinden habersiz çalışan her bir zincir halkasına yönelik

[262]Yu Zhigang, "Cyber Variants of Traditional Crimes and Criminal Law Responses", Social Sciences in China, Cilt.32, No.1, Yıl.2011, ss. 66-79.

gerçekleştirilebilecek saldırı tüm sistemi felç edebilir. Suçun sonuçlarındaki siber varyasyonlar da genellikle zararı ifade eder. Bu durumu örneklendirerek kısaca açıklarsak; siber alanda, A, sunucu tarafından B'ye saldırıldığında B sunucusu normal çalışmasını sağlayamayıp felç olur. Böylece B sunucusunun hizmetinin altındaki web sitelerinin hiçbiri ziyaret edilemez. Bu durum, A'nın saldırısının doğrudan sonucudur. Fakat değişen her örnekte sonuç farklı olabilir. Suçların sonuçlarındaki siber farklılıklar, konunun ne kadar zor, karmaşık ve etkisinin belirsiz olduğu gerçeğini göstermektedir. Buradan çıkaracağımız sonuç ise kişisel çıkarlarımızı değil de grup çıkarlarını düşündüğümüzde kendimiz için en iyi kararı vereceğimizdir.

Zor, karmaşık ve etkisi belirsiz olan internetin suç amacıyla kullanıldığını en güzel gösteren örnek, artarak devam eden hacker endüstrisidir. Hacker endüstrisi ile birlikte kendi çıkarları için bilgisayar programları yazmak, dağıtmak, satmak ve para aklamak gibi amaçlarla virüs ve saldırı programlarının alımı ve satımı yeni bir branş oluşturmuştur. Devletlerde bu boşluğu etkili bir şekilde kendi çıkarları doğrultusunda kullanmaktadır. Kısaca; geleneksel siber suçlar, geleneksel ceza teorilerinin, adaletinin ve mevzuatının etkinliğini ciddi şekilde etkilemiş ve aşındırmıştır. Bu sebeple; internet bağlantısına yönelik hukuki değerlendirmede, kavrama ortak bir suç olarak bağımsız bir statü verilirse failler ana suçlu olarak ele alınabilir. Aynı zamanda bu soruna yönelik bir diğer çözümde, ceza hukuku teorisinin güncellenmesi ve yeni siber suçları kapsayacak şekilde geleneksel yasalarının yorumlanması ve kullanılma kurallarına yönelik siber suçlara mücadeleye yönelik yeni mevzuatın getirilmesidir. Yani ortak suçluların muamelesine yönelik bir model oluşturulmalıdır. Bu modelle birlikte siber alanda suç işleyen aktörlerin cezai sorumluluğunu tespit etmenin etkili bir yolunu sunulacaktır.

Özellikle bu tezde kurumsalcı teoriyle birlikte vekalet yükümlülüğü ile sorumluluğun devletler tarafından kabul edilmesi gerektiği vurgulanmaktadır. Yani devletler kendi içlerindeki tüm alanların ve dışarıya karşı oluşabilecek tüm saldırıların özel veya kamu olsun sorumluluğunu alması gerekmektedir. Bu sorumlulukta üst otorite kurum ve kurallarla kontrol edilmelidir. Aslında bu bir ortak hukuk ajansı doktrinidir. Bu teori altında, siber uzayın ağ bütünlüğü içinde ağ yöneticisi yani asıl olan astın eylemlerinden sorumlu olmasıdır. Eğer bu konuda

anlaşılırsa internetin karanlık yüzü tarafından kötü amaçlar için kullanımı(botner, virüs, solucan, ddos vb.) sınırlandırılabilir. Bu sorun başka türlü çözülemez. Çünkü internet, bir zamanlar var olan herhangi bir çevrimiçi etik kodu yok etti. Bugün bilgisayar ve internet artık hayatın her yerinde olumsuz amaçları da içermektedir.

3.3.3. Siber Savaş Teknikleri

Ayrı bir imzası ve coğrafi özelliği olan bir füze fırlatmasının aksine siber taktik kullananlar, kökenlerini kolayca gizleyebilirler. Bu yüzden siber tehditleri incelemeye çalışırken, menşe noktasının belirlenmesi çok zordur. Bu kapsamda siber etki alanlarına yönelik tehditler birkaç şekilde sınıflandırılabilir. Bunlar; bireysel ve hükümet gibi aktörlere göre; hedefe göre, finans sektörü veya savunma departmanı gibi; veya virüs, solucan veya hizmet reddi gibi silahına göredir.[263] Aktör açısından, siber taktikleri hain amaçlarla kullanan kişiler bireysel bilgisayar korsanları, organize suç grupları, istihbarat servisleri ve hükümetlerdir. Aktörlerin çeşitliliğinin gösterdiği gibi, siber alana giriş engelleri düşüktür. Bir siber saldırıyı gerçekleştirebilmek için sadece iyi bir internet bağlantısı, iyi bir bilgisayar ve teknik saldırıları nasıl yapacağını bilmek yeterlidir. Ne yazık ki, üçü de ucuz, hızlı ve kolaydır. Bu durum da tehditleri ve siber müdahaleleri arttırmaktadır. Yani siber uzayda her birey kendi içinde bir süper güç olmuştur. Böylece, siber alanda, insan ve ulusal güvenlik ayrılmaz bir şekilde bağlantılı bir ortam yaratmıştır. Tüm bu durumlar siber alanın diğer alanlara eşdeğer bir savaş alanı olarak ele alınıp alınmayacağı konusunda anlaşmazlıklar yaratmaktadır.

Aynı zamanda, siber saldırıları gerçekleştiren gruplar, eylemlerinin planlama ve hazırlık aşamalarında büyük özen göstermekte ve her saldırı türü, yöntemi ve süresi bariz kalıplar içermemektedir. Bu durumda yerel kolluk kuvvetlerinin, suçluların gelecekteki eylemlerini tahmin etmesini zorlaştırmaktadır. Bu durum uluslararası sistemde de aynı şekilde bir bilinmezlik yaratmaktadır. Genel olarak bu durumu incelediğimizde siber saldırılarda suç ile sosyal kontrol arasında bir ilişki vardır. Bu ilişkideki odak noktası suçun rasyonalitesi ve sosyal kontrolün dolandırıcılık, suç önleme, kolluk kuvvetleri ve yaptırım sistemleri ile bağlantısını

[263]Derek S .Reveron, Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World, Georgetown University Press / Washington, Dc, 2012

görebilmektir. Bu tezde incelenen vaka çalışmalarında da görüleceği üzere uluslararası düzende siber suç ağına yönelik etkili bir şekilde kurallar, düzenlemeler ve yaptırımlar geliştirilememiş olması siber suçların sosyal dinamikleri harekete geçirmek için farklı tekniklerle aktif olarak kullanılmasına yol açmaktadır.[264]

Siber suçlular tarafından kullanılan ilk teknik, kârlı ödemeleri tahmin etmek için elde edilen sonuçları tersine mühendislik kapasitesi ile birlikte kullanarak finansal kazanç sağlamaktır. Bir diğer yöntem makineleri, sistemleri, bilgisayarları vb. bir çok yapıyı rasgele gözlemleyerek stratejik bilgileri ve verileri casusluk marifetiyle ele geçirmektir. Üçüncü teknik, yasa dışı yazılımları yasal olanların bilgisayar arayüzleri ve programlarında kullanmaktır. Tüm bu farklı teknik türlerinden de anlaşılacağı üzere siber ortamda alternatif çok fazladır. Bu yüzden siyasi, hukuki, ekonomik, askeri, sosyal ve kültürel tüm alanları kapsamlı bir şekilde içeren yönetişimsel bir kontrol organizasyonu oluşturulması şarttır.

3.4.Siber Savaş Kavramına Yönelik Tartışmalar

Günümüzde yaşananları siber savaş olarak adlandırabilmemiz için konuyu farklı başlıklar altında açıklamamız gerekmektedir. Çünkü yaşanan bir olaya savaş dediğimizde söz konusu gerçekleşen olayın ekonomik, coğrafi, tarihî, biyolojik, psikolojik, sosyolojik ve siyasi bütün yönleri kapsayan çok disiplinli bir kavram olarak değerlendirilmesi şarttır. Her disiplinin kendine göre bir savaş tanımı bulunmaktadır. Günlük kullanımda da sıkça rastlandığı üzere, hastalıklarla savaşmak, kötülüklerle savaşmak veya yoksullukla savaşmak gibi içerisinde savaş teriminin yer aldığı birçok ifade bulunmaktadır. Bu ifadeler incelendiğinde tümünün içeriğinde bir mücadele olduğu görülmektedir.

Clausewitz'e göre savaş[265], kendi irademizi karşı tarafa kabul ettirmek maksadıyla uygulanan, en az iki aktör arasında görülen, silahlı güçler tarafından yürütülen, zaman ve mekân fark etmeksizin içerisinde güç kullanımı barındıran bir çatışma ve şiddet hareketidir. Clausewitz savaşı bir bukalemun'a benzetir. Bukalemun örneğinde olduğu gibi savaşın da niteliği değişmekte ancak doğası sabit kalmaktadır. Özetle; Clausewitz bakışıyla savaş, politikanın bir başka aracıdır. Peki

[264]John L. McMullan ve David C. Perrier, "Controlling Cyber- Crime and Gambling: Problems and Paradoxes in the Mediation of Law and Criminal Organization", Police Practice and Research: An International Journal, Cilt.8, Sıra.5, Yıl. 2007, ss. 431-444.
[265]C. Clausewitz, Savaş Üzerine, Çev. Koçak, S. Doruk yayınları, 2015.

siber savaş var mıdır? Eğer varsa diğer savaş türlerinden nasıl ayrılır? Bu doğrultuda bu bölümün ilk adımında siber savaşın ölümcül, araçsal ve politik güç eylemi olarak neyi teşkil ettiği, ikinci adımında siber savaşın ne olmadığını, üçüncü adımda ise siber saldırılarla başa çıkmak için ne yapılması gerektiğini ayrıntılarıyla açıklamaya çalışacağız.

Bu bağlamda; siber savaşın tanımı sadece siber casusluk, suç, dijital isyan veya terörizm içermemekle birlikte bütüncül ve komplike bir yapıyı içinde barındırır. Casusluk yapmak, bilgi toplamak için yolunuzu kesmez, bilgi eklemez, veriyi değiştirmez, ağa veya ağın kontrol ettiği fiziksel alandaki şeylere zarar vererek bozmaz. Fakat Casusluk savaşa yol açabilir. Örneğin; Soğuk Savaş sırasında, Amerika Birleşik Devletleri ve Sovyetler Birliği milyarlarca casusluk gerçekleştirdi. 1960'ların sonunda, ABD'nin Kuzey Kore'ye karşı casusluk çabaları neredeyse iki kez savaşa yol açtı. Yada; Amerikan elektronik casusluk gemisi Pueblo'nun, seksen iki mürettebat üyesi ile ele geçirilmesi sonrasında ABD Hava Kuvvetleri EC-121 elektronik casusluk uçağının Kuzey Kore kıyılarında vurularak öldürülmesi gibi gelişmeler savaşa giden süreci pekiştirmiştir.[266] Ayrıca günümüzdeki siber ortamla Soğuk Savaş'taki casusluk süreci aynı değildir. Siber casusluk birçok yönden daha kolay, daha ucuz, daha başarılı ve geleneksel sonuçlardan daha hızlı sonuç verir. Siber uzayın sahip olduğu bu avantajlar sayesinde bir hamleyle daha fazla ülkenin birbirini gözetleyebileceği ve bundan daha fazlasını yapabileceği bir fırsat elde edilebilir.

Aynı zamanda siber casusluktan önce, bir casusun ne kadar bilgi çalabileceği veya verebileceği zararın boyutu sınırlıydı. Fakat günümüzde siber faaliyetlerin hızı, hacmi ve küresel erişiminin ne kadar çok olabileceğinin en güzel örneği Lockheed Martin tarafından geliştirilen beşinci nesil bir avcı uçağı olan F-35'in bilgilerinin hacklenmesinde görebiliriz. F-35 verilerinin çalınması 2007'de başladı ve 2009'a kadar devam etti. Nisan 2009'da, birisi veri depolama sistemlerine girdi ve terabaytlarca veriyi çaldı. F-35'in gelişimi ile ilgili çalınan bilgilerin ne olduğu ise tam olarak hala bilinememektedir. Bilgileri dışa aktarmadan önce şifreleyerek izlerini yok eden bu izinsiz girişler için yetkililer saldırının izi konusunda Çin'de bir

[266]Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books ss 108-115.

IP adresine izin gittiği yönünde açıklama yapılmış olsa da Çin hükümeti bu saldırıyı üstlenmemiştir.

F-35 programının terabaytlarca bilgisinin hırsızlar tarafından başarıyla yakalanmadan hacklendiği bu olaydan peki ne anlamalıyız? Terabaytlarca bilgiden kastımız Britannica Ansiklopedisinin on kopyasına eşdeğer, 32 cilt ve 44 milyon kelimeden 10 kat fazla bir basılı dokümanına eşittir. Bu sayının ne kadar büyük olduğunu şöyle bir örnekle daha iyi anlayabiliriz. Bir Soğuk Savaş casusu bu kadar bilgiyi gizlice bir tesisten çıkarmak isteseydi, küçük bir minibüs ve forklift kullanması gerekirdi. Ayrıca yakalanma veya öldürülme riski de vardı. Fakat siber casuslukla F-35 ile ilgili bilgileri çalan casuslar hiçbir zarar görmeden bunu saniyeler içinde gerçekleştirdi. Bu örnek, en iyi şekilde korunan bir yerin bile siber silaha karşı nasıl savunmasız olabileceğini göstermektedir. Bu olayda da görüldüğü üzere siber ortam günümüzde casusluk anlamında verilerin elde edilmesi ve bu bilgilerin suç, terör ve savaş üçgeninde kullanılması için temel oluşturmaktadır. Özellikle 2007'de Estonya'ya yönelik gerçekleştirilen siber saldırılar siber ortamda sürecin sadece casusluk içermediği ve gerçekleşen uygulama sorunlarının çözülmesi için olayların yasal kategorilere ayrılmasının zorunluluğunu göstermektedir.

Bir diğer yandan siber uzayda yaşanan bir siber savaş var mı? sorusunun cevabı nedir? Teknolojik değişimler, büyüme ve internetin evrimi sonucunda altyapı ve ağa bağlı bilgisayar sistemlerinin askeri silah ve uygulama sistemlerinin içine girmesiyle birlikte dünya çapında bilgi ve iletişim alt yapılarına yönelik sivil ve endüstriyel güvenlik ihlalleri gerçekleşmeye başlamıştır. Yukarıda bahsedilen siber saldırıların sosyal kontrol organizasyonunu şekillendirmedeki etkili rolü ve hacker endüstrisinin artan önemi, bilgisayar korsanlarına ve kötü amaçlı yazılımlara karşı savunmasız olan bu askeri yapılarda da ciddi oranda tehdit oluşturmuştur. Artan bu tehditlere karşı caydırıcılık oluşturması amacıyla başta ABD ordusu olmak üzere birçok ülke sanal dünyaya yönelik yeni bir siber komutanlık kurmuştur. ABD Siber Komutanlığı (USCYBERCOM) planlar, koordine eder, entegre eder, senkronize eder ve faaliyetlerin yürütülmesini sağlar. Bunu yaparken de siber suç, hacktivism, casusluk (ticari, askeri ve politik) ve savaş gibi 4 ana bölümde faaliyetlerini yürütür.[267]

[267]Misha Glenny ve Camino Kavanagh, "800 Titles but No Policy,Thoughts on Cyber Warfare, American Foreign Policy Interests", The Journal of the National Committee on American Foreign Policy, Cilt.34, Sıra.6, Yıl 2012, ss.287-294.

ABD'de bu ordunun kurulmasına giden süreç 2007 ilkbaharında Estonya'nın yaşamış olduğu ezici saldırıya, internet altyapısı kullanılarak gerçekleşen dünyanın ilk siber savaş eylemine gider. Bu olay hem NATO hem de ABD başta olmak üzere tüm dünyada dalgalanma etkisi yaratmıştır. Küresel olarak yaşanan bu dalgalanmayla birlikte dönemin ABD Savunma Sekreteri Robert Gates, ABD Siber Komutanlığı'nın kuruluşunu açıklayarak kara, deniz, hava ve uzaydan sonra beşinci boyutu oluşturan ve ilk insan yapımı askeri alan olan siber uzayı onaylamıştır. Savaş senaryolarına karşı oluşturulan bu komutanlık sonrasında ABD ve İsrail'in düşmanı İran'ın stuxnet olayıyla birlikte başına gelenlerde bu yeni savaş boyutunu destekler olguları ortaya çıkarmıştır. Bu açıdan bakıldığında ABD Siber Komutanlığı ve Stuxnet çevresinde kümelenmiş virüs birlikteliği, İran'ın nükleer zenginleştirme tesislerine hedef alındığını açık bir şekilde söyleyebiliriz. Aynı zamanda bu olayın siber silahlanma yarışı için başlangıç ateşini ortaya çıkardığı da gerçektir. Çünkü bu olay sonrasında Rusya ve Çin gibi ülkelerde bu yeni alanda faaliyet yürütmeye başlamıştır.

Bu sürece gerçekçilik açısından bakarsak zaten tehdit altında olduğumuz inancı doğrultusunda "Dijital Pearl Harbor" benzeri tasarlanmış büyük bir saldırı olasılığı ağa bağlı herkeste korku yaratmıştır. Aynı zamanda sosyal ve ekonomik altyapılardan bilgisayar ağına gizlice sunulan kötü amaçlı yazılımlar tahribat yaratabilir. Örneğin; siber savaşta ülke çapında bir elektrik kesintisi, zehirli gaz bulutları, rafineriler petrol yakması, trenlerin raydan çıkması, uçakların düşmesi, finansal sistemdeki verilerin silinmesi gibi birçok senaryo olabilir. Ayrıca askeri açıdan da siber uzayda yukarıda yaşanan bu gelişmeler siber uzayın savaş sistemlerinin ve ordunun bir parçası haline geldiğini göstermektedir.

Tüm bu anlatılanlar ışığında bu tezde üzerinde durduğumuz asıl nokta belirsizlik ve şüphenin olduğu yerde korkunun olduğu bunun ise tehdidin oluşmasına yol açtığıdır. Bu yüzden güncel güvenlik stratejilerinden ve gerçekleşen çatışmalardan yola çıkarak siber savaş kavramları içerisinde internet çok önemli ve etkili bir silahtır. Yaşanan örnek vakalar da bu önemi ortaya koyan en önemli kanıttır. Fakat hala siber savaşın varlığı konusunda ciddi tartışmalar bulunmaktadır. Bu tartışmaları "Siber Savaş Gerçekleş(me)di mi?" Şeklinde kısaca açıklarsak;

Siber savaştan bahsedebilmemiz için siber savaşın geçmişte hiç gerçekleşmediği, şimdiki zamanda gerçekleşmeyeceği ve gelecekte meydana

gelebileceği yönündeki görüşlere odaklanmamız gerekmektedir. Ayrıca bugüne kadar yaşanan örnek vakaları bu tezde ayrıntılarıyla incelediğimiz gibi politik güdümü olan siber saldırılar, savaşın kendisi kadar eski olan sabotaj, casusluk ve yıkım gibi etkinlikleri içinde barındıran sofistike versiyonlarda incelenmelidir. Bu doğrultuda Stuxnet siber savaşın Hiroşima'sıdır tezine karşı çıkanlar ve siber savaşın gerçekleştiğini reddedenler ortaya ne koymaktadır? Bu anti tez görüşler tezimizi doğru bir zemine oturtmamıza fayda sağlayacaktır.

Örneğin; Thomas Rid'e göre; günümüzde siber savaş gerçekleşmiyor ve gelecekte de siber savaşın gerçekleşmesi olası görülmüyor. Bunun yerine, tüm geçmiş ve mevcut siyasi siber saldırılar yıkılma, casusluk ve sabotaj şeklinde gerçekleşmektedir. Aynı zamanda; siber savaşın gerçekleşmediğini Clausewitz'in savaş konseptinde sunduğu üç ana unsura dayandırmıştır. İlk unsur savaşın, düşmanı irademizi yapmaya zorlamak için şiddet içeren bir karakterle gerçekleşmesidir. Saldırgan bir eylemi bir savaş eylemi olarak nitelendirmek için eylemin ölümcül, araçsal ve politik olması gerektiğine dayandırır. İkinci unsur savaşın enstrümanı ve karakteridir. Bir savaş eylemi her zaman etkili, araçsal ve bir sonu olmalıdır. Fiziksel şiddet veya tehdit gibi kavramlar da kuvvet araçlarıdır. Amaç siyasi bir niyet, araçlar ise savaştır. Üçüncü unsur savaşın siyasi doğasıdır. Bir savaş eylemi her zaman politiktir. Savaşın amacı, düşmanı savunmasız hale getirmek için komutanları geçici olarak kör edebilir. Savaş asla tek bir karar olmamakla birlikte her zaman politik bir amaçtır. Yani Clausewitz'in en ünlü ifadesiyle, 'Savaş, siyasetin sadece başka yollarla devam etmesidir. Bu doğrultuda Thomas Rid, Clausewitz'in savaş konseptinde sunduğu üç ana unsura dayanarak siber savaşın olmadığına ulaşmıştır. Rid'e göre; savaşta güç kullanımı şiddetli, araçsal ve politikse, her üç kriteri de karşılayan siber suç olmadığını en çok alıntı yapılan vakalar üzerinden 4 önemli vaka değerlendirmiştir. [268] Bu vakaları bu görüş çerçevesinde incelersek;

- Şiddet içermeyen Sibirya Siber Saldırısı:

1982 yılında Sibirya'da Urengoy-Surgut – Chelyabinsk doğal gaz boru hattında yaşanan patlama, tarihte nükleer olmayan ve siber teknoloji kullanılarak gerçekleştirilen en büyük ve ilk şiddet içeren siber saldırıdır. Bu olay kapsamında Soğuk Savaş sırasında Sovyetler Birliği ve ABD arasında casusluk faaliyetlerinin

[268]Thomas Rid, "Cyber War Will Not Take Place", Journal of Strategic Studies, Cilt.35, Sıra.1, Yıl. 2012, ss.5-32.

yürütüldüğü dönemde Rus boru hattı yetkilileri Kanada'dan SCADA olarak bilinen yazılımı gizlice çaldılar. Rusların Kanada'dan gizlice çaldıkları yazılımın içinde ise ABD yetkilileri truva atı virüsü yüklemiştir. Rusların yazılımı çalmaya başladıklarını fark eden ABD yetkilileri operasyonu durdurmak yerine yazılımın içine virüs yerleştirmeyi tercih etmiştir. Böylece bu virüsle birlikte pompaları, türbinleri ve vanaları kontrol eden kod bir süre normal çalışacak ve daha sonra pompayı sıfırlayacak şekilde programlanmıştır. Sonucunda da Rusların çaldığı yazılım bir süre sonra bozulmuş, boru hatlarındaki akışı anormal seviyelere çıkartmış ve borunun patlamasına sebep olmuştur. Casusluk faaliyetlerinin alan değiştirmesi gerektiğini gösteren ilk siber saldırı örneği can kaybına neden olmadan birçok maddi zarara yol açmıştır.

Rid'e göre olayla ilgili mevcut kanıtlar o kadar ince ve şüpheli ki, kanıtlanmış bir vaka olarak sayılmaz. Aynı zamanda Clausewitz'in ilk kriteri olan şiddeti karşılayan saldırı sonucunda hiçbir insan hayatının kaybına neden olmamıştır. Bu yüzden siber savaştan bahsedilemez.

- Can Kaybı Yaşanmayan ve Siyasal Desteği Olmayan Estonya:

Nisan 2007'nin sonlarında Estonya'nın üçte ikisi interneti kullanırken bankacılık işlemlerinin de yüzde 95'i elektronik ortamda gerçekleşmekteydi. O dönemde Estonya'ya yapılan bu saldırı Rid'e göre yönlendirilmemiş bir protesto eylemi ya da yolu tıkayan gemilerin bir eylemi gibi siyasi değildir. Çünkü DDoS saldırısı araçsal olarak taktik bir hedefe bağlı değildir. Yani siyasal bir desteği yoktur. Bu yüzden savaş olarak görülemez.

- Rusya ve Gürcistan Konvansiyonel Savaşı

Ağustos 2008'de Rusya ve Gürcistan arasında Güney Osetya konusunda ortaya çıkan bölgesel anlaşmazlıkta 7 Ağustos'ta Gürcistan Ordusu, Güney Osetya'nın ayrılıkçı kuvvetleri tarafından gerçekleştirilen provokasyonlara saldırarak tepki gösterdi. Bu saldırıdan bir gün sonra Rusya geleneksel askeri harekâta ek olarak bu süreçle bağlantılı bir şekilde Gürcü web sitelerine siber saldırı başlattı.

Gürcistan'a gerçekleştirilen siber saldırılar ise şu şekildeydi. Örneğin, hizmet reddi saldırıları ile Gürcistan kamu ve özel sektörlerindeki web siteleri, Parlamento gibi hükümet web siteleri ve aynı zamanda haber medyası, Gürcistan'ın en büyük ticari bankası ve diğer küçük web siteleri tahrif edildi. Dönemin Gürcistan

Cumhurbaşkanı Mikheil Saakashvili Hitlere benzetilen görseller yayınlandı. Gürcistan hükümeti ise bütün bu saldırılar hakkında Rusya'yı suçladı. Fakat Rusya saldırıların resmi sponsorluğu kabul etmedi.

Bu doğrultuda yazara göre saldırganların saflarını ve saldırı hacmini derinleştirmeye yönelik gerçekleştirilen bu kötü amaçlı yazılımlar ve hizmet reddi saldırıları savaşın aksine şiddet içermiyordu. Saldırının ana hasarı hükümetin uluslararası iletişim kurma yeteneğini sınırlamak ve küçük ülkenin sesini kritik bir anda duyurmaktı. Yani etkisi ve faydası sınırlıydı.

- Karmaşık Saldırı Boyutu ve Stuxnet:

Stuxnet o güne kadarki kullanılan tüm siber silahlardan farklı olan ve oyunun kurallarını tamamen değiştiren bir olay oldu. Stuxnet belirli hedeflere karşı yüksek düzeyde yönlendirilmiş bugüne kadarki bilinen en karmaşık siber saldırıdır. Bu saldırı geleneksel bir ağa bağlı olmadan faaliyetlerini sürdüren İran'ın Natanz'daki nükleer zenginleştirme programına karşı solucan kullanılarak gerçekleştirilen sabotaj eylemidir. Bu eylemde mühendisler aylarca süren sıkı çalışmalarda solucanın enfeksiyon geçmişini özetlemek ve tersine mühendislik yaparak solucanın tehdit ve amacını anlamakta zorlandı. Hassas veya korumalı bilgilerin çıkarılması amacıyla planlanan bu saldırı ne suç ne de savaş aynı zamanda da bir casusluk faaliyetidir.

Bu kapsamda Thomas Rid, siber suçu klasik terminolojiye göre açıklayarak suçun çoğunlukla apolitik olduğunu belirtmiştir. Rid'e göre savaş, daima politiktir. Yıkılma, casusluk ve sabotaj gibi her üç faaliyet de devletleri ve özel aktörleri içerebilir. Suçluların da üniformalı askerleri gizlediğine dair şimdiye kadar kesinleşmiş bir siber savaş eylemi yoktur. Bu yüzden siber suç siyasi olabilir fakat cezai olsun ya da olmasın bilinen tüm siyasi siber suçlar ne ortak suç ne de ortak savaştır. Amaçları yıkılmak, casusluk veya sabotajdır. Her üç durumda da, Clausewitz'in üç kriteri karşılanmamaktadır. Bu durumu sabotaj kavramı bağlamında değerlendirebilir.

Sabotaj, bir ekonomiyi veya askeri sistemi zayıflatma veya yok etme amaçlı olabilir. Tüm sabotajlar ağırlıklı olarak tekniktir, ancak elbette sosyal etkileştiricileri kullanabilir. Sabotajda kullanılan araçlar her zaman fiziksel yıkıma ve açık şiddete yol açmayabilir. Şiddet kullanılırsa, insanlar değil, her şey öncelikli hedeflerdir. Nihai amaç, maliyet-fayda hesabını değiştirmek olabilir. Ayrıca sabotajın,

operasyonel ve hatta stratejik etkileri vardır. Örneğin; saldırı kimliğinden kaçınmanın en muhteşem örneklerden biri olan İsrail Hava Kuvvetlerinin Suriye'nin hava savunma sistemlerini kör ederek İsrail savaş uçaklarının tamamını radara yakalandırmadan hedeflerine ulaşmasını sağlaması gibi bir amaca hizmet etmemiştir.[269] Bu doğrultuda yazara göre stuxnet sabotajı kendi başına siber olmasına rağmen askeri bileşen olmadan kendi başına bir saldırı olmasından dolayı bir savaş eylemi olmayabilir çünkü siyasi belirsizlik, aşırı şiddet içermemekte ve kimlikten kaçınma nihai amaca hizmet edebilir.

Sonuç olarak tüm bu örnekler doğrultusunda Thomas Rid tüm bu yaşanan süreci yıkım kavramıyla açıklamıştır. Ulaşılmak istenen yıkımlar otoriteyi, bütünlüğü ve yerleşik bir otorite veya düzenin oluşturulmasını hedefleyebilir. Ancak yıkıcı faaliyetin daha sınırlı nedenleri de olabilir. Yıkımda kullanılan araçlar her zaman açık şiddet içermeyebilir. Yıkım her zaman bireylerin sadakatlerini etkilemeyi amaçlar yaygın bir propaganda aracı olarak da kullanılabilir. Yıkım isyandan daha geniş bir kavramdır: yıkım, ayaklanmanın aksine, şiddet gerektirmez. Başarılı olmak için yerleşik bir emrin devrilmesini hedefler. Yıkımın potansiyel olarak sınırlı aracını anlamak için teknik olmayan duygusal nedenler olabilir.

Ayrıca siber saldırılar sayesinde yıkıcı faaliyete girmek daha kolay hale geldi.[270] Böylece geleneksel bilgelik, siber uzayın saldırı ve savunma yapısını değiştirdi. Bu durum da standart siber argüman giderlerini azaltarak saldırganların fırsatlarını arttırmakta aynı zamanda riskleri azaltıp hasar miktarını arttırmaktadır. Çünkü özel kod göndermek özel kuvvet göndermekten daha kolaydır.[271] Bu doğrultuda, son yıllarda sofistike ağı etkin kullanan sabotaj, casusluk ve yıkım eylemleri elbette askeri operasyonları destekleyebilir fakat tek başına ölümcül bir Pearl Harbor örneğini yaşayabileceğimiz siber savaş oluşturamaz.

Bu görüşün tam tersi olacak şekilde bir siber savaş eyleminin varlığını kabul edenler de vardır. Bu görüşü savunanlara göre siber savaş gerçek güç kullanımından çok daha fazla bir etkiye sahip olabilir. Siber saldırıların etkisi insanlar üzerinde

[269]David A. Fulghum, Robert Wall and Amy Butler,Israel Shows Electronic Prowess, https://warsclerotic.com/2010/09/28/israel-shows-electronic-prowess/ ET:09.01.2020.
[270]Thomas Rid and Marc Hecker, The Terror Fringe, Cilt.158, Aralık-Ocak 2010, ss.3-19.
[271]Martin Libicki, Cyberdeterrence and Cyberwar, Carand Corporation Santa Monica, 2009, ss.32–3.

ciddi yaralanmalara veya ölümlere yol açabilir. Askeri birimler savunmasız hale getirilebilir.

Yoram Dinstein'a göre siberden kaynaklanan böyle bir tahribat suç şiddet içermese de sonuçları açısından bir savaş eylemi olabilir.[272] Dahası, yüksek oranda ağa bağlı olarak şiddet içermeyen siber saldırılar ekonomik sonuçlara da yol açabilir.

Lıeutenant Colonel ve Scott W. Beidleman da siber savaş eyleminin olduğunu şu temellere dayandırmaktadır. 1990'larda internetin ortaya çıkışından bu yana, tüm kullanıcıların siber alanda barışçıl amaçlarla hareket etmemesi siber uzay aracılığıyla gerçekleşen saldırıların tehdidi ve etkisi iber ortamda yaşanan bir savaş ortamına dönüştürmüştür. Yani, 1990'ların başında internetin halka açılmasından bu yana siber uzayın barışçıl kullanımı azalmaya başlarken siber saldırıların büyüklüğü ve sıklığı ters oranda artmaya başlamıştır. Bu doğrultuda Lıeutenant Colonel ve Scott W. Beidleman, siber saldırıların bir devletin ulusal güvenliğine son derece ciddi zararlar vermesi potansiyeli üzerinden siber saldırıyı belirli koşullar altında bir savaş eylemi olarak incelemektedir. Ayrıca, geleneksel caydırıcılık kavramlarının siber saldırganlığı caydırdığını üzerine durmaktadırlar.[273]

Bir diğer yandan bu yazarlar siber savaş kavramını ortaya atarken de şu noktalara değinmektedir. Ya bir gün büyük bir barajın kontrol sistemleri birdenbire selleri serbest bırakırsa, nükleer santrallerin güvenlik sistemleri arızalanırsa, büyük havaalanlarının hava trafik kontrol sistemleri kapanırsa veya finansal büyük bankaların ve borsaların işlemleri durdurulursa? Ya bunların hepsi eşzamanlı olursa? Bu ihtimaller yirmi birinci yüzyılın siber savaş gerçekliğidir. Bu yüzden Estonya ve Gürcistan'a yönelik saldırılarda görüldüğü gibi devletlerin ulusal güvenliğini bu kadar önemli derecede etkileyebilecek bir tehdit için internette, uluslararası toplumun devletin eylemlerini yönetecek kodlanmış, onaylanmış bir normu ve norm organı kurulmalıdır.

Son olarak yukarıda kritik alanlara yönelik gerçekleşebilecek saldırıların sonuçları ile oluşan siber caydırma sorunu birkaç temel soruyu ortaya çıkarmaktadır. Bunlar, Siber saldırı kuvvet kullanımı mı? Bir savaş eylemi mi? Geleneksel

[272]Yoram Dinstein, Computer Network Attacks and Self-Defense, International Law Studies 76, 2002, ss.103.
[273]Lıeutenant Colonel Scott W. Beıdleman, Defınıng And Deterrıng Cyber War, U.S. Army War College strategy research Project, 2009.

caydırıcılık kavramlarını yapan siber alanda hakim mi? Bu soruları cevaplamak zordur çünkü uluslararası toplum üzerinde siber saldırganlığa ilişkin ortak, kodlanmış, yasal standartlar üzerine fikir birliğine varılamamıştır. Bu yüzden internetin ortaya çıkması on yıldan fazla olmasına rağmen hala devletlerin siber uzaydaki eylemlerini kısıtlamak için normlar ve yaptırım organı yoktur. Fakat, bu organa ihtiyaç vardır çünkü siber uzayla birlikte artan kapsam ve yıkıcılık siber saldırılar ve siber savaşı ulusal çıkarlar için bir tehdit olarak göstermektedir. Bu tehdidi tanımladığımızda, siber savaşı tanımlar ve siber saldırıları bir eylem olarak mevcut uluslararası hukuk kuralları doğrultusunda savaş kavramı ile ilişkilendirebiliriz. Sonuç olarak bu ilişkilendirmeye dayanarak çatışma kavramı üzerinden gerçekleşen olayları bir savaş dönemi şeklinde göstermekteyiz.

3.4.1. Konvansiyonel Savaş ve Siber Savaş Kavramlarının Karşılaştırılması

Günümüzde siber savaş yaşandığını iddia edebilmemiz için şuan ülkeler arasında yaşanan krizlerde devletlerin uyguladığı taktik, yöntem ve stratejileri geçmişte ne olarak adlandırıldığını bilmemiz gerekmektedir. Siber savaşlarla geçmiş savaşlar arasında uygulanan benzer stratejik yöntemleri incelememiz için önce "Savaş" kavramının ne olduğunu açıklamalıyız. Güç, güvenlik, çıkar, dış politika kavramlarıyla yakından bağlantılı olup uluslararası sistemin yapısına, aktörlerin yeteneklerine, kullanılan silahların türüne göre dönüşüm ve değişimleri içeren savaş olgusu Uluslararası İlişkiler disiplininin en önemli analiz alanını oluşturmaktadır. Bu bölümün temel amacı kavramsal ve teorik çerçeveyi oluşturarak savaş çalışmalarının gelişimini geleneksel savaş 'tan siber savaşa geçişteki benzerlik şeklinde ele almaktır. Şimdi bu geçişi kısaca açıklarsak; [274]

- Ortaya çıkan bu yeni savaş kavramı henüz kesin sınırları olmayan bir teoridir. Siber savaşlar, geleneksel savaşlardan farklı olarak birinin kazancı öbürünün kaybı şeklinde gerçekleşmemektedir. Çünkü böyle bir savaş her iki tarafa da büyük kayıplar yaşatacaktır.
- "Savaş"; bir devlet veya devletler grubunun, diğer bir devlet veya devletler grubuna karşı güç kullanarak diplomatik yollarla çözülemeyen sorunlarını

[274]Nejat Eslen, Tarih Boyu Savaş ve Strateji, İstanbul, Q-Matris Yayınları, 2003, ss. 13-15.

çözmesi anlamına gelmektedir. Bir ülkenin politik ve sosyal yapısı, ekonomik gücü ve coğrafi konumu, silahlı kuvvetlerinin yapısını ve savaşın karakterini belirler. Bu durum siber savaşlar içinde geçerlidir.

- Şiddetin büyüklüğü, savaşın amacına ve araçlarına göre değişir. Politika bir araç olarak kullandığı savaşın amacını ve uygulanacak şiddetin derecesini belirler. Bunun yanında "Savaş" politik bir amaca hizmet eden politik bir eylemdir. Bu sebeple politikadan ayrı düşünülemez. Politik amaca hizmet etmesi savaşın mantığını oluşturur. Savaşın yönetimi ayrı bir uzmanlık gerektirmekle birlikte kendine özgü prensipleri vardır. Savaşın ana hatları politika tarafından belirlenir. Siber uzay alanında ana hatlar siyasi irade tarafından belirlenmekle birlikte bu alanın yönetimi politik hedefler doğrultusunda uzman ordu birimleri tarafından gerçekleştirilmektedir.
- Savaş bir şiddet kullanma alanı olduğu ve sonrasında gözyaşı ve acı yaratması sebebiyle doğasında tehlike vardır. Siber alanda oluşan riskler siber tehdit kavramını ortaya çıkarmaktadır. Devletler siber saldırılara ve siber savaşlara karşı önlem alabilmek için siber tehdit kavramını önceliklerine almakta bu sebeple de günümüz devlet yapılanmalarında siber birimler kurarak bu tehditlerin ve tehlikelerin önüne geçmeyi planlamaktadır.
- Savaş belirsizlik alanıdır. Siber alanda aynı şekilde içinde belirsizlikleri barındırmaktadır. İçinde barındırdığı belirsizlik ve kolay gizlenebilme imkânı ise devletlerin bu yolu seçmesine yol açmaktadır.
- Rastlantı ve şans alanı olarak görülen geleneksel savaş yöntemleri aynı şekilde siber savaş içinde geçerlidir. Çünkü Stuxnet gibi bir virüsün güvenlik imkânlarının en üst düzeyde sağlandığı bir tesise sokulması bir siber savaş olarak değerlendirilse de içinde rastlantı ve şansı barındırmaktadır.
- Geleneksel savaşta önemli bir unsur olan insan faktörü siber savaşlar içinde geçerlidir. Özellikle hackerlar tarafından yürütülen siber savaşlarda artık beyaz şapkalı hackerlar bir araya toplanarak ülkeler tarafından siber ordular oluşturulmaktadır.

- Geleneksel savaşlar ile günümüz siber savaşları arasındaki bir diğer önemli hususta moral değerleridir. Napoleon Bonaparte; Savaşta moral unsur, diğer unsurlara oranla bire karşı üç değerindedir. Carl con Clausewitz; moral değerler savaşın en önemli değerleridir. Bunlar savaşın tüm unsurlarını etkileyen ruhtur. Sözleri önemlidir.[275] Bilgisayar ve interneti araç olarak kullanan siber savaşların geleneksel savaşlardan moral değerleri etkileme kapasitesi olarak da bir farkı yoktur. Bir ülkenin tüm elektrik, finans ve sağlık şebekesinin çökmesi veya kritik bilgilerinin başkaları tarafından ele geçirilmesi o ülkenin moral değerlerini etkileyebilir.
- Stratejik sanat, savaşın değişmeyen unsurları olan zaman, mekân ve kuvvetin yanı sıra beşeri, sosyal, kültürel, politik, etik, ekonomik teknolojik unsurları ve savaşın doğasında var olan belirsizlikleri, rastlantıları ve zorlukları dikkate almalıdır. Bu bağlamda siber savaş ve bilgiye dayalı stratejik savaş günümüz savaşlarının en önemli boyutunu oluşturmaktadır. Bu savaşta amaç düşmanın bilgi alt yapısını çökertmektir.
- Klasik anlayışa göre kuvvet(güç), zaman ve mekân(coğrafya) stratejinin üç önemli unsurudur. Bu üç unsur siber uzay alanında internet sayesinde şekillenerek bilgisayarlar, yazılım ve teknik araçları temel unsurların arasına eklemektedir. İnternet öncesinde de teknolojik gelişmeler savaş unsurlarını etkilemekteydi. Devletler teknolojik unsurlardan faydalanarak silah üretmeye başlamış; ok, yay, mızrak ve kılıçla başlayan bu çaba önce konvansiyonel silahlarla devam etmiş, sonrasında nükleer silahların kullanılması ve hatta uzayın savunma amaçlı kullanımıyla doruk noktasına ulaşmıştır.[276] Son olaraksa günümüzde siber silahlar konuşulmaya başlamıştır. Geçmişte halk, siyasi irade ve ordu unsurlarını içine alarak karşı tarafı en az zararla yenmek veya gizli bilgilerine ulaşmak gibi hedefleri ihtiras, psikolojik baskı ve akıl yoluyla gerçekleştiren politikaları günümüz siber dünyasında da kullanılmaya başlamıştır.

[275]Napoleon Bonaparte, "Savaş ve Strateji İle İlgili Görüşlerim", Çeviren, Gündüz, E. Q-Matris Yayınları, İstanbul, 2003.
[276]Isaac Asimav, "Bilim ve Buluşlar Tarihi", Çev. Topçugil, E. İmge Kitabevi Yayınlan, Ankara, 2006.

Mary Kaldor ‘’ In Defence of New Wars’’ adlı makalesinde savaş konusunda önemli çalışmaları olan birçok düşünür gibi savaşların değişim ve gelişim gösterdiğini kabul etmekle birlikte Clausewitz‘in yaklaşımlarının günümüzdeki savaşları analiz etmeyi kolaylaştırdığını belirtmiştir.[277] Bu yaklaşım çerçevesinde; savaşın temelinde üç ana unsur bulunmaktadır. Bunlar; en az iki tarafın varlığı, şiddet içermesi ve organize insan gruplarının var olmasıdır. Bu kapsamda günümüzde yaşanan siber çatışmaların yapısını analiz ettiğimizde geçmişte uygulanan strateji, taktik ve hedeflerle benzerlik taşıdığını aşağıdaki 4 örnekte görebiliriz. Bunlar;

- ✓ İlyada ve Odysseus destanlarında da anlatılan Truva Savaşı uzun yıllar süren bir savaştır. Bu savaşta büyük surlar arkasına saklanan Truva’nın temel stratejisi düşmanın surlarından içeriye geçmesine izin vermeyerek zafere ulaşmaktır. Aynı şekilde siber saldırılarda böyledir. Siber savaşçıların içeriye sızma yöntemi hiçbir şiddet içermeden sadece koruma duvarlarının arasından hedefe ulaşacak bir tünel bulmaktır. Günümüz siber dünyasında uygulanan truva savaşı ise koruma duvarlarından sızmak için bir tünel vazifesi gören Modern Bir Truva Atı virüsüdür. Truva Atı adı verilen zararlı yazılımlar, bilgisayarlara bir uygulama vasıtasıyla ya da internetten indirilen bir dosya üzerinden bulaşır. Bilgisayarlara bulaşmasının ardından ise arka planda çalışarak izini belli etmeden, bilgisayardaki tüm verileri ele geçirmek üzerine tasarlanmış bir virüs türüdür. Karşı taraf ele geçirildikten sonra ise istenilen herşey yapılabilir. Aslında mantık aynıdır. Güvenlik duvarlarını savaşmadan aşarak içeriye sızmaktır.
- ✓ M.Ö. 331 yılında Pers İmparatorluğu ve Makedonya arasında gerçekleştirilen Gaugamela Savaşında Pers lideri Darius savaşta stratejik bir önem sağlayan tırpanlı savaş arabalarını kullanmıştır. Bu tırpanların özelliği ilk başta karşıdan bakanlar tarafından görülmüyorken içeriden yapılacak bir hamleyle birden açılarak düşmanları imha edebilmesidir. Büyük ordusunun yanında bu araçlarla birlikte ciddi bir güç haline dönüşen Perslere karşı Büyük İskender “Fare Kapanı” stratejisini kullanarak stratejik zekâsı sayesinde galibiyet kazanıştır. Bu strateji günümüz siber savaşlarında da değişik bir yöntemle hala

[277]Mary Kaldor, “In Defence Of New Wars”, International Journal of Security and Development, 2013, ss.1-16.

kullanılmaktadır. Örneğin; Amerika gibi siber dünyayı domine eden güçler kendilerine karşı gelecek virüsleri anlayıp onlara karşı çözüm yolu geliştirebilmek için internet sistemlerinde bilerek bazı kapıları açık bırakmaktadır. Böylece tünel görevi gören bu kapılardan giren virüsler devletler tarafından yakalanmaktadır. "Honeypot" sistemi olarak isimlendirilen bu sistemi açıklarsak; bilgi sistemlerine izinsiz erişen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sunucudur. Bu sunucunun işleyişi ise şu şekildedir. Siber saldırıyı düzenleyen saldırgan gördüğü sisteme sanki gerçek bir sistemmiş gibi saldırmayı dener. Böylece honeypot devreye girer. Honeypot'un devreye girmesiyle birlikte siber saldırıyı düzenleyen saldırganın hareketleri, saldırı tekniği ve saldırganın nereden hangi yöntemleri kullanarak saldırmış olduğu analiz edilir. Bu sayede gerçek sistemde oluşabilecek saldırılara karşı sistem korunmuş olur. Fare Kapanı stratejisi ve honeypot stratejisinin ortak noktası saldırganın en çok sevdiği ve kendine en güvendiği yerden hareket etmesini sağlamaktır. Böylece rakip en güçlü olduğu yerde en büyük zaafından vurulur. Bu stratejinin benzeri Napolyon tarafından da zamanında kullanılmıştır. Örneği daha da sadeleştirirsek; bal seven birisi, bal küpünü görür görmez ve bir de açlık hissi varsa küpün içerisine elini sokmak isteyecektir. Çünkü dışarıdan bakıldığında, içerisinde bal olduğu izlenimi edinecek, dolayısıyla bal küpünün içine elini attığı anda arılar tarafından sokulacaktır. Mantık aslında bu kadar basittir.

- ✓ Bir diğer örnek ise tünel stratejisidir. Tarih boyunca birçok ülke geçmiş savaşlarda kalelerin içine sızmak için yer altından tünel kazardı. Osmanlı Devletinde de savaşlarda kullanılmak üzere ordunun içinde Lağımcılar adı altında bir birim vardı. Lağımcılar adı altındaki bu grup kazdıkları tünel sayesinde ordunun kalenin içine girmesini sağlamaktaydı. Bu sayede düşman yok edilip kaleler de içten fethedilirdi.Günümüz siber dünyasında bu stratejiye benzer şekilde kullanılan yöntem ise VPN, Virtual Private Network (Sanal Özel Ağ) sistemidir. Kısaca, VPN sistemi internete başka bir IP adresi üzerinden bağlanılmasını sağlayan hizmettir. Böylece bilgisayar fiziksel olarak bulunduğu yerden karşıdaki ağa şifreli (kripto anlamında) bir tünel açar. Bu tünel içinden iletilen bilgi dışarıdan bakıldığında şifreli olduğu için görüntülenemez. Fakat

konuya hâkim siber güvenlik uzmanları veya siber ordular ise bu bilgilere ulaşabilir.

- ✓ Geçmiş savaş taktikleri ile günümüz siber stratejileri arasında benzerlik kuracağımız son örnek boş kale taktiğidir. Kısaca bu taktiği açıklamamız gerekirse; Çinli General Zhuge Liang kendisinden sayıca çok üstün olan ve kaleyi istila etmeye gelen düşman ordularına karşı kalenin bütün kapılarını açmıştır. Bütün askerleri görülmeyecek şekilde kalenin içerisinde gizlemiş ve kendi de kapının önünde saz çalar şekilde düşmanı beklemektedir. Bunun bir tuzak olduğunu ve içerde çok büyük bir ordunun kendilerini beklediğini düşünen düşmanlar ise korkarak geri dönmüştür. Böylece Sun Tzu'nun deyimiyle; Çinli General Zhuge Liang savaşmadan kazanılmıştır. Günümüz siber dünyasında bu stratejiye benzer şekilde kullanılan yöntem ise DDoS yani Distributed Denial of Service (Dağıtık Hizmet Engelleme) saldırılarıdır. Kısaca bu saldırıların özü bilgi güvenliği unsurlarından erişilebilirliği hedef almasıdır. Siber dünyada kurulan her sistem; kullanıcı sayıları, hat kapasitesi, anlık istek sayısı gibi unsurlar için belli değerler öngörülür ve bu değerlerin biraz daha üstünde yükü kaldırabilecek şekilde tasarım yapılır. DDoS saldırıları bu kapasitenin üstünde veri ve talep oluşturulması yöntemiyle sistemin kitlenmesini sağlar. Bu çerçevede DDoS saldırılarında da Boş Kale Taktiğinde de mevcut kapasityi çok üstünde göstermek ve karşıyı kilitlemek hedeflenmektedir. Sun Tzu'nun dediği gibi savaşı kazanan taraf soğukkanlı ve kararlı olmalıdır. Savaşların kaderini güçler değil zekâ belirler. Akıllı olan taraf daha savaş başlamadan kazanır. Düşmana yakınken uzak, uzakken ise kendisini yakın gösterebilir. Savaşta bir komutan güçlü olduğu halde güçsüz, güçsüzken ise kendini güçlü gösterebilir. Sadece savaşta her şeyde olduğu gibi algılarla oynamak, rakibi manipüle etmek için çok önemlidir. İşte bunu çok iyi bilen Zhuge Liang ve günümüz siber dünyasında en önemli role sahip ülke olan Çin ve Rusya gibi ülkelerin kullandıkları bu yöntem tek askerini bile kaybetmeden düşmanı geri püskürtmektedir.

Bu benzerlikler ışığında şu sonuca ulaşabiliriz. Tarih boyunca savaşların çıkma sebepleri bugüne kadar hep aynı olmuştur. Ülkelerin ve bireylerin çıkar çatışmaları, güç mücadelesi, vatanseverlik ve ideoloji unsurlarıdır. Bugünkü siber savaşlarında mantığı aynıdır. Aynı zamanda; teknolojide hayatın her zamanında

askeri güçle birlikte kullanılmıştır. Günümüzde siber ağlar üzerinde yaşanan siber savaş içinde ordu birimleri kendi içlerinde siber lejyonlar bulundurmaya başlamıştır. Anarşik sistemde gerçekleştirilen taktik ve stratejik hamleler sonucundaysa bu çatışma derinleşerek kapsama alanı genişlemiştir. Bu yüzden klasik bir savaşta kullanılan taktik ve stratejiler ışığında[278] günümüzde gerçekleşen siber savaşlarda aktörler tarafından amaçlanan hedeflerdeki benzerlikler şunlardır;

- ✓ *Moral Stratejisi:* insanları motive edecek imkânları kısıtlayarak, morallerini yüksek tutmalarını engelleyip savaşı kazanmayı hedeflerler. (Gürcistan, Estonya)
- ✓ *Ekonomi Stratejisi:* en az maliyetle hedeflere ulaşma fırsatı sağlar. Ekonomi stratejisi ile düşmana doğrudan saldırmak yerine kapana kıstırmak için bekler. Tüm imkânları en ekonomik şekilde kullanarak bir savaşın gizli giderlerini en aza indirmeyi hedefler. Örneğin; yitirilen zaman, boşa harcanan siyasi iyi niyetler, intikam almaya kararlı ve acı içindeki bir düşman, insan kaybı, silah kaybı vb.
- ✓ *Savunma Savaşı Olarak Karşı Saldırı Stratejisi:* ABD, Stuxnet ile birlikte ilk saldırıyı yaptığı için kendi stratejisini ortaya çıkarmıştır. Buda stuxnete karşı Çin, Rusya ve İran gibi ülkelerin çözüm almasına ve ABD'ye karşı stratejiler belirlemelerine yol açmıştır.
- ✓ *Caydırma ve Yıpratma Stratejisi:* Caydırma ve yıpratma konsepti; zayıfın güçlüye karşı uygulayacağı stratejidir. Düşmanla savaşmanın en iyi yolu, başlangıçta size saldırmasını engellemektir. Bu sebeple; İran ABD'nin konvansiyonel bir savaşta istediğini elde edemeyeceğini ABD'ye göstererek siber savaş yöntemini kullanmasını zorunlu hale getirmiştir. Caydırma stratejisi ile aktörler arasındaki siber tehdit ve siber saldırı unsurlarının rakibe karşı aleni olarak uygulandığında bu çatışmanın neye mal olacağına emin olamadıklarından dolayı gizli yürütülmesini zorunlu kılmaktadır.
- ✓ *Sıcak Savaşsız Strateji:* ABD gibi güçlü bir düşman karşısında Çin ve Rusya aktif bir siber savaş stratejisi uygulamaktadır. Gerçekleştirilen bu pasif

[278]Robert Greene, ve Joost Elffers, Çev. Doruker, F. 33 Stratejide Savaş, Altın Kitaplar Yayınevi, İstanbul, 2018.

saldırganlık stratejisi ile Çin ve Rusya başta olmak üzere tüm aktörler gerçekleştirdikleri siber saldırıları gizli olarak uygulamaktadır.

- ✓ *İstihbarat Stratejisi:* Gelişen teknolojisi sayesinde savaş öncesi istihbarat uygulamaları da siber alana kaymış ve bu alanda casusluk ve istihbarat faaliyetleri yürütülmektedir. Özellikle İsrail, Çin, İngiltere ve Rusya gibi ülkeler siber istihbaratı çok iyi kullanmaktadır.
- ✓ *Ağırlık Merkezi Stratejisi:*Ağırlık merkezi stratejisi ile saldırı gerçekleştirilecek düşmanın en kritik alt yapı noktası belirlenerek saldırı buraya gerçekleştirilir. Bu strateji ile birlikte en önemli nokta vurularak direnişi hızlı ve ani bir şekilde yok etmek hedeflenir.
- ✓ *Diplomatik Savaş Strateji*: pazarlık öncesi ve sırasında karşı tarafa büyük baskı yaratıp karşı tarafa istekleri kabul ettirmek hedeflenir. Siber uzay alanında üst otorite belirlenememesi diplomatik siber savaş stratejisi uygulanmasını engellemektedir.
- ✓ *İttifak stratejisi:* Siber uzayda gerçekleştirilen saldırılarda aynı anda birbirlerine rakip birden fazla ülkeye ve ağa saldırı ve manipülasyon düzenlenebilir. NATO'nun Estonya'ya karşı gerçekleştirilen saldırıdan sonra Talin'de bir Güvenlik Merkezi kurması bu sebepten gerçekleşmiştir. NATO tarafından gerçekleştirilen bu koruma kalkanı ile siber uzayda İttifak stratejisinin ilk örnekleri görülmüştür.
- ✓ *Terör Hareketleriyle Zincirleme Tepki ve Panik Yaratma:* Bu stratejide klasik terör faaliyetleri eğer siber terör faaliyetleri ile birlikte yürütülürse çok ciddi boyutlara ulaşabilme ihtimali bulunmaktadır.
- ✓ *İçeriden yıkma:* günümüzde artık devletlerin bütün hayati bilgileri sanal dünyada bilgisayarlar ve internet sayesinde networkler üzerinde saklanmaktadır. Bu bilgilerin ele geçirilmesi bir ülkenin içten fethedilmesi anlamına gelmektedir. Bunun en iyi örneği stuxnet virüsünün yayılması sürecidir. Aylarca İran ne olduğunu anlayamadı. Virüs sürekli kendini yeniledi. İçeriden yıkma stratejisinin uygulandığı bir diğer siber savaş Rusya tarafından Gürcistan ve Ukrayna ya karşı gerçekleştirilen saldırılarda kullanılan içeriden yıkmaya yönelik iç cephe stratejileridir.

- ✓ *Baskın Stratejisi*: Baskın stratejisi ile düşmanın hiç beklemediği bir anda aniden ve beklenmeyen bir yöntemle uygulanan siber strateji düşmana daha büyük etki yaratmaktadır.
- ✓ *Topyekûn İmha Stratejisi*: Estonya ve Venezuela siber saldırısında olduğu gibi düşmanı çembere alarak bütün unsurlarını bir arada imha etme stratejisi uygulanmıştır. Böylece her taraftan bitmeyen bir baskıyla dış dünyayla bağlantı kesilerek toplumda oluşan bu kargaşa zincirleme tepki stratejisi ile birlikte belirsizlik ve panik yaratarak kargaşa oluşturup mağlup olunmasına yol açar.

Savaşla sonuçlanan çatışmaların yönetiminde bazı konularda geleneksel ve siber yöntemler arasında farklılık içermektedir. Kısaca bu farklılıkları açıklarsak;

Tablo 9 Klasik Savaş ve Siber Savaş arasındaki Farklar

Kriterler	Klasik Savaş	Siber Savaş
Saldırı Kaynağı	Saldırının kaynağını bulmak kolaydır.	Saldırının kaynağını bulmak zor, hatta bazen imkansızdır.
Hızı	Bir füzenin, uçağın, tankın, veya muhaberedeki diğer silahların hızı kadardır.	Işık hızındadır.
Taktik ve Stratejiler	Güvenlik İkilemi, Caydırma, Sızma, Kandırma, Savaşmadan Kazanma, En az maliyetle Kazanma gibi stratejiler her ikisinde de kullanılmaktadır.	Truva Atı, Bal küpü, Fare Kapanı, (VPN) ve (DDoS saldırıları)
Hasar Tespiti	Fiziksel etkilerden dolayı hasar tespitini Kontrol etmek, izlemek ve önlemek kısmen memnun kolaydır.	Nerde ve ne kadar hasar oluştuğunu tespit etmek imkansızdır.
Silah Sistemleri	Tabanca, top, tüfek, bomba, uçak, gemi, tank, füze, radar, denizaltı vb.	Çipler, bilgisayarlar, bilgi sistemlerinde kullanılan diğer donanım ve yazılımlar
Teknoloji İhtiyacı	İleri teknoloji gerektirir.	Çok yüksek bir teknolojiye ihtiyaç duymamaktadır. Mevcut bir bilgisayar kullanılması mümkündür.
Maliyeti	Kullanılan silah sistemlerinin maliyetiyle bağlantılı olduğundan pahalıdır.	Ucuzdur. Bazen bir bilgisayarda etkili olmak mümkündür.
Coğrafya	Savaşın etkili olduğu bölgeleri içerir.	Herhangi bir coğrafya ve sınır tanımaz.
Etkisi	Çoğunlukla fiziksel alanla ilgilidir.	Çoğunlukla bilgi ve iletişim sistemleri alanında etkilidir.
Motivasyon	Askeri, siyasi ve ekonomik fayda	Askeri, siyasi ve ekonomik fayda
Kullanılan araç	Silah, bomba vb. araçlar	Çipler, bilgisayarlar, bilgi sistemlerinde kullanılan diğer donanım ve yazılımlar
Karşılaşılan risk	Eylemi gerçekleştiren yaşamsal risk altında	Eylemi gerçekleştiren hakkında Herhangi bir risk yok
Etki alanı	Saldırının yapıldığı alan ve bölge ile sınırlı	Ulusal ve uluslararası boyutlarda etkili
Güvenlik	Kısmen sağlanabilir.	Tespit etmek ve yok etmek imkansız.
Uygulanacak ceza	Suçun niteliğine göre belli	Suçun niteliğine göre belli
Hedef Kitle	Devletler,Bireyler,organize örgütler	Devletler, kurumlar, firmalar
İstihbarat	Soğuk Savaş dönemi sonuna kadar savaş öncesi istihbarat, devlet istihbaratı üzerine kurulmuştu; insan ve teknik istihbarat vasıtaları kullanılarak gizli bilgilere ulaşıldığından hata oranı yüksektir.	Günümüzde istihbaratın pek çok işlevi (toplama, analiz, örtülü operasyonlarvs.) devlet dışı aktörlerin (özel şirketler, hackerler, vekil gruplar) uzmanlığına bırakılmıştır. Masa başından bilgisayar ve yazılımlar sayesinde gerçekleştirilir. Direk bilginin kaynağına ulaşıldığından hata oranı düşüktür.
Terör	Kritik tesisler, hükümet temsilcilikleri, güvenlik birimleri ve normal vatandaşa yönelik sansasyon yaratacak ve fiziksel zarar verecek eylemler	Siyasi ve Ekonomik fayda Motivasyonuyla ve Araç olarak Bilgisayar tabanlı şiddet ve tatmin yolu kullanılarak Devletlere karşı yürütülür.
Temel alınan ve öncelikli olan faktörler	Soğuk Savaş sonrası kaos ve hiyerarşik yapının bozulması, anarşik yapı, rekabet ve güç elde etme mücadelesi	Teknolojik gelişmeler, siber istihbarat ve siber caydırıcılık
Tarihsel Başlangıcı	Thucydidese kadar gitmektedir.	1980'lerin başında ARPANET'in henüz büyümekte olduğu dönemlerde, aslında bugünkü yapının temeli atılmıştır.
Ordu	Tüm devletlerin kendilerine ait düzenli ordu birlikleri mevcut olmakla birlikte resmi olmayan terör grupları vasıtasıyla da yürütülmektedir.	Siber çatışmaların etkisinin ve sonuçlarının boyutunu ciddiye alan ve siber dünyada aktif rol oynayan ABD, Rusya, Çin, İsrail, gibi ülkeler ve NATO gibi örgütlenmeler kara, deniz, hava ve uzaydan sonra beşinci bir askeri kuvvet olan siber orduyu devreye sokmuşlardır.

3.4.2. Soğuk Savaş ve Siber Savaş Kavramlarının Karşılaştırılması

Savaş aracı olarak 1. ve 2. Dünya Savaşından farklı olarak, nispeten Soğuk Savaş dinamiklerine benzer nitelikte psikolojik yapı, karşılıklı gerilim, her an saldırı olma korkusunu içeren ama teknolojinin gelişmesiyle birlikte bunu konvansiyonel ve nükleer savaş araçları vasıtasıyla değil de siber silahlar yöntemiyle uygulayan bir savaş türü günümüzde yaşanmaktadır.

Her savaş türü bir sonraki savaş türünün nedeni ve sonucudur. Soğuk Savaş'ta siber savaşın doğmasının bir nedenidir. SSCB'nin ekonomik ve teknolojik yapıdaki değişime ayak uyduramaması bu savaşın bitmesine yol açmıştır. Bu sebep ise aynı zamanda siber savaşın başlangıcı olan internetin doğuşu, gelişimi ve yükselişini ortaya çıkarmıştır.

Soğuk Savaş'tan bugün konuştuğumuz siber savaş kavramının ortaya çıkması bir nedendir. SSCB'nin ekonomik ve teknolojik yapıdaki değişime ayak uyduramaması bu savaşın bitmesine yol açmıştır. Bu sebep aynı zamanda siber savaşın başlangıcı olan internetin doğuşu, gelişimi ve yükselişini ortaya çıkarmıştır. Nasıl 1. ve 2. Dünya Savaşı tamamen birbirinden farklı bir savaş modeli ise, soğuk savaş ve siber savaşta birbirinden farklı iki savaş modelidir. Ama birbirlerini tetiklemiştir. Yani Soğuk Savaş'ın bitmesiyle birlikte savaşın önlenmesine yönelik çabalar siber savaşın tetiklenmesine yol açmıştır. Soğuk Savaşta başlangıç, yumuşak, sert ve gerileme dönemi yaşanırken, Soğuk Savaş'ta şuan başlangıç aşamasını tamamlayarak yumuşak döneme geçiş süreci yaşamaktadır.

Her iki savaşta küresel dünyayı içeren bir savaştır. Şuan yumuşak bir şekilde yükselme dönemini yaşayan siber çatışmalar uluslararası ilişkilerde dış politika stratejilerinin belirlenmesi süreçlerinde aktif olarak kullanılmaktadır. Siber uzay hakkında uluslararası hukuk kurallarında misilleme yasağının bulunmaması, karşılıklılık ilkesinin olmaması, bilinmezliği içinde barındırması, kanunlara aykırı olmaması gibi sebeplerden dolayı çatışmalarda sıklıkla kullanılmaktadır. Bu bağlamda gerçekleşen tüm çatışmalar savaş hukukunda veri iletişimi ve veri koruması süreçlerine yönelik gerçekleşen siber savaş dönemi olarak gösterilmektedir.[279]

[279]Hans Joachim Heintze ve Pierre Thielbörger, a.g.e ss.24

ABD ve İsrail'in Ortadoğudaki projelerinde rakip gördüğü ve özellikle Rusya tarafından örtülü bir şekilde desteklenen İran'ın nükleer faaliyetlerini durdurma hedefi doğrultusunda Stuxnet virüsünün yayılması gibi etmenler bu savaşın olduğunu göstermekledir. Ayrıca Soğuk Savaş döneminde Sovyetler tarafından saldırıya uğrama korkusuna sahip ülkeler günümüz siber dünyasında da bu hissi farklı boyutlarda yaşamaktadır. Rusya'nın izlemiş olduğu siber stratejilerin NATO üyesi ülkelerini korkutması bunun en güzel örneğidir.

Aynı zamanda; Soğuk Savaş'ın siber savaştan farkı iki kutup arasında yaşanmıyor olmasıdır. Caydırma ve çevreleme stratejisi Soğuk Savaş'ta uygulanırken siber savaşta hibrit yöntemler ve enformasyon çağı etkili olmuştur. Siber caydırıcılıkta nükleer caydırıcılık gibi korku salmakta ve cesaret kırmaktadır. Çünkü aynı saldırının kendisine karşı yapılabilme ihtimali ülkelerin bu yeni silahı aleni kullanmalarını engellemektedir. Nasıl Soğuk Savaş Berlin Duvarının yıkılmasıyla birlikte yıkıldıysa, siber savaşta artık kurumların, şirketlerin ve devletlerin internet sistemlerine erişimlerinde güvenlik duvarlarını yıkmaları ve kullanmamalarıyla sonlanacaktır. Çünkü tüm devletlerin bağımsızlığını, toprak bütünlüğünü, siber alt ve üst yapılarını, bilgilerine erişimini, alt yapılarına zarar vermeye yönelik saldırılarını sonlandıracağı bir üst yapı organizasyon kurulmaması halinde bunun etkisinin artacağını gelişmeler göstermektedir. Bu sebeple siber güvenlik konusunda uluslararası hukuk alanında ortak egemenlik kuralları ve bir üstünlük sağlanması gerekmektedir. Fakat devletler siber çatışmaların uluslararası örgütlenme ile uluslararası hukuk ve yargı içinde kurallar altına alınmasına karşı gelmektedir. Nasıl Soğuk Savaş döneminde devletlerarası aktif çatışmalar ve savaşlar 2. Dünya savaşındaki gibi olmayıp azaldıysa siber savaş döneminde de aktif savaş sayısı azalmaktadır. Çünkü devletler istediklerini yumuşak güç olarak siber saldırı stratejileri ve siber casusluk planları ile gerçekleştirmektedir. Yani stratejik davranışın unsurları değişmemiştir, değişen yalnızca bunların uygulanacağı durumların çok daha karmaşık hale gelmesidir.[280] Siber uzayın asimetrik özellikleri de bu karmaşıklığın asıl sebebidir.

Sonuç olarak; iletişim dünyayı değiştirmekte, şekillendirmekte ve dönüştürmektedir. Örneğin; Afganistan savaşında CNN izleyen biriyle El- Cezire

[280]Lawrence Freedman, "Strateji" , Çev. Dişbudak, B.Ç. Alfa Yayınları, İstanbul, 2014, ss.41.

izleyen birinin savaşa ve Usame Bin Ladin'e bakışı ve aldığı bilgiler farklıdır. World Wide Web'in de yarattığı bilgi akışı ve etkisi farklıdır. Siber uzay bu algının yaratılmasında en önemli araçtır. Ayrıca bu algı yönetiminde artık büyük devletler, küçük devletlere karşı bile her türlü silahlı saldırıdan ziyade ekonomik, siyasi, diplomatik ve siber yöntemleri kullanmaya başlamıştır. Bunun en güzel örneği; 21. yüzyılda bu alanı en başarılı kullanan Rusya'nın son yıllarda NATO üyesi Estonya'ya veya eski Sovyet coğrafyasında Gürcistan ve Ukrayna gibi ülkelere yönelik gerçekleştirdiği saldırgan hamlelerde görebiliriz. Bu hamleler, yeni bir dünya savaşına giden süreçte yeni bir alan olan siber uzayı Rusya'nın aktif bir şekilde kullandığını bu bağlamda değerlendirebilir.

DÖRDÜNCÜ BÖLÜM

FARKLI ÜLKELER ve ULUSLARARASI KURUMLAR ÖZELİNDE SİBER GÜVENLİK ANLAYIŞLARININ VE POLİTİKALARININ KARŞILAŞTIRMALI ANALİZİ

Tezimizin bu bölümünde "Siber Savaş" ların oluşmasına yol açan amaçlar, bu savaşlarda kullanılan araçlar, bu savaşlarda başarıya ulaşmak için gerçekleştirilen stratejiler, bu alanı kullanan aktörlerin politikaları ve şuana kadar gerçekleşen çatışma örnekleri özelinde ülkeler ve kurumlar özelinde karşılaştırmalı olarak siber güvenlik anlayışlarının ve politikalarının analizleri gerçekleştirilecektir.

Teknolojinin ve internetin gelişmesi ve yaygınlaşmasıyla birlikte beşinci boyut alanı olan siber uzay alanında devletler ordular kurmakta, bütçeler oluşturmakta ve faaliyetler yürütmektedirler. Günümüz bilgi çağında devletlerin kurdukları bu siber orduların potansiyel güçleri, çalışma yapıları, tehditleri ve riskleri birbirlerinden farklıdır. Tüm bu farklılıklar sonucunda anarşik yapının da etkisiyle aktörler hayatta kalabilmek için konuya stratejik yaklaşmak zorunda kalmıştır. Örneğin; Çin günümüzde ABD ekonomisini zayıflatmak için kendi siber gücünü kullanmaktadır. Aynı şekilde Rusya eski coğrafyasına yönelik hâkimiyetini tekrar kazanmak için geleneksel savaş yöntemlerinin yanında siber saldırıları kullanmaktadır. ABD ise yüz yüze kaldığı bu siber güvenlik riskinden dolayı NATO içerisinde özellikle Estonya örneğinde de olduğu gibi bir ittifak sistemi oluşturmaya çalışmaktadır.

Siber savaşların etkisinin ve sonuçlarının boyutunu ciddiye alan ülkeler kara, deniz, hava ve uzaydan sonra beşinci bir askeri kuvveti devreye sokmuşlardır. Özellikle siber dünyada aktif rol oynayan ABD, Rusya ve Çin gibi ülkeler; siber saldırılara karşı savunma ve saldırı timleri oluşturmuştur. Aynı zamanda bu ülkeler taşeron hackerlar da kullanmaktadır. Resmi ordular veya taşeron hackerlar vasıtasıyla şu ana kadar yaşanmış siber saldırılar, bir ülkenin elektrik şebekesini çökertecek, ayaklanmalar çıkararak ülkeyi ele geçirilebilecek, nükleer tesislerini patlatılabilecek bir güce sahip olduğu bu bağlamda değerlendirebilir. Bir başka ifadeyle, siber saldırılar hayatın her alanını olumsuz yönde etkileyebilecek bir güce sahiptir. Örneğin; Bir ülkenin bütün enerji sistemi yok edildiğinde tekrar faaliyete sokulması sanıldığı kadar kolay değildir. Böylece bütün hayat bir anda etkilenebilir.

Bu durum ise domino etkisiyle diğer bağımlı ülkeleri etkileyebilir. Bir ülkenin sadece enerji sektörüne yapılan bir saldırı ile sistemlerinin çalışamaz hale gelmesi o ülkenin tüm iletişim, finans ve ulaşım sektörünü, hatta barajların etkilenmesiyle insanların suya ve yemeğe ulaşımını etkileyebilir. Oluşacak kargaşa çerçevesinde insanlar ölebilir. Üretim durabilir. Böylece bu saldırıyı gerçekleştiren rakipte bu sonuçlardan etkilenebilir. Yâda saldırıya uğrayan tarafta aynısını diğer tarafa yapabilir.[281] Bu anlatılanlar ışığında bu yeni savaş alanında herkesin herkesi heceleyebileceği bir anarşik korku sürecinin yaşandığını rahatlıkla söyleyebiliriz.

Yukarıdaki tüm olası etkilerden anlaşıldığı üzere klasik hayatta olduğu gibi günümüz siber dünyasında da iyi ve kötü birlikte bulunmaktadır. Uluslararası anarşik yapı içerisinde üst çatı ve kuralların belirlenmediği sistemde kurallar net olarak oturtulamamıştır. Bu durumda siber saldırıların, doğası gereği nerden geldiğinin kesin olarak bilinememesi de etkili olmuştur. Ama önemli olan bu etkinin sağladığı avantajdan dolayı dünya da birçok siber saldırının gerçekleşmiş olmasıdır. Sonuç olarak tezin bu bölümünde kısaca günümüzde devletler tarafından gerçekleştirildiği iddia edilen ve uluslararası sistemin hâkim aktörleri arasında şu ana kadar yaşanmış siber çatışma örnekleri ve çatışma sürecince uygulanan stratejiler incelenecektir.

4.1. Amerika Birleşik Devletlerinin Analizi

ABD'nin geçmişte ve günümüzde uluslararası ilişkilerin en önemli aktörlerinden biri olmasında 1. ve 2. Dünya Savaşına girerek savaşın ve dünya'nın seyrini değiştirmesi etkili olmuştur. Soğuk Savaş'ın bitmesiyle birlikte ABD, dünyanın tek hâkimi konumuna gelmiş olsa da şuan bu konumunu koruyamamaktadır. Bu duruma karşı "Yumuşak güç" kavramının yaratıcıları Joseph Nye ve Robert O Keohone; ABD'nin sert gücüne ek olarak geliştirdiği yumuşak güç unsurlarıyla birlikte 21. yüzyılda da üstünlüğünü sürdürebileceğini belirtmektedir. Fakat Donald Trump ile birlikte ABD'nin yumuşak güç unsurlarını kaybettiği görülmektedir. Trump ile birlikte ABD'nin gerçekleştirdiği ticaret savaşları sonucunda ona karşı oluşan blok her geçen gün daha da güçlenmektedir. Bu durumu açmamız gerekirse; ekonomik kaynaklar Batı'dan Doğu'ya kaymaktadır. Çin; ekonomik gücü, büyük nüfusu, gelişen teknolojisi ve askeri gücü ile parlayan bir yıldız olmaya devam etmektedir. ABD ise Donald Trump ile birlikte artan borç yükü

[281]Sınger veFrıedman. S. G. ve S. S. Ss. 173.

sebebiyle ekonomik gücünü, siyasal ve kültürel cazibesini, NATO vb. uluslararası kuruluşlardaki yıllardır oluşturduğu müttefik ilişkilerindeki güveni ve askeri gücünü kaybetmektedir. [282]Bu durum ekonomik ve teknolojik değişimlerin politik ve askeri değişimleri doğurduğunu göstermektedir. Ayrıca ekonomi ve teknoloji ulusun başarı ve başarısızlıklarının tek sebebi de değildir. Coğrafya, askeri teşkilatlanma, ulusal moral, ittifak sistemi de devletlerin nispi güçlerini etkilemektedir.

Aynı zamanda bugüne kadar geliştirilen Uluslararası İlişkiler kuramları genel olarak, uluslararası politikayı üç anahtar kavram ile açıklamaya çalışmıştır: güç, yapı ve hegemonya. Gramsci'ye göre hegemonya uluslararası sistemdeki en kuvvetli devletin veya belirli bir bölgedeki hâkim devletin konumunu tanımlıyordu. Bu bağlamda; hegemonya hâkim devletin moral, politik ve kültürel değerlerinin topluma ve alt gruplara yayılmasına olanak verir. Cox'a göre tarihsel olarak iki hegemon gücün (ABD ve İngiltere) temel olarak kullandığı düşünce "serbest ticaret"ti ki, bu düşünce diğer çevrelere ve pazarlara nüfuz etmek için gerekli yolu açmaktaydı. Şüphesiz ABD, bu anlayış çerçevesinde neo-liberalizm ile hegemonya üretmekteydi. Fakat bilgi devrimi ile birlikte e-ticaretin gelişmesi Çin'in durdurulamaz yükselişine sebep olmuştur. Bu durumda yeni dünya düzeninde yaşanabilecek Amerikan hegemonyasını tehdit etmiştir.

Hegemonya ve hâkimiyet arasındaki fark Machiavelli, Gramsci ve Nye gibi pek çok düşünür tarafından tartışılmış bir konudur. Machiavelli, Gramsci ve Nye'e göre büyük bir güç hâkimiyete, zorlamaya ve sert güce dayanmaz. Machiavelli'ye göre büyük güce itaatin nedeni saygı olmalıdır. Gramsci, büyük gücün, gönüllülüğe ve düşünmeksizin işbirliğine ittiğini söylemektedir. Nye'e göre hâkim güç iş birliğine ikna ederek hegemonik güç olur. Bu ikna düzeyi ise yumuşak güçle çıkarları ortak imiş gibi göstererek sağlanır. Ancak hegemonik istikrar teorisine göre büyük güçler, kendi pozisyonlarını sürekli izin almaksızın tek taraflılık ve sert güçle sağlarlar.

Küresel ekonomiye, dünya ticaretindeki payı yönünden veya askeriye harcadığı bütçe yönünden bakıldığında hegemon gücün ABD olduğu görülmektedir.

---

[282]Portland, The Soft Power 30, A Global Ranking Of Soft Power 2019, ss.40 https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf ET.05.02.2021.

Fakat küresel güç olmak, sadece ekonomik güç ile dünya piyasasını belirlemek değildir. Ekonomik gücün güvenliğini sağlamak veya yeni ekonomik pazarları kontrol altına almak ve gerektiğinde ele geçirmek üzere hazır, kullanılabilir bir ekonomik ve askeri güce sahip olmak da gerekir. ABD sahip olduğu eşsiz konumla, yumuşak güç araçlarını etkili bir biçimde kullanarak klasik bir hegemonyacı bir güç olmak yerine dünyaya liderlik yapan bir güç olma amacıyla dış politikada bir Amerikan kültürü yaratmıştır. Fakat günümüz dünyasını şekillendiren Amerikan himayesindeki değer zaman içinde bu rüzgârı tersine döndürmüştür. Hedef küresel hegemonyadır. Gerçekler ise dünya'nın anarşik yapısıdır. Soğuk Savaş sonrası dönemden beri ABD her ne kadar en büyük güç olsa da Çin ve Rusya bu anarşik yapıda Amerika'ya hegemon olma fırsatını tanımamaktadır.

Soğuk Savaş sonrası dönemden beri ABD'nin bu uzunlukta bir üstünlük dönemini sürdürmesi beraberinde birçok güç avantajı getirmiştir. Bu avantajlardan bazıları şunlardır; kendi topraklarının geleneksel saldırılara karşı güvenli olması, müttefik ülkelerdeki üs avantajını kullanarak sınırlarının ötesinde proje geliştirme gücü, yıkıma uğramamasından kaynaklı resmi savunma bütçesine daha fazla pay ayırması ve internetin yaratıcısı olmasından dolayı teknolojik araçlardaki tüm değişim ve dönüşümde en büyük payı onun almasıdır. Fakat kaynakların paylaşıldığı bir dünyada güvenlik politikası için güvenli bir yol izlemek ve diğer güçler üzerindeki stratejik üstünlüğü sürdürmek çok zordur. ABD'nin de yaratıcısı olduğu siber uzay teknolojisi onun stratejik güç konumunu her geçen gün aşındırmaktadır. Yani internet kavramlarının ortaya çıkmasında öncü olan ABD, Endüstri 4.0 ve Toplum 5.0 ile birlikte avantaj ve dezavantajı bir arada yaşamaktadır. Bu bağlamda dünyanın önde gelen gücü ABD, siber alanın oluşturduğu yeni gerçeklere kurumsal yanıtın verilmesinin ön saflarında yer almaktadır. Bunu en güzel ABD'nin siber uzay konusunda liderlik pozisyonunda ilerleyerek, siber tehditlere karşı bilinen en güçlü ulusal güvenceleri oluşturması ve yenilikçi ruhuyla diğer hükümetlere örnek olmasında görebiliriz. Ayrıca siber güvenlik açıklarıyla mücadele için istihbarat, askeri vb. sorumlulukları çok çeşitli federal, özel sektör veya CERT / CC gibi departmanlara dağıtmıştır. Böylece kuruluşların sahip olduğu göreceli teknolojik avantajlar sayesinde dış tehditler ve veri eksikliği ile oluşan güvenlik ikilemine karşı

ajanslar arasında paylaşım, işbirliği ve teknik yeterlilik için çalışmalar yürütmüştür.[283]

ABD'nin uluslararası sistemdeki bu rol model tavrı kendi içindeki uygulamalarından da kaynaklanmaktadır. Özellikle 2001 olaylarından sonra ABD, internet güvenliği politikasında önemli bir revizyona giderek İç Güvenlik Bakanlığı (DHS) 'ye siber internet güvenliğinin sağlanması, acil durum planları ve uyarı sistemlerinin geliştirilerek savunmanın yapılması için sorumluluk verdi. 2003 Siber uzay stratejisiyle siber sistemin savunmasında CERT / CC işbirliği ile ulusal bir CERT (US-CERT) şeklinde ikili bir yaklaşım getirdi. Sonuç olarak, DHS daha önce ihmal edilmiş bir savunma alanı için sorumluluk üstlendi. (federal sivil ağlar (.gov alan adları). Ancak bütün bu gelişmelere karşın internet savunma stratejilerinin bölümlendirilmesi yönündeki yasal bir çerçevede sıkıntılar vardır. Bu sıkıntılı süreçte Amerika Birleşik Devletleri bugün üç ana araç kullanmaktadır: politik diplomasi, askeri güç ve ekonomik güçtür. ABD ulusal güvenlik stratejisi ve etkinliğini sağlayabilmek için bu üç temel stratejik işlevin bir araya getirilerek uygulanması gerekir.[284]

Siber güvenlik için geçerli olan bu üç ana araç kullanılarak oluşturulan Amerika'nın en büyük stratejisinin amacı ve geleceği ABD'nin kurmuş olduğu ittifak sistemlerini korumak ve günün şartlarına göre yeniden tanımlamaktır. Bu tanımlamayı oluşturmasındaki en önemli birimse ordudur. ABD orduda tüm savaş türlerine karşı mücadele edebilecek esnek bir yapı oluşturmaktır. Bu yüzden siber uzayda aktif faaliyet yürütmek için ordu birimi olarak Siber Kuvvetler Komutanlığını kurmuştur. Aynı zamanda, NATO ittifakında bu ordunun benzeri bir yapı kurulmasını sağlayarak geçmiş ittifak deneyimini geleceğe yönelik şekillendirmektedir.

ABD'nin bu yeni ordu birimini kurarak siber uzay alanına odaklanmasının üç temel sebebi vardır. Birinci sebep; uzun menzilli bombardıman uçaklarının, kıtalararası balistik füzelerin ortaya çıkmasıyla beraber topyekûn bir nükleer çatışma ihtimalinin ortaya çıkması sonucu ülkelerin kendini savunma ihtimalinin azalması

[283]Nazli Choucri, Stuart Madnick ve Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives", Information Technology for Development, Cilt.20, No.2, Yıl.2014, ss.96-121.
[284]Richard L. Kugler, "Policy Analysis in National Security Affairs: New Methods for a New Era", National Defense University Press, Washington, 2006, ss.87.

yüzünden savaşları bu tarz yeni bir çatışma boyutuna dönüştürmek. Bir diğer sebep; teknoloji, imalat ve finansta Amerika'nın tartışmasız üstünlüğünün azalarak özellikle Çin'in bu alanda güç kazanmasından dolayı bu alanı kendi lehine etkili bir şekilde kullanmaktır. Üçüncü ve son sebep "Endüstri 4.0 ve Toplum 5.0" çerçevesinde teknolojinin gelişmesi ve internetin hayatımıza girmesiyle bilginin önem kazanması ve dünyanın birbirine daha bağımlı hale gelmesiyle yeni teknolojik değişimlere ve oluşabilecek tehditlere karşı önlem almaya ayak uydurmaktır.

Küresel veya bölgesel siyaset açısından ABD'nin uluslararası ilişkilerdeki konumunu belirleme çabalarında stratejik ön alıcılık doktrini ya da yaygın kullanımıyla Bush Doktrini de önemli bir süreç oluşturmuştur. Stratejik ön alıcılık doktrini, "haklı savaş" kavramı ya da yaygın kullanımıyla Bush Doktrinidir. Haklı savaş kavramıyla birlikte küreselleşmenin geçirdiği evrim ve teknolojik gelişmeler sonucunda 21. yüzyılda ABD tehdit olarak algıladığı ülkelere gerçekleştireceği müdahalesini, yaşayacağı çatışmasını, güç parametrelerini, caydırıcı unsurlarını, tehdit ve güvenlik algılarını haklı göstermeyi hedeflemiştir. Örneğin; bu doktrinin ilk uygulama sahasını Irak savaşı oluşturmuştur. İkinci ABD-Irak Savaşında Bush hükümeti konvansiyonel saldırı öncesinde Irak ağlarına hacker'lar vasıtasıyla girerek psikolojik bir savaş yürütmüştür. Sonrasında "Şer Ekseni" olarak ilan edilen ülkelerden biri olan İran'a karşı konvansiyonel bir savaşın etkilerinin olumsuz sonuçlar doğuracağından yola çıkan ABD ve İsrail aynı hedeflere ulaşabilmek için siber savaş ve normal savaşı bir arada yürüten Stuxnet silahını ortaya çıkarmıştır. Bu sebeple; Neocon'lar tarafından yönlendirilen ABD Stratejik hedeflerine ulaşmada siber silahlar önemli bir araç olmuştur.[285]

Ayrıca milli güç unsurları coğrafya, nüfus, doğal kaynaklar, ekonomik güç, askeri, politik, psikolojik ve enformasyon gücüdür. Milli güç hedeflerine yönelik gerçekleştirilen saldırılarda yumuşak güç kavramını ortaya çıkarır. Geçmiş savaşlardan farklı olarak günümüz siber savaşları ne sert güç kullanma ne de yumuşak güç kullanma şeklindedir. Bu savaş türleri bütün boyutları kapsamakta olan "akıllı güç" (smart power) olarak adlandırılmaktadır. Akıllı güç olarak kullanılan bu silahlar uluslararası ilişkilerin doğasındaki çatışma olgusu ve bunun beraberinde getirdiği güvenlik çalışmalarını her geçen gün dönemin koşullarıyla birlikte yeniden

[285]Abdullah Özkan, "21. yüzyılda ABD'nin Küresel Stratejileri", Tasam Yayınları, İstanbul,2006 ss.11-15.

şekillendirmektedir. ABD sahip olduğu eşsiz konumla, yumuşak güç araçlarını etkili bir biçimde kullanarak klasik hegemonyacı bir güç olmak yerine dünyaya liderlik yapan bir güç olma amacıyla dış politikada bir Amerikan kültürü yaratmıştır.[286] Böylece; Neoconlar ve ABD yeni Amerikan yüzyılı projesi ile Pax Americana'dan Mutlak Hegemonyayı hedeflemeye başlamıştır. Bu sebeple, günümüz dünyasını şekillendiren interneti bir diğer ifadeyle siber uzayı, ilk olarak kendi himayesinde geliştirdiği için en güçlü şekilde kullanmayı hedeflemektedir. Hedef küresel hegemonyadır. Peki, gerçekler nedir? Gerçekler siber Dünya'nın anarşik yapısıdır. Çin ve Rusya bu anarşik yapıda Amerika'ya hegemon olma fırsatını tanımamaktadır. Bu sebeple Amerika Ulusal Savunma Stratejisini oluşturmak zorunda kalmıştır.

Amerika bu strateji kapsamında da kendisine düşman olan ülkelere karşı deneme saldırıları gerçekleştirmektedir. Örneğin; 7 Mart 2019 tarihinde ABD tarafından Venezuela'ya yönelik gerçekleştirildiği iddia edilen siber saldırıda; tüm ülkeyi karanlığa gömen elektrik kesintileri meydana gelmiştir. Devlet Başkanı Nicolas Maduro, ülkenin neredeyse tamamını ışıksız bırakarak, iletişimi ve internet erişimini de sekteye uğratan elektrik kesintisinin ardından bu sabotajı araştırmak için Rusya, Çin, İran ve Küba'dan uzmanlarla bir komisyon kurulması talimatı vermiştir. Aynı zamanda, Devlet Başkanı Nicolas Maduro saldırıdan ABD yi sorumlu tutmuştur.[287]

Irak, Suriye, İran ve son olarak da Venezuela ya yönelik ABD tarafından gerçekleştirildiği iddia edilen bu siber saldırılar ABD'nin önleyici müdahale bakışında siber yöntemleri kullandığını gösterir. Çünkü yumuşak güç kullanımının aslında en güzel örneğini oluşturan siber savaşlar uluslararası terörizm faaliyetleri adı altında ülkelere kendilerini gizleme imkânı sunmaktadır. Bu doğrultuda; Joseph Nye ve yumuşak güç unsuru kavramı; ABD'nin siber dünya 'da hâkim olmak için uygulamaya koyduğu siber stratejilerini şekillendiren bir kaldıraçtır. Özetlemek gerekirse küreselleşmeyle birlikte dünyayı birbirine tamamen bağımlı hale getiren küresel ağ internet yumuşak güç oluşturmuştur. Böylece ekonomiden, finansa, enerjiden sağlığa tüm hayati alanlar siber uzay alanına geçmiştir. Buda yumuşak güç

[286]Gültekin Sümer, "Amerikan Dış Politikasının Kökenleri ve Amerikan Dış Politik Kültürü", Uluslararası İlişkiler, Cilt 5, Sayı 19, Güz 2008, ss. 119-144.
[287]Ivan Alvarado, Venezuela'da Darbe Girişimi, Sputniknews, 08.03.2019, https://sptnkne.ws/kTjW ET.26.02.2020.

kullanma kapasitesini tüm ülkeler açısından arttırmıştır. Böylece dünya sürekli bir savaş halinin olduğu bir anarşik hale dönüşmüştür. Bu sebeple; siber uzayın hâkim olduğu günümüzde 7/24 savunma ve saldırı stratejisi oluşturma çabası vardır.[288]ABD'de bu düzende başrolü çekmektedir.

4.1.1. ABD'nin Siber Savaş Kabiliyetlerinin İncelenmesi

ABD, 2 Kasım 1988'deki ilk internet solucanı vakasından sonra ABD hukukunda siber kovuşturmaya neden olacak güçlüklere karşı düzenlemeler geliştirilmeye ve USCERT'ler kurmaya başladı. Siber saldırıların yarattığı tehditler zaman içinde büyüdükçe, ABD yasası iç hukukta ve uluslararası hukukta siber saldırılara uygulanabilecek belirli ilkeler hakkında konuşmaları ve tartışmaları arttırmaya başladı. Bu tartışmalar ışığında ABD'yi diğer ülkelerden ayıran gerçek ortaya çıkarak ABD'deki kritik altyapının çoğu özelleştirildi. Zaten ABD'de bu sebeple uluslararası hukuk içerisinde bir üst otorite kurulması, hukuk düzenlemesindeki cezai ve yaptırım kararlarının belirlenmesi ve sorumlunun nasıl belirleneceği gibi kriterlere karşı çıkılmıştır.

2003 yılında Bush yönetimi siber alanı kritik ulusal altyapıların sinir sistemi olarak açıklamıştır.[289] Bu açıklama sonrasında gelişen ABD siber politikası, 2008'de dönemin Başkanı Bush'un kapsamlı Ulusal Siber Güvenlik Girişimi'ni kurmak için başkanlık direktifini imzalamasıyla süreç daha da belirginleşti. İlk olarak, DHS ağ bağlantılarının sayısını azaltmakla görevlendirildi. İkincisi, federal web sitelerine giden ve web sitelerinden gelen trafiği izleyen isteğe bağlı bir DHS programı, Ulusal Güvenlik Dairesi makamına devredildi. Son olarak, CNCI planı doğrultusunda Ar-Ge'yi arttırmayı, siber karşı istihdamı koordine etmeyi amaçlayan çeşitli hükümleri ve hükümet kuruluşları arasında bilgi paylaşımını teşvik etmeyi hedefledi. Mayıs 2006'da, ABD Dışişleri Bakanlığı'na virüs bulaştığı yönündeki açıklamalar bir füzenin kurulmasından önce gerçekleştirilen ilk testler olmuştur. Çünkü siber saldırılar, üretken bir ağın, yani ağa bağlı zayıflıklarını ortaya çıkarmaktadır. Böylece bu stratejiyle birlikte sistem esnekliği ve güvenlik riski katlanarak artmakta rakipler

[288]Abdullah Özkan, 21. yüzyılda ABD'nin Küresel Stratejileri, Tasam Yayınları, İstanbul,2006 ss.89-92.
[289]Derek S .Reveron, "Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World", Georgetown University Press, Washington, 2012.

ise bu esnek güvenlik riskini barındıran yapıları kendi çıkarları doğrultusunda kullanmaktadır. 2008 yılında ABD ordusunun Ortadoğu'daki bir üstünde askeri bilgisayar ağ sistemlerine takılı olarak kullanılan bir bilgisayara takılan taşınabilir bellekle saldırı düzenlendiği ve gizli belgelerin yabancı istihbarat kurumlarının eline geçtiği resmi ağızlarca açıklandı. Yabancı bir istihbarat teşkilatı tarafından yerleştirilen flash sürücünün zararlı bilgisayar kodu hem sınıflandırılmış hem de sınıflandırılmamış sistemlerde tespit edilmeden yayılmıştır.[290] Sonuç olarak, ABD Savunma Bakan Yardımcısı William J. Lynn bu saldırıyı "ABD askeri bilgisayarlarının en önemli ihlali olarak sınıflandırdı ve önemli bir uyandırma çağrısı olarak hizmet ettiğini" söyledi. Çünkü operasyon el planlar, gözetim verileri ve silah planları da dâhil olmak üzere rakipler ABD ağlarından binlerce dosya edindiler. Böylece büyük bir silahlı kuvvetlerin bilgi savunması yeniden oluşturulmak zorunda kaldı.

Amerika'nın siber alanı korumada başarısızlığını en acil ulusal güvenlik sorunlarından birisi olarak gören dönemin Başkanı Barack Obama Ekim 2009'u ulusal siber güvenlik bilinci ayı olarak ilan etti.[291] Bu açıklamadan bir ay sonra eski bir NATO komutanı, '' Siber güvenlik tehdidi gerçektir."[292] şeklinde açıklamada bulunmuştur. Her ne kadar ABD'nin en üst kademesinden siber güvenlik hakkında bilinçli açıklamalar gerçekleştirilse de bürokratik adaptasyonun önündeki engeller ve verimsiz organizasyon yapıları sorunu pekiştirerek tehditleri arttırır. Bu yüzden ABD siber politikaları ve mekanizmaları büyük ve karmaşık olsa da uygulama aşaması diğer hükümetlere önemli sinyaller vermiş ve bir model oluşturmalarına yardımcı olmuştur.

Bu model kapsamında 2010 yılında ABD Siber Komutanlığı'nın (USCYBERCOM) kuruluşu "tam spektrumlu askeri siber operasyonları yürütme" misyonu ile meydana gelen değişiklikleri göstermektedir. Bu değişiklikler, silahlı çatışma yasasının siber operasyonlar için nasıl geçerli olduğu ve siber teknolojilerin

---

[290]Washington Post, ABD Savunma Bakan Yardımcısı: Bütün Askeri Sırlarımız Çalındı, Hürriyet, 26.08.2010, https://www.hurriyet.com.tr/gundem/abd-savunma-bakan-yardimcisi-butun-askeri-sirlarimiz-calindi-15630544, ET.12.02.2020

[291]Derek S .Reveron, Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World, Georgetown University Press / Washington, Dc, 2012

[292]CSIS Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency, Aralık 2008, ss.49-65. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf ET:20.01.2020.

devletler tarafından kullanımı arasındaki ilişkiyi temel almaktaydı. 2011 yılına gelindiğinde; Pentagon'un iki numaralı ismi William J Lynn, Savunma Bakanlığı'nın siber alanı 'militarize edemeyeceğini belirterek güçlü siber savunmaların kurulması, bir donanmanın okyanusu militarize etmeye çalışması gibi olduğunu belirtmiştir. Fakat bu durum da farkında olmadan güvenliği analiz etmek için siber alandaki fikirlerin ve kavramların militarize edildiğini göstermektedir. Yani kısaca özetlemek gerekirse, William J Lynn ve siber uzaya ilişkin 2011 Pentagon raporu, savaşa değil silahlara odaklanarak, savaş analojisinin sınırlarının çizilmesi gerektiğini belirterek siber savaşta suçun sağladığı avantaj rolüne değinmiştir.

Siber suç'un oluşturduğu tehditlere karşı ABD'nin çabasına kısaca bakarsak, ABD, çekinceleriyle Siber Suç Konvansiyonuna taraftır. Siber tehditlere yanıt olarak kurumsal yapılanmada INTERPOL'ün 7/24 ağıyla bazı yapısal benzerlikleri paylaşan IC3, ABD'nin internet suçlarının raporlanması için merkezi bir irtibat noktası sağlaması amacıyla oluşturulmuştur. Ulusal bir raporlama sistemi için başarılı bir model olarak hizmet veren IC3'ün en büyük dezavantajı ise toplam siber olayların sadece bir kısmını işlemesidir. Çünkü FBI anketlerinin de belirttiği üzere çoğu internet suçu bildirilmemektedir. Bu yüzden FBI 2003 yılında kurduğu işbirlikçi Bilgisayar Suç Görev Kuvvetleri ile 2006 yılında kurduğu yerel bilgisayar korsanlığı ve fikri mülkiyet birimleri ile birlikte polis teşkilatlarının yerel siber suçları soruşturmasına yardımcı olmaktadır. Bu doğrultuda siber suçların önlenmesine yönelik ABD içinde geliştirilen kurumsallaşma sürecinde de siber tehditlere verilen yanıtlar erken bir aşamadadır. Bundan dolayı hükümetlerin ulusal güvenlikle ilgili siber suç soruşturmaları, kovuşturmalar, tutuklamalar ve demografik veriler hakkında istatistiksel verileri kamuya açıklaması da pek olası değildir. Zaten, birçok ülkedeki gibi ABD'de de siber suçlarla ilgili güçlü ve yeterli mevzuat bulunmamaktadır.

ABD'nin siber suç bakışından tekrar savaş bakışına dönüş yaparsak; ABD siber savaş teknolojisinin gelişmesine yönelikte çok önemli stratejik hamleler gerçekleştirmektedir. Örneğin; bilgisayar endüstrisinin ve dijital teknolojinin gelişmesinde merkez rol oynayan Silikon Vadisinde; Assle, İntel, Hawlett, Packard, Oracle ve IBM gibi saygın yüksek teknoloji şirketleri günümüz siber savaşlarının

gelişmesinde önemli bir dönemeci yaratmıştır.[293] Bilgisayar ve Telekomünikasyon ilişkisiyle yaratılan bilgisayar ortamındaki iletişim çerçevesinde siber ordu ve siber casusluk adı altında siber saldırılar ve siber savaşların ilk fitili bu bölge sayesinde ateşlenmiştir.[294] Bu bölgede oluşturulan arge faaliyetleri çerçevesinde ciddi siber silahlar geliştirilmekte bu silahlar ise ABD'nin ulusal çıkarları doğrultusunda gerekli birimlerce kullanılmaktadır. Gelişen yıllarda da siber uzaya ayrılan bütçeler bu ortak çaba neticesinde sürekli artış göstermiştir. Bu durumu ABD Hükümetinin 2017-2020 Mali Yılı İçin Siber Güvenlik İçin Önerilen Bütçesinde görebiliriz.[295]

Silikon vadisinde geliştirilen yeni ve özel yazılımlar sayesinde siber tehditler artık sadece bilgisayar sistemlerine verdikleri zararlar (sistemlere sızma, sistemlerden bilgi çalma ve sistemlere asılsız bilgi koyma) ile sınırlı kalmamaktadır. Bir ülkenin kritik olarak kabul edilebilecek haberleşme sistemlerine, bilgisayar sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde, asimetrik bir harp çeşidi olarak ortaya çıkmasına yol açacak siber silahlar bu bölgede üretilmektedir. Örneğin; The Guardian Gazetesi ve Wall Street Journal'ı kaynak gösterek Hürriyet gazetesinde yayınlanan bir habere göre;[296] The Guardian Gazetesi, Pentagon'un açıkladığı yeni stratejinin, silahlı saldırılar kapsamına siber silahları da dâhil ederek, Birleşmiş Milletler'in (BM) meşru müdafaa hakkına adapte olabileceğini belirtmiştir. ABD'ye yönelik siber saldırıların önüne geçmek için resmi bir strateji oluşturmayı amaçlayan Pentagon, hazırladığı bu yeni stratejisi çerçevesinde, ABD'nin yabancı bir ülkeden gelecek siber saldırıları "savaş nedeni kabul edebileceği ve askeri müdahaleyle karşılık verebileceğini" belirtmiştir. Wall Street Journal'ın da duyurduğu bu stratejinin ne kadar caydırıcı olacağı konusunda kararsızlık olsa da bu yeni strateji, siber saldırıların geleneksel bir savaş ilanına denk gelebileceğini açık bir şekilde ortaya koymaktadır. Bir diğer örnek ise ABD'nin yüzyıllardır süre gelen stratejik ortağı olan İngiltere'nin Savunma Bakanı Nick

[293] Nick Dyer Witheford, "Siber Marx Yüksek Teknoloji Çağında Sınıf Mücadelesi", Çev.Çakıroğlu, A. Aykırı Yayıncılık, İstanbul, 2004 Ss 145.
[294] Witheford, S.M.Y.T.Ç.S.M., ss.183
[295] Clement, C. Proposed Budget Of The U.S. Government For Cyber Security İn FY 2017 To 2020, Statista, March 2019, https://www.statista.com/statistics/675399/us-government-spending-cyber-security/ ET.31.01.2020.
[296]New York Times/Guardian, Pentagon'dan Tarihi Adım, Hürriyet, 01.06.2011, http://www.hurriyet.com.tr/gundem/pentagondan-tarihi-adim-17925614 ET.05.02.2020.

Harvey'in sözleridir. Nick Harvey, "siber alandaki eylemlerin gelecekteki savaş alanlarının bir parçasını oluşturacağını" belirtmiştir.[297]

Bu örnek açıklamalar ışığında ABD'nin bu çatışma çeşidinde ulaşmak istediği hedef ve strateji diğer aktörlerden farklı olabilir. Rusların ABD'ye yönelik siber operasyonları bilgi toplama ve gelecekteki hedeflere ilişkin saldırı kabiliyetleri geliştirmeye yöneliktir. Çin'in motivasyonu para kazanmaktır. Amerikan siber stratejisi sanıldığı gibi savunma değil, Amerikan çıkarları ve etkisini geliştirmek için saldırı üzerine kuruludur. ABD, siber güvenlikte savunma ve saldırıyı birleştirmiştir. Dünya ekonomisini kontrol etme hakkına sahip olduğu varsayımı ile bankacılık işlemleri, borsa faaliyetleri ve diğer tüm ekonomik girişimleri kendi siber sistemleri üzerinden denetleme ve cezalandırma hakkını kendinde görmektedir. IMF ve Dünya Bankasının ABD'de konumlanması para gönderimini sağlayan SWİFT sisteminin ABD'de kurulması bunun en güzel resmedilmiş halidir. Kısaca günlük yaşamımız, ekonomik canlılığımız ve ulusal güvenliğimiz istikrarlı, güvenli ve esnek bir siber alana bağlıdır. Siber alan hem fiziksel hem de siber tehditlerden ve tehlikelerden kaynaklanan çok çeşitli risklere karşı savunmasızdır. Bu kapsamda siber güvenliğin sağlanması amacıyla 16 Kasım 2018'de dönemin başkanı Trump, 2018 Siber Güvenlik ve Altyapı Güvenliği Ajansı Yasasını imzaladı. Bu dönüm noktası yasa DHS içindeki eski Ulusal Koruma ve Programlar Direktörlüğü'nün (NSSD) misyonunu yükseltmekte ve Siber Güvenlik ve Altyapı Güvenliği Ajansı'nı (CISA) kurmaktadır. Böylece CISA, siber saldırılara karşı savunma için ulusal kapasiteyi geliştirerek ve siber güvenlik araçları, olay müdahale hizmetleri ve ortak departmanların ve ajansların temel operasyonlarını destekleyen '.gov' ağlarını korumak için federal hükümetle birlikte çalışmaya başlamıştır.[298]

Ayrıca Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS) gibi kuruluşlar ABD'nin siber strateji gerçekleştirmesinde büyük katkı sağlamıştır. Örneğin; dünyanın en büyük zorluklarını ele almak için pratik fikirler geliştiren, ulusal güvenliğin geleceğini tanımlamayı amaçlayan ve kar amacı gütmeyen bir politika araştırma kuruluşu olan Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS), ülke ve

[297]Guardian, İngiltere'den Gizli Siber Silah, Hürriyet Gazetesi, 01.06.2011, http://www.hurriyet.com.tr/gundem/ingiltereden-gizli-siber-silah-17916922 ET.10.10.2019.
[298]DHS, Cybersecurity, U.S. Department of Homeland Security, October 23, 2019, https://www.dhs.gov/topic/cybersecurity, ET.28.02.2020.

bölgeye göre mevcut siber stratejiler ve yasalar çerçevesinde küresel siber stratejiler endeksi yayınlamıştır. Bu Endeks, sivil ve askeri ulusal siber savunma, dijital içerik, veri gizliliği, kritik altyapı koruması, e-ticaret ve siber suçları ele alan birçok ulusal stratejiyi içermektedir. [299]Buna ilave olarak CSIS, BM Silahsızlanma Araştırmaları Enstitüsü ile ortaklaşa, siber uzayda sorumlu Devlet davranışına ilişkin uluslararası normların tartışmasını açmak, genişletmek ve uluslararası toplum tarafından daha fazla ilerlemeyi desteklemek için yeni fikirler belirlemek için çalıştaylar gerçekleştirmiş olsa da bu fikirler tam olarak ABD yetkilileri tarafından olumlu bir karşılık bulmamıştır.

2020 yılına geldiğimizdeyse ABD devlet kurumları ve özel sektör şirketleri, Çin Devlet Güvenlik Bakanlığı'na (MSS) bağlı tehdit aktörlerinin siber saldırılarına karşı yüksek alarm durumunda oldukları konusunda uyarıldı.[300]Çünkü Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) ve Amerika Birleşik Devletleri Adalet Bakanlığı tarafından siber tehdide ilişkin 14/09/2020 tarihinde ortak bir güvenlik danışmanlığı yayınlandı.[301] Bu doğrultuda Çin ve Rusya'nın hamlelerini tehdit olarak gören ABD, yapay zeka projelerine hız verdi. Bu kapsamda; Çin ve Rusya'nın yapay zekâ kullanımının ABD ve Avrupa'nın ortak değerlerini tehdit ettiğini söyleyen ABD Savunma Bakanlığı Müşterek Yapay Zeka Merkezi Direktörü Korgeneral John Jack Shanahan, teknoloji alanında "nefes kesen" hızdaki gelişmeler nedeniyle yapay zekayı Amerikan ordusuna dâhil etme sürecini hızlandırdıklarını açıkladı.[302]

Sonuç olarak; günümüzde teknolojik gelişmelerin etkisiyle ülkeler, aniden büyük bir kriz yaşayabilir böylece iç ve dış dengesini bir anda kaybederek hızlıca yok olabilir. Teknolojik gelişmeler sayesinde geri plandayken bir anda üst noktalara çıkabilir aynı zamanda en üst noktada yaşamını sürdürürken bu konumunu

---

[299]Center For Strategic and İnternational Studies(CSIS), Global Cyber Strategies Index, 2020 https://csis-website-prod.s3.amazonaws.com/s3fs-public/Cyber%20Regulation%20Index%20V2%20%28002%29.pdf , ET.06.10.2020.

[300] Sarah Coble, CISA Sayıs Chinese Hacking Groups Warning, İnfo Security Magazine, https://www.infosecurity-magazine.com/news/cisa-sayıs-chinese-hacking-groups/, ET. 17.09.2020.

[301]The Cybersecurity and Infrastructure Security Agency (CISA) has consistently observed Chinese Ministry of State Security (MSS), Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity, https://us-cert.cisa.gov/sites/default/files/publications/AA20-258A-Chinese_Ministry_of_State_Security-Affiliated_Cyber_Threat_Actor_Activity_S508C.pdf, ET.17.09.2020.

[302]Değer Akal, ABD Ordusunda Yapay Zeka Devri, Deutsche Welle Türkçe, 16.01.2020, https://p.dw.com/p/3WGJu ET28.02.2020.

kaybedebilir. Yani teknoloji ve siber uzay aslında tüm devletlere güvenlik politikalarını oluşturmalarında hem avantaj hem de dezavantaj sağlamıştır. Bugün dev Amerikan siber güvenlik alt yapısı bile çökertilebilmektedir. Bu durum ve bilinmezlikse anarşik yapıyı daha da arttırmaktadır. Bu anarşik yapıda her ülkenin dış politika ve milli güvenliğini sağlama stratejisi farklıdır. Bu yüzden Amerika Birleşik Devletleri ve diğer birçok ülke, Çin, Rusya, İsrail vb. sanal boyutta çatışmaya hazırlanmaktadır. Örneğin; Amerika Birleşik Devletleri'nde dönemin Başkanı Obama dijital altyapıyı bir ‘‘ stratejik ulusal varlık olarak göstermiştir. Sonrasında ABD'nin geleceği için ön gördüğü "Aktif Milli Stratejiyle"yi ilan ederek 2010 yılında siber uzaya yönelik ordu birimi kurması bunun en güzel kanıtıdır. Bu siber ordu komutanlığının başına ise sivil kökenli Microsoft'un eski güvenlik şefi Howard Schmidt'in atanması bu ordunun diğer tüm ordu birimlerinden farklı bir prensipte olacağını gözler önüne sermiştir. ABD'nin başlattığı bu süreç domino etkisiyle diğer ülkelere de sıçramış ve onlar da kendi siber ordu birimlerini kurmuştur. Bu ülkelerden biride Türkiye'dir. Türkiye'de 2013 yılında siber komutanlığın kurulmasıyla birlikte bu süreç başlamış olsa da bu orduyu kurmak siber alanda mücadele edebilmek için tek başına yeterli değildir. Çünkü siber mücadele yürütebilmek için savunma sanayi %100 milli yazılım kullanmalı, kendi silahlarımız üretilmeli ve bağımlılık mümkün olduğunca azaltılmalıdır. Bu bağlamda Türkiye'de Amerika'daki gibi çalışan bir ordu şekli bulunmadığını açıkça söyleyebiliriz.

Aynı zamanda; ABD, 2011 yılında siber uzay operasyon strateji prensibinde, siber güvenliğin devlete ait tüm birimlerin ortak çabası ile mümkün olacağı belirterek ABD Savunma Bakanlığı öncülüğünde uluslararası yasalara uygun olarak siber saldırı ve savunma faaliyetlerini geliştirmek için gerekli kurumsal yapılanma, teknik ve araç ekipmanları ve görevli personelleri oluşturmuştur. Çünkü; ABD Siber Güvenlik yapısında meydana gelebilecek bir tehdit sosyal ve kültürel alanda da çok büyük sonuçlar doğurabilir. Örneğin; göçebe ruhlu Amerikan toplumu için 4 temel husus bulunmaktadır. Bunlar uygun fiyatlı petrol(enerji), otomobil (ulaşım), internet(sosyal medya) ve hamburger (Gıda)dir. Bunları derinden etkileyecek bir yapı tüm ülkeyi etkiler. Bu durumda Amerika'da savaş sebebi olarak sonuçlanabilir.

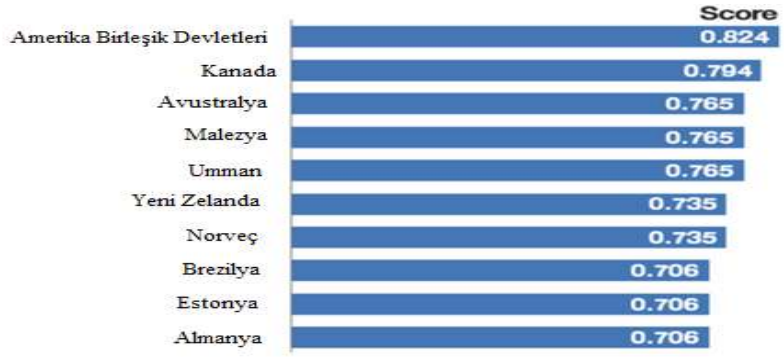
4.1.2. ABD'nin Siber Savaş Faaliyetleri

Ülkeler rakiplerinin siyasal otoritelerini zayıflatmak için ekonomik ve sosyal sistemini, nüfusunun psikolojik durumunu, toplumu istikrarsızlaştıracak yapıları harekete geçirmek gibi faaliyetleri siber ortamda yürütmektedir. Asimetrik tehdit unsurlarını kullanan ve aktif gerginlik içeren bu siber çatışma sürecinde egemen bir devlete veya aktöre yönelik haksız müdahaleler gerçekleşmektedir. Bu doğrultuda Google, Facebook ve Twitter gibi dünyanın en önemli sosyal medya sitelerinin hepsinin ABD'de kurulu olduğu (viral sorunlu)yapıda Çin ve Rusya gibi büyük ülkeler kendi milli güvenliklerini sağlamak için bir dizi çözüm üretmektedir.[303]

ABD tarafından başlangıçta iyi amaçlar için üretilen ve kısa bir zamanda tüm dünyaya yayılan internet infaz, casusluk, ceza, suç veya savaş hukukunu delmek gibi kötü amaçlarla kullanılan bir silah haline dönüşerek viral sorun haline gelmiştir. Örneğin; Stuxnet'ten beri devlet kurumları ve özel güvenlik şirketleri Avrupa ve Amerika'da çoğaldı. Çin ve Rusya gibi siber alanda güçlü ülkelerde bu alanda gözetim, kontrol ve millileşme mekanizmalarını uygulamaya koydu. Şüphesiz siber alanda şuan için ülkelerin gerçekleştirdikleri tüm çabalara rağmen en önemli üç güç ABD, Rusya ve Çin'dir. İkinci kademedeyse İsrail, Fransa, Almanya ve İngiltere gibi ülkeler bulunmaktadır. Uluslararası Telekomünikasyon Birliği (ITU)'nun egemenlik ve yargı yetkisi konusunda anlaşma sağlanamadığından şimdilik siber ortamda kontrollü barış vardır. Yani ülkeler bu güçlerini aleni olarak birbirlerine karşı kullanmamaktadır. Bu kontrollü barış sürecinde ülkeler internette siberden korunmak için millileşerek kendi intranetlerini üretme ve diğer devletlere karşı kullanmak için makul siber saldırı silahları geliştirmeye devam etmektedir.

Yukarıda bahsettiğimiz gibi ABD her ne kadar siber uzayda en önemli güç olsa da siber uzayın kendine has yapısından dolayı aynı zamanda savunmaya en fazla ihtiyaç duyan ve kritik altyapıların internet bağımlılığından dolayı en güvensiz ülkedir. Amerika'nın kritik altyapısının bu şekilde olması yüzünden dönemin 2. Başkanı Bush siber alanının Amerika'nın işletim sistemindeki sinir sistemi olduğunu belirterek kontrol sistemleri için öneminden bahsetmiştir.[304] Siberin yaratıcısı ABD'nin bu konuya hassasiyetini aşağıdaki şekilde açıkça görebiliriz;

[303]Misha Glenny ve Camino Kavanagh, a.g.e. , ss.287-294.
[304]George W. Bush, National Strategy to Secure Cyberspace, Washington, Şubat 2003.



Şekil 8 Siber Ataklara En iyi Hazırlanan Ülkeler [305]

ABD'nin siber ataklara karşı bu hassasiyetini 2018 yılında Küresel Siber Güvenlik Endeksi'ne (GCI) dayalı olarak siber güvenliğe en fazla bağlılık gösteren ülkelerin sıralandığı aşağıdaki tablo doğrulamaktadır. Yasal, teknik, organizasyonel, kapasite geliştirme ve işbirliği gibi beş sütun çerçevesinde tüm ülkelerden elde edilen verilerin oranlamasıyla oluşan Tabloda da görüldüğü üzere Birleşik Krallık, GCI skoru 0,931 ile ilk sırada yer alırken ABD ise GCI skoru 0.926 endeks puanıyla ikinci sırada yer almaktadır.

Tablo 10 2018'de Küresel Siber Güvenlik Endeksi'ne (GCI) Dayanarak Siber Güvenliğe Bağlılığı En Yüksek Ülkeler [306]

	GCI Puanı	Yasal	Teknik	Örgütsel	Kapasite Geliştirme	İşbirliği
Birleşik Krallık	0,93	0,20	0,19	0,20	0,19	0,15
ABD	0,93	0,20	0,18	0,20	0,19	0,15
Fransa	0,92	0,20	0,19	0,20	0,19	0,14
Litvanya	0,91	0,20	0,17	0,20	0,19	0,16
Estonya	0,91	0,20	0,20	0,19	0,17	0,15
Singapur	0,90	0,20	0,19	0,19	0,20	0,13
İspanya	0,90	0,20	0,18	0,20	0,17	0,15
Malezya	0,89	0,18	0,20	0,20	0,20	0,12
Norveç	0,89	0,19	0,20	0,18	0,19	0,14
Kanada	0,89	0,20	0,19	0,20	0,17	0,14
Avustralya	0,89	0,20	0,17	0,20	0,18	0,14

[305]Downin, L. Why We Need To Measure Military Cyber Power, Weforum, 29.03.2018, https://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power , ET.31.01.2020.

[306]Clement, C. Countries With The Highest Commitment To Cyber Security Based On The Global Cybersecurity Index (GCI) İn 2018, Statista, Mart 2019, https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/ ET.31.01.2020.

Bu bağlamda siber güvenlik, içerdiği risk ve tehditler ile aktörlerin etkileşimleri bakımından karmaşık bir araştırma ve uygulama alanıdır. ABD'nin siber güvenlik çalışmalarını Jeopolitik ve Uluslararası İlişkiler bağlamında geleneksel güvenlik yaklaşımlarından ayıramayız. Zaten yukarıdaki tabloda ABD'nin bu ayrılmaz önemini ortaya koymaktadır. Bu sebeple geleneksel güvenlikte İsrail'in tamamen müttefiki olan ve stratejik olarak güvencesini sağlayan ABD özellikle Ortadoğu'daki politikalarında İsrail düşmanlığına sahip İran konusunda da İsrail'le aynı fikre sahiptir. Bu yüzden İran'ın nükleer silah geliştirme çabaları hem ABD hem de İsrail'de ciddi bir korku yaratmaktadır. İran'ın verdiği bu korkuya karşılık geleneksel güvenlik yaklaşımında İsrail Ortadoğu'da bulunan diğer ülkelerden nüfus ve yüz ölçümü olarak daha küçük olmasından dolayı ABD desteğine muhtaçtır. Fakat bu dezavantajlı durum siber güvenlikte çok daha ileridedir.

İsrail etrafındaki tüm ülkeler ile siyasi çekişmesi olan ve bu nedenle sadece fiziksel anlamda bir savunmanın yeterli olmayacağı, bekasını sürdürebilmesi için teknolojik alanda da savuma stratejisi geliştirmek zorunda olan bir ülkedir. Bu kapsamda İsrail siber güvenlikte başarı elde edebilmek için üç temel uygulama gerçekleştirmektedir. Bunlar: siber ordu kurulması, ulusal savunma kurumları ile özel sektör işbirliğinin kurulması ve siber güvenlik alanındaki girişimcilerin desteklenmesidir. Aynı zamanda, siber savaş için siber istihbaratı en iyi kullanan ülke olan İsrail, savunma bakanlığı (IDF)'na bağlı MOSSAD altında Unit 8200 ve C4I adında iki adet "elit birim" kurmuştur. IDF altındaki bu elit kurumların hepsi birbiri ile birlikte çalışmakta ve konvansiyonel savaşla birlikte kullanılmaktadır. İsrail'in bu özellikleri çerçevesinde İran, İsrail ve ABD'nin kendisine yönelik siber saldırılar gerçekleştirdiklerini iddia etmektedir. Bu konu hakkında iki güzel örnek bulunmaktadır. Bunlardan birincisi Arap Baharı'nda yaşanan gelişmelerde İran halkının da kışkırtılması, ikincisi ve daha önemli olanı ise stuxnet olayıdır. Kısaca bunları açıklarsak; ilk olarak hem İran seçimlerinde hem de Amerikan seçimlerinde karşılıklı olarak seçimlere siber saldırılar yoluyla müdahale yapıldığına yönelik karşılıklı suçlamalar bulunmaktadır. Bu çerçevede İsrail ve ABD, İran halkını ve muhalefetini hedef alarak Arap Baharı'nda yaşanan gelişmelerin bir benzeri şeklinde siber yöntemler kullanılarak rejime karşı ayaklanma tetiklenmiştir. İkinci olay İsrail

ve ABD'nin İran'a yönelik stuxnet adı altında gerçekleştirdiği siber saldırıdır. Bu saldırı çerçevesinde İran'da uranyum zenginleştirme tesislerindeki teknolojik süreçleri yöneten bilgisayarlar hedef alınmış ve nükleer faaliyetlerin durdurulması hedeflemiştir. Kısaca stuxnet sürecini açıklarsak;

Tarihteki, fiziksel etkisi doğrudan görülebilen ilk 'ciddi' siber saldırı olarak kayıtlara geçen ve 2010 yılında İran'ın uranyum zenginleştirme tesislerine yapılan saldırılarda kullanılan stuxnet isimli solucan, eğer bulaştığı bilgisayarda SCADA yazılımı bulunuyorsa, kendini aktive ederek bilgisayar ağına zarar verme özelliği taşıyordu. SCADA yazılımı, sanayi donanımını kontrol eden, motorları regüle eden, valfların açılıp kapanmasını sağlayan bir işleve sahipti. Özetle, Windows© güvenlik açığını kullanarak İran'da bulunan Natanz Uranyum Zenginleştirme Tesisindeki 984 adet SIEMENS marka santrifüjü hedef alan ve işlemez hale getiren bu saldırı, sadece 500 kilobayt büyüklüğünde bir dosya ile yapılmış ve İran'ın nükleer programının en önemli noktasını imha etmeyi başarmıştı.[307] Stuxnet'in internet ile bağlantısı olmayan SCADA Sistemini hedef alması Stuxnet'in USB bellek üzerinden bulaşan ve Windows işletim sistemini kullanarak yayılan bir solucan olduğunu düşündürmektedir. Stuxnet saldırısının asıl hedefi; İran nükleer tesislerinde kullanıldığı bilinen Siemens SCADA sistemlerinin yönetim yazılımı olan SIMATIC WinCC/Step7 yazılımına ulaşmaktır. Yani bugüne kadar oluşturulan tüm solucanlardan farklı olarak stuxnet tamamen hedefe özel olarak hazırlanmış bir silahtır. Böylece İran'ın Natanz tesislerindeki kontrol mekanizması etkilenmiştir.[308]

Stuxnet virüsü bir yıldan fazla bir süre İran ağlarının içinde bulunmuş ancak nükleer bilim adamları başlangıçta tesislerde çıkan sorunların bir seri arızadan kaynaklandığını düşündüklerinden anlaşılamamıştır. Bu durum stuxnetin mükemmel bir bütünlük içinde sinsiliğini ortaya koymuştur. Amacı tamamen siber savaş olan Stuxnet virüsünden zarar gördüğünü resmi olarak açıklayan İran, sanal âlemin reel âlem üzerinde ne kadar etkili ve ciddi boyutlara ulaşabileceğini herkese göstermiştir. İran'ın, ABD ve İsrail tarafından ortaklaşa olarak kendisine gerçekleştirildiğini iddia ettiği bu saldırı, endüstriyel sistemleri gizlice gözetleyen, gerektiğinde kendini

[307]Oğuz Bozoklu, ve Celal Zaim Çil, Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:1, 2017, ss.6- 26

[308]Şener Çelik, "Stuxnet Saldirisi ve ABD'nin Siber Savaş Stratejisi: Uluslararasi Hukukta Kuvvet Kullanmaktan Kaçinma İlkesi Çerçevesinde Bir Değerlendirme", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 15, Sayı: 1, 2013, ss.137-175.

yeniden programlayabilen siber saldırıların karışık bir siber savaş aracı olarak kullanıldığının göstergesidir.[309] Çünkü burada belirtilen ölçüt savaşın iki taraf arasında olan ve bir tarafın diğer tarafa isteklerini zorla yaptırdığı, ulusal iradesini hiçe saydığı bir yapıya işaret etmesidir. Doğal olarak siber savaşta bu yapının elektronik alanda gerçekleşen halidir. Stuxnet olayını aslında bir savaş provası şeklinde gerçekleşen çatışma örneği olarak görmemizin sebebi ise şunlardır;

İran'a göre nükleer gelişim kendisi için hak ve olması gereken bir şeyken ABD ve İsrail'e göre bu durum; kötü 'nün resmedilmiş hali olan ve ''Şer Ekseni'' olarak adlandırılan ülkelerden biri olan İran'ın daha büyük kötülük yaratma mücadelesidir. Bu sebeple; İran'ın güçlü alt yapısı çökertilmelidir. Askeri bir müdahalenin çok daha büyük etkileri olacağından Amerika Birleşik Devletleri ve İsrail'in çözümü uluslararası alanda suç olarak görülmeyen Stuxnet solucanını yaymak olmuştur. Siber Savaş'ın bir aracı olarak karşımıza çıkan bu siber silah siber savaş kavramının etkisinin ne kadar büyük olabileceğini tüm dünyaya göstermiştir. Böylece, siber savaş enstrümanları sayesinde güç santralleri, fabrikalar ve birçok teknolojik tesisin kontrolsüz bir silaha dönüşebilecek bir güç olabileceğini herkese göstermiştir.

Aynı zamanda bu siber silah birçok ülkeyi de alarma geçirerek özel önlem almasına yol açmıştır. Tüm dünyayı bu kadar etkileyen stuxnet solucanının arkasında kim olduğu resmi olarak diğer siber saldırılarda olduğu gibi kanıtlanamamıştır. Fakat İran bu saldırıdan bir grup hackerı suçlamak yerine İsrail ve Amerika Birleşik Devletlerini sorumlu tutmuştur. Bu ülkeler ise itiraf etmek veya sorumluluk almak istemediklerinden bu iddiaları asla kabul etmemiştir. İran'ın iddialarını destekler açıklamalar ise uzmanlardan gelmiştir. Analistler, Stuxnet yazılımının oluşturabilmesi için ileri bilgisayar tekniklerine sahip, çok iyi eğitim almış ve finanse edilmesi gereken hackerları içinde barındıran birkaç devletin böyle bir yazılımı üretebileceğini belirtmektedir. [310]

Eğer Stuxnet'i anlamak istiyorsak büyük resmi görebilmemiz çok önemlidir. İsrail asla İran'ın nükleer silah geliştirmesini istemeyen ülkelerin başında

[309]David. E. Sanger, Obama Order Sped Up Wave of Cyberattacks Against Iran, The Newyork Times, 1 Haziran 2012 https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html ET.10.10.2019.
[310] Nurullah Aydın, a.g.e. ss.137-152.

gelmektedir. Bu sebeple, İran'ın nükleer tesislerini durdurmaya yönelik bir saldırının arkasında İsrail'in olduğunu iddia etmek çok normaldir. Çünkü İsrail'e göre İran=Terör saldırıları, fanatikler, radikaller, dindar bağnaz ve acil durdurulması gereken bir tehdittir. Bu duruma stratejik açıdan yaklaştığımızdaysa şu hususu vurgulamamız gerekmektedir. Düşmanı durdurmak ve kazanmak için onun en değerli en hassas noktasından vurmamız gerekir. İran'ın en hassas noktası onun nükleer alt yapısı idi. Bunu durdurmak ise en çok ABD ve İsrail'in işine gelirdi. Bu yüzden ulaşılmak istenen hedef ve elde edilen sonuç kıyaslandığında siber strateji geliştirme eksikliğinin ülkelerin en hayati noktasını etkileyebileceğini görmüş oluyoruz. Ayrıca Stuxnet'in 13 gün boyunca gizli kalıp, beklemesi, gözlemlemesi ve sonrasında ele geçirdiği bilgiler çerçevesinde saldırısını gerçekleştirmesi onun planlı olduğunu göstermektedir. Geleneksel Savaşlar planlama ve taktik aşamasını içinde barındırır. Doğru zamanı bekleyip sonrasında saldıran stuxnet domino etkisiyle sürekli bir diğer sistemi etkileyerek ilerleyen bir silahtır. Bu yüzden İran'ın en kritik sistemlerinin çalışma prensibini bozarak İran'ın nükleer zenginleştirme çabasını yavaşlatmıştır. ABD ve İsrail bu saldırıyla birlikte İran'a "nükleer programını durdurmazsan seni böyle vururum" mesajı vermiştir. Burada önemli olan günümüz bilgi çağında; Bir devletin başka bir devletin bilgisayar sistemine ve ağlarına hasar vermesi ve kesintiye uğratması olarak tanımlanan Siber Savaş'ın aslında tam olarak bu şekilde yürütülüyor olmasıdır. [311]

Burada en önemli risk İsrail ve ABD tarafından gerçekleştirildiği iddia edilen bu saldırı eğer büyük ve güçlü Rusya ve Çin gibi ülkeler tarafından Amerika'ya karşı gerçekleştirilirse durumun ne olacağıdır? Ya da siber savaşlarda tahmin edilenden daha büyük felaketler ortaya çıkabilir mi? Bu ciddi bir sorudur. Bu sorular altında ABD ve İran arasındaki mücadeleye döndüğümüzde ABD ve İsrail'e karşı konvansiyonel bir savaşta hiçbir şansı bulunmadığını bilen İran ise kendisine yönelik gerçekleştirilen bu saldırılara karşı aktif bir strateji uygulamaktadır.

İran'ın uyguladığı aktif strateji çerçevesinde ABD ve İsrail tarafından siber saldırılarla birlikte uygulanabilecek muhtemel bir konvansiyonel askeri müdahaleyi bu ülkeler için maddi ve siyasi anlamda oldukça maliyetli hale getirerek bekasına yönelik bu girişimden onları caydırmayı hedeflemektedir. Bunu sağlamak için de

[311]K.Knake ve Clarke, ag.e. ss.3-9

klasik bir silahlanma yarışından ziyade en büyük tehdit olarak gördüğü ABD ve İsrail'in zayıf yönlerine, hassas noktalarına odaklanarak bu ülkeler ile siber veya hibrit alanda karşılaşmayı tercih etmiştir. Bu kapsamda siber yöntemler ve istihbarat örgütleri vasıtasıyla Hizbullah ve Hamas gibi örgütleri kullanma yoluna gitmiştir. Bir diğer örnekte; 2020 yılının başlarında ABD'nin Kasım Süleyman'iyi öldürmesinden sonra Irak'taki iki ABD üssüne füze saldırısıyla misillemede bulunan ve siber saldırı düzenleyip ABD'nin İHA'larını yere indiren İran yetkilileri " Eğer ABD karşılık verseydi bölge çapında büyük bir harekâtın başlangıcı olacaktı" şeklinde açıklamada bulunmuştur. Yani bir siber saldırı resmi olarak misilleme olarak kullanılmıştır.[312] Bu olay sonrasında ABD-İran çatışmasının siber uzaya geçebileceği konusunda da özellikle Amerikalı uzmanlardan ciddi uyarılar gelmiştir.[313] İsrail de ise İran'ın hem casusluk hem de sabotaj operasyonları yürüttüğünü ve İran Ordusu'nun siber savaş kabiliyetlerini dış kaynaktaki siber tehdit güçlerini kullanarak gerçekleştirdiği yönünde İran'ı suçlar şekilde açıklamalar gerçekleşmiştir.[314]

Yukarıda belirtilen tüm bunlar iddiada kalmış ve şuana kadar hiçbir devlet resmi olarak yaptıklarını kabul etmemiştir. Gerçek olan tek şey aktörler arasında gerçekleşen çatışmalarda siber silahların bir etki unsuru olarak kullanıldığıdır. Bu yüzden bu açıklamaları algı operasyonu olarak da düşünebiliriz. Artarak devam eden bu iddialar bundan sonra özellikle İran ve ABD özelinde karşılıklı siber çatışmaların artarak devam edeceği bu bağlamda değerlendirilebilir.

4.2. Rusya'nın Analizi

Sovyetler Birliği de Rusya'da uluslararası sistemde saygı duyulan ve korkulan bir ülkedir. Her ikisi de dönemlerinde kültür, coğrafya, askeri ve teknolojik unsurlarını avantajlı bir stratejik savaş unsuru olarak kullanmıştır. Sovyet Stratejisini miras alan Rusya karmaşık ve anarşik uluslararası sistemde güncel araçları

[312]Amir Kholoosi, İranlı Komutan: ABD'den Karşılık Gelseydi Daha Fazla Saldırı Düzenleyip Binlerce Can Kaybı Verdirecektik, Sputniknews, 09.01.2020, https://sptnkne.ws/AWU9 ET.28.02.2020.

[313]Shannon Bond, Iran Conflict Could Shift To Cyberspace, Experts Warn, NPR Organization, 21 Ocak2020,https://www.npr.org/2020/01/21/797449708/iran-conflict-could-shift-to-cyberspace-experts-warn ET.28.02.2020.

[314]Dorothy Denning, How Iran's Military Outsources İts Cyberthreat Forces, Times Of Israel, 22 Ocak2020,https://www.timesofisrael.com/how-irans-military-outsources-its-cyberthreat-forces/ ET.28.02.2020.

kullanarak merkezi ve sürekli bir gerilimin içinde en önemli güç olma hedefinde ilerleyen bir aktör olmayı hedeflemiştir.[315] Bu doğrultuda Rusya'nın geçmişten gelen stratejik kültürü doğrultusunda hem nükleer hem konvansiyonel hem de siber alanda savunma ve saldırı kapasitesini bir arada kullanmayı hedeflediği görülmektedir.

Bir siber saldırının ne zaman bir savaş eylemine dönüştüğü, kimin suçlu olduğunun öğrenilmesi yöntemi hala bulanıktır. Günümüzde uluslararası kabul görmüş bir hukuk kuralı olmadığı için anarşik siber uzay alanında devletler zarar görmeden faaliyetlerini sürdürmeye çalışmaktadırlar. Bu anarşik ortamda siber faaliyetleri en çok düzenleyen ülke Rusya'dır. Rusya'nın bugünkü güvenlik anlayışının temeli aslında Mikhail Gorbaçov'un Mart 1985'te iktidara geldiğinde, güvenliğin tek başına askeri güçle sağlanamayacağı yönündeki anlayışa gitmektedir. Sonrasında Rusya tarafından da devam ettirilen bu stratejik bakış öncelikle siber saldırıların savaşın birinci boyutu olarak kullanılmasına yol açmıştır. Böylece Rusya siber saldırılar sayesinde ekonomik ve teknolojik olarak karşı taraf savaşa hazır hale getirilmiştir.

Genel olarak Rusya'nın sahip olduğu zenginlikler; yer altı kaynakları, halkın entellektüel potansiyeli ve geniş topraklarıdır. Ancak 90'lı yıllarda devletçiler tarafından liberalizmden uzaklaşılmasıyla Rusya ekonomik, bilimsel ve teknik olarak gelişmiş ülkelerin gerisinde kalmıştır. Günümüzde ise Rusya'nın üç temel sorunu vardır. Bunlar; ekonomik sistem eksikliği, deniz gücü eksikliği ve nüfusunun hızla azalmasıdır. Bu eksiklikleride rakiplerinden hızlı davranarak yeni oluşan siber uzayda güçlenip hâkimiyet kazanmayı hedefleyerek gidermeye çalışmaktadır.

4.2.1. Rusya'nın Siber Savaş Kabiliyetlerinin İncelenmesi

NATO'nun genişlemesi, ABD'nin Çevreleme Politikası çevresinde Rusya'nın etrafına füze sistemlerini konuşlandırması, Birleşmiş Milletler 'de Orta Avrupa veya Orta Doğu hakkındaki tüm tartışmalarda Rusya'nın karşısında politikalar üretilmesi gibi sebepler yüzünden Rusya'da güvenlik politikaları çok önemli olmuştur. Güvenlik politikalarının bu artan önemi doğrultusunda Rusya, günümüz teknolojik şartlarında karşısında duran bu rakip ülkelerle gireceği bir savaşın olası etkilerinin

[315]Paul Kennedy, "Savaşta ve Barışta Büyük Stratejiler", Çev. Fethi, A. Totem Yayıncılık, İstanbul, 2014, ss.168.

tahmin ettiğinden çok daha tehlikeli boyutlara ulaşabilme ihtimalinden dolayı stratejisini " yasadışı enstrüman kullanarak yumuşak güç uygulama " gibi alternatif bir politika izlemeye döndürmüştür. [316]

Rusya bu yumuşak güç silahlarını kullandığında ise meşruiyet sorunu ortaya çıkmaktadır. Bu süreçte Rusya, Batı'yı savaşçılıkla suçlayarak Rusya'nın kendi güvenliğini sağlayabilmesi için batılı ülkelerin zayıf güvenlik duvarlarını kıracak bu siber silahları kullanmak zorunda olduğunu vurgulamaktadır. Aynı zamanda Rusya müttefiklerini ABD karşıtı olan yarı çevre ülkeler (Venezuela, İran, Belarus, Kazakistan vs.) ile oluşturmaktadır. Bu duruma karşı ABD ise Rusya müttefiki olan özellikle İran ve Venezuela'ya karşı aynı siber silahları kullanarak ciddi saldırılar gerçekleştirdiğini ABD'nin çatışma örneklerinde ayrıntılarıyla açıklamıştık.

Bu doğrultuda Soğuk Savaş'tan farklı bir boyutta devam eden Rusya- ABD rakipliğinde Rusya'nın güvenlik yapımının analizinde siber silahlar ciddi bir öneme sahiptir. Rusya'nın uluslararası güvenlik söylemleri de bunu doğrulamaktadır. Örneğin; 2020 yılında gerçekleştirilen söylemler çerçevesinde Rusya, ABD ve NATO'ya yönelik tedirginlik içeren açıklamalar yapmaya devam etmiştir. Bu açıklamaları kısaca açıklarsak; Rusya ile ABD'nin nükleer silahlarını sınırlandırmalarını içeren START-3 (Yeni START) Anlaşması'nın uzatılması konusunda görüşmeler devam ederken Rusya Dışişleri Konseyi'nin genel toplantısında konuşan Dışişleri Bakanı Sergey Lavrov, Washington'un nükleer silahlar ve stratejik istikrar alanında gerilimi tırmandırmaya yönelik adımlar attığını ifade etti. Aynı zamanda NATO hakkında da konuşan Lavrov, NATO'nun operasyonel faaliyetlerini uzaya ve siber alana taşıyarak oldukça tehlikeli bir oyun başlattığı uyarısında bulundu.[317] Bu açıklamalar ışığında; Rusya'nın uluslararası güvenlik mimarlarının ortak vizyonlarını incelersek Rusya'nın siber güvenliğe bakışını daha iyi anlayabiliriz.

Bir diğer yandan; Rusya'nın uluslararası güvenlik vizyonun temelini ciddi bir rakip olarak gördüğü Batı bloğu oluşturmaktadır. Soğuk Savaş'ın da etkisiyle birlikte Soğuk Savaş sonrası dönemde Batı'nın tamamen karşı olduğu Rus güvenlik açılımları belli çatışma örnekleriyle zaman zaman vücut bulmaktadır. Özellikle Batı

[316] Kaldor ve Rangelov, a.g.e, ss.408-414.
[317] Sputnik, Rusya: ABD Nükleer Silahlar Alanında Gerilimi Tırmandırmaya Yönelik Adımlar Atıyor, Sputnik News, 21.01.2020, https://sptnkne.ws/Bd66 ET.28.02.2020.

tarafından, Rusya'nın güvenlik politikalarının meşru olmadığına yönelik iddialar Gürcistan ve Estonya gibi çatışmalar sonrasında hâkim olarak kullanılmıştır. Fakat Rusya bu görüşlere aldırış etmeden siber silahların asimetrik etkisini kullanarak rakiplere karşı yumuşak güç uygulamaya devam etmektedir. Başka bir deyişle, Rusya'nın saldırıları karşısında dış rakipler meşruiyet konusunda ikna olmasalar da saldırıları durdurma konusunda başarılı olamamışlardır. Bunun en büyük sebebide Rusya'nın Birleşmiş Milletler Güvenlik Konseyindeki daimi üyeliğindeki veto yetkisini kullanmasıdır.

Batı karşısında Rus güvenlik politikasını meşrulaştırmanın ikinci yolu kurumlara üyeliktir. BM kurumlarında Batı'ya karşı izole olan Rusya, Moskova - Şanghay İşbirliği Örgütü gibi bölgesel güvenlik örgütlerine üye olarak karşı cephe oluşturmakta ve klasik bir güvenlik ittifakı olarak değil, dış politikada gerçekleştirdiği politikalarda kendisine destekçi sağlamak şeklinde strateji geliştirmektir. Sonuçta, Şanghay İşbirliği Örgütü, Abhazya ve Güney Osetya olmak üzere iki ayrılıkçı bölgeyi tanıyarak Rusya'nın Gürcistan'a karşı savaşında Rusya'yı desteklemiştir. Bu durum da ABD ve Batı'ya karşı Çin-Rusya stratejik ortaklığını geliştirmekle birlikte Rusya'nın Çin'e karşı politik ve ekonomik bağımlılığını da arttırmaktadır.[318]

2009 yılında Rusya ve Çin Şanghay İşbirliği Örgütü çerçevesinde uluslararası bilgi güvenliği alanında bir işbirliği anlaşması imzaladılar. Daha sonra, 2011'de her iki ülke de Birleşmiş Milletler'e bilgi güvenliği için uluslararası bir davranış kuralları önerisi sundu. Sonrasındaysa Mayıs 2015'te Rusya ve Çin arasında siber uzay için "Saldırmazlık Paktı"[319] olarakta ifade edilen uluslararası bilgi güvenliği alanında işbirliği ve ortak önlemler konusunda ikili bir anlaşma imzalandı. Kuşkusuz, Çin ve Rusya arasındaki ikili ilişkiler "bir saldırmazlık paktı" şeklinde son yıllarda güçlendirildi. Ancak Çin ve Rusya'nın siber güvenlik ilişkisinin yakınlığı birbirleriyle olan bağlarına bağlı bir ittifak kurmak yerine, ABD ile ilişkilere bağlı gelişmektedir. Çin ve Rusya'nın algıladığı ABD'nin tek kutuplu dünya görüşü ve

[318] Nojonen, Matti. "Introduction: Adjusting to the great power transition." In Russia-China Relations. Current State, Alternative Futures, and Implications for the West, edited by Arkady Moshes and Matti Nojonen. Helsinki: Finnish Institute of International Affairs. 2011, ss17-18.
[319] Elaine Korzak, Is This China and Russia's "Nonaggression Pact" for Cyberspace?, 21.08.2015, https://nationalinterest.org/blog/the-buzz/china-russias-nonaggression-pact%E2%80%9D-cyberspace-13654 , ET.07.02.2021

değerlerine meydan okumak için çok kutupluluğun savunulması şeklinde siber uzayda da işbirliğini temel alır.[320] Bu birlikteliğin siber alanda da devam edeceği yönündeki iki taraflı açıklamalar başta ABD başta olmak üzere AB ve NATO gibi örgütlere üye devletleri de endişelendirmektedir.Çünkü AB ve NATO'ya üye devletlerin güvenlik korkuları Rusya'dan bağımsız düşünülemez.

Bu doğrultuda Rusya'nın son yıllarda geliştirmiş olduğu Uluslararası Güvenlik Vizyonları Avrupa'nın uzun süredir devam eden bir korku altında olmasının asıl sebebidir. Böylece Rusya yeni güvenlik yaklaşımı ile kendi güç kaynaklarını asimetrik yöntemleri kullanarak "yurtdışında" güçlendirmeyi hedeflemektedir. Aslında Rusya siber alanda kullandığı bu asimetrik stratejilerle bir güvenlik mimarı görevi üstlenmektedir. Çünkü şuanda siber silahları kullanarak gerçekleştiren saldırıların büyük çoğunluğu Rusya tarafından gerçekleştirilmektedir. Rusya'nın Uluslararası Güvenlik Vizyonları hakkında yorum yapan Yevegeniv Primakov'a göre; günümüz dünyasında ABD'nin küreselleşmede lider rol oynaması dünyanın tek kutuplu olduğunu göstermemektedir. Tam tersine tüm bu eğilimler tek kutuplu değil, çok kutuplu bir dünyaya gidişe tanıklık edildiğinin göstergesidir.[321]

Rusya'nın bu çok kutuplu anarşik yapı içerisinde güvenlik mimarlığı rolünün şekillenmesinde etkili olan birkaç prensip vardır. Bunları kısaca açıklarsak; 9 Eylül 2000 tarihli "Information Security Doctrine of the Russian Federation" (RF Enformasyon Güvenliği Doktrini) Rusya'nın siber güç olma yolundaki ilk temel belgesidir. Bu doktrin, Rusya'nın enformasyon güvenliği konusundaki yol haritasını, prensiplerini, amaçlarını ve konu kapsamındaki resmi görüşlerini genel hatlarıyla ortaya koymuştur. 2011 yılında açıklanan "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space" (Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler) isimli doküman Rus Ordusu'nun Ön Siber Savaş Doktrini şeklinde tanımlanmıştır.[322] Son olarak dönemin Rusya Genelkurmay Başkanı General Valery Gerasimov'in

[320]Yuxi Wei, China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty, The Henry M. Jackson School Of İnternational Studies, University Of Washington, 21.06.2016, Https://Jsis.Washington.Edu/News/China-Russia-Cybersecurity-Cooperation-Working-Towards-Cyber-Sovereignty/ ET.24.02.2020.

[321] Yevegeniv Primakov, 11 Eylül ve Irak Müdahelesi Sonrası Dünya, Doğan Kitap,2004.

[322] Ali Burak Darıcılı ve Barış Özdal, "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi" İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi, Cilt.4, No.1, Yıl.2017, ss.19-40.

"hibrid savaş" olarak kavramsallaştırdığı "Gerasimov Doktrini"'nin 2000 yılında Vladimir Putin'in devlet başkanı seçilmesiyle Rus dış politikasında başlayan yeni dönemle birlikte kullandığı en önemli stratejilerinden biri haline gelmiş olmasıdır. Bu bağlamda, Gerasimov Doktrini temel olarak askeri niteliğe sahip olmayan yöntemleri kullanmayı dolayısıyla da daha az insan kaybı ve maliyet ile sıcak çatışma süreçlerini yönlendirmeyi ve yönetmeyi amaçlamaktadır. Gerasimov Doktrinin ulaşmak istediği hedefler, askeri bir müdahale öncesinde, hedef bölge, ülke, topluluk ya da devlete yönelik olarak siber saldırılar ile avantaj sağlanması, hedefin yıpratılması, psikolojik savaş yöntemleri ile baskı altına alınması, moralinin bozulması, savunma direncinin kırılması, kritik altyapılarına zarar verilerek ekonomisinin zarara uğratılmasıdır.

Son olarak; Rusya Devlet Başkanı Vladimir Putin; Rusya "Son yıllarda savunma sanayi şirketleri, siber savaş birliklerinin karşılaştıkları tüm görevleri başarıyla çözebilmelerini sağlayan ve özellikleri bakımından yabancı benzerlerinden üstün olan 20'den fazla elektronik harp ekipmanı geliştirdi" şeklinde bir açıklama yaparak mevcut siber savaş sistemlerinin Suriye'deki operasyonlar sırasında aktif olarak kullanıldığına değinmiştir.[323] Aslında tüm bu saldırgan tavırlar Rusya'nın Sovyetler Birliği zamanına dönme hayalinin göstergesidir.

4.2.2. Rusya'nın Siber Savaş Faaliyetleri

Rusya siber saldırı kabiliyetlerini, bilgisayar sistemlerini hedef almanın ötesinde; istihbarat, karşı istihbarat, elektronik harp, düşman iletişimini aksatma, probaganda gibi çok geniş bir alanda kullanmaktadır. Rusya'nın düzenlediği iddia edilen bu saldırılardan bazıları ise şunlardır; 2007 yılında Estonya'ya, 2008 yılında Gürcistan'a, 2014 yılında Ukrayna'ya ve 2016 yılında Amerikan Başkanlık Seçimlerine yönelik siber saldırılar gerçekleşti. Kısaca bu saldırı örnekleri üzerinden süreci açıklarsak;

[323]Михаил Климентьев, Putin, Siber Savaş Sistemlerini İyileştirme Çağrısı Yaptı, Sputnik News, 04.12.2019, https://sptnkne.ws/AAaF ET.03.03.2020.

- **Estonya Siber Saldırısıyla Birlikte Talin Mükemmeliyet Merkezinin Kuruluşunun Yeni Siber Uzay Dünya Düzenine Etkisi**

27 Nisan 2007'de büyük bir hizmet reddi saldırısı ile başlayan Estonya siber saldırısı, bir devletin diğer bir devleti hedeflediği bilinen ilk siber vaka olarak kabul edilir. Bu ilk siber saldırı örneğinin neden Estonya ile başladığını daha iyi yorumlayabilmemiz için kısaca Estonya'yı açıklamamız gerekir.

Estonya 1991 yılında Sovyetler Birliği'nden bağımsızlığını ilan ettiğinden beri bilgi ve iletişim teknolojisi konusunda kendini geliştirerek Avrupa'nın en kablolu ülkelerinden biri olmuştur. Saldırının olduğu dönemde Estonyalıların yüzde 65'inden fazlası geniş bantta erişime sahip ve toplumun neredeyse tüm idari işlevleri internet ile çevrimiçi bir şekilde yürütülmekteydi. Her gün çevrimiçi gazete okuyanlar, banka işlemlerini yapanlar, ülke içi ücretsiz Wi-Fi ile cep telefonu kullananlar, hükümet işlemlerinde e-devlet uygulamaları gerçekleştirenler, yemeklerdeki ödemelerini kredi kartı ile gerçekleştirenler, sağlık, eğitim ve adli sistemlerdeki işleyişte internet kullanımı ve daha fazlası olacak şekilde ülke tamamen kablolu bir haldeydi.

Sovyetler Birliği'nin eski bir parçası olan ve 1,3 milyon nüfusa sahip bu kablolu ülke hiç beklemediği bir anda beklemediği bir şekilde saldırıya maruz kalmıştır. Bu saldırı kimilerine göre savaş kimilerine göre ise bir saldırıydı. Fakat bu karmaşayı özetleyen en güzel açıklamalardan biri Madis Mikko'ya aittir. Estonya savunma bakanlığı sözcüsü Madis Mikko, "Bir bankaya veya havaalanına bir füze çarptıysa, bunun bir savaş eylemi olduğunu söylemek kolaydır." "Ama aynı sonuç bir siber saldırı nedeniyse, buna ne diyorsunuz?" "Bizi dünyanın geri kalanından kesmeye çalıştılar." Dedi.[324] Estonyalı en üst düzey bir lider tarafından gerçekleştirilen bu açıklama doğrultusunda kısaca Estonya Siber Savaş sürecini açıklarsak;

Saldırı, Estonya'nın Talinn şehir merkezindeki II. Dünya Savaşı'nda Naziler tarafından öldürülen Kızıl Ordu askerlerini anan bir Sovyet heykelinin kaldırmasından kısa bir süre sonra 27 Nisan'da başlamıştır. Bu olay sonrasında Moskova'da Kremlin yanlısı gençlik grupları Estonya büyükelçiliğini bloke etti ve

[324]Lıeutenant Colonel ve Scott W. Beıdleman, "Defınıng And Deterrıng Cyber War", U.S. Army War College Strategy Research Project, 2009.

Estonya büyükelçisini taciz etti. Estonya'nın en hassas noktası, internet'i yoğun bir şekilde kullanması nedeniyle bir siber saldırıya açık olan konumuydu. Saldırıda zaten bu en savunmasız bölgesinden geldi. Böylece süreç başlamış oldu.

Saldırının ilk günlerinde, normalde günde yaklaşık 1.000 ziyaret alan hükümet Web siteleri saniyede 2.000 ziyaret alarak kullanılamaz hale geldi. Estonya başbakanının bilgi teknolojisi danışmanı Sten Hansson da bu durum hakkında "Bu, ülkemizin güvenliği için bir tehdittir." şeklinde açıklamalarda bulundu. Devam eden süreçte Estonya'nın bu denli etkilendiği saldırılardan Rusya'nın sorumlu olduğu yönünde iddialar ortaya atıldı. Örneğin; Atlanta internet güvenlik şirketi SecureWorks Inc.'in güvenlik araştırmacısı Joe Stewart, "Rusya'nın Estonya'da gerçekleşecek bu tür faaliyetler için oldukça uzun bir geçmişi var" şeklinde açıklama gerçekleştirdi.[325] SSCB zamanında bir parçası olan Estonya'ya karşı Rusya tarafından düzenlendiği iddia edilen bu siber saldırılar(Dağınık Servis Engelleme Saldırısı- DSES) çok sayıda botnet adı verilen ağ tarafından dağınık olarak farklı yerlerde aynı anda aynı hedefe yapılan saldırılardı. Rusya'nın siber saldırılarla ilgili sahip olduğu "botnet" varlıkları da bu iddiaları desteklemişti.

Rusya tarafından gerçekleştirildiği iddia edilen saldırılar ülkenin en az korunan sınırı olan internet üzerinden gelmişti. Estonya Savunma Bakanları Rusya tarafından gelebilecek füze saldırıları, deniz bombardımanı, hava saldırıları ve tank ilerlemeleri tehdidi beklerken dijital bir istila vardı. Ülkenin tüm alt yapısına yönelik yetkisiz bir kullanıcı tarafından yasadışı bir şekilde eşzamanlı olarak (bazen bir kerede binlerce) bilgisayar tarafından ülkenin tüm lider bankaları kuşatma altına girmiş ve hükümet iletişimi azalmıştı. Kısaca düşman düzinelerce hedefe saldırmıştı. Dışarıda, her şey sessizdi. Geleneksel sınır kontrolünü gerçekleştiren muhafızlar saldırı bildirmemiş ve Estonya hava sahası ihlal edilmemişti. Fakat ortada bir acil durum vardı. Estonya siber saldırısının, uluslararası güvenlik açısından bir milat olması ve ilk kabul edilmesi de bu bilinmezlikten kaynaklanmaktadır.

Sonuç olarak Estonya Siber Saldırısının önemi daha önceden kimsenin aklına gelmeyen yeni bir savaş yöntemini ve temelini oluşturmasıdır. Ayrıca eski yasaların yeni teknolojiler sayesinde değiştirilerek yeni güvenlik dinamiklerinin oluşturulması gerektiğini ortaya çıkarmıştır. Çünkü ABD, Rusya ve Çin gibi aktif rekabet içinde

[325]Christopher Rhoads, Politics and Economics: Cyber Attack Vexes Estonia, Poses Debate, The Wall Street Journal, 18.05.2007. https://www.wsj.com/articles/SB117944513189906904 ET:17.01.2020.

olan karşıt cephelerin bulunduğu günümüzde Estonya'nın 2007 de uğradığı siber saldırı ufak bir ülke olduğundan dolayı önemsiz görünebilirdi. Fakat şu hususun gözden kaçırılmaması gerekmektedir. Bu olay her ne kadar önemsiz gibi görünse de 1. Dünya Savaşını başlatan Avusturya- Macaristan veliahdı Ferdinand'a düzenlenen suikast kadar tetikleyici bir eylem olmuştur.[326] Bunun en önemli kanıtı ise Estonya olayı sonrasında Gürcistan, İran ve Venezuela gibi ülkelerle devam eden birçok önemli siber saldırının meydana gelmesidir.[327] Aynı zamanda Estonya saldırısı başta İngiltere ve ABD olmak üzere küresel ölçekli devletler ile NATO gibi önemli bir askeri örgütlenmenin savunma politikalarını revize ederek siber güvenlik stratejisi geliştirmelerini zorunlu kılmıştır.[328]Bu yüzden Estonya olayı eğiticidir.

Bunların yanında 2007 yılında Estonya'ya yönelik tüm bankaları, kamu kurumları ve özel sektörü çalışamaz hale getiren bu siber saldırılar siber alanda yaşanan topyekûn savaşın ilk örneğidir. Hem NATO hem de Avrupa Birliği üyesi olan Estonya, böyle bir dijital cephede daha önce hem kendisinin hem de hiçbir ülkenin savaşmamış olmasından dolayı güvenliğini kendisi sağlayamamıştır. Bütün bu gelişmelerin ardından Estonya Hükümeti, devlet kurumlarıyla birçok özel işletmenin internet sitelerini çökerten ve ülkenin temel elektronik altyapısına yönelik olan bu siber saldırıdan Rusya'yı sorumlu tutarak konuyu NATO'nun en yüksek organı olan Kuzey Atlantik Konseyine götürmüştür.[329] Fakat Estonya Cumhuriyeti'nin NATO üyesi Estonya için müttefik bir ülkeye yapılan saldırıda ittifakın saldırgana saldırmasını zorunlu kıldığı NATO'nun Madde 5'i uygulanmamıştır.[330] Bunun birçok sebebi vardır. Kısaca bu sebepler şunlardır; bu saldırı tipinin daha önceden bilinmemesinden dolayı 5. Maddenin siber saldırıyı kapsamaması, uluslararası hukukta bir savaşa girmeyi meşru kılan unsurların siber

[326] Arthur, C. That Cyberwarfare By Russia On Estonia? It Was One Kid.. İn Estonia, The Guardian, 25.01.2008, https://www.theguardian.com/technology/blog/2008/jan/25/thatcyberwarfarebyrussiaon ,ET.30.01.2020.

[327]Jeffrey Carr, İnside Cyber Warfare Massing The Cyber Underworld,O'Reilly, 2010 https://books.google.com.tr/books?id=5LIyXzpKhYsC&printsec=copyright&hl=tr#v=oness&q&f=false ET.10.10.2019.

[328]Merve Yazıcı, İlk Modern Siber Atak: Estonya, TUIC Akademi, 04.09.2015, http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ ET.30.01.2020.

[329]BBC, Estonya'ya Siber Saldırı, BBC Türkçe, 17.05.2007, http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml , ET.31.01.2020.

[330]Joshua Davis, Hackers Take Down the Most Wired Country in Europe, Wired Magazine, Cilt.15, Sıra9, 21 Ağustos 2007.http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia , ET:17.01.2020.

savaşlarda tanımlanmamış olması [331] ve Rusya'nın saldırı sorumluluğunu inkar etmesidir. Tüm bu sebeplerden dolayı NATO'dan topyekûn kendini savunma maddesini tetikleyecek şekilde Estonya egemenliğinin ihlal edildiği bahane edilerek NATO tarafından Rusya'ya karşı bir saldırı gerçekleştirilmedi.

Rusya'nın NATO'ya resti şeklinde de görülen bu olaydan sonra NATO her ne kadar Madde 5'i devreye sokamasa da savaş sonrasında bazı politikalar geliştirdi. Örneğin Estonya'da siber saldırıları önceden görmeyi ve saldırı durumunda ülkenin korunmasını hedefleyen bir kale (Tallinn merkezli Siber Savunma Merkezi) oluşturmuştur. Aynı zamanda, Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku) yayınlanarak yürürlüğe girmiştir.[332] Bu hedef kapsamında 2008 yılında NATO Estonya'ya siber askerler yollayarak onarım ve koruma faaliyetlerine başlamış olsa da geçmişteki Soğuk Savaş algısı ile diğer ülkelerde de benzer korkular artmaya başlamıştır.

- **Gürcistan Siber Saldırısı**

Estonya gibi NATO üyesi olmasa da, Gürcistan da bir NATO ortağıdır. Gürcistan Nisan 2008 Bükreş Zirvesinde ve Kasım 2010 Lizbon Zirvesi'nde, belirtilmemiş bir zamanda NATO'ya "üye olacak" şeklinde ilan edilen bir ülkedir. Sovyetler Birliğinin çöküşünden sonra tarafını Batı olarak belirleyen Gürcistan ile Rusya arasında birçok anlaşmazlık yaşanmıştır. Rusya ve Gürcistan arasındaki bu çatışma örneklerini incelemeden önce kısaca Gürcistan'ın en önemli noktalarını açıklarsak süreç daha kolay anlaşılabilir.

Gürcistan Cumhuriyeti, Karadeniz boyunca Rusya'nın doğrudan güneyinde yer alan coğrafi olarak Rusya'dan daha küçük bir ülkedir. Gürcistan'ın Sovyet kontrolü, merkezi Rus hükümeti olarak 1991 yılına kadar sürse de konumu göz önüne alındığında hala Moskova'nın "etki alanı" içindedir.

Gürcistan bağımsızlığını ilan ettikten bir süre sonra Rusya'nın da etkisiyle bir kez daha kargaşa içine girdi. Bu olaylardan sonra Gürcistan Güney Osetya ve Abhazya olmak üzere iki bölgenin kontrolünü kaybetti. Rusya'nın da etkisiyle bu

[331]Sınger ve Friedman, a.g.e. , ss 167-170.
[332]Milli Güvenlik Kurulu Genel Sekreterliği, Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku), https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku ET.29.01.2020.

bölgelerdeki yerel Rus nüfusu Gürcüleri yenmeyi başardı. Daha sonra, Temmuz 2008'de, Güney Osetya isyancıları (veya Rus ajanları), bir dizi füze saldırısı düzenleyerek Gürcistan ile çatışmayı kışkırttı. Gürcistan ordusu da topraklarında gerçekleşen bu füze saldırılarına tepki vererek 7 Ağustos'ta bölgeyi işgal etti. Olayların ardından Rus ordusu siber savaşçılarıyla birlikte Gürcistan ordusunu Güney Osetya'dan hızla çıkardı.[333] Rusya'nın 8 Ağustos 2008'de Gürcistan'ı işgal etmesiyle başlayan gerginlikler beş gün sürdü ve ezici bir Rus zaferiyle sona erdi. Bu beş günlük savaşa eşlik eden siber saldırılar sonrasında savaştan çıkan sonuç Batı'nın Rus eylemlerini kınaması ve artan gerilimlerin yanında Abhazya ve Güney Osetya'nın bağımsızlıklarının Batı karşıtı Rusya ve Birleşmiş Milletler üyesi bazı bağımsız devletler tarafından resmen tanınmasıdır.[334]

2008 yılında Gürcistan ve Rusya arasında yaşanan Güney Osetya savaşının bu tez açısından önemi ise Rusya'nın siber saldırı kabiliyetini ortaya çıkarmış olmasıdır. Bu savaş sırasında Rusya tarafından gerçekleştirilen botnet ve ddos saldırıları sonrasında; Gürcistan cumhurbaşkanı saakashvilinin web sayfasında "win+love+in+Rusia" kelimeleri kullanılarak sayfa erişilemez hale getirilmiş, Gürcistan parlamentosunun sayfasında dönemin cumhurbaşkanının hitlere benzetildiği görseller yerleştirilmiş, Gürcistan'daki birçok site çökmüş, hükümetinin resmi sayfaları çalışmaz hale gelmiş, halkın CNN ve BBC sayfalarına erişimi engellenmiş ve Gürcü bankaları çalışamaz hale getirilmiştir.[335] Özellikle Avrupa'daki bankalarla ilişkileri durunca ekonomik tedirginlik artmış bu da halkın moralini bozduğu bu saldırıların sorumluluğunu Rusya gene üstlenmemiştir.

Rusya ve Gürcistan arasında yaşanan bu savaştan yıllar sonra 2019 yılına geldiğimizde tekrardan Gürcistan'da web sitelerini bozan ve en az iki büyük televizyon istasyonunun yayınını kesintiye uğratan büyük bir siber saldırı gerçekleşmiştir. Bu saldırı sonrasında da ABD, İngiltere ve Gürcistan yetkilileri tekrar Rusya'yı suçlamıştır. Örneğin; ABD Dışişleri Bakanı Mike Pompeo "28 Ekim 2019'da Rusya Genelkurmay Ana İstihbarat Müdürlüğü (GRU)'nun Gürcistan'a

[333]Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books ss.1-20.
[334]Jim Nichol, "Russia-Georgia Conflict in South Ossetia: Context and Implications for US Interests", Congressional Research Service Report for Congress, 24 Ekim 2008.
[335]D.W. Rusya, "Gürcistan'ı Sanal Alemde De Vurdu", Deutsche Welle, 18.08.2008, https://p.dw.com/p/F09O , ET.30.01.2020.

yönelik bir siber saldırı gerçekleştirdiğini ilan ederek Rusya'yı bu davranışı durdurmaya çağırmıştır.[336]

Sonuç olarak insan ve malzemeden ziyade bilgi teknolojisi ve internetin yayılması artık tüm düşmanların güç kapasitelerini dışarıdan etkileyebilme fırsatı sunmuştur. Aynı zamanda; günümüzde büyük güç aktörlerinin elinde "nükleer silahlar"'ın bulunması sebebiyle klasik savaş ve siber savaş bir arada yürütülmektedir. Rusya ve Gürcistan arasında yaşanan bu savaş "karma savaş" kavramının ve uygulamasının ilk adımı olarak kabul edilebilir.[337]

Her ne kadar bazı bilim adamları Gürcistan'da yaşanan siber olayların topyekûn savaşın ilk örneği olarak tanımlasa da şuan için bunu tanımlamak çok zordur. Şuan için bilinebilecek tek gerçek mevcut bir fiziksel (operasyonel) savaş sırasında geleneksel savaş yöntemleri kullanılırken devletlerin siber saldırıları da gerçekleştirdiğidir. Bu savaş örneğinde Rusya Gürcistan'a karşı geleneksel savaş yöntemlerinde üstün olabilmek için ciddi bir güç kazanmıştır. Buradan da şu ortaya çıkmaktadır. Siber savaş tek başına belki faydalı olamayacak bile olsa geleneksel savaş yöntemleriyle birlikte kullanıldığında çok ciddi sonuçlar yaratabilmektedir. Beklenmeyen bir anda ve doğru zamanda yapılan ani siber saldırılar çok düşmanlara karşı etkili olabilir. Bu durum Gürcistan savaşında fazlasıyla kendini göstermiştir.

- **Ukrayna Siber Saldırısı**

2014 yılında Rusya Federasyonu, Ukrayna'ya bağlı Kırım'ı bilinen savaş taktikleri yerine ağırlıklı olarak Ukrayna'nın iç güçlerini kullanarak işgal etmiştir. Rusya'nın Ukrayna krizi süresince kullandığı taktikler, askerî ve sivil aktörlerin ortak politik amaç için koordineli kullanımını ve hedef ülkedeki iç dinamiklerin manipüle edilmesini öngörmektedir. 2015 yılında Ukrayna'ya yönelik gerçekleştirilen BlackEnergy Virüsünün elektrik santrallerini etkilemesiyle Ukrayna'nın doğusunda 80 bin kişi 6 saat boyunca elektriksiz kalmıştır. Rusya'nın savaş sırasında iç

[336]Ryan Browne, "US And UK Accuse Russia Of Major Cyber Attack On Georgia", CNN, 20.02.2020,https://edition.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html ET.28.02.2020.
[337]Jakob Hedenskog ve Carolina Vendil Pallin, Russian Military Capability in a Ten-Year Perspective, FOI Report, 2013, ss.103-115.

dinamiklerin manipüle edilmesini temel alan bu stratejisi Ukrayna ile benzer özellikleri taşıyan diğer NATO ülkelerinde ciddi korku ve tehdit oluşturmuştur. Aslında Rusya'nın gerçekleştirmeye çalıştığı bu strateji siber savaşın psikolojik savaş boyutunu ortaya koymaktadır.

Aynı zamanda Ukrayna'daki olaylar başlamadan önce Gerasimov tarafından ilan edilen Rusya Siber Savaş Doktrini de bu çatışmada Rusya'nın rolünü gözler önüne sermektedir. Bu yüzden birçok akademisyen tarafından Ukrayna'da yaşanan olaylar Rusya'nın siber savaş tekniklerini kullanıldığı ve şekillendirdiği laboratuvar ortamı olarak tanımlanmaktadır.

- **ABD Seçimlerine Yönelik Siber Saldırı**

21. yüzyılda her alanın siber uzay ile bağlantılı olmasından kaynaklı olaran özellikle güvenlik ve istihbarat alanında kendine özgü bir hegemonya yaratmıştır. Bu yüzden hem ülkelerin siber saldırılara karşı kritik alt yapılarının güvenliğinin sağlanması hem de istihbarat servislerinin teknolojik gelişmelerle birlikte günün şartlarına yönelik istihbarat toplama faaliyetlerini dönüştürmek için hem iç siyasette hem de dış siyasette siber silahlar kullanılmaya başlanmıştır. Günümüzün modası olan elektronik casusluk ya da siber espyonajın iç siyasette kullanıldığına dair birçok örnek vardır.

Elektronik casusluk ya da siber espyonaj'ın kullanıldığının en güzel örneği 2016 ABD Başkanlık Seçimleridir. 2016 yılında Amerikan Seçimleri öncesinde; CIA'nın da içinde bulunduğu Demokrat Parti yetkililerinin özel elektronik yazışmaları Wikileaks'e sızmış ve internette yayınlanarak Trump'ın seçimleri kazanması yönünde Rus hackerlar tarafından seçim sonuçlarına yönelik müdahale gerçekleştirildiği iddia edilmiştir. Rusya'nın ABD'ye yönelik müdahalesini anlatan bu olay hakkında en çarpıcı açıklamalardan birini ise David Shimer yapmıştır.

David Shimer'in "Rigged:America, Russia, and One Hundred Years of Covert Electoral Interference" (Hileli: Amerika, Rusya ve Seçimlere Gizli Müdahalenin Yüz Yılı) adlı kitabında 2016 ABD Başkanlık seçimlerine Rusya'nın müdahale ettiğini örnekler özelinde iddia etmiştir. Bu bağlamda özellikle "seçimlere gizli müdahale" kavramını açıklayan Shimer şu hususların var olması özeline iddialarını dayandırmaktadır. Kısaca bunlardan bahsedersek;

- Bir Başkan ya da Başkan adayının başka bir ülkedeki bir lider ya da partiyi açıkça desteklemesinin bu kapsama girmediği,
- Müdahale edilen ülkede seçim sürecinin yaşanması gerektiği,
- Ülkeye yönelik aktif uygulamaların/operasyonların yapılması gerektiği,
- Seçim/oy verme sürecini engelleme/değiştirme girişimlerinin olması gerektiği,
- Kamusal tanınırlığı olan kişilerin özel hayatlarına dair bilgilerin yasadışı şekillerde ele geçirilerek toplumla paylaşılması,
- İnternet trolleri kullanılarak, sosyal medyada düzenlenen organize saldırı ya da destek kampanyalarının gerçekleştirilmesi,

gibi yollarla elde edilen, bir başka ifadeyle çalınan bilgilerin bir aday ya da parti lehine kullanılması gerektiğini belirtir. Sonuç olarakta Rusya'nın Donald Trump lehine seçimlere müdahalede bulunduğunu ima edere Amerikan demokrasisini işlemez ve Amerikan halkının sorunlarını çözülemez hale getirmeye çalıştığını belirtmektedir.[338]

2018 yılı içerisinde de ABD yetkilileri, Çin'de üretilen teknolojik aletlere Çinin daha üretim aşamasında virüs yerleştirdiğini iddia etmiştir.[339] 2019 yılı içerisinde ise ABD merkezli teknoloji şirketi Symantec, Çinli hacker'ların ABD Ulusal Güvenlik Ajansının siber yazılımını ele geçirip saldırı için kullandığını iddia etmiştir.[340] Bir diğer örnek; 2019 yılı Ocak ayında Almanya'da aralarında Cumhurbaşkanı Frank W. Steinmeier ve Başbakan Angela Merkel'in de bulunduğu yüzlerce siyasetçinin bilgisayarına gerçekleştirilen siber saldırılarda görebiliriz.

[338]David Shimer, "America, Russia, and One Hundred Years of Covert Electoral Interference" , Knopfjournal,ABD,2020,ss.6-10. https://books.google.com.tr/books?id=hbfNDwAAQBAJ&printsec=frontcover&dq=David+Shimer&hl=tr&sa=X&ved=2ahUKEwjUhvmOwZ3tAhX6CRAIHVrFBf0Q6AEwAHoECAUQAg#v=onepage&q=David%20Shimer&f=false ET.25.11.2020.

[339]İslam Doğru, Çin'de Üretilen Bilgisayar Ekipmanlarında Casus Çip İddiası, Anadolu Ajansı, 04.10.2018, https://www.aa.com.tr/tr/dunya/cinde-uretilen-bilgisayar-ekipmanlarinda-casus-cip-iddiasi/1273175 , ET.28.01.2020.

[340]TRT haber, Çinli hacker'lar ABD'ye ABD'nin siber yazılımıyla saldırdı, 05.05.2019, https://www.trthaber.com/haber/dunya/cinli-hackerlar-abdye-abdnin-siber-yazilimiyla-saldirdi-414599.html ET.28.01.2020.

4.3. Çin'in Analizi

Çin büyüklüğü ve tarihsel birikimi ile uluslararası sistemin içerisinde özellikle ekonomik bir güç olarak yükselişini sürdürmeye devam etmektedir. Ekonomik güç olarak dünyanın en büyük gücü olan ABD'ye meydan okuyan Çin, dördüncü endüstri devrimi sonucunda internetin her alanda kullanılmasının etkisiyle çok önemli bir yumuşak güç unsuru haline gelmiştir. İnternetle çalışan teknolojik tüm cihazlara olan artan bağımlılık ise beşinci tip toplumları kontrol etme mücadelesi sürecini doğurmuştur. Çin ise bu süreçten maksimum fayda elde ederek ABD'ye karşı ciddi avantaj sağlamıştır.

Soğuk Savaş sonrasında uluslararası sistemin değişmesi üzerindeki etkisi bu denli fazla olan Çin (PRC) teknolojik olarak ileri düzeyde gelişmiş bir ülke olmuştur. Teknolojik olarak bu kadar gelişmiş olması da onun hâlâ çözülmemiş sınır ve bölgesel anlaşmazlıklar ile karakterize edilen geleneksel tehditlere odaklanmasının yanında siber tehditlere de odaklanmasını zorunlu hale getirmiştir.

4.3.1. Çin'in Siber Savaş Kabiliyetlerinin İncelenmesi

Küresel internet yönetişimi ile birlikte internet, iletişim ve bilgi etrafında yeni bir politika biçimi yaratmaktadır. İnternet yönetişimi politikasındaki bu yenilik internetin ulus ötesindeki artan kitlesel etkileşim ölçeği, kontrol dağılımı ve kolaylaştırma kapasitesinden gelmektedir. İnternet yönetişimi genel olarak ABD hegemonyasına tabidir. Çin'in aksine, ABD'nin yaydığı internetin uluslararası ortamındaki yönetişimi daha kapitalist, özgür ve özel sektör tabanlıdır. Fakat internetin kurucusu olan ABD'nin karşısında özel sektör yerine kamuyu temel alan Çin'in bu süreci Soğuk Savaş'ın sahip olduğu özgürlükler değer tartışmalarının yeni bir internet versiyonudur. Örneğin; Çin Halk Cumhuriyeti'ndeki (PRC) için İnternet, Çin Komünist Partisi'nin (ÇKP) kontrolü sağlama kapasitesi ve gerçek Çin'in interneti bir araç olarak kullanarak dünya ticaretine hâkim olma amacıyla gerçekleştirdiği çifte bir meydan okumadır.

Çin ve İnternet arasındaki ilişki karmaşık bir ilişkiye dayanır. Bu paradoksal ilişki içerisinde; Çin sosyalist pazar ekonomisinin (KOBİ) büyümesi için küreselleşen bir ağ oluşturmayı hedeflemektedir. Aynı zamanda; internet'in küresel olarak yayılmasını bu kadar kolaylaştırmak için uğraşan Çin, dışarıdan etkiyi

minimize eden bir "Büyük Güvenlik Duvarı" (GFW) nın da kurucusudur. Çin bu büyük güvenlik duvarı sayesinde egemenlik sınırları içerisinde her şeye gücü yeten gözetim, iyi organize edilmiş propaganda kampanyalarına duyarlı bir nüfus, yaygın ve sinsi bir siber saldırı ve siber casusluk kaynağının kontrolünü sağlamıştır.[341]

Çin'in Büyük Güvenlik Duvarı'nın en önemli özelliği internet üzerinde lisanslama gereklilikleri, geniş devlet mülkiyeti, yurt içinde uygulanabilecek giriş kontrolleri, kimlik belirleme ve kullanıcıların gözetimi gibi uygulamalar geliştirerek geniş bir özdenetim ve otosansür uygulamaktır. Çünkü Çin topraklarında internet Çin egemenliğinin yetkisi altındadır. Bu yüzden Çin'in internet egemenliğine saygı duyulmalı ve korunmalıdır. İnternet güvenliğini bilinçli olarak koruma görevi ise Çin yasaları ve düzenlemelerine aittir. Bu kadar korumacı bir ülke içindeki halk da doğrudan siber milliyetçiliğinin mantıklı bir uzantısı olarak uluslararası anarşik sistemde görev üstlenmektedir.

Çin'in uluslararası anarşik sistemdeki önemini açıklamak ve güvenlik tehditlerinin tanımlamasını sağlamak için Mary Kaldor'un da vurguladığı Yan Xuetong'ın güvenlik analizine değinmemiz gerekir.[342] Yan Xuetong'a göre; gerçek dünyada mutlak güvenlik olmayacaktır çünkü tehlikeler, tehditler ve olaylar tamamen kaldırılamaz. Mutlak ulaşılamaz lığın bir sonucu olarak güvenlik, barış her zaman belli bir güvensizlik derecesi ile korunur. Bu yüzden barış güvenliğe eşdeğer olmamakla birlikte ilk barış sadece silahlı çatışmanın olmaması anlamına gelir. Aynı zamanda barış döneminde, güvenlik derecesi ülkeden ülkeye değişir.

Çin'in menfaatlerinin küresel ölçekte genişlemesi ve yoğunlaşması Çin'in dünyadaki rolünü değiştirerek güvenlik çıkarlarını her zamankinden daha canlı hale getirmiştir. Böylece yirmi birinci yüzyılda Çin'in tehditleri geleneksel ve geleneksel olmayan güvenlik tehditleri olmak üzere iki ana kategoriye ayrılmıştır. Geleneksel güvenlik tehditleri askeri bir bileşen içeren ve diğer uluslardan kaynaklanan tehdit olarak nitelendirilebilir. Geleneksel olmayan güvenlik tehditleri ise "ulusal sınırları aşan, askeri alanın ötesine geçen, öngörülemeyen ve / veya beklenmeyen, iç/dış unsurlara sahip ve geleneksel güvenlik tehditleriyle iç içe olan unsurları içerir.

Çin gelişen ekonomik ve teknolojik alt yapısından dolayı geleneksel olmayan tehditlere karşı özel önlem almak zorunda kalmıştır. Geleneksel olmayan güvenlik

[341]Ronald Deibert, John Palfrey, Rafal Rohozinski, ve Jonathan Zittrain, a.g.e , ss.177-195.
[342] Kaldor ve Rangelov, a.g.e. , ss.371-408.

tehditleri kapsamında Çin'in ekonomik performansındaki etkileyici gelişme ile eşzamanlı olarak Çin'in, savunma bütçesi de ciddi oranda bir artış göstermiş ve modernize çalışmalarına başlamıştır. Bu modernizasyon sürecinde siber güvenlik ciddi bir önem arz etmektedir. Çünkü uluslararası sistemdeki çatışmalar dijitalleşmektedir. Çatışmaların dijitalleşmesi ise Çin'in artan küresel çıkarları doğrultusunda küresel güvenlikteki rolünü arttırmasını zorunlu hale getirmektedir. Bu sebeple Çin'in ordu kabiliyetleri ve yetenekleri siber silahlardan gelebilecek tehditlere yönelik oluşturulacak siber güvenlik faaliyetleri çerçevesinde yenilenmektedir.

Bir diğer yandan, Çin'in ekonomik büyümesiyle birlikte küresel ilişkilerdeki etkisi de artmaktadır. Çin'in küresel ilişkilerde daha fazla rol oynaması küresel düzen üzerinde bazı temel etkilere yol açmaktadır. Bunlar; küresel güvenlikteki rolünün artması, dünya çapındaki kaynaklara olan ilgisinin artması, e-ticaretin dünya çapında hızla büyümesiyle birlikte küresel olarak iletişim ve ulaşımın daha kolay, hızlı ve ucuz hale getirilmesi gibi roller üstlenmesidir. Böylece Çin'in uluslararası ilişkilerde kullandığı politikalarının değişmesiyle eşzamanlı ilerleyen süreçte Çin'in dünya meseleleri üzerindeki etkisi artmıştır.[343] Bu durum uluslararası ilişkilerin anarşik yapısı içerisinde iki tip sorunu ortaya çıkarmıştır. Bunlar Güvenlik İkilemi ve Yükselen Güçlerin İkilemidir. Başta ABD olmak üzere Çin'in hem ekonomik hem de teknolojik olarak bu kadar büyümesi başta ABD olmak üzere birçok ülkede ciddi korku yaratmıştır. Çin ise artan gücünü sağlamlaştırmak ve güvenlik risklerini azaltmak için siber alanda casusluk faaliyetlerine başlamıştır. Böylece Çin ve ABD arasında artan güvenlik ikileminin de etkisiyle dünya hâkimiyetini kontrol etme mücadelelerinde aktif bir savaşa dönüşmeyecek şekilde iyi huylu bir stratejik siber çatışma süreci başlamıştır. Böylece Çin, ABD'ye karşı siber alanda stratejik bir rakip olmuş ve küresel güvenlikteki rolünü her geçen gün daha da arttırmıştır.

İnternetin küresel ekonomi için önemi, istikrardaki etkisi, hizmetlerin kullanılabilirliğindeki rolü, kullanıcılarına sağladığı kalitesi ve sağladığı uygulamaların güvenlik riskleri teknolojinin de sürekli gelişmesine bağlı olarak her geçen gün artmaktadır. Bu durum internetin yönetişim ihtiyacını ortaya çıkarmaktadır. Bu doğrultuda, internet yönetişimiyle ilgili egemenlik, güvenlik,

[343]Sun, Xuefeng, "The Dilemmas of the Rise of China", Elcano Royal Institute, Madrid, 2012.

istikrar, mahremiyet, uluslararası koordinasyon, fikri mülkiyet hakları vb. birçok konuda risk olduğu konusunda tartışmalar devam edecektir. Bu tartışmaların asıl sebebi internet yönetişiminin tam olarak sağlanabileceği küresel bir çözüm gerçeğinin oluşturulamamasıdır.

Aynı zamanda; siber uzay ile ilgili sorunları anlayarak çözüm üretilebilmesi için internetin yanında donanım ve yazılımlarında ayrıntılı olarak incelenmesi gerekir. Donanım ve yazılımdaki gelişmelerle birlikte, internet'e erişimi kısıtlamak için karmaşık filtreleme teknolojileri giderek daha fazla uygulanmaktadır. Bu sorun hem hükümetler hem de şirketler düzeyinde gerçekleşmektedir. Ancak, güvene dayalı internet'in açık doğası göz önüne alındığında, bir ülkenin kısıtlamaları, çok dikkatli bir şekilde ele alınmazsa, herkesin içinde yaşadığı küresel internet bundan olumsuz etkilenecektir. Bu sorunu anlamak için, internet yönlendirmesini, DNS ve kök ad sunucularının davranışını ve internet geçişlerinin ekonomisini dikkate almak gerekir. Bu süreci Çin üzerinden açıklamamız için öncelikle Çin'in interneti diğer ülkelerden farklı olarak ne şekillerde sansürlediğini daha net incelememiz gerekir. Çin'de izlenen yöntemlerden biri, Çinli kullanıcıların DNS isteklerine geçersiz yanıtlar vermektir. Örneğin, şu anda, bir Çin DNS sunucusu www.facebook.com için bir IP adresi olarak 46.82.174.68 döndürüyor, aslında, tüm meşru Facebook IP'leri 66.220.xy veya 69.63.xy şeklinde görünür. Bu durum de www.twitter.com, www.youtube.com ve diğer birçok alan içinde aynı şekildedir. Ancak görünüşte rastgele, ancak genellikle yönlendirilmeden sahte IP'ler döndürülür. Bu seneryo, küresel internetin kırılganlığını ve esnekliğini göstermektedir. Kırılgandır çünkü sonuçta güvene dayalıdır ve neredeyse herkes bu güveni kasten veya kazayla ihlal edebilir (ve bunun masum bir hata olmadığını düşünmek için bir neden yoktur). Dirençlidir, çünkü herhangi bir vidalama veya kontrol girişimi için genellikle birçok alternatif veya geçici çözüm vardır.

Son olarak Çin'in Dış Politikasında Siber İstihbarat Stratejileri önemli bir yer tutmaktadır. Bunu kısaca açıklarsak;

İstihbarat insanlığın ilk günlerinden bu yana vazgeçilmez bir eylemdir. İstihbaratı, istihbarat örgütlerini anlamadan anlamak mümkün değildir. İstihbarat örgütleri modern toplumlarda istihbaratın temel araçları olarak çok etkin bir

konumdadır.[344] İstihbaratın temel ilkeleri sürat, kesinlik ve doğruluktur. İstihbarat gerekleri ise şunlardır; maksadına uygun olmalı, yaratıcılık ve hayal gücü içermeli, tehlike ve fırsatlarla ilgili bilgi toplamakla yetinmemeli, objektif olmalıdır. Bunlara ek olarak; adanmışlık ve yenilikçilik gerektirir. Ekip ve örgüt işidir. Milli bir felsefeye dayanır.[345]

Tarih boyunca yöneticiler hem kendi hem de devletin güvenliğini sağlayabilmek için istihbaratı yoğun ve değişik oranlarda devlet yönetiminde kullanmışlardır. İstihbaratçılık için dünyanın en eski mesleklerinden birisi ifadesinin kullanılması, istihbarat tarihi hakkında da bilgi edinmemize yardımcı olmaktadır. İstihbarat tarihi, insanlık tarihinden bugüne teknolojik gelişmelerle de bağlantılı bir şekilde kademeli olarak gelişim göstermiş olan bir bilim dalıdır. 17. yüzyılda istihbarat askeri nitelikli bir faaliyetti. 19. yüzyılda Napolyon savaşları boyunca tam zamanlı bir faaliyet haline gelmeye başladı. 20. yüzyılda istihbarat kavramı ekonomik ve siyasi dönüşümle yakından ilgili stratejik ve operasyonel taktiklerin oluşturulmasında kurumsallaşmaya dönük bir yapıya dönüştü. Günümüzde ise istihbarat kavramı teknolojik gelişmelerle ve internetin hayatın her alanına girmesiyle birlikte bilişim alanındaki ilerlemelerin yanında siber alana geçmiştir. Bu doğrultuda istihbarat faaliyetlerini Çin özelinde açıklamamız için Sun Tzu felsefesine ve yaşanan teknolojik gelişmelere bakmamız gerekmektedir.

M.Ö. 500'lü yıllarda yaşamış olan Çinli Komuttan Sun Tzu ya göre; savaşın 5 kuralı vardır: ölçme, değerlendirme, hesaplama, kıyaslama ve zaferdir. Mevzi ölçmeyi, ölçme değerlendirmeyi, değerlendirme hesaplamayı, hesaplama kıyaslamayı, kıyaslama ise zaferi doğurur.'' demiştir. Yine Sun Tzu; ''düşmanı ve kendinizi biliyorsanız, yüzlerce savaşa bile girseniz sonuçtan emin olabilirsiniz.'' demiştir. Kendinizi bilip düşmanı bilmiyorsanız, kazanacağınız her zafere karşın yenilgiyle de tanışabilirsiniz. Ne kendinizi ne de düşmanı biliyorsanız, sizin için gireceğiniz her savaşta yenilgi kaçınılmazdır.'' açıklamasını yaparak istihbaratın önemini vurgulamıştır. Aynı zamanda Sun Tzu Savaş Sanatı adlı eserinde istihbaratı faaliyet ve bilgi olarak ikiye ayırmıştır.[346] Bu dönemde Çin'in istihbarat ve psikolojik savaş mekanizmasının başlıca hedefi Türkler olmuştur. Bu kapsamda Sun Tzu'nun

[344]Ümit Özdağ, İstihbarat Örgütleri, Kripto Yayınları, Ankara, 2017.
[345]Ümit Özdağ, İstihbarat Teorisi, Kripto Yayınları, Ankara,2018, ss. 29-40.
[346] Sun Tzu, Savaş Sanatı, Hasan Alı Yücel Klasikleri Türkiye İş Bankası Yayınları, İstanbul, 2018.

istihbaratın önemi hakkındaki görüşleri çok önemlidir. İstihbarat tarihi ve İstihbaratın ne olduğunu tam anlamıyla tamamladıktan sonra günümüzdeki Çin'in istihbarattaki öncelikli hedeflerini açıklayabiliriz;

- ✓ Herhangi bir tehdit unsuru harekete geçmeden önce tehdidin boyutunun ve zamanının tespit edilmesi
- ✓ Devlete karar verme konusunda yardımcı olacak bilgiler sağlama
- ✓ Ülkenin ve vatandaşın korunması, güvenliğinin sağlanması
- ✓ Devlet bilgilerinin, ihtiyaçlarının ve stratejilerinin saklanması
- ✓ Diğer hükümetlerin benzer faaliyetlerinin etkisizleştirilmesi
- ✓ Diğer hükümetlerin ve grupların davranışlarını etkileyecek örtülü operasyon süreçleridir.
- ✓ Başarılı ve etkili bir istihbarat düzenlemek için düzenli bir uygulama ile belirgin ve yerleşik bir görevlendirmeyle süreci sistematik bir şekilde yönetmektir.

Günümüzde siber uzay ile ilişkili güvenliği sağlama ve karşı tarafa saldırma faaliyetlerinde bir şekilde yukarıda ayrıntılarıyla bahsettiğimiz siber casusluk faaliyetlerini yürüten Çin, ABD'nin siber dünyadaki tartışılmaz üstünlüğüne karşı meydan okumaktadır. Çin büyüyen ekonomisiyle birlikte kendini siber alanda ispatlama çabasına girmiştir. Rusya öncelikle SSCB'den kopan ülkelere siber saldırılarıları bir tehdit unsuru olarak göstermekte iken, Çin istihbarat faaliyetlerinde siber dünyayı etkili şekilde kullanmaktadır. Böylece bu üç ülke siber dünyayı önemli bir şekilde kullanmaktadır.[347]

21. yüzyılda ABD ve Çin arasında gerçekleşen rekabet askeri, siyasi, ekonomik, teknolojik ve kültürel alanlarda başta güvenliği temel alarak başat güç olma mücadelesi şeklinde gelişmektedir.[348] Potansiyel düşmanlar siber uzay alanına yönelik yetenek, kabiliyet ve stratejilerini geliştirmiştir. Örneğin; ABD'ye karşı özellikle Çin ve Rusya siber güç faaliyetlerini arttırarak siber alanda ABD' ye karşı ciddi bir tehdit oluşturup yıkıcı etkiler yaratmaktadır. Aynı zamanda; askeri güç potansiyeli olarak ABD'ye karşı ciddi bir rakip olarak gözükmemelerine rağmen

[347]Taner Altınok, ve Haydar Çakmak, "Suç, Terör ve Savaş Üçgeninde Siber Dünya", Barış Platin Yayınevi, Ankara, 2019.
[348]Ozan Örmeci, "21. yüzyılda ABD-Çin Rekabeti", SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi, Sayı:29, Ağustos 2013, ss.1-14.

özellikle Çin tarafından desteklenen İran ve Kuzey Kore gibi ülkeler siber alanı çok iyi kullanarak kendilerine ciddi bir avantaj sağlamış ve ABD'nin rekabet gücünü azaltmıştır.

İnternetin kuruluşunda ana rol oynayan ve tüm dünyada en büyük siber güce sahip ABD'nin karşısında hem ekonomik hem nüfus hem de coğrafya olarak artan güce sahip olan Çin, siber uzayı siber casusluk, siber istihbarat, siber saldırı için kullanarak özellikle ABD'nin güvenlik sistemlerini ciddi derecede olumsuz etkilemektedir. Bu doğrultuda, siber istihbarat ve rakiplerin stratejik alt yapılarına sızma faaliyeti Çin'in en etkili istihbarat aracıdır. Örneğin; ABD ve NATO tarafından hazırlan F-35 taarruz uçağı yazılım kodlarının siber yöntemlerle Çin tarafından çalındığı yönünde söylentiler bulunmaktadır.[349] ABD F-35 projesi ile düşman uçaklara üstünlük sağlamayı hedeflerken 2009 yılının Nisan ayında verileri depolama sistemine yetkisiz giriş yapıldığının açıklanması ve hangi bilgilere ulaşıldığının net olarak açıklanamaması ciddi bir soru işareti oluşturmuştur. Bu saldırının Çin "İP" lerine uzanması bu saldırının Çin tarafından yapıldığı üzerine bir iddianın ortaya çıkmasına yol açmıştır. Bu durum; siber istihbarat sayesinde rakip ülkelerin teknolojilerini, gizli bilgilerini, askeri güçlerini ve daha birçok önemli bilgiyi elde etmenin mümkün olduğunu göstermektedir.

Günümüzde istihbarat yukarıdaki örnekteki gibi her ne kadar siber casusluk şekline dönüşse de istihbaratın temel ilkeleri siber uzay içinde değişmemektedir. İstihbaratın temel ilkeleri: planlama, sürat, kesinlik, doğruluk, uygunluk, yenilikçilik, yaratıcı zekâ ve ekip işidir. Askeri istihbarattan kastımız sadece kara, deniz, uzay ve hava değildir. Artık teknik gelişmelerle birlikte siber dünyada bu alana girmektedir. Teknolojik gelişmelerle birlikte artık sadece bilgisayarlar değil, telefonlar, tabletler, evdeki televizyonlar ve hatta buzdolapları gibi eşyalar bile internete bağlı hale gelmiştir. Böylece kişisel verilerden devletin önemli verilerine herşey dijital ortamda saklanır hale gelmiştir. Çevrim içi sistemler, veri tabanları ve bulut depolama alanları artık siber istihbaratın hedefleri arasındadır. Tüm bu dijital verilere ulaşmak için yapılan istihbarata ''siber istihbarat'', ülkeler arasındaki bilgiyi ele geçirme savaşına'' siber savaş'' yada '' enformasyon savaşı'' denir. Ekonomisi güçlü ve öngörüsü yüksek devletlerin hepsi güvenliklerini sağlamak için siber alana

[349]Habertürk, F-35 Savaş Uçağı Verileri Çinliler Tarafından Hacklendi, 16.10.2017, https://www.haberturk.com/f-35-hacklendi-1674633-ekonomi , ET.14.12.2019.

yatırımlarını arttırmaktadır. Fakat Çin dünyadaki teknolojik araçların üretim merkezinde olduğu için bu alanda en önemli aktörlerin başında gelmektedir.

2009 yılında Siber Muharebe ve Güvenlik birimlerini kuran ABD, özellikle Rusya ve Çini siber alanda bir tehdit olarak gördüğünü defalarca kez açıklamıştır. Çünkü Çin bu alanda hem saldırı hem savunma kapasitesine yönelik yatırımlar yapmakta, birimler kurmakta ve kendi intranet(firewall duvarı= Çin Seddi) yapısını oluşturup kullanmaktadır. Eğer bu hızı üst otorite kurularak engellenmezse, atom bombasına göre riski az olup etki kuvveti daha yüksek olan bu savaş boyutu tüm dünyayı felakete sürükleyecek bir ortamı hazırlayabilir.

1990 yıllarında ABD'nin tek güç kalarak Soğuk Savaş'ı kazanmasının ardından internetin gücünün arttırması Çin'in dış politika stratejisini de değiştirmesine yol açmıştır. Daha önce, sayısal üstünlüğü ile ABD'yi yenebileceğini düşünen Çin, artık ordusunu küçültüp, yeni teknolojiler yaratıp siber uzayda üstünlük sağlayarak ön plana çıkmayı hedeflemektedir. Bu sebeple, ABD üzerinde siber casusluk faaliyetleri yürütmekte, siber ordu birimleri kurmakta, hacker grupları oluşturmakta ve kendi siber uzayını korumak için alt yapı geliştirmek gibi faaliyetleri birbiriyle bağlantılı olarak sürdürmektedir. Örneğin; Çinli elektronik devi Huawei Pekin yönetimi ve Çin gizli servislerine olan yakınlığından dolayı birçok ülkede eleştirilmektedir. Çin şirketini siber güvenlik riski olarak sınıflandıran ABD, Huawei teknolojisinin casusluk faaliyetlerinde kullanıldığını öne sürerek 6.12.2018 tarihinde Huawei'nin kurucusu ve sahibi Ren Zhengfei'nin kızı Meng Wanzhou Vancouver'da gözaltına almıştır.[350] Tüm bu gelişmeler aslında ABD tarafından siber uzayda en tehlikeli aktör olarak kabul edilen Çin'in, sadece karanlık bir süper güç değil aynı zamanda dünyanın en büyük internet kullanıcı sayısına da sahip olmasından kaynaklanmaktadır. Dünya'nın en fazla kullanıcısına sahip olan Çin'de siber casusluğun Devlet ve Devlet Dışı Aktörler arasındaki ilişkilerdeki kullanımının artması da gayet normaldir.

Sonuç olarak; 1990'ların başından bu yana Çin'in gerçekleştirdiği reform sürecinin asıl amacı, Batı teknolojisinden ve Batı'nın liberaline yaklaşmadan küresel pazar ekonomisiyle ticareti kullanarak sürekli ekonomik kalkınma sağlamaktır. Bu sebeple; Çin, internet gelişimini reformunu ve politikalarını, Endüstri 4.0'ın

[350]Deutsche Welle, Huawei'nin Sahibinin Kızı Kanada'da Gözaltına Alındı, Deutsche Welle, 06.12.2018, https://p.dw.com/p/39YfO ET.29.01.2020.

modernizasyon yönelimini artırmak için önemli bir fırsat olarak görerek internet'in geliştirilmesi için bir dizi politika geliştirdi. Çin'deki internet, ülkenin reformlarını oluşturan politikalarla birlikte gelişmiştir. Toplum 5.0'ın tartışmalarıda bu şartlara dayanmaktadır. Kısaca, Çin'in ekonomisi ve toplumu hızla ilerlemeye devam ettikçe ve insanların kültürel ürünlere olan talepleri artmaya devam edecek böylece internet daha fazla insana ulaşacak bu da daha fazla kullanıcı talebine yol açacaktır. İnternetin artan bu öneminden dolayı Çin küresel sahnede güçlü bir devlet haline gelmeye devam ederek diğer güçlü devletler gibi rakipleriyle siber uzayda güç ve casusluk oyunlarına katılacaktır. Zaten Çin'in internet tabanlı düşmanlarını izlemek ve bozmak için siber suç taktiklerini kullandığını Batı'daki ülkeler ısrarla vurgulamaktadır. Örneğin; ABD - Çin Ekonomik ve Güvenlik İnceleme Komisyonu (USCESRC) İnternet ilişkilerini 2010'daki rapor doğrultusunda yeniden yapılandırdı. Bunda China Telecom'un hatalı ağ trafiği rotalarının büyük miktarda internet trafiğini ele geçirmesi sebep olmuştur.[351] Bu olay sonrasında Batı, Çin'in siber casusluğu konusunda endişe duymaya başladı. Sonrasında ise İnternet devi Google, Çin'deki varlığını sorgulamaya başlayarak ülkeden kaynaklanan "sofistike ve hedefli" bu siber saldırılar sonrasında Çin'deki operasyonlarına son verebileceğini söyledi.[352] Yani süreç hem ekonomik hem de siyasi anlamda bu kadar hassas bir hal aldı. ABD destekli Google ve Çin arasındaki bu güvenlik ihlallerine yönelik suçlamalar sadece özel bilgilerin çalınması ile ilgili de değildi. Aynı zamanda insan hakları aktivistlerinin e-posta hesaplarını da hedefliyordu. 2010 yılındaki bu süreçte; internet devi Google, Çinli yetkililerin uyarılarına karşın Çin'deki arama motorunda Çin'in casusluk yaptığı gerekçesiyle sonuçları sansürlemeyi durdurdu. Çin ise Google'ı Çin pazarına girerken verdiği, yasalar uyarınca arama sonuçlarını filtreleme yönündeki 'yazılı taahüdünü' ihlal etmekle suçlayarak yasalara uydukları sürece ülkede faaliyet gösterebileceklerini belirtti. Çünkü Çin yasalarına göre, yetkililerin kullanıcı etkinliğini izlemelerine yardımcı olmak ve bunları kaldırmak veya politik olarak hassas içeriğin yayınlanmasının ve yayınlanmasının önlenmesi hakkı vardır.

[351]U.S.-China Economic and Security Review Commission (USCESRC), 2010 Report to Congress of the U.S. – China Economic and Security Review Commission at the 11th Congress, Second Session, Kasım 2010. https://www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf ET:24.01.2020.

[352]Google,May Pull Out of China after Gmail Cyber Attack, BBC News, 13 Ocak 2010, http://news.bbc.co.uk/2/hi/8455712.stm. ET:24.01.2020.

Bu hak doğrultusunda Google Çin'e özel sansürlü arama motoru oluşturarak gerginliği sona erdirdi.[353] Fakat bu durum Batı'nın bakışı ile Çin'in iç politikası hakkında doğrudan bir çatışma yaşandığının göstergesidir.

Yukarıda anlattıklarımız ışığında siber alanda güvenliği sağlamak için birçok ülkenin siber ortamda milli egemenliklerini sağlama çabası içerisinde olduğunu rahatlıkla söyleyebiliriz. Fakat Çin internette dünyanın en sofistike hareketlerin görüldüğü ve siber ortamdaki en katı filtreleme, engelleme ve kontrol sistemlerini uygulayan ülkedir. Çünkü Çin hükümetinin internet sansürü hakkında doğrudan yargı yetkisi ve güçlü kontrol araçları vardır. Bu bağlamda Çin'in özel sektör üzerinde ağ bağlantılı bir otoriteryanizm kurduğu görülmektedir.[354]

Ayrıca, Çin hükümeti ülkede internet penetrasyonunun hızla artmasından dolayı, 2010 yılında yayınladığı İnternet Beyaz Kitabında ülke çapında internet ve mobil penetrasyonun yaygınlaşmasını stratejik bir öncelik olarak ilan etmiştir. Böylece Çin'in uzun vadeli küresel ekonomik rekabet gücünün arttırılabilmesi ve dış politika süreçlerinin belirlenmesinde yerli internet ve Telekomünikasyon sektörü kritik bir öneme sahip olmuştur.[355] Çin'in iç politikasında üzerinde durulan en önemli nokta ise Çin Halk Cumhuriyeti (ÇHC)'nin, Çin Komünisti tarafından yönetilen tek partili bir devlette dayanmasıdır. Bu noktada Çinli şirketlerin iç politikayı desteklemesi ve pekiştirmesi beklenirken kominist otoriteye karşı gelebilecek siber tehditlere karşı da rol oynamaları beklenmektedir. [356]

4.3.2. Çin'in Siber Savaş Faaliyetleri

Çin'in mevcut siber yapıyla bir çatışma halindedir. Bu çatışmanın resim bulmuş hali ise ICANN düzenlemesidir. Mevcut internet yönetişimi rejimi, Çin'in tercihleri ile iki farklı şekilde çatışmaktadır. Birincisi, Çin'deki geleneksellik yerine, internet'in liberalizmin mirası olmasıdır. Yani, internet faaliyetlerinin ve sosyal

[353] Deibert, Palfrey,Rohozinski, ve Zittrain, a.g.e , ss.190-196.
[354] Rebecca MacKinnon, Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom, a paper presented at Liberation Technology in Authoritarian Regimes Conference, sponsored by the Hoover Institution and the Center on Democracy, Development, and the Rule of Law(CDDRL),StanfordUniversity,11–12Ekim2010, http://rconversation.blogs.com/MacKinnon_Libtech.pdf ET:24.01.2020.
[355]Information Office of the State Council of the People's Republic of China, The Internet in China, 08.06.2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm ET:24.01.2020.
[356]David Talbot, China: Our Internet Is Free Enough, MIT Technology Review,16.06.2010, http://www.technologyreview.com/web/25592/ss1/ . ET:24.01.2020.

kullanımlarının özgürce, özel sektör temelli ve ulus ötesi yönetişim biçimini temel alacak şekilde ekonomik ve politik normlarla bağlantılı olmasıdır. Bu yapı içerisinde tezde de belirttiğimiz gibi internet için yaygın bir özdenetim kuralları ve kurumlarının oluşturulması şarttır. Burada ulus devletlerarasında ciddi görüş farklılıkları bulunmaktadır. İkincisi, ABD'nin mevcut internet yönetişimindeki ayrıcalıklı rolüdür. Çin ve ABD arasında gerçekleşen ticaret ve teknoloji çatışmaları, saldırı ve istihbarat suçlamaları da bu bağlamda gerçekleşmektedir.

Çin'in devlet merkezli görüşüne göre, internet özgürlüğü ABD'ye bilginin kontrol ve yönetiminde hegemonik bir güç kazandırır. Bu yüzden Hillary Clinton'ın "İnternet özgürlüğü" girişimlerindeki Çin casusluğu iddiası ve Çin'in ABD'nin emperyalizm suçlamaları karşılıklı olarak aynı mantıksal temele dayanır. Özellikle ABD'nin Çin'in Büyük Güvenlik Duvarı 'nın dışa aktarılması talepleri Mart 2010'da, Çin'de bulunan kök sunucular tarafından Çin dışındaki internet kullanıcılarının erişimlerinin (Facebook, YouTube ve Twitter) gibi popüler Web sitelerine zarar vermesiyle daha açıktan dillendirilmeye başlamıştır.[357] İki ülke liderleri arasında yukarıda bahsettiğimiz bu çatışmalar hep bir kontrol, yönetim, denetim gibi birçok alanda internetin yönetişimi ile ilgili sorunları kapsamaktadır. Bu süreçte ABD uluslararası sistemde kullanılması ve kontrolün sağlanması için ICANN'ın kurulmasını ve herkesin üye olmasını desteklemiştir. Fakat Çin ABD'nin internet üzerindeki hâkimiyetini arttırmamak ve kendi ulusal internet ağını dışa bağımlı yapmamak için ICANN'a karşı soğuk bakmıştır. Çin ve ABD arasında net ayrışmazlığa düşüren ICANN'ı kısaca açıklarsak;

Türkiye'de İnternet Tahsisli Sayılar ve İsimler Kurulu adıyla hizmet veren ICANN(Internet Corporation of Assigned Names); tüm internet kullanıcılarının geçerli adresler bulabilmesi için DNS teknik unsurlarının yönetimini yapmaktadır. Üst düzey alan adlarının (.com, .info vb.) kullanılma yetkilerini dağıtarak kontrollerini sağlayan ICANN kendi tabiriyle internet protokolü (IP) adresi alanı tahsisi, protokol tanıtıcı ataması, genel (gTLD) ve ülke kodu (ccTLD) üst düzey alan ismi sistemi yönetimi ve kök sunucu sistemi yönetimi işlevlerinden sorumlu kar amacı gütmeyen bir oluşumdur. Küresel internet topluluklarının bir araya gelerek

[357]Earl Zmijewski, Accidentally Importing Censorship, Renesys Blog, 30.03.2010, http://www.renesys.com/blog/2010/03/fouling-the-global-nest.shtml ET.24.01.2020.

oluşturduğu ICANN; internetin kullanıcılara belirli etik kuralları çerçevesinde ulaşmasını hedeflemektedir.

ICANN'ın küresel sistemdeki bu rolüne, 2001 yılında toplantılarına temsilci göndermeyi bırakan Çin karşı çıkmıştır. Aslında tam bu yüzden dünyanın iki büyük gücü arasındaki internet yönetişimi mücadelesinde Uluslararası Telekomünikasyon Birliği (ITU) sorun çözücü bir görev üstlenebilirdi. ITU tarafından, internetle ilgili konularda hem teknik hem de politika ile ilgili hususları kapsayan 101, 102, 133 sayılı alınan kararlar bu yönde olumlu bir ışık vermişti. Ayrıca İnternetle ilgili kaynakların dünya çapında yoğun bir şekilde konuşlandırılması ve doğrudan ağa bağlı IP özellikli tüketici cihazlarının entegrasyonu ile IPv4 adreslerinin tükenmesi sorunu ve IPv6'nın konuşlandırılması konusunda daha iyi farkındalık yaratılması amacıyla (2002,2005 ve 2008) çalıştaylar düzenlendi.[358] Tüm bu gelişmelerin üzerine 2006 ve 2010 yıllarında dönemin İTÜ Genel Sekreter Yardımcısı seçilen Çinli Houlin Zhao ve Genel Sekreter Dr. Hamadoun I. Touré siber alanda ITU'nün görev üstlenmesi için ciddi çalışmalar yürütmüştür. Sonrasında ise 23 Ekim 2014 tarihinde Çinli Houlin Zhao'nun ITU Genel Sekreteri seçilmesi bir fırsat olmuştur. Fakat bu dönemde Rusya'nın da siber alandaki çözüm için desteği olmasına rağmen ABD'nin çekimserliğiyle Bölgesel İnternet Kayıtları (RIR'lar), İnternet Protokolü (IP), bölgelerindeki sağlayıcılar (İSS'ler), kuruluşlar ve hükümet için egemenlik modellerine uygun hale gelebilecek bir politika üretilemedi.[359] Bu sebeple, Rusya ve Çin büyüyen ekonomilerinin yanında siber alanda en büyük güce sahip olan ABD'nin üstünlüğünü tartışmalı hale getirebilmek için günümüzde yaşanan başta ticaret savaşları olmak üzere birçok sektörde siber alanı etkili olarak kullanmaktadır.

Çin kendi içinde ICANN düzenlemesini gerçekleştirirken dışarıda da aktif politikalar izlemektedir. Kısaca bu süreci açıklarsak;

1990'larda Soğuk Savaş'ın bitmesi ile birlikte anarşik yapıda gerçekleşen güç değişimleri ve internetin ortaya çıkmasıyla birlikte tüm hayatın ve araçların sanal ortama geçmesi sonucunda oluşan yeni süreçte Çin bir ulusun sistematik olarak yapacağı her şeyi yaptı. Yaptığı bu hamlelerle Soğuk Savaş sonrası çok kutuplu bir

[358]Sureswaran Ramadass, A Study on the IPv6 Address Allocation and Distribution Methods, International Telecommunication Union, Geneva, 2009. https://www.itu.int/dms_pub/itu-t/oth/3B/02/T3B020000020001PDFE.pdf ET:24.01.2020

[359]Houlin Zhao, ITU and Internet Governance, İnput To The Seventh Meeting Of The ITU Council Working Group on WSIS, Geneva,12 – 14 Aralık 2004.

hal alan dünya da ABD'nin özellikle ekonomik anlamda en büyük rakibi oldu. Çin ekonomik anlamdaki başarısını teknolojik gelişmelerinde etkisiyle tüm dünyada arttırdı. Özellikle nesnelerin interneti ile birlikte **i**nternet'in hayatın her alanında kullanılmaya başlamasıyla birlikte e-ticaretin de gelişmesi sonucunda Çin, ekonomi dışında siyasi, askeri ve istihbarat konularında siber alana olan ilgisini arttırdı. Böylece Çin siber alanda hem savaş yetenekleri hem güvenlik faaliyetleri hem de casusluk faaliyetleri için ciddi çalışmalar yürütmeye başladı. Tüm bu çalışmalar sonrasında özellikle rakibi ABD tarafından Çin saldırgan siber savaş yeteneğini kullanan bir ülke ilan edildi. Çin ise aynı şekilde ABD'yi suçlayarak kendi güvenliğini sağlayabilmek için kendi siber savaş askeri birimlerini oluşturdu. Böylece siber alanda çatışma süreci karşılıklı olarak hızlandı.

1990'ların sonunda ABD'yi caydırmak için bu kayıt dışı savaşın başlatıldığından bahsederek bu çatışma süreci hakkında görüşler sunan Robert K. Knake'a göre ekonomik büyüme ve savunma harcamalarını içeren çeşitli nedenlerden dolayı, Çin ABD'nin siber savaş rakibidir. Washington'daki Çin Büyükelçiliği sözcüsü Wang Baodong, Amerikan endişesinin Soğuk Savaş kalıntısı olduğunu belirterek "Çin'in ABD'ye karşı siber saldırıların veya siber casusluğun arkasında veya arkasında" olduğu iddialarım haksız, sorumsuz, yanıltıcı ve kasıtlı olduğuna değinmiştir. Bu açıklamaların Çin'in tehdit hislerini artırmak için üretildiğinden bahsederek bu iddiaları reddetmektedir.[360] Karşılıklı bu suçlamalardan sonra kısaca Çin tarafından gerçekleşen çatışma örneklerini incelersek;

İlk olarak, Sırp güçleri tarafından 1999 yılında Kosova Savaşı'nda gerçekleşen Kosova'daki katliamı durdurmak ABD ve NATO destekli hava saldırısından sonra gerçekleşen olaylardır. Bu hava saldırısıyla, ABD savaş uçağındaki ve akıllı silahlarındaki mekanik arıza sonucunda hedef Yugoslav Federal Tedarik Müdürlüğü olması gerekirken koordinatlar 200 metre saparak Çin'in Belgrad Büyükelçiliği'ni bombalamıştır. Bu olay sonrasında Çinliler ABD büyükelçilikleri ve konsoloslukları dışında protesto gösterileri düzenlediler. Çin'de BM ve diğer organlardan yapılan başvurularla mağdurlar için tazminat talep etti. Aynı zamanda Büyükelçilik bombalamasından en az 12 saat sonra Çin'in Kızıl Hackerlar Birliği

[360]Quoted in Ellen Nakashima and John Pomfret, China Proves to Be an Aggressive Foe in Cyberspace,Washington Post, November 11, 2009. www.washingtonpost.com/wp-dyn/con tent/article/2009/11/10/AR2009111017588_pf.html .ET:20.01.2020.

ABD web sitelerine karşı binlerce siber saldırı başlatmıştır. Böylece bazı ABD ve NATO web sayfaları tahrif edildi.[361]

Çin'in siber saldırılarıyla alakalı bir diğer örnek Çinli hacktivistler tarafından 2001'de gerçekleşmiştir. 2001 yılında bir ABD "casus uçağı" Çin hava sahasına girdiğinde ve Çin avcı uçağı tarafından zorlandığında pasifikte çarpışmıştır. Bu olay sonrasında ABD'nin izinleri dışında kendi sınırları içerisinde istihbarat faaliyeti yürütmesinden öfkelenen Çinliler, Çin jeti düşünce Beyaz Saray'ın sitesine saldırmıştır. Amerika'nın en büyük sitelerinden twitter, spotify, netflix, amazon, reddit, gibi uygulamalara yönelik Ddos siber saldırıları düzenlenmesi sebebiyle tüm halkın bu uygulamalara erişimi kesilmiştir. Bu olay sonrasında ABD'den gelebilecek saldırılara karşı güvenliğin sağlanması fikrinin acil bir önem kazanmasından dolayı 2003 yılına kadar Çin, siber savaş birimlerinin kurulduğunu açıklamıştır. 2003 yılında bu birim kurulduktan sonra Pentagon'a göre, Hainan Adası'nda PLA Üçüncü Teknik Departmanı ve Lingshui Sinyalleri İstihbarat Tesisinde Çinliler siber alanda savunma ve daha önce hiç görülmemiş siber silahlar tasarladı. Bu silahlar; bilgi keşiflerini yürütmek, bilgi bombaları bırakmak, bilgi çöpü yaratmak, bilgi aldatmacasını uygulamak, bilgi savunmasını organize etmek, ağ casus istasyonları kurmak ve network ağ verilerini değiştirmek gibi birçok amaca hizmet edebilecek teknik kapasiteye sahipti.[362] Bu sebeple Amerika da, siber güvenliğe yönelik ilk belgesi olan 2003 tarihli The National Strategy to Secure Cyberspace adlı belgeyi yayınlamıştır.[363] ABD'nin siber savaş birimlerinin kurulduğunu zamanlar Çin ise ABD internet trafiğini ve DoD iletişimini izlemek için Küba'da Castro hükümetinin izniyle ABD'den uzak olmayan iki "ağ casus istasyonu" kurdu. Titan Rain olarak bilinen bu dönem bugüne kadarki en kötü siber casusluk dönemlerinden biridir. Bilgisayar korsanları savunma yüklenicisi Lockheed Martin, diğer askeri yerlere yönelik terabaytlarca veri için mücadeleye girişmiştir.

2007 yılına gelindiğinde Çin'in Avrupa ağlarına yönelik saldırılarının da devam ettiğini özellikle Almanya'daki mevkidaşı Hans Remberg'in, Pekin hükümetini Alman Şansölyesi Angela Merkel'in bilgisayarına saldırmakla suçladığı

[361]Clarke ve Knake, a.g.e. , ss.20-30.
[362]Clarke ve Knake, a.g.e. , ss.20-30.
[363]Reuters, Dijital Dünyada Kaos Yaşanıyor: 3. Dalga Başladı, Sputniknews, 22.10.2016, https://sptnkne.ws/c4W4, ET.30.01.2020.

ifadelerde görebiliriz. Çin hükümeti, ABD ve Avrupa ağlarının penetrasyonları, büyük kopyaları başarıyla kopyalayıp elindeki veri hacmiyle onlara ürün ihraç edebilecek bir seviyeye gelmiştir. Aslında Çin'in siber savaş gelişimi tuhaf bir şekilde şeffaf ilerlemiştir. Ancak ABD istihbarat yetkilileri siber uzayda Çin'i Rusya kadar büyük bir tehdit görmemektedir. 2010 yılına gelindiğinde Amerikan arama motoru Google, hacklendiğini açıklayarak verilerin Çin tarafından çalındığını iddia etmiştir. Hilary Clinton'da bu saldırıların sorumlusunu Çin olarak göstermiş olsa da Çin bu iddiaları yalanlamıştır.[364] Fakat 2010 yılında ABD-Çin Ekonomik ve Güvenlik İnceleme Komisyonu tarafından Kongreye sunulan raporda tüm internet hedeflerinin% 15'ine gelen ve giden trafik, devlete ait bir Telekomünikasyon şirketi olan China Telecom'a ait sunucular üzerinden yönlendirildiği belirtmiştir. Böylece komisyona göre Çin'in internet trafiğini kontrol etme ve manipüle etme yeteneği artmış olduğundan önlem alınmalıdır.[365] 2011 yılına gelindiğinde The Independent Gazetesi Rusya ve Çin'in siber saldırılarda ortak hareket ettiğini belirtilerek G8 ülkelerinin ekonomik ve siyasi verilerinin Rusya ve Çin tarafından beraber çalınmaya çalışıldığı yönünde Çine yönelik saldırı ve casusluk iddiaları ortaya atmıştır. 2018 yılında ise iddialar ve suçlamalar daha çok yazılım üzerine kaymaya başlamıştır. ABD yetkilileri, Çin'de üretilen teknolojik aletlere Çinin daha üretim aşamasında virüs yerleştirdiğini iddia etmiştir.[366] 2019 yılı içerisinde ise ABD merkezli teknoloji şirketi Symantec, Çinli hacker'ların ABD Ulusal Güvenlik Ajansının siber yazılımını ele geçirip saldırı için kullandığını iddia etmiştir.[367] 2020'nin ilk günlerine girdiğimizdeyse ABD Adalet Bakanlığı, özel kredi kuruluşu Equifax'a yönelik Çin Halk Kurtuluş Ordusu'na mensup 4 kişiyi siber saldırıdan sorumlu tutarak suç duyurusunda bulundu.[368]

---

[364]Johnson Bobbie, US Asks China To Explain Google Hacking Claims, Theguardian, 31.01.2010, https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us ET.14.12.2019.
[365] Jaikumar Vijayan, Report Sounds Alarm on China's Rerouting of US Internet Traffic, Computerworld, 18 Kasım 2010, https://www.computerworld.com/article/2514493/update--report-sounds-alarm-on-china-s-rerouting-of-u-s--internet-traffic.html ET:20.01.2020.
[366]İ. Doğru, Çin'de Üretilen Bilgisayar Ekipmanlarında Casus Çip İddiası, Anadolu Ajansı, 04.10.2018,https://www.aa.com.tr/tr/dunya/cinde-uretilen-bilgisayar-ekipmanlarinda-casus-cip-iddiasi/1273175, ET.28.01.2020.
[367]TRT haber, Çinli Hacker'lar ABD'ye ABD'nin Siber Yazılımıyla Saldırdı, 05.05.2019, https://www.trthaber.com/haber/dunya/cinli-hackerlar-abdye-abdnin-siber-yazilimiyla-saldirdi-414599.html ET.28.01.2020.
[368]Dpa, ABD'den Çinli Askerlere Siber Saldırı Suçlaması, Deutsche Welle Türkçe, 10.02.2020, https://p.dw.com/p/3XZf1 ET.28.02.2020.

Tüm bu örnek vakalarda incelendiğinde sonuç olarak; Çin'deki "İnternet" daha çok bir şirketin, bir intranetin iç ağı gibidir. Hükümet hizmet sağlayıcıdır ve bu nedenle ağın savunmasından sorumludur. Çin'de, hükümet "Çin'in Büyük Güvenlik Duvarı" ile ağı aktif olarak savunur. Bu yüzden Çin'in mevcut ağ saldırılarına açık olmayacak kendi tescilli işletim sistemi, uluslararası alanda teknik sorun çözümü uygulanmasını geciktirmiştir.[369] Fakat Amerika Birleşik Devletleri'nde durum bunun tamamen tersidir. Çünkü ABD özel mülkiyetle işletilmektedir. Bu yüzden de Çin ve ABD arasında genelde siber çatışmalar gerçekleşmektedir. Eğer Çin ile ABD arasında bir savaş çıkma ihtimali ortaya çıkarsa, bu sefer siber alanda güç üstünlüğü olan mücadeleden galip olarak çıkacaktır. Çünkü siber uzay çağında siber silahların sofistike cephaneliği düşmana karşı yıkıcı bir etkiye dönüşebilir. Bunun en önemli sebebi de artık orduların internet olmadan çalışma yeteneğine sahip olmamasıdır. Lojistik, komuta ve kontrol, filo konumlandırma, hedefleme, ateşleme gibi her şey yazılım ve internet teknolojilerine dayanmaktadır. İşin ilginç tarafı da bunların hepsi aynı evdeki bilgisayarlarımız gibi güvensizdir, çünkü hepsi aynı kusurlu temellere, aynı güvensiz yazılım ve donanımlara, aynı teknolojilere dayanmaktadır. Bu yüzden aktörler özellikle bilgi sistemleri ve ağlarının güvenliği ile yazılım alanında ciddi bir üstünlük mücadelesi vermektedir. Bu mücadele verilirken de zaman zaman yaşanan güvenlik krizleri çatışma örnekleriyle somutlaşmaktadır.

Çin özelinde de birçok çatışma örneği mevcuttur. Örneğin, Çin, ulusal, kültürel güvenliği ve rejim istikrarını dengelemek için siber alanda ciddi anlamda mücadele etmektedir. Bu sebeple Dünyanın en gelişmiş internet sansürü ve gözetimine sahip olmasının yanında dünyanın en büyük internet nüfusuna ev sahipliği yapan ülke de Çin'dir. Çin'in sahip olduğu bu özellikler onun özellikle siber alanda gerçekleşen saldırılar hakkında çok konuşulan bir ülke olmasına yol açmaktadır. Son zamanlarda siber casusluk, vatansever hack ve hırsızlık açıklamalarının artması da özellikle ABD ile Çin arasında fikri mülkiyet konusunda hem bölgesel hem de küresel düzeyde gergin bir rekabet oluşmasına yol açmıştır.[370] Zaten telnet saldırılarının en yüksek yüzdesinin (menşe ülkeye göre) Çin (% 13.78)

[369]Richard A. Clarke ve Robert K. Knake, "Cyber War The Next Threat to National Security and What to Do About It", Harper Collins e-books ss.70-80.
[370]Deibert, Palfrey,Rohozinski ve Zittrain, a.g.e, ss.5.

olması da bu süreci kanıtlamaktadır.Aynı zamanda siber güvenliği sağlamak için en güncel mevzuat Fransa, Rusya ve Almanya ile birlikte Çin'dedir. [371]

4.4. NATO'nun Siber Güvenlik Stratejisi ve Politikaları

4.4.1. NATO'nun Siber Operasyonlardaki Amaç ve Zorlukları

İttifak'ın caydırıcılık ve savunma tutumunu bir bütün olarak güçlendirmek ve desteklemek için kara, deniz ve havada nasıl etkili çalışılıyorsa siber ortamda da ittifak olarak gerçekleştirilmesinin gerekliliği 2018 yılında Brüksel'de teyit edildi. Fakat her ne kadar teyit edilse de bu konudaki en büyük zorluk, sonucunun askerî olmasına rağmen bu sonuca sadece askerî yoldan ulaşılamayacak olmasıdır.

2016'da siber uzayın bir operasyon alanı olarak görülmesinden sonra Ekim 2018'de NATO kurulacak Siber Uzay Operasyonları Merkezi ile ilgili çalışma gerçekleştirildiğini duyurmuştur. Siber Uzay Operasyonları Merkezi, siber uzay güvenliği konusunda farkındalık yaratmak, ittifak operasyon ve misyonlarının siber uzay boyutunun merkezî planlamasını yapmak ve siber uzay operasyonları ile ilgili koordinasyonunu gerçekleştirmekten sorumlu olacak şekilde planlanmıştır. Ayrıca, Brüksel Zirvesi'nde müttefik ülkelerin kendi ulusal siber varlıklarının ittifak'ın operasyon ve misyonlarına ne şekilde entegre edilebileceği konusunda NATO'nun savunmaya yönelik yönergesiyle tutarlı bir görüş sergilediler. Bu görüş; siber alanı NATO'nun diğer alanlarda Müttefiklerin İttifak operasyon ve misyonlarına tahsis ettikleri tanklar, uçaklar ve gemilerle nasıl kendini savunuyorsa, siber savunma alanında da bunun yapılması gerektiğini ve siber alanın yeni bir savaş silahı olduğunu kabul ettiklerini göstermektedir.

NATO'nun güvenlik politikası içerisinde siber kavramını kullanmasının yanında işbirliğini geliştirmek, çözümler üretmek ve koordine etmek için Estonya olayından sonra Siber Savunma Mükemmeliyet Merkezi kurulmuştur. Bu mükemmeliyet merkezi kapsamında NATO, üyelerine eğitim, öğretim ve tatbikat programları ile uygulama geliştirmeleri için yardımcı olmaktadır. Fakat her ülkenin kendi milli ulusal siber güvenlik mekanizmalarının, kurallarının ve kurumlarının olmasından dolayı tek bir vücut olunamamaktadır.

---

[371]Personel Writer, SA Ranks As 31st Worst Country At Cyber Security, İTWeb, Johannesburg, 04.03.2020, https://www.itweb.co.za/content/5yONPvEg2YkMXWrb ET.09.04.2020.

4.4.2. NATO'nun Siber Savaş Faaliyetleri

NATO, siber savaş kavramının ortaya çıkmasıyla birlikte doktrinini değiştirmiş ve konunun teknik ve hukuki boyutunu tartışmak üzere çalışmalara başlamıştır. 2007 yılında Estonya'nın maruz kaldığı siber saldırı ise hazırlık boyutunu farklı bir boyuta taşıyarak resmi bir "NATO Siber Savunma Politikasının" hazırlanmasına yol açmıştır. 2010 yılındaki Lizbon zirvesindeyse siber savunmanın sürekli olarak NATO gündeminde bulunması yönünde temel bir karar alınmıştır. 2011 yılında NATO Siber Savunma Politikası ve Siber Savunma Eylem Planı'nın detayları kabul edilmiştir. Siber savunma politikasındaki siber tehditler, yeni stratejik kavram doğrultusunda 5. maddede ifade edilen toplu savunma görevini yerine getirmesi için potansiyel kaynak olarak tanımlanmaktadır. Bu yüzden 2012 yılında NATO Bilgisayar Olayları Karşılama Kapasitesi'nin (NATO Cyber Incident Response Capability - NCIRC) tamamen operasyonel hale gelebilmesi için 58 milyon Avroluk bir kontrat imzalanmıştır.[372] Bu doğrultuda NATO'nun kurumsal gücünün arttırılması ve olaylara daha etkili müdahale edebilmesi hedeflenmiştir. Böylece geçmişten gelen Rus tehditlerine yönelik korkuların siber ortamda da önüne geçilmesi planlanmıştır.

Colin S. Gray'a göre günümüzde artık askeri yetenekler; hava gücü, uzay gücü, bilgiye dayalı savaş, siber savaş ve stratejik bilgi savaşı gibi alanlarda güvenlik, politik ve stratejik mücadeleleri kapsamaktadır.[373] Colin S. Gray'in stratejik kültür bakışı çerçevesinde; bu açıklamalar Soğuk Savaş ruhunun aslında bam başka bir boyutta içinde tehdit, korku ve riskleri içerecek şekilde tamamen güvenlik kaygısını baz alacak şekilde devam ettiğini yani geçmişteki korkuların siber savaş boyutunda yaşandığını göstermektedir. Benzer bir süreç olmayan ve birbirlerinden tamamen farklı bir boyutta yaşanan Siber Savaş yıllarını Soğuk Savaş ile aynı kefeye koyamayız. Her ne kadar içinde bulunduğumuz siber savaş sürecini Soğuk Savaş ile aynı kefeye koyamasak da Soğuk Savaşın bitmesiyle beraber uluslararası sistemin güvenlik dinamiklerinin değişerek siber güvenliği önemli hale getirdiği tartışmasız bir gerçektir.

---

[372]Neil Robinson, Başarılı Bir Siber Savunma İçin Harcama Yapmak, NATO Dergisi,2017 https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html , ET 29.01.2020.

[373]Colin S. Gray, Modern Strateji, Çev. Öz, H. Truva Yayınları, 2008 ss.249.

Soğuk Savaş'ın bitmesinden sonra özellikle Rusya ve NATO üyesi ülkeler arasında günümüzde siber savaş yaşanmaya başlamıştır. Bu iddianın gerçekliğini ortaya koymamızda Kuzey Atlantik Antlaşması'nın 5'inci maddesi çok önemlidir. [374]

17.10.2018 tarihinde dönemin NATO Genel Sekreteri Jens Stoltenberg, Rusya'nın "siber saldırılar" düzenlediğini iddia ederek, Madde 5'in devreye sokulabileceğini belirttiği sözleri[375] siber uzayın uluslararası ilişkilerin güvenlik literatüründeki önemini gösteren en güzel örneklerden biridir. Kuzey Atlantik Antlaşması'nın 5'inci maddesi müttefiklerden birine karşı yapılan saldırının bütün müttefiklere karşı yapıldığını belirtmekte ve bu kapsamda kullanılabileceğine yönelik bir bildiri şeklinde olmuştur. Aynı zamanda, NATO'nun toplu savunma, kriz yönetimi ve işbirliğine dayalı güvenlik yaklaşımını ittifakların siber alandaki faaliyetlerinde yürütme niyeti böylece herkes tarafından görülmüştür.

Soğuk Savaşın bitmesiyle beraber uluslararası sistemin güvenlik dinamikleri değişmiştir. Böylece NATO ve karşısında Rusya yeni durumun gereklerine göre yeniden yapılanmıştır. Bu doğrultuda Dünya'nın en büyük askeri örgütlerinden biri olan NATO'nun Siber Strateji kavramına bakışı; Colin S. Gray'in stratejik kültür bakışını destekler nitelikte stratejik olsun olmasın, geçmişte paylaşılan kültürün bir şekilde davranıştan ayrılmasının mümkün olmadığı tezini ortaya çıkarmaktadır. Çünkü NATO'nun Soğuk Savaş döneminde yaşadığı geçmiş korkularının 21. yüzyıl güvenlik bakışını şekillendirdiği yönünde stratejik kültürle bir bağ kurulabilir. Aynı zamanda Rusya'nın geçmişten gelen hep Avrupa'ya hâkim olma, süper güç olma fikri gelecek siber savaş stratejilerinin altında yatan dış politika oluşturmaya yönelik bir stratejik kültür yarattığı düşünülebilir. NATO ülkeleri ve Rusya arasında

[374]Madde 5 Taraflar, Kuzey Amerika'da veya Avrupa'da içlerinden bir veya daha çoğuna yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle bir saldın olursa BM Yasası'nın 51. Maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak ve diğerleri ile birlikte, silahlı kuvvet kullanımı da dahil olmak üzere gerekli görülen eylemlerde bulunarak saldırıya uğrayan Taraf ya da Taraflara yardımcı olacakları konusunda anlaşmışlardır. Böylesi herhangi bir saldın ve bunun sonucu olarak alınan bütün önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Güvenlik Konseyi, uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığı zaman, bu önlemlere son verilecektir. NATO, 4 April 1949 The North Atlantic Treaty,WashingtonD.C.,10Nisan2019,https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=en, ET.24.11.2020.

[375]Türkiye Gazetesi, NATO Gözünü Kararttı! Büyük Tehdit https://www.turkiyegazetesi.com.tr/fotogaleri/nato-gozunu-karartti-buyuk-tehdit-16610.aspx?O=6, ET.29.01.2020.

gerçekleştiğini iddia ettiğimiz bu siber çatışma sürecinin gelişimi hakkında her iki taraf açısında da siber sürecini kısaca incelersek şu hususlara değinmemiz gerekir;

- **NATO Tarafı Gelişmeler**

Soğuk Savaş'ın bitmesinden sonra İttifak'ın güvenliğini hedef alan siber tehditlerin giderek daha sık, karmaşık, yıkıcı ve zorlayıcı olmaya başlamasıyla birlikte siber saldırılara karsı savunma yeteneklerini güçlendirmenin gerekliliği ilk kez 2002'de Prag'da yapılan Zirve toplantısında görüşüldü. O günden beri siber konusu NATO zirvelerinin gündeminde giderek önemini arttırmış ve 2008 yılında Bükreş Zirvesi ile NATO'nun, savaş kavramında yaşanan değişikliğe cevap verecek yeniden yapılanmaya dönüşmesine yönelik Strateji Belgesi oluşturulmuştur. Bu çerçevede Zirve Bildirgesi'nin 46. maddesinde, NATO'nun bu değişimin sağlanması için gereken kaynağı temin edeceği belirtilmiştir. Bükreş Zirvesi sonrasında siber güvenlik alanında iki önemli gelişme yaşanmıştır. Bunlar; Brüksel Merkezli NATO Siber Savunma Yönetimi Otoritesi ve Estonya Tallinn merkezli bir NATO Siber Savunma İşbirliği Mükemmeliyet Merkezi'nin kurulmasıdır.19 Kasım 2010'da Lizbon'daki NATO Zirvesi içinde siber sorunları resmen tanıyan ittifak misyonu yeni bir stratejik kavram yarattı. Siber saldırıların daha sık, daha düzenli ve daha pahalı hale gelmemesi için NATO'nun önleme, tespit etme, savunma yeteneğimizi daha da geliştirme yönünde söz verildi. Ayrıca NATO siber saldırılara karşı ulusal siber savunma yeteneklerini geliştirmek, planlamak ve koordine etmek yönünde de adım atmaya karar verdi. Bu karar doğrultusunda; NATO ve NATO organlarını merkezi siber koruma altına alarak siber sisteminin ülkelere daha iyi entegre edilmesi yönünde üye ülkelerde farkındalık, uyarı ve yanıt geliştirilmesi hedeflenmiştir.[376]

8 Haziran 2011 tarihinde revize edilen NATO Siber Savunma Politikası, NATO'yu ittifakı'ın temel görevleri olan kollektif savunma ve kriz yönetimini gerçekleştirmek için iletişim ve bilgi sistemlerinin korunmasında merkezileşmiş ve koordineli bir yaklaşım sunmuştur.[377] Özellikle Estonya, Gürcistan ve Ukrayna gibi birçok saldırıdan sonra siber tehditlerin ittifakın sınırlarını aşındırmasından dolayı

[376]Active Engagement, Modern Defence, NATO, 19 Kasım 2010, www.nato.int/cps/en/natolive/official_texts_68580.htm. ET: 20.01.2020

[377]NATO Defence Ministers Adopt New Cyber Defense Policy,NATO, 8 Haziran 2011, at www.nato.int/cps/en/natolive/news_75195.htm. ET: 20.01.2020

NATO üyesi ülkeler, özel sektör ve akademik çevre için bir işbirliği ihtiyacı ifade edilmiştir. Yeni belirlenen NATO Siber Savunma Politikasına göre;[378]

- ✓ NATO'nun kolektif ve savunma kriz yönetiminin planlama sürecine siber savunma hususları entegre edilecek,
- ✓ NATO ve müttefikler için kritik olan siber varlıkların korunması ve savunmasına odaklanılacak
- ✓ Güçlü siber savunma yetenekleri geliştirilecek,
- ✓ NATO'nun kendi ağlarının korunması merkezileştirilecek,
- ✓ Kritik alt yapıların korunmasında müttefiklere yardım edilecek,
- ✓ Ortaklar, uluslararası kuruluşlar, özel sektör ve akademik çevreyle birlikte çalışılacak,
- ✓ Farkındalık programları geliştirilecek,
- ✓ Tallinn'den uzmanlık ve destek alınması için müttefikler teşvik edilecektir.

Fakat NATO'nun prensip siber savunma faaliyetleri doğrultusunda açıklanan bu politika yaklaşımlarından hangi pratik eylemlerin akacağı hala belirsizliğini korumaktadır.[379]

2014 yılında Müttefikler, siber savunmayı toplu savunmanın ayrılmaz bir parçası haline getirdiler ve herhangi bir siber saldırının NATO'nun temelini oluşturan antlaşmanın toplu savunma maddesinin (5.Madde) yürürlüğe konmasına yol açacağını beyan ettiler. Ayrıca 2016'da, siber uzayı askerî operasyon yürütme alanı olarak kabul edilerek ulusal ağların ve altyapıların siber ortamda savunulmasının öncelikli olarak güçlendirilmesi gerektiği yönünde karar verdiler.[380]

03.10.2018 tarihinde ABD Savunma Bakanlığı'nın uluslararası güvenlik konularında Baş Danışman Katie Wheelbarger, NATO'nun talep etmesi halinde, Rusya'nın artan siber faaliyetlerine karşı Amerika Birleşik Devletleri'nin NATO müttefiki ülkelerle siber savaş yeteneklerini ortak çalışma için kullanmaya hazır olduğunu belirterek sürece başka bir boyut kazandırmıştır. Bu yeni boyutla birlikte

[378]Uğur Akyazı, Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, Ankara 20-21.10.2013, ss.216-220.

[379]NATO, Defending Against Cyber Attacks, www.nato.int/cps/en/natolive/topics_49193.htm. ET: 20.01.2020.

[380]Brent Laura,NATO'nun Siber Uzaydaki Rolü, NATO Dergisi, 2019, https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/TR/index.htm ET.29.01.2020.

2018 yılı içerisinde Rusya'nın 300 bin asker ile düzenlediği tarihinin en büyük ve kapsamlı tatbikatına cevap olarak NATO, Rusya sınırı yakınında "Trident Juncture 2018" askeri tatbikatı yapacağını ilan etmiştir. 2018 yılında yapılan bu tatbikatların en önemli sebebi NATO'nun Kırım'ın Rusya tarafından ilhakı ve Polonya, Litvanya, Letonya ve Estonya gibi ülkelerin yaşadığı Rusya endişesidir.

- **Rusya Tarafı Gelişmeler**

NATO'nun izlediği politikalar karşısında Rusya'daki gelişmeleri izlediğimizde gözümüze çarpan en önemli figür Rusya Genelkurmay Başkanı Valery Gerasimov'dir. Dönemin Rusya Genelkurmay Başkanı Valery Gerasimov'un 27 Şubat 2013 tarihinde "Military Industrial Kurier Dergisi'nde" yayınlanan "The Value of Science in Prediction" adlı makalesinde ortaya koyduğu askeri yaklaşım Gerasimov Doktrini olarak adlandırılmaktadır. Gerasimov Doktrini temel olarak askeri niteliğe sahip olmayan yöntemleri kullanmayı dolayısıyla da daha az insan kaybı ve maliyet ile sıcak çatışma süreçlerini yönlendirmeyi ve yönetmeyi amaçlamaktadır. Gerasimov Doktrinin ulaşmak istediği bu hedefler, askeri bir müdahale öncesinde, hedef bölge, ülke, topluluk ya da devlete yönelik olarak siber saldırılar ile avantaj sağlanması, hedefin yıpratılması, psikolojik savaş yöntemleri ile baskı altına alınması, moralinin bozulması, savunma direncinin kırılması, kritik altyapılarına zarar verilerek ekonomisinin zarara uğratılmasıdır.

Bu doktrin yeni bir savaş tarzı, "genişletilmiş modern savaş teorisi", hatta "tam bir melez veya özel bir savaş vizyonu" dur. Rusya'nın gerçek, ama farklı bir meydan okuma tarzıdır. Çevreye korku ve kaos salmayı hedefleyen bu teori gibi birçok rus doktrini vardır. Fakat Rusya tarafından ortaya konan bu siber strateji dikkati dağıtmak, bölmek ve demoralize etmek için geniş bir politik hedefi içinde barındırmaktadır. 21. yüzyılda savaşlar artık ilan edilmiyor ve başladıktan sonra, daha önceden bilinmeyen bir şablona göre gelişiyor. Zayiat ve yıkım ölçeği, yıkıcı sosyal, ekonomik ve politik sonuçlar açısından, bu tür yeni çatışmalar herhangi bir gerçek savaşın sonuçlarıyla karşılaştırılabilecek bir seviyeye gelmiştir. Zaten bütün bu çatışmalar, bilgi çatışması eylemleri ve askeri kuvvetlerinin eylemleri de dahil olmak üzere gizli bir karaktere sahip askeri ve teknolojik araçlarla desteklenmektedir. Gerasimov'un burada işaret ettiği şey, Rus ordusunun uygun bir

şekilde kullanılması gerektiğidir. Bu çerçevede Rusya'yı açıklarken belirttiğimiz gibi Rusya tarafından birçok saldırı gerçekleştirmiştir.

4.5. Avrupa Birliği'nin Siber Güvenlik Stratejisi ve Politikaları

Avrupa güvenliği fikri hem ulus devlet hem de kolektif politika yapma fikriyle bir arada ilerlemiştir. Yüzyıllardır süre giden Avrupa'daki düşmanlığın ve savaşların sonrasında güvenliği oluşturmak için sürekli arayışlar olmuştur. Fakat en olumlu sonuçlanan çözüm 2. Dünya Savaşından sonra gerçekleşmiştir. 2. Dünya Savaşı sonrasında, dönemin (Fransa Dışişleri Bakanı) Robert Schuman ve Eski Milletler Cemiyeti Genel Sekreteri Jean Monnet'in tasarısına dayanarak, 9 Mayıs 1950 tarihinde, Stratejikleri (kömür ve çelik) birleştirmek için pragmatik karar alındı. Bir başka açıdan bakarsak o günün stratejikleri kömür ve çelik bugünün siberiydi. Devam eden süreçte 1951 yılında Avrupa Kömür ve Çelik Topluluğu (AKÇT) kuruldu. Böylece Avrupa'nın "büyük iç savaşının" biteceğine inanılıyordu. Bu inançla 1957'de imzalanan Roma Antlaşması ile süreç geliştirilerek, kömür ve çeliğin yanı sıra diğer sektörlerde de ekonomik birliği kurmak amacıyla, Avrupa Ekonomik Topluluğu (AET) bir yıl sonrada Avrupa Atom Enerjisi Topluluğu (EURATOM) kuruldu. 1965 yılında imzalan Füzyon Antlaşması ile de bu kurumların hepsi birleştirilerek Avrupa Topluluğu oluşturuldu. Avrupa Birliği ile sonuçlanan bu sürecin güvenlik ve istikrarla alakalı bütünleşme çabası ise 27 Mayıs 1952'de imzalanan Avrupa Savunma Topluluğu'nu Antlaşmasına ve Pleven Planına gitmektedir. [381]

Avrupa Savunma Topluluğu'nun oluşturulması için ortaya atılan Pleven planında ön plana çıkan noktalardan bazıları şunlardır; planda ilk olarak Avrupa ordusunun hangi temelde kurulacağı ve örgütlenme şekli belirtilmiştir. İkinci olarak Birleşik Avrupa'nın siyasal kurumlarına bağlı, Atlantik Okyanusu'nun diğer yakasındaki batılı kuvvetlerle işbirliği içinde olan ve tek bir siyasal ve askeri otorite altında olan bir ordu öngörülmektedir. Oluşturulacak bu ordu hem insan gücünün hem de tüm maddi unsurların mümkün olduğunca kaynaşmasıyla oluşmalıdır. [382]

[381]Kaldor ve Rangelov, a.g.e. , ss.355-371.
[382]Armağan Gözkaman, Avrupa Savunma Topluluğu'nun Reddi Üzerine Bir Analiz, Beykent Üniversitesi Sosyal Bilimler Dergisi, Cilt.7, No.2, Yıl.2014, ss.6-19.

Avrupa Savunma Topluluğunun başarısızlığından sonra, Dönemin Fransa Başkanı Charles De Gaulle 1961'de ortak bir dış politika ve ortak bir savunma politikasının oluşturulması hedefiyle siyasi entegrasyon için ikinci girişim olan Fouchet Planınıyla hükümetler arası bir temsili temsil eden yeni bir "Devletler Birliği" oluşturmasını önerdi. Fakat bu girişim de başarısız oldu. Sonuç olarak, Avrupa Birliği'nin sorumluluğunda olan entegre bir Avrupa ordusu tasarlansa da bu tam olarak hala aktif hale getirilememiştir. Bu durum siber uzayda karşılaşılan suç, terör, casusluk ve savaş dörtgeninde de devam etmektedir. Avrupa Birliği'nin güçlü ve kritik ülkeleri kendi içlerinde siber ordu birimleri oluştururken siber alandaki güvenliklerini ne AB'ye ne de NATO'ya bırakmamaktadır. Kısaca güvenlik söz konusu olduğunda hem coğrafi hem de politik açıdan siber alanın muğlaklığıyla "Avrupa" birliği kurulamamıştır.

1992 Maastricht Antlaşması uyarınca, güvenlik sadece bir politika alanı olarak görülerek Avrupa'nın entegrasyon projesine güvenlik ve savunma gibi kriterler belirli ölçütler dahilinde eklenmiştir. Avrupa Ordusu'nun hala kurulamamış olması sebebiyle de Avrupa Birliği siber uzayda, bölgesel olarak nüfuz sahibi olmak için askeri olmayan güç biçimlerine bel bağladı. Böylece; Avrupa güvenliğini sağlamak için siber suçlar, siber terör tehditleri ve siber güvenlik kapsamında sınırlandırmalara giderek Avrupa Polis Teşkilatı (EUROPOL) ve Avrupa Ağı ve Bilgi Güvenliği'nin oluşturulması Ajansı (ENISA) hakkında çok sayıda karar yayınladı. Çünkü günümüz dünyasında bilişim sektörüne yönelik gerçekleşen ilerleme ve gelişmelere bağlı olarak, mevcut fiziki alanda gerçekleşen iş ve eylemlerin sanal ortama taşınmasıyla birlikte tehdit algılamaları da değişmiştir. Değişen bu tehdit algısıyla birlikte uluslararası ilişkilerin şekillenmesinde, üstünlük mücadelesi, ittifak ilişkisi ve taraf olmada yeni bir mücadele alanı olarak kullanılan siber uzay iktisadi, ekonomik, sosyal ve siyasi hayatı büyük ölçüde zarara uğratabilmektedir. Siber uzayda tarafların çıkarlarının örtüşmediği durumda meşru olmayan yöntemlerle kullanılan siber saldırılar ve bu saldırılara karşı geliştirilen politikalar ve araçlar siber uzayda güç mücadelesini ortaya çıkarır.

AB'nin siber güvenlik politikaları ve güvenlik stratejilerinin temeli kritik alt yapıların korunmasını sağlamaya dayanır.[383] Bunu yaparkende Avrupa Birliği siber

[383]Mehmet Eren, a.g.e , 80-90.

güvenlik hakkında yasal düzenlemeler gerçekleştirmektedir. Gerçekleştirilen bu yasal düzenlemelerden 2013 yılında yayınlanan Cybersecurity Strategy for the European Union (AB için Siber Güvenlik Stratejisi) en önemli belgedir. Bu belgeyle birlikte AB kritik alt yapı ve siber güvenlik bağlantısı vurgusu yapıp ortak bir siber güvenlik politikası oluşturulmasını, politikaların ve kurumların bu bağlamda işleyişlerini vurgulamaktadır. Uluslararası ortamda Avrupa Birliği'nin siber güvenlik hususuna önem vermesi uluslararası aktörler arasında siber güvenlik konusunun ne kadar önemsendiğinin göstergesidir.

AB strateji belgesi uluslararası düzeyde, koordinasyon ve işbirliği geliştirilmesi için rehber bir belge olarak örnek alınabilir. Fakat uygulama aşamasında siber güvenlik anlamında tam olarak karşılığını bulamamıştır. Bu yüzden daha çok önem verilmeli ve yatırım yapılmalıdır. Böylece gelecekte yaşanabilecek büyük veri kayıpları gerçekleşmeden önlenebilir. Aynı zamanda; Avrupa Birliği tarafından kritik olarak kabul edilen sektörler 10 Ekim 2001 tarihli 574/2001 sayılı bildiride belirtilmiştir. Bu bildiride Avrupa komisyonu kritik alt yapıların kapsam, büyüklük ve zaman etkisi vurgulanmıştır. Bu yasal düzenlemeler çerçevesinde belirlenen siber güvenlik stratejisi/ilkeleri/eylemleri 2004 Yılında AB' de siber güvenliğin sağlanması konusunda koordinasyon oluşturması için AB Ağ ve Bilgi Güvenliği Ajansı(European Union Agency for Network and İnformation Security ENISA) adıyla bir tüzel kişilik kurulmuştur. Bu bağlamda siber güvenlik politikasının kurumsallaşmasında Avrupa Birliğinin Ağ ve Bilgi Güvenliği Kurumu (ENISA)'nın kurulması en önemli adımdır.

4.5.1. AB'nin Ortak Güvenlik ve Savunma Politikası (OGSP)Çerçevesinde Siber Güvenlik Politikası

AB strateji belgesinde belirtilen temel haklar, demokrasi ve hukukun üstünlüğü gibi kavramlar siber uzayda da korunması gereken temel ilkeler olarak belirtmiştir. Bir diğer önemli nokta internetin özgürlüğü ve refah seviyesini arttırmada pozitif etkisi bulunduğudur. Bu yüzden AB tarafından Avrupa dijital tek pazarının sağlanması ve dijitalleşme kapsamında hem vatandaşların güveninin sağlanması hem de refah seviyesinin artması hedeflenmektedir. Siber suçların

önlenmesi ve ortak işbirliğinin sağlanması görevide en önemli aktör olan devletlere düşmektedir.

AB siber güvenlik ilkeleri " AB'nin temel değerleri", " temel hakların, düşünce özgürlüğünün, kişisel bilgilerin ve gizliliğin korunması", " herkes için erişim" " demokratik ve etkili çok paydaşlı yönetişim" ve " güvenliği sağlamak için paylaşılmış sorumluk" olarak 5 ilke şeklinde belirtmektedir. Bu bağlamda AB'nin temel değerlerinin sadece fiziksel dünyada değil dijital dünyada da geçerli olduğu belirtilmektedir. Günlük hayatta geçerli olan yasaların, teamüllerin ve normların siber uzayda da geçerli olduğu belirtilmiştir. Avrupa Birliği düzeyinde güçlü ve etkili yasaları temel alacak şekilde kamu-özel ortaklığı siber güvenlik için geçerli ve uygun bir platformdur. AB siber güvenlik strateji belgesi de kamu ve özel paydaşlarla bir arada koordinasyon ve işbirliği sayesinde siber güvenliğin yürütülebileceğini vurgulamaktadır.

Ortak Güvenlik ve Savunma Politikası(OGSP) çerçevesinde siber güvenlik politikasını geliştirmek için 2013 yılında yayınlanan Cybersecurity Strategy for the European Union (AB için Siber Güvenlik Stratejisi) Strateji belgesinde siber güvenlik için siber savunmanın gerekli olduğu belirtilmiştir. OGSP Misyonu çerçevesinde siber savunma stratejisi belirlemek, riskleri çıkarmak, gereklilikleri ve teknolojileri değerlendirerek geliştirmek, üyeler arasında diyalog ve koordinasyonu sağlamak, uluslararası ortaklarla diyalog sağlamak gibi sorumluluklar siber güvenlik kriterlerinin belirlenmesinde önemli bir rol üstlenmektedir.[384] Ayrıca hem NATO hem de AB'ye üye olan devletlerarasında izlenecek siber politikaların mükerrerliğinde ve farklılığında ne olacağı üzerinde durulması gereken önemli bir husustur.

4.5.2. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)'nin Siber Rolleri ve Sorumlulukları

Bilgi çağının hızla gelişmesiyle birlikte sadece devletler ve kurumlar değil AB gibi uluslar üstü yapılanmalarda özellikle siber saldırılarla mücadele konusunda çalışmalar başlatmış, nitelikli insan geliştirmek için bütçeler oluşturmuş ve eğitim

[384]European Commıssıon, Cybersecurity Strategy Of The European Union: An Open, Safe And Secure Cyberspace, Brussels, 7.2.2013, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf ET.14.01.2021.

programları belirlemiştir. Bu doğrultuda tüm bu faaliyetleri gerçekleştirebilmek için ulusal düzeyde olduğu gibi AB düzeyinde de siber güvenlik ile ilgili birçok aktör bulunmaktadır. ENISA, EUROPOL ve EDA gibi kolluk ve savunma ajansları arasında koordinasyon ve işbirliği siber güvenlik konusunda pratik çözümler üretile bilinmesi için gereklidir. Çünkü sanal dünyayı analiz etmek için ülkelerin genel prensipleri, ulusal askeri stratejileri, ekonomik ve teknolojik yapıları, siber araç ve tekniklerin kullanılmasının izlenmesi gibi kriterler belirleyici rol oynamaktadır. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) da tam bu süreçte önem kazanmaktadır.

Kısaca Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)hakkında bilgi vermemiz gerekirse; Avrupa Ağ ve Bilgi Güvenliği Ajansı, ABD'nin en güçlü ve iyi finanse edilen siber ajansı olan CYBERCOM'a eşdeğerdir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) ilk olarak BT sektöründe uzun deneyime sahip bir fizik profesörü tarafından yönetilen Ajansın misyonu enerji endüstrisi, sigorta şirketi mühendisliği, havacılık, savunma ve uzay endüstrisi gibi temel konularda bir Ağ ve Bilgi kültürü geliştirmeyi hedeflemektedir. Bu doğrultuda AB Üye Devletlerinin desteğiyle Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) ve Ortak Araştırma Merkezi (JRC) tarafından Kritik Bilgi Altyapılarının Korunması amacıyla 2010 yılında ilk siber Avrupa raporu yayınlanmıştır.[385]

2010 yılında gerçekleşen ilk siber Avrupa raporu ile birlikte Cyber Europe 2010 tatbikatı gerçekleştirilmiştir. Avrupa ülkelerinden bu tatbikat için gelen uzmanlar ve bilgisayar korsanları internet kullanılarak Avrupa çapında kritik çevrimiçi hizmetlerin felç edilme ihtimaline karşı simüle edilmiş araçlarla birlikte çalıştılar. [386]Simülasyon alıştırması hayali bir senaryoya dayanan bu tatbikatın amacı, Avrupa'daki ülkeler arasında büyük ölçekli saldırılara yanıt vermeye çalışmak, güvenlik risklerini azaltmak ve akıllı telefon kullanma fırsatlarını arttırmak için iletişim ve işbirliğini tetiklemekti. 2010 yılında başlayan bu tetikleme çabası hala devam etmekle birlikte tam anlamıyla bir sonuca ulaşamamıştır.

---

[385]European Network and Information Security Agency, Cyber Europe 2010 Evalution Report, 2011, ss.1-46.

[386]SecurityWeek News, ENISA Issues Report on 'Cyber Europe 2010' Cyber Security Exercise, 2011 https://www.securityweek.com/enisa-issues-report-cyber-europe-2010-cyber-security-exercise, ET. 14.01.2021.

4.6. Siber Savaşların Önlenmesine Yönelik Uluslararası Kurum ve Mekanizmalarının İncelenmesi

4.6.1. Uluslararası Siber Tehdit ve Suçlara Karşı Kurumsal Tepkiler

Tarihten günümüze yaşanan tüm savaşların temelinde yatan asıl sebep temel güçlerin ekonomik varlıkları elde etme mücadeleleridir. Yani bir aktörün daha da güçlenmesi ve zenginleşmesi için "Fetih" şarttı. Çünkü fetih gerçekleştiğinde şehirler yağmalanıp, değerli madenlere el konulur, halk öldürülerek kazanç sağlanırdı. 21. yüzyılda bu yolla kar elde etme ihtimali azalmıştır. Bu yüzden günümüz siber dünyasında hâkim olan küresel ticaret sisteminde siber silahlar kullanılarak maddi kazançlar sağlanmakta ve düşmana çok ciddi ekonomik zarar verilebilmektedir. Bu durum emperyalist devletler için hem büyük bir avantaj hem de büyük bir risk taşımaktadır. Çünkü siber savaş riski artık büyük devlet "ya da küçük devlet gibi bir kavramı ortadan kaldırmıştır. Küçük ve güçsüz bir devlet bile artık güçlü bir ABD'ye ciddi zararlar verebilme kapasitesine sahiptir.

Bir diğer yandan günümüzde yaşanan kur savaşları, ticaret savaşları aslında hep siber savaş olarak adlandırdığımız bu dönemin etki silahlarıdır. Çünkü bir ülkenin parasının kıymeti o ülke için'' Aşil'in topuğudur.'' Günümüz neoliberal küresel serbest piyasanın hâkim olduğu siber dünyada bir ülkenin parası ve enerji sistemleri çökerse bununla beraber her şeyi çöker. Kazanan devletin zaferiyse Pirus Zaferi" (yıkıcı büyüklükte kayıplar pahasına kazanılan bir zafer) nden farklı olmayacaktır. Örneğin; internet bankacılığı ile artık her işlem internetten yürümektedir. Asla görülmeyen elektronik paralarla hesap işletiliyor ve para avcısı olunabiliyor. Bu avcılığı ise siber savaş, siber saldırı, siber casusluk ve siber terör gibi yollarla hem devletler hem de devlet dışı aktörler gerçekleştirebiliyor. Tüm dünyayı finansal olarak etkileyebilecek bir siber saldırı tüm dünyada büyük bir kaos yaratabilir. Bu sebeple artık savaşlar cephelerde değil, doğrudan bir devletin, milletin unsurlarını hedef alıp, sanal ortamda öncelikle ekonomik varlıklarına yönelik gerçekleşmektedir. Devletlerin Merkez Bankasını hacklemek ve Swift Sistemi üzerinden para çalmak ta son zamanlarda gelişen konuların başında gelmektedir. Bu durum devletlerin asıl hazinesi olan merkez bankalarının ve ulusal bankalarının ne

kadar güvenli olduğu sorusunu sormamıza yol açmaktadır. Bu durumun önüne geçmek içinde sanal dünya da ordu, polis ve istihbarat birimleri kurulmuştur. [387]

Aynı zamanda siber uzayda güvenliği sağlamanın bu kadar zor olması ve her aktörün tehdit altında bulunması siber güvenlik ürünleri ve hizmetleri için ciddi bir pazar oluşturmaktadır. Siber güvenlik ürün ve hizmet pazarına yönelik arz/talep dengesini yaratan pazarın boyutunu tam olarak ölçebilmekse çok zordur. Fakat sadece askeri ve istihbarat faaliyetleri dâhilinde küresel siber güvenlik pazarının yıllık 150 milyar dolar civarında olduğu düşünülmektedir. [388] Bu rakamdan yola çıkarak ekonomik olarak ne kadar önemli bir pazarın oluştuğunu bu bağlamda değerlendirilebilir.

Bir diğer yandan siber güvenliğin politik ekonomisi piyasa taleplerine cevap vermektedir. Bunu başka bir şekilde ifade edersek; eğer bu alanda çatışmalar ve saldırılar artarsa siber güvenliğe yönelik talep de artar. Böylece daha fazla arz ihtiyacı ortaya çıkar. Bu yüzden bu alandan ekonomik olarak faydalanan kesimler bu tehditlerin artması ve aktörlerde korku oluşması için ciddi çabalar göstermeye devam edecektir.

Bu çatışma sürecinin arttığının en güzel örneği ise tezin üçüncü ve dördüncü bölümünde ayrıntılarıyla açıkladığım savaş tanımı ve çatışma örnekleri üzerinde görülmektedir. Bu tezde ayrıntılı olarak açıkladığımız hem Doğu hem de Batı, siber uzayın politik ekonomisinden maksimum düzeyde faydalanmak için ellerinden gelen bütün çabayı gösterecek buda gerçekleşen çatışmalar ekseninde "siber savaş süreci" ni yoğunlaştıracaktır.[389]

Ayrıca 5G ve IoT'un aktörleri siber saldırılara karşı daha savunmasız hale getirmesi her iki tarafında bulut ve siber güvenlik yaklaşımlarını yeniden değerlendirmesini zorunlu kılacaktır. Çünkü Dünya her zamankinden daha bağlantılı bir hale gelmiş bu durumda daha güçlü pazarlar ve günlük eylemlerimizi kapsayan merkezi teknolojilere bağlılığı sürekli olarak ortaya çıkarmaktadır. Endüstri 4.0 sonucunda oluşan bütün bu teknolojik gelişmeler kesintisiz bağlantıya

[387] Ramazan Kurtoğlu, a.g.e. , ss. 108.
[388] International Telecommunication Union (ITU), Key Global Telecom Indicators for the World Telecommunication Service Sector, 2010 Figures, http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html. ET:23.01.2020.
[389]Dorid Dor, These Will Be The Main Cybersecurity Trends İn 2020, Weforum Organizasion, 07 Ocak 2020,https://www.weforum.org/agenda/2020/01/these-will-be-the-main-cybersecurity-trends-in-2020/ ET.28.02.2020.

dayanmaktadır. Dijital dönüşümümüz devam ettikçe, daha uyumlu ve bağlantılı bir toplum (Toplum 5.0) oluşturmaya devam edeceğiz. Böylece verilerimizin her zamankinden daha fazla platform tarafından paylaşılmasıyla veri merkezinde, nesnelerin interneti (IoT) cihazlarında, bulutta ve olayda eğilim artacaktır. Ancak bu eğilim büyük fayda maliyet sürecini doğuracaktır. Bu yeni süreçte Batı ve Doğu güçleri teknolojilerini ve istihbaratlarını giderek daha fazla siber araç, yazılım ve cihazlara bağımlı hale getirdikçe verilerimiz de o kadar hassas olacaktır. Bu durumda yeni bir çevrimiçi olarak gerçekleşecek siber savaş sürecini yoğunlaştıracaktır. Özellikle ABD ve Çin arasındaki ticaret kan davası ve bu iki büyük ekonominin birbirinden ayrılması bu siber çatışma sürecinin açık bir işaretidir. Aynı zamanda; kendi etki alanlarını pekiştirmek ve genişletmek isteyen küçük ülkelerden kaynaklanan siber saldırılar, büyük ülkeler tarafından finanse edilen ve sağlanan proxy çatışmaları olarak kullanılmaya devam edecektir.

Sonuç olarak; siber uzayın yaygınlık, ölçek ve kapsamı her geçen gün artarak dünyanın temel bir özelliği haline gelmiştir. Hem gelişmiş dünyada hem de gelişmekte olan dünyada farklı boyutlarda olmak koşuluyla siber uzay yeni bir gerçeklik yaratmıştır. Bu gerçeklikte uluslararası ilişkilerde siber politik hakkında teorileşme alanının oluşması zorunlu kılınmıştır.[390] Bu çaba içerisinde siber güvenliğin politik ekonomisinin siber alanda bir uluslararası kurumsal "ekosistem" oluşturması için kurumların normları ve ilkeleri resmileştirilmesi şeklinde bir yapı oluşturması gerekir. Çünkü fiziksel dünyadaki faaliyetleri izlemek için olağan mekanizmalar, istatistikler, standartlar, ölçümler, vb. kriterler "sanal" izlerde veya karşılıklarında elverişli değildir. Bu durum ise "sanal" ın doğasının fiziksel olanla çelişmesinden gelmektedir. Örneğin; "Sanal" alandaki tehditler "süreç içinde" izlenmektense, olaydan sonra tanımlanır. Yani siber alanda erken uyarı sistemi olmamakla birlikte henüz sadece birkaç erken sinyal vardır. Bu yüzden de bu konuda ciddi bir ihtiyaç vardır.

Bireyler, şirketler veya hükümetler yani hiçbir varlık internetin sahibi değildir. Hükümetlerin siber alanda faaliyet gösterme konusunda da tekelleri yoktur. İyi bir bilgisayarı veya telefonu olan herkes internet ve bilgisayar aygıtlarını kullanabilir. Bu durum hükümetlerin siber alanda güvenliklerini sağlamalarını daha

[390]Choucri, Madnick ve Ferwerda, a.g.e. , ss.96-121.

zor hale getirmektedir. Böylece siber alanda ortaya çıkabilecek bir tehditten herkes kendi bağımlılığı ölçüsünde zarar görür.

Tehditlerin en tehlikeli halinin vücut bulduğu savaş kavramıyla internet ilişkilendirildiğinde, askerler için internet hem bir araç hem de hedeftir. Şeffaflık, şüphe ve karşı yanıltıcı iddiaları azaltmayı amaçlar. Kara, hava veya deniz gibi geleneksel savaş alanlarının aksine, hükümetler siber uzayda tek güç değildir. Aksine, bireyler aktif olarak faaliyet yürütebilir. Örneğin; uydu görüntüleri eskiden ABD istihbarat topluluğu tarafından oldukça sınıflandırılmış ve sınırlı olarak kullanılmaktayken günümüzde, Google Earth kullanan herkes her yerin görüntülerine yasal olarak erişebilmektedir.[391] Bu sebeple hem ulusal hem uluslararası güvenlik tehditlerini siber ortam kolaylaştırmaktadır.

Geleneksel olarak aktörler ulusal güvenliklerini askeri veya diğer tehdit edici izinsiz girişlere karşı devlet sınırları üzerinden sağlamaktır. Zamanla bu basit doktrin daha kapsamlı bir asimetrik güvenlik görüşü haline gelmiştir. Böylece, siber uzayın inşası güvenlik ve sürdürülebilirlikte yavaş yavaş yeni bir zorunluluklar kümesi ve tamamen yeni bir devlet sistemi yaratmıştır. Bu bağlamda tüm devlet ve devlet dışı kuruluşlar için güvenliğe yönelik tehditler, hayatta kalma zorunlulukları, sınır koruması, sosyal uygulanabilirlik ve hükümeti içeren genel bir vizyona dönüştü. Kısaca siber güvenlik, (sınırların savunulması) ve gözden geçirilmiş görüş (askeri güvenlik, toplum, ekonomi, çevre güvenliği ve yönetişimin güvenliği) gibi her alanda kapsayıcı güvenliğin kritik bir özelliği haline geldi.

Buna ilave olarak bilgi teknolojisi geliştirme bağlantıları ve çeşitli siber gelişim süreçleri incelendiğinde siber uzay ile ilgili uluslararası politika söylemlerinin merkezinde tüm sürece katılmak isteyen paydaşlara yönelik WSIS hedefleri önemli bir tepkidir. Dünya Bilgi Toplumu Zirvesi'ni (WSIS) şekillendirme ve yönetme sürecinde alınan kararlar BM merkezli bir girişim olarak devlet düzeyinde yapılmış ve yalnızca egemen devletler "karar vericiler" olarak hizmet vermiştir. Bu doğrultuda siber güvenlikle ilgilenen WSIS hedefleri, gelişimsel süreçlerle geniş ölçüde tutarlıdır. Örneğin; WSIS, her biri küresel bir konferans olarak duran üç aşamadaki (2003Cenevre'de / 2005 Tunus'ta /2013'de Paris'te)

[391]Derek S .Reveron, Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World, Georgetown University Press, Washington, 2012.

toplantılarında kalkınmanın sosyal, çevresel ve siber alandaki sürdürülebilirliğe bağlı olduğunu belirtmiştir.[392]

4.6.2. Uluslararası Siber Tehditlere Karşı Tasarlanmış Mekanizmalar

- **Bilgisayar Acil Müdahale Ekipleri (CERT'ler) ve Örgütsel Yapıları**

CERT'ler uluslararası güvenlik ekosisteminde önemli bir rol oynamaktadır. Ancak temel yetkinlikleri veya kendi tanımladığı sorumluluklar konsensüs oluşturma, mevzuat veya bilinçlendirmeye dayanır. Genel olarak, sağlam verilerin eksikliği temeldeki üç faktöre dayanır. İlk olarak, doğayı çevreleyen belirsizlikler nedeniyle siber verileri ölçmek zordur. Teknolojik gelişimin hızlı temposu ve standart sağlayan kuruluşların eksikliği tanıda ve sınıflandırılmada önemli farklılıklara yol açmaktadır. İkincisi, CERT verilerinin yayılması, toplanması veya doğrulanması ile görevlendirilmiştir. Son olarak, merkezi bir otorite veya gönüllü kuruluş yoktur.

Siber tehditlere yanıt olarak kurulan Bilgisayar Acil Müdahale Ekipleri (CERT'ler) ulusal otorite altında, uluslararası kapsamda oluşturulmuş, ancak hükümetler arası değildir. CERT'ler güvenlik acil durumlarına odaklanmak, geçerli güvenlik teknolojisi kullanımını teşvik etmek ve ağ sürekliliğini sağlamak gibi hem fiziksel arenadaki "gerçek" alanda hem de siber güvenlik ortamında göze çarpan bir rol oynamaktadır. Ayrıca CERT'lerin çoğunluğu kar amacı gütmeyen kuruluşlar olarak kurulmuş olsa da, birçoğu son yıllarda kamu-özel sektör ortaklıklarına geçti. Sonuç olarak, birçok CERT faaliyetleri aktif tehdit izleme ve bilgi alışverişini içermekle birlikte siber güvenlik topluluğu için nicel veriler sağlamaya çalışır.

Geleneksel kurumsal teori temelinde CERT'ler incelenirse hedefleri ve düzenlemeleri bir hayli karışıktır. Prensip olarak, yardımcı olma amacıyla oluşturulan CERT'ler ortak bir yapı ve omurga paylaşır. CERT'ler esas olarak kendi odak alanlarında (akademik, özel, ulusal ve bölgesel) veya ilgili uzmanlık alanlarına (kimlik avı, virüsler ve bilgi) odaklanarak güvenlik sağlamaya çalışırlar. Bu roller, her bir ekibin bütçesine göre büyük ölçüde kendi kendine tanımlanır.

- **Koordinatör kuruluşlar**

[392]Nazli Choucri, Stuart Madnick ve Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives", Information Technology for Development, Cilt.20, Sıra 2 , 2014, ss.96-121.

Siber uzay ve siber erişim genişledikçe, tek bir kuruluşun artan güvenlik olayları ile başa çıkması zorlaşmıştır. Bu yüzden CERT / CC faaliyetlerini yeniden düzenlemek zorunda kalmıştır. Bu yeni düzenlemeyle birlikte, CERT / CC'ler ortaya çıkan olaylara doğrudan yanıt vermek yerine öğrendikleri derslere rehberlik, koordinasyon ve standartlar sağlamaya odaklanarak operasyonel kontrolü işbirliğine dayalı bir yapı ile bölgesel organizasyonların kurulması için temel oluşturulmasına dayandırmıştır. Bugün, CERT ağı, CERT / CC'nin kapsamı ve kontrolünün genişlemesi ulusal CERT'lerin geliştirilmesinde de etkili bir rol oynamaktadır.

- **Ulusal CERT'ler**

CERT / CC gibi koordinatör kuruluşlar tarafından sürdürülen işbirliği yapısı güvenlik ekipleri arasındaki bilgi akışını açıkça kolaylaştırmaktadır. Ancak CERT'lerde hangi örgütlerin bölgesel mülkiyete sahip olduğu ve ulusal bir saldırı durumunda eylemleri koordine etme yetkisi gibi konular belli değildir. Çünkü, ulusal siyasal sistemlerin ve bürokratik uygulamaların çeşitliliği, yasal ve yargı çeşitliliğinin gerçeklerini daha da kötüleştirerek sivil ağları savunmada meşruiyet sorunu yaratmaktadır.

Her ne kadar ulusal CERT'ler bölgesel otorite ile donatılmış olsalar da, Ulusal CERT'ler sivil ağlara saldırı durumunda suç şebekelerini kapatmak ve failleri kovuşturma konusunda yargı yetkisinden yoksundur. Sonuç olarak, ulusal CERT'ler öncelikle teknik siber tehditlere müdahale etmek ve bunları önlemek için yeterli olmayan bir koordinasyon çabasıdır.

Bir diğer yandan; tehditler ve siber saldırılar kurumsal anlayışın teorik temelleriyle yakından ilgilidir. Tanımı gereği, uluslararası örgütler egemen devletlerden oluşmaktadır. Bu tanımdan yola çıkarak siber uzay oluşturulmadan çok önce birçok kuruluş kurulmuştur. Hepsi de siber mekânların ve çoğunlukla önemli veri sağlayıcılarının büyük kullanıcılarıdır.

İşbirlikçi ve hiyerarşik ilkelere dayanan CERT'lerin aksine, uluslararası örgütler, egemen varlıklar olarak statülerine göre tanımlanmış ve kendi resmi yetkileri ile hareket etmeleri beklenen eşit aktörlerden oluşur. Herhangi bir büyük uluslararası kuruluşun güvenliği göz önünde bulundurduğunda siber mekânların da yaygınlığı düşünülürse günümüzde bütün bu aktörlerin siber uzaya odaklanması kaçınılmazdır. Kısaca bu çabalardan bazılarını incelersek;

- **Ekonomik İşbirliği ve Kalkınma Örgütü**

2002 yılındaki "Bilgi Sistemleri ve Ağlarının Güvenliği için Kılavuzu" ndaki teknik incelemeler ve 2005 yılındaki "Bilgi Sistemleri ve Ağlar için Güvenlik Kültürünün Geliştirilmesi" konulu yönergeler çıkarmıştır. Bu yönergeler çerçevesinde 2002'den beri siber güvenlik alanında aktif olarak yer almaktadır.

OECD çerçevesi, OECD'nin temel misyonunun resmi bir uzantısını temsil eder ve tüm üye devletler için ortak bir yaklaşım sunar. Bu yaklaşım çerçevesinde de kamu kurumları, ortaya çıkan siber güvenlik konusunda gönüllü olarak belirli işlevleri yürütür.

- **Uluslararası Telekomünikasyon Birliği**

Uluslararası Telekomünikasyon Birliği'nin (ITU) temel görevlerinden biri standartlaştırmaktır. İnternet bağlantısını izlemek için kullanılabilecek Telekomünikasyon teknolojisi ve sürüm istatistiklerini yansıtan mevzuat, farkındalık, öz değerlendirme, botnet'ler ve CERT'lere çeşitli kaynaklar sunar. Ayrıca, ITU gelişmekte olan ülkeleri siber suçlar konusunda eğiten bir rehber de sunmaktadır.

ITU, göreve özgü temel yetkinlikleri doğrultusunda uluslararası tehditlere cevap verecek ve dünya bilgi toplumu zirvesi eylemlerinin(WSIS) uygulanmasını koordine edecek bir sorumluluk almıştır. Bu sorumluluk çerçevesinde; Mayıs 2007'de dönemin ITU Genel Sekreteri Hamadoun I. Touré, siber güvenliği sağlamak, siber terörizmle mücadele etmek, siber tehditlerden korunmaya odaklanmak ve tehditlere karşı işbirliği oluşturmak için Küresel Siber Güvenlik Gündemi'ni (GCA) başlattı. ITU bu küresel savunma sistemine ulaşma çabalarının bir parçası olarak da, Eylül 2008'de, o yıl Mayıs ayında kurulan ve merkezi Kuala Lumpur yakınlarındaki Cyberjaya'da bulunan Uluslararası Çok Taraflı Ortaklık (IMPACT) şeklinde küresel bir müdahale merkezi 20 Mart 2009'da resmen açıldı.[393]

Bir kamu-özel girişimi olan IMPACT, küresel toplumun saldırıları önleme, savunma ve müdahale etme kapasitesini geliştirmek için birlikte çalışan hükümetlerin, endüstri liderlerinin ve siber güvenlik uzmanlarının ittifakının sağlanmasını temel alır. ITU ve IMPACT arasındaki bu işbirliği, ITU'nin üye 191 ülkesinin, 7/24 müdahale merkezlerinin, kritik altyapı ağlarının ve yazılımın

[393]İnternational Telecominication Union, Making An IMPACT On Global Cybersecurity, İTU News, Ekim 2009, https://www.itu.int/net/itunews/sayıs/2009/08/22.aspx ET.05.02.2020.

geliştirilmesine yönelik dünya çapında oluşturulan güvenlik kuruluşlarının kaynaklarını bir araya getirme çabasıdır. Bu savunma çabasının temeli gerçek zamanlı bir uyarı sağlaması ve siber güvenliği teşvik etmek için kaynak ve uzmanlık hizmeti verilmesini hedeflemektedir.

IMPACT yalnızca Mart 2009'dan beri faaliyette olmasına rağmen, yakın gelecekte teknik güvenlik verilerinin önemli bir sağlayıcısı olabilecek gibi durmaktadır. Bu bağlamda teknolojik yetkinliklere göre yetki vermek, temel yetkinliklerini geliştirmek, düzenleyici alanını genişletmek ve siber güvenliği teşvik etmek gibi orijinal misyonunun bir parçası olarak uluslararası toplumun tehditleri yeni bir kurum kurmak yerine Birleşmiş Milletler çatısı altındaki bu kurumun mevcut organizasyonel güçleriyle siber güvenliğin sağlanabilmesi için bu kuruma yetki verilmesi mantıklı görülebilir. Zaten bu tezde de ısrarla üzerinde durulan konuların başında bu öneri gelmektedir.

- **Kuzey Atlantik Antlaşması Örgütü**

Kuzey Atlantik Antlaşması Örgütü tarafından 2007'de Estonya'ya (NATO üyesi) yönelik yapılan koordineli saldırıların ardından siber alana yönelik çalışmalar gerçekleştirerek NATO'nun teknik müdahale kolu Siber Savunma Mükemmeliyet Merkezi kuruldu. Fakat NATO üye ülkelerini eğitmek, saldırı tatbikatlarını yürütmek ve uluslararası siber saldırı durumunda NATO'nun yapacakları stratejileri belirlemek üzerine çalışan bu merkez beklentileri karşılayamamıştır.

Bir diğer yandan, ihtiyaçların tam olarak karşılanamaması sebebiyle birçok ülke siber savunma ağlarının güvenliğinin sağlanmasında kendi geleneksel ordularına güvenmeyi ve siber savaş için kendi stratejilerini geliştirmeyi seçmiştir. Çünkü NATO üyelerinin hepsinin ortak bir soruna ortak bir yaklaşımda bulunmak istediklerine yönelik ortaya güçlü bir kanıt konulamamıştır.

- **Avrupa Ağ ve Bilgi Güvenliği Ajansı**

Avrupa Birliği, siber suçlar, siberler tehditler ve siber güvenlik kapsamında sınırlandırmalara giderek Avrupa Polis Teşkilatı (EUROPOL) ve Avrupa Ağı ve Bilgi Güvenliğinin oluşturulması Ajansı (ENISA) hakkında çok sayıda karar yayınladı.

ENISA; ağ ve bilgi güvenliği sorunlarını önlemek, ele almak ve bunlara yanıt vermek, büyük ölçüde farkındalık yaratmak, internet güvenliği uygulamalarını teşvik

etmek, bölgesel CERT'lerle çalışmak ve bölgeye karşı kapsamlı bir savunma sağlamak gibi faaliyetler yürütmektedir. Endüstri 4.0 ile birlikte temel güvenlik zorlukları ve siber tehdit faktörlerinin değişmeside bu faaliyetlerin çıkış noktasını oluşturmaktadır. Bu kapsamda; kullanıcıların cihazlarla ilgili olası sorunlardaki farkındalık eksikliği, teknolojik ve güvenlik standartlarının yokluğu, operasyon eksikliği, endüstriyel tesisler ve BT altyapılarının güvensiz alt yapısı, artan bağlantı nedeniyle güvenlik sorunlarının farkında olunamama endişesi ve yeterli beceriye sahip olan figürlerin eksikliği gibi konular önemli bir hal almıştır. Dolayısıyla Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı ENISA bu konulara değinilmektedir. Örneğin; Avrupa Birliği Siber Güvenlik Ajansı (ENISA), 2004'ten beri Avrupa'nın siber güvenliğini sağlamak, siber güvenlik yeteneklerini geliştirmek, üye devletlere tavsiye ve çözüm sunmak, diğer paydaşlarla yakın işbirliği içinde çalışmak gibi görevler üstlenmektedir.

Ayrıca, büyük ölçekli sınır ötesi siber güvenlik olaylarına veya krizlerine işbirliğine dayalı bir yanıtın geliştirilmesini desteklemek için Kasım 2018'de hazırladığı yönergeler doğrultusunda Mayıs 2019'dan beri siber güvenlik sertifikasyon programları hazırlamaktadır. Bu programlar doğrultusunda yeni teknolojilerle siber saldırılara karşı daha savunmasız olunacağı bu sebeple de siber güvenliğe yatırım yapmanın çok önemli olduğunu vurgulamıştır. Aynı zamanda ENISA, gerekli işbirliklerini teşvik etmek ve ilgili tehdit ve risklerin farkındalığını arttırmak için Avrupa Birliği genelinde Endüstri 4.0, akıllı üretim ve endüstriyel IoT cihazları gibi terimlerdeki risk ve tehditleri sınıflandırılarak siber güvenlik için ortam oluşturmayı ve duruşunu iyileştirmeyi amaçlamaktadır. Bu durumu dönemin ENISA Çekirdek Operasyonlar Bölüm Başkanı Steve Purser'ın "Endüstri 4.0 çerçevesinde öngörülen gelişmiş dijitalleşme, endüstrilerin fiziksel ve dijital dünya arasındaki sınırları işleme ve bulanıklaştırma biçiminde bir paradigma değişikliğidir." Sözlerinde de görebiliriz. [394]

Tüm bu anlatılanlardan da anlaşıldığı üzere siber güvenliğin işbirliği çerçevesinde oluşturulabilmesi için ortak güvenlik standartlarının oluşturulması gereklidir.Bu kapsamda ENISA siber güvenlik için teknik standartların mevcut

[394]Enisa, Cybersecurity Is A Key Enabler For Industry 4.0 Adoption, Enisa News, 19 Kasım 2018, https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption ET.28.02.2020.

parçalanmasını aşmada bir önceliktir.[395] Avrupa Ağı ve Bilgi Güvenliği'nin oluşturulması Ajansı (ENISA)'nın bu öncelikli konumu 2004'te Avrupa Konseyi'nin onayladığı tek bağlayıcı uluslararası mevzuat olan siber suçlar sözleşmesi çerçevesinde gerçekleşmektedir. Bu sözleşme, siber suçun suçluğunu tanımlar, kolluk kuvvetlerini görevlendirir. Sözleşmeyi desteklemek için Avrupa Konseyi, kolluk kuvvetlerinin eğitimi ve ulusal mevzuatın iyileştirilmesi şeklinde iki farklı eylem planı uygulamaktadır.Aynı zamanda bunlara ek olarak, Avrupa Konseyi, ulusal siber suçların ilerlemesi hakkında kanıt ortaya koymak için geniş bir veri tabanı tutarak nitel veriler sağlamayı böylece niceliksel analiz için gerekli istatistikleri sağlamayı hedefler. Ancak, siber ortamda nesnel olarak suçu belirlemek zordur. Uluslararası mevzuat da genellikle tepkisel olmakla birlikte genellikle teknolojik çabaların gerisindedir. Dolayısıyla, sözleşme hükümlerinin ulusal siber suç mevzuatının yasal çerçevesine uyarlanması belirsizliğini korumaktadır.

Sonuç olarak; uluslararası anarşik yapı içerisindeki rakipler arasındaki güç mücadelesinin savaşa dönüşmesi yerine işbirlikçi bir temelle çözülebilmesi veya çözülemeyecek durumlarda siber güvenlik alanında bilgi paylaşımının hızını arttırmak ve bu tehditleri bertaraf etmek için gerçekleştirilmesini beklediğimiz kurumsal çabalardan bazıları şunlardır;

a. Büyük bir şemsiye ağ ile özerk kuruluşlar arasındaki tehditler için uyum sağlanmalıdır.
b. Siber tehditlere odaklanmak için tasarlanmış kar amacı gütmeyen kuruluşların arttırılması (CERT / CC, FIRST ve özel CERT'ler) gerekmektedir
c. Gelişmiş devletlerarasındaki etkileşimleri yönetmek için kurulmuş bir dizi uluslararası kurumun (OECD vb.) çabaları bu süreci pekiştirir.
d. Bilgi teknolojisi potansiyelini ilerletmek için tasarlanmış uluslararası konferanslar küresel olarak siber sorunların siyasi profilini yükselterek sürdürülebilir kalkınmaya (WSIS) geçişi kolaylaştırır.

[395]Enisa, *Industry 4.0 Cybersecurıty: Challenges and Recommendatıons, The EU Agency For Cybersecurıty*, May 2009,https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport ET.28.02.2020

e. Temel misyon ve yetkinliklere sahip işlevsel uluslararası kuruluşlar (özellikle ITU) siber güvenliği görevlerinin bir parçası olarak benimsemiştir.
f. Ulusal düzeyde bu karmaşık ve koordinasyonsuz yanıtlara rağmen, iç yapılar aktörler tarafından yetkilendirilmiş belirli kurumlar siber suçlara yanıt vermekle gittikçe daha fazla görev almaktadır (özellikle ABD'deki FBI, AB'deki ENISA vb.).
g. Bağlayıcı uluslararası mevzuatın geliştirilmesi (yani Siber Suç Sözleşmesi) kırılganlık duygusunu, farkındalık düzeyini ve yanıtları koordine etme ihtiyacını artırmıştır.
h. Daha resmi çerçeveli askeri ve istihbarat ağlarının savunmasına odaklanan stratejiler(ör. CCDOE, CNCI) geliştirilmeye başlamıştır

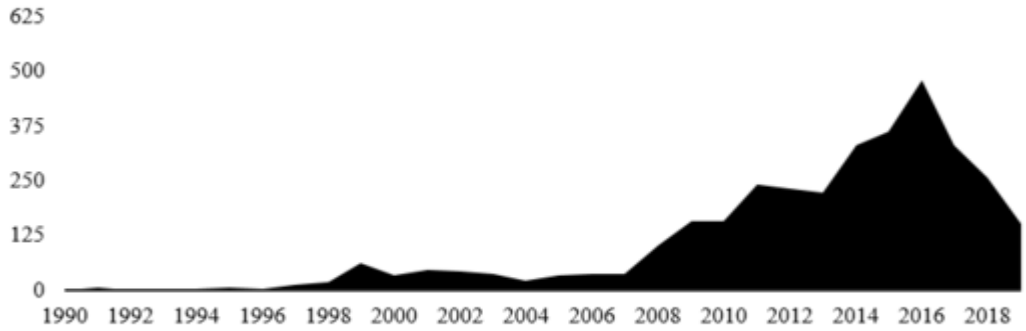
Siber güvenlik için ortaya konan tüm bu kurumsal çabalar bazı temel sonuçlar doğurur. Kısaca bunları açıklarsak;

a. Bilgi teknolojisi uluslararası toplumun politika önceliklerinde olan ve sürdürülebilir kalkınma bağlantısının ayrılmaz bir parçası olmuştur.
b. Mevcut kurumsal manzara, tehditlere karşı kritik öneme sahip bir güvenliğin sağlanması için tüm modları ve siber kaynakları kapsayan bir şemsiye olmalıdır.
c. Birden fazla bağlam ve çeşitli kurumsal motivasyonlar göz önüne alındığında oluşabilecek siber krize karşı tepkiler koordineli ve proaktif yanıt yoluyla gerçekleşmelidir.
d. Tüm kalkınma düzeylerindeki karmaşık küresel gündem nedeniyle, uluslararası siber normların geliştirilmesinde devletler istekli değildir.
e. Kamu, özel ve gönüllü kuruluşlar arasında sektörler arası işbirliği mevcut savunma ağındaki delikleri kapatmak için geçici bir önlem olarak hizmet etmektedir.
f. Şimdiye kadar, tamamen siber alanı kötüye kullanmakla uğraşan büyük terörist grupları görülmemiştir.
g. Şimdiye kadar, siber alanı saldırı ve casusluk faaliyetlerine yönelik kötü amaçlar için kullandığını hiçbir devlet resmi olarak kabul etmemiştir.

h. Modern toplumun merkezinde, suçluların, terörist grupların ve diğerlerinin devlet otoritesine karşı işlevleri tehdit potansiyelini kurumsal bakışa taşımaktadır. Başka bir deyişle, bu durum güvenliğin "talep" de etkin "arz" da ise yeterli olmadığını göstermektedir.
i. İnternet'in kullanımı giderek arttıkça kurumsal bu modeldeki sonuçların aynı şekilde devam etmesi beklenemez.

4.6.3. Siber Savaşları Düzenleyen Uluslararası Yasalar ve Uygulamada Yaşanan Sorunlar

Siber uzayda caydırmanın geleneksel alanlardaki caydırıcılıktan daha zor olmasından dolayı siberle ilgili mevcut literatürde bir düşüş modası yaşanmaktadır. Bu düşüş modasının en büyük sebebide siber saldırıların yürütülmesi ucuzken savunmasının zor olmasıdır. Bu kapsamda; Siber saldırıların uluslararası alanda arttığı 2010-2016 yılları arasında yayınlar artarken 2016 yılından itibaren siber caydırıcılıkla ilgili yayınlardaki önemli düşüş, entelektüel bir olgunlaşma olmadığını göstermektedir.



Şekil 9 Siber Caydırıcılıkla İlgili Dergi Makaleleri, Kitap Bölümleri ve Araştırma Raporları, Ocak 1990 - Ocak 2020[396]

Bu sebeple siber caydırıcılıkla ilgili küresel düzeyde akademik çalışmaların önem kazanması ve arttırılması şarttır. Çünkü şuana kadar yaşanan siber savaşlarda, karşılıklı olarak askeri personellerin bir araya geldiği, askeri tesislerin veya ekipmanların kullanılmasıyla düşmanın savaş kabiliyetlerinin düşürüldüğü, etkisiz

[396]Guest Blogger for Net Politics, *Cyber Deterrence Is Dead. Long Live Cyber Deterrence*! Council on Foreign Relations, 18.02.2020, https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrenceET.28.02.2020

hale getirmek veya yok etmek amacıyla resmi olarak ilan edildiği bir siber savaş gerçekleşmedi. Bunun yerine siber saldırılar sınırlı bir etkiyle geleneksel savaşa eşlik etti. Bu saldırılarda genellikle tahrif edilen hükümet web siteleri, hizmet reddi saldırıları ve veri çalma işlemleriyle kısıtlı kalmıştır. Siber saldırılar, ölümcül olmalarına rağmen, fiziksel bir saldırı ile aynı "yumruk" a sahip değildir. Ancak bunlar bir savaş tehdidi oluşturmaz diyemeyiz. Çünkü burada ortaya çıkan temel sorun uygulama sorunudur.

Uygulama sorunu çerçevesinde bir siber olay meydana geldiğinde, olandan daha fazla yorum genellikle saldırının arkasında kimin olduğuna odaklanmaktadır. Bir siber olayda ne olduğu ve etkinliğin hangi kategorisine ait olduğu genellikle kafa karıştırıcı ve tartışmalıdır. Bu yüzden özellikle suç kriterlerinin belirlenmesi, onaylanan kanun, kural ve yönetmelikler çerçevesinde saldırılar, casusluklar, sabotajlar, yıkımlar ve güç kullanımları durdurulmalı, kurallara uymayanlar uluslar üstü bir otorite tarafından cezalandırılmalıdır. Böylece aktörler arasında ortaya çıkan güvenlik ikileminin etkisi azalabilir.

Bu kapsamda; özellikle diğer devletlere karşı düzenli olarak siber saldırı düzenleyen Rusya, Çin ve ABD gibi ülkelerin BM Genel Kurulunda siber casusluğu, siber sabotajı vb. yasaklama önerisi getirmeleri bu zorlukları azaltarak kendi güvenliklerini sağlamalarını kolaylaştıracaktır. Fakat bu ülkeler henüz bu konuya olumlu yaklaşmamaktadır. Aynı zamanda bu ülkelerin kabul etmesi halinde siber suçlara karşı oluşturulan ve uluslararası işbirliğini içeren bir uluslararası anlaşma olan (Avrupa Konseyi Siber Suç Sözleşmesi) bu konuda güzel bir alt yapı oluşturacaktır. Fakat bir model teklifinde bulunabilmemiz için mevcut uluslararası yasal rejiminde ortaya konulması gerekmektedir.

Günümüzde yaşanan siber saldırıların büyük bir çoğunluğunda uluslararası toplumun ya da devletlerin büyük bir desteği bulunmamaktadır. Bu durumu Estonya ve Gürcistan örneklerinde gerçekleştiği gibi sponsor devletler özelinde inceleyebiliriz. Burada sponsor devletten kastımız saldırıların arkasında olan, kışkırtma yaptığına yönelik kanıtlar bırakan, sorumluluktan kaçmak için ortaya çıkmayan ve siber uzayın gizemiyle kimliğini saklamaya çalışan devletlerin varlığıdır. Sponsor devlet kavramı ortaya çıktığında uluslararası hukuk kapsamında aşağıdakileri dikkate alan bir yasal rejim oluşturulması şarttır.

Siber uzayın belirsizlik düzeyinden dolayı uluslararası alanda iki katmanlı bir sistem gereklidir. Bunlardan birincisi barış zamanı için varsayılan bir durumdur. Diğeri ise uluslararası bir silahlı çatışma durumuna yönelik belirlenecek şartlardır.

Avrupa Birliği Direktiflerinin de etkisiyle oluşturulan evrensel hizmetin kapsamı ITU'nün de direktifiyle barış zamanında uygulanacak yöntemler bir çok ülkede gerçekleştirilmiştir. Örneğin; Türkiye'de 2008 yılında ilan edilen Elektronik Haberleşme Kanunu MADDE 35 – (1) "İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık tarafından belirlenir." Hükmüyle barış zamanında sanal ortamda uygulanacak yetkiyi devlet kendisine almıştır.[397] Bu yetki durumu uluslararası alanda da kabul edilirse Estonya örnek vakası özelindeki bir olayda rahatlıkla suçlu Rusya gösterilip ITU Şartı'nı ihlal etmekten sorumlu tutularak, Estonya tarafından uluslararası hukuk uyarınca tazminat talebinde bulunabilirdi. Bu aslında çok karışık bir durum değildir. Nasıl UNCLOS'ta; "Bir denizaltı kablosunun veya boru hattının kırılması veya yaralanması durumunda her devlet bunu sağlamak için gerekli yasa ve yönetmeliği kabul ediyorsa bu durum siber uzayda da olabilir. [398] Fiber optik denizaltı kabloları içeren bu yasaklar ve cezalar siber uzayda da pek ala uygulanabilir. Böylece, devletlere karşı gerçekleştirilen siber saldırılar cezalandırılabilir.

Bir diğer yandan konumuza Birleşmiş Milletler özelinde devam ettiğimizde "Birleşmiş Milletler Şartı"[399]nın özellikle 39,41, 42 ve 52. Maddeleri siber uzaya yönelik bir yol haritasının sunulabilmesi için çok önemlidir. Bu maddeleri kısaca açıklarsak;

- Madde 39'un Barışa Yönelik Tehditler, Barışın İhlalleri ve Saldırganlık Davalarına İlişkin Eylemler başlığı altında " Güvenlik Konseyi, barışa, barışın ihlaline veya saldırganlığa yönelik herhangi bir tehdidin varlığını belirleyecek ve uluslararası barışı korumak veya eski haline getirmek için 41.

[397]Bakanlar Kurulu, Elektronik Haberleşme Kanunu, Resmi Gazete Sayı 27050, 10.11.2008, https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm ET.10.02.2020.
[398]United Nations Convention on the Law of the Sea, Breaking Or İnjury Of A Submarine Cable Or Pipeline,Article113,ss.64https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf, ET:20.01.2020.
[399]Charter of the United Nations, Chapter VII Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression and Chapter VIII, Regional arrangements Article 39,40,41,42 and 52, https://legal.un.org/repertory/art52.shtml, ET:20.01.2020.

ve 42. maddelere göre hangi önlemlerin alınacağına karar verecek veya tavsiyelerde bulunacaktır. ”

- Makale 41; “Güvenlik Konseyi, kararlarını yürürlüğe koymak için hangi silahlı kuvvetlerin kullanımını içermeyen tedbirlerin kullanılacağına karar verebilir ve Birleşmiş Milletler Üyelerini bu önlemleri uygulamaya çağırabilir. Bunlar ekonomik ilişkilerin ve demiryolu, deniz, hava, posta, telgraf, radyo ve diğer iletişim araçlarının tamamen veya kısmen kesilmesini ve diplomatik ilişkilerin kıdemini içerebilir. ”
- Makale 42; “Güvenlik Konseyi, 41. maddede öngörülen tedbirlerin yetersiz olacağını veya yetersiz olduğunu düşünürse, uluslararası barış ve güvenliği korumak veya geri yüklemek için gerekli olabilecek hava, deniz veya kara kuvvetleri tarafından gerekli önlemleri alabilir. Bu tür eylemler Birleşmiş Milletler Üyelerinin hava, deniz veya kara kuvvetleri tarafından yapılan gösterileri, ablukaları ve diğer operasyonları içerebilir. ”
- Makale 52 Bölgesel düzenlemelerin 2. Fıkrasında; “Birleşmiş Milletler ‘in bu tür düzenlemelere giren veya bu kurumları oluşturan üyeleri, yerel anlaşmazlıkların söz konusu bölgesel düzenlemeler veya bu tür bölgesel kurumlar tarafından Güvenlik Konseyine havale edilmeden pasifik olarak çözülmesi için her türlü çabayı göstereceklerdir.” 3. Fıkrasında ise; “Güvenlik Konseyi, söz konusu bölgesel düzenlemelerle veya söz konusu bölgesel ajanslar tarafından ilgili devletlerin inisiyatifiyle veya Güvenlik Konseyinin referansı ile yerel anlaşmazlıkların pasifik olarak çözülmesini teşvik edecektir.” şeklinde belirtilmektedir.

Sonuç olarak; Estonya, Gürcistan veya gelecekteki oluşabilecek bir olay fark etmeksizin saldırıya uğrayan bir devlet saldırının geldiği devletteki sorumluların adalete teslim edilmesini veya cezalandırılmasını isteyebilmelidir. Çünkü bir siber saldırı silahlı saldırı düzeyine yükselirse siber silahtan kaynaklanacak güvenlik zafiyetinin giderilmesi çok daha zor olabilir. Dahası bu tezde gerçekleştirilmesini önerdiğimiz vekalet yasası, üst otorite kurulmasının zorunluluğu uluslararası norm ve kaidelerin zorunluluğuna yöneliktir. Bu doğrultuda savaş kuralları ve uluslararası kaideler günümüz tehditlerini tam olarak kapsamamaktadır. Bu yüzden bu kuralların siber savaş kriterlerini içine alacak şekilde revize edilmesi gerekmektedir. Bu revize

işleminin gerçekleştirilmesindeyse küresel bir çaba şarttır.Bu yüzden BM tarafından ortaya konacak yaptırımlar veya cezai eylemler, siber saldırganlar için güçlü bir caydırıcılık yaratmalıdır.

4.7. Siber Savaşların Önlenmesine Yönelik Uluslararası Kurum Yapısı Model Önerisi

Uluslararası toplum Birleşmiş Milletler ’in (BM) kuruluşuna kadar tarih boyunca birçok savaş ve çatışma yaşamış olsa da uluslararası arenada kuvvet kullanımını yasaklayamamıştır. Her ne kadar neoliberal değerler çerçevesinde oluşturulan BM tarafından uluslararası ilişkilerde güç kullanımı yasaklanmış olsa da çatışma ve savaşlar tamamen sonlanmamıştır. Ayrıca, uluslararası ilişkilerde kuvvet kullanımı yasaklansa da ortaya çıkacak savaş/ların ve çatışma/ların sınırlarını belirlemek de Silahlı Çatışma Hukukunda önemli bir görev üstlenmektedir.

Bu kapsamda Uluslararası hukuk genel olarak ve uluslararası insani yardım yasası ("IHL") veya uluslararası insan hakları hukuku ("IHRL"), Birleşmiş Milletler (BM) Sözleşmesi, Lahey ve Cenevre Sözleşmeleri ve ilgili antlaşmalar devletler arasındaki “kuvvet kullanımının hukuki sonucu”, “güç kullanımı”, saldırganlık ve savaş eylemlerini sınırlandırmanın veya değerlendirmenin tek temelidir.

BM Sözleşmesinde Madde 2 (7)’deki Birleşmiş Milletler tarafından iç işlere müdahale edilmemesi maddesi ve Madde 2 (4)’deki ile tanımlanan "kuvvet kullanımı çerçevesinde uluslararası ilişkilerdeki tehdit veya güç kullanımı yasağı maddeleri çok önemlidir. "Adil" bir bilgi savaşının gerçekleştirilebilmesi için öncelikli olarak yapılması gereken siber saldırıların klasik bir silahlı saldırıdan farklını ortaya koyarak bu maddelerin siber silahları da içine alacak şekilde yükseltilmesidir. Bunun ardındanda siber silahların sınırlandırılmasıdır.

Avrupa Siber Suçlar Sözleşmesinden yola çıkarak hazırlanacak kapsamlı bir şekilde evrensel siber hukuk kurallarıyla birlikte vekalet yükümlülüğü oluşturulur, bir üst otoriteyle birlikte uluslararası hukuk kuralları ortaya konur ve böylece geçerli bir kendini savunma uygulaması oluşturulursa saldırganlığın reddedilemez kanıtı ortaya çıkar. Ortaya çıkan bu durumda her devletin üzerine düşen sorumluluğu yerine getirmesi zorunluluğunu ortaya çıkarır. Aynı zamanda bu zorunluluk her devletin önleyici veya öngörülen siber saldırılara ve yaklaşmakta olan tehlikelere

karşı kendini savunma hakkını veya her türlü misilleme gerçekleştirmesine de katkı sağlayacaktır.

Ayrıca çevrimiçi söylenen veya yapılanlarla ilgili yasal sorumluluk alınması gerektiği halde günümüzde yaşanan bilgi çağında, geleneksel suçların siber varyantları konusunda uygulanacak ceza hukuku teorisi, mevzuat ve ceza adaletinde karmaşık bir yapı bulunmaktadır. Bu yüzden internet kullanıcıları ister birey ister devlet olsun çevrimiçi söyledikleri ve yaptıklarıyla ilgili yasal sorumluluk almak zorundadır.

Yargı perspektifinden bakıldığında, gerçek alanda işlenen bir suçu mevcut yasalar çerçevesinde atamak kolayken siber alanda aynı suç işlendiğinde, atamak genellikle zordur. Fakat bu zorluğu hafifletmenin bir yolu vardır. Bu yol internetin özünde bir bilgi ortamı olması sebebiyle siber alanda sanal mülkiyet kavramıdır.

Özellikle bu tezde sanal mülkiyet kavramıyla birlikte alınması gereken yasal sorumluluk sonucunda kurumsalcı teoriyle birlikte vekalet yükümlülüğü ile sorumluluğun devletler tarafından kabul edilmesi gerektiği vurgulanmaktadır. Yani devletler kendi içlerindeki tüm alanların ve dışarıya karşı oluşabilecek tüm saldırıların özel veya kamu olsun sorumluluğunu alması gerekmektedir. Bu sorumlulukta üst otorite kurum ve kurallarla kontrol edilmelidir. Aslında bu bir ortak hukuk ajansı doktrinidir. Bu teori altında, siber uzayın ağ bütünlüğü içinde ağ yöneticisi yani asıl olan astın eylemlerinden sorumlu olmasıdır. Eğer bu konuda anlaşılırsa internetin karanlık yüzü tarafından kötü amaçlar için kullanımı(botner, virüs, solucan, ddos vb.) sınırlandırılabilir. Yani ortak suçluların muamelesine yönelik bir model oluşturulmalıdır. Bu modelle birlikte siber alanda suç işleyen aktörlerin cezai sorumluluğunu tespit etmenin etkili bir yolu sunulacaktır.

Bir diğer yandan uluslararası alanda oluşturulmasını önerdiğimiz bu modellemenin bazı temel sebepleri vardır.Bunlar;

- Uluslararası Telekomünikasyon Birliği (ITU)'nun egemenlik ve yargı yetkisi konusunda anlaşma sağlanamaması,
- Şimdilik siber ortamda kontrollü barışın var olması,
- ICANN'ın küresel sistemdeki rolüne Çin'in karşı çıkması,
- AB strateji belgesinin uluslararası düzeyde, siber güvenlik anlamında koordinasyon ve işbirliği geliştirilmesi için rehber bir belge olarak kalması,

- Silahlı Çatışma Hukukunun güncellenme ihtiyacı,

  Örneğin; hangi siber silahların kullanılabileceği, hangilerinin yasaklancağı ve izin verilen siber silahlar hakkında kuralların siberin kendi karakteristik özelliklerine göre kriterlerin belirlenmesi gerekir. Aynı zamanda bu çatışma hukukunun kim tarafından konulacağı ve nasıl uygulanacağı sorundur. Siber uzayın Uluslararası İlişkiler sisteminde yeni bir savaş alanı olarak kullanıldığını iddia etmemizin sebebide aslından bundan kaynaklanmaktadır.
- Yüzyılı aşkın bir süre önce uluslar, çatışmalardan ve savaştan kaçındığında veya insan acısını en aza indirmek istediklerinde Cenevre Sözleşmesi gibi uluslararası hukuk kurallarını geliştirdiler. Aynı zamanda yeni teknolojiler ortaya çıktıkça, ülkeler biyolojik, kimyasal ve lazer silahlarını kısıtlayan antlaşmalar doğrultusunda yeni kuralları koyup koymayacaklarını tartıştılar. Bununla birlikte, geleneksel bilgelik, sahip olduğumuz yasaların benzer şekilde siber alanı kapsayacak şekilde genişlemesi gerektiğini bu bağlamda değerlendirilebilir. Savaş kuralları ve uluslararası kaideler günümüz tehditlerini tam olarak kapsamamaktadır. Bu yüzden bu kuralların siber savaş kriterlerini içine alacak şekilde revize edilmesinin gerekliliği,
- Vekalet yükümlülüğü ihtiyacı,
- Siber savaşı mümkün kılan üç kritik hususun "internet tasarımındaki kusurlar; donanımdaki kusurlar ve yazılım; daha fazla kritik sistemi çevrimiçi duruma getirme hamlesi"nin kontol altına alınması,

Bu temel sebepler ışığında tezimizde sunduğumuz model önerisinin üç temel saç ayağı vardır. Eğer bu üç ayak birlikte oluşturulabilirse o zaman uluslararası ilişkilerdeki anarşik yapı içerisinde aktörlerin siber güvenliği daha kolay sağlanabilir. Bunlardan ilki siber silah tehditlerinin azaltılabileceğine yönelik uygulamalar, ikincisi kurumsal çerçevede siber güvenlik sürecini yönetebilecek örnek ve son olaraksa modeli destekleyecek bakışlardır.

a) Siber Silah Tehditlerinin Azaltılabileceğine Yönelik Uygulamalar

Siber silahlardan gelecek tehditleri öngörebilmek için oluşturulan veri modelleme ve veri geliştirme süreçleri ile Saldırı Tespit Sistemleri uluslararası anarşik sistemde gerçekleşen siber çatışmalarda kullanılmaktadır. Bu Saldırı Tespit Sistemleri (IDS)ni

gerçekleştirmek için oluşturulan birçok örnek vardır. Örneğin; Veri madenciliği tekniklerinin bir IDS oluşturmak için nasıl kullanılabileceğini göstermek amacıyla Columbia Üniversitesi tarafından İngilizce ismi "Audit Data Analysis and Mining" olan ADAM projesi geliştirilmiştir. Ağ tabanlı bir anormal durumu algılama sistemi olan ADAM projesi; daha sistematik ve otomatik bir şekilde normal ağ davranışını saldırı gerçekleşmeden öğrenir.[400] Bir diğer örnek ise Minnesota Üniversitesi tarafından gerçekleştirilen MINDS projesi kapsamında veri madencilik teknikleri kullanılarak bilgisayar ağları ve sistemleri üzerine gerçekleştirilebilecek saldırıların nasıl otomatik olarak tespit edilebileceği gösterilmektedir.[401]

Bu sistemlerin hiçbiri 7/24 güvenli bir yapı asla sunamaz. Bu sistemler sadece alternatif yöntem sağlayarak riski azaltan bir ön uyarı mekanizması oluşturur. Böylece uyarı korelasyon teknikleri ile oluşturulan "saldırı senaryoları" sayesinde düşük seviyeli izinsiz girişler veya siber saldırılar önlenerek siber güvenlik sağlanabilir. Bu durum ise uyarı korelasyonunun olasılık alarmlarını tanımlamak için bir modellemedir.[402] Aslında bu modelleme üzerinden siber alanda uygulanan çatışmaların bu alanda gerçekleştirilecek düzenlemeler sayesinde barış ortamının oluşturulabileceği tezine ulaşmayı neoliberal kurumsal yaklaşım çerçevesinde uyguladık. Bu tezde uyguladığımız bütün bu siber silah türleri suç, terör ve savaş üçgeni arasında neorealistlerin belirttiği gibi sürekli devam eden bir çatışma serüvenini ortaya çıkarmaktadır. Yukarıda da bahsettiğim gibi bu siber silahlara karşı alınabilecek önlemler olsa da bu daimi bir çözüm değildir. Bu sebeple; bu süregiden çatışma serüveninde siber silahlar kullanılarak gerçekleştirilen web ve ağa bağlı bilgisayar teknolojisinin üç olumsuz yönü vardır. [403] Bunlar; siber suç, casusluk ve savaştır. Siber tartışmalar suç ve casusluk boyutunda gerçekleştiğinde tartışma olmazken savaş kavramını tanımlamada sorun yaşanmaktadır. Bu sorunu çözecekse

[400]Daniel Barbara, Ningning Wu ve Sushil Jajodia, "Detecting Novel Network İntrusions Using Bayes Estimator",. In Proc. First SIAM Conference on Data Mining, Chicago, Nisan 2001. ss.1-17

[401]Paul Dokas, Levent Ertoz, ve Pang Ning Tang, "Data Mining for Network Intrusion Detection", Computer Science Department University of Minnesota, The United StateOfAmerica,ss.21-30 https://pdfs.semanticscholar.org/8bac/ad4990b3dd0ced614e596eb1a6d98865d693.pdf ET:24.01.2020

[402]Ning P., Xu D., Learning Attack Strategies from Intrusion Alerts, Proc. ACM Computer and Communications Security Conf, 2003. ss 1-17. http://discovery.csc.ncsu.edu/pubs/ccs03-ids-full.pdf ET:24.01.2020.

[403]Misha Glenny ve Camino Kavanagh, "800 Titles but No Policy,Thoughts on Cyber Warfare, American Foreign Policy Interests", The Journal of the National Committee on American Foreign Policy, Cilt.34, N:6, Yıl 2012, ss.287-294.

yetkilendirilen kurumun ortaya koyduğu hukuki kuralların ve cezai mueyyidelerin uygulanmasıdır.

b) Kurumsal Çerçevede Siber Güvenlik Sürecini Yönetebilecek Örnek

Bu tezde neoliberal kurumsalcı teori çerçevesinde ısrarla vurguladığımız uluslararası bir üst otoritenin kurulması tezi politik ekonomi kapsamında değerlendirildiğinde uluslararası kurumların gelişmesini sağlamak için kavramsal referans çerçevemizi "talep" ve "arz" üzerine odaklamamızın gerekmektedir. İlk olarak, internet kullanımının artmasıyla birlikte kullanım biçimleri genişlemiştir. İkincisi, birçok hükümet sadece kendi ağlarının güvenliğini değil, aynı zamanda ilgili vatandaşlarının güvenliğinin de tehdit altında olduğunu ve siber güvenlik açıklarının devam ettiğini kabul etmiştir. Üçüncü olarak, kritik alanlardaki tehdit azaltma stratejileri geliştirme çabaları açık bir uçurumu güçlendirmektedir. Son olarak, büyük ve küçük, büyüyen bir dizi siber olayın hükümetleri işaret etmesidir. Bu sebeple, siber politik ekonominin sahip olduğu güç ve bu gücün ortaya çıkaracağı fırsat ve tehditler bu tezdeki iddialarımızı destekleyen önemli konulardır. Aynı zamanda uluslararası kuruluşların ve hükümetler arası kilit kurumların siber güvenlik konularına katılımına yönelik teorik yaklaşımlar tarihsel ve kavramsal temellere dayanır. Bazı ortak endişeler ve paylaşılan varsayımlarda, altta yatan problemlerle ilgili genel motivasyonlar, varsayımlar ve perspektiflerde önemli ölçüde her aktör için farklılık göstermektedir. Bu temel teorik özellikler siber kurumsal faaliyetlerle de yakından ilgilidir.

Tüm bu anlatılanlar çerçevesinde günümüzde hala uluslararası rekabet ortamında kullanılan siber kavramlar üzerinde aktörler arasında küresel bir uzlaşma sağlanmasına yönelik bir niyet olmadığı görülmektedir. Siber uzayın barışçıl kullanımı için tüm bu maddeler baştan kabul edilerek küresel standartlar ve normlar üzerinde uluslararası işbirliğinin oluşturulması gereklidir. Bu sonuca ulaşırken de saldırılara karşı yapılacak mukabelenin şeklinin ve sınırlarının nasıl çizileceği, karar alma sürecinin nasıl olacağı, uluslararası iş birliğinin ne şekilde sağlanabileceği, ortak savunma ve ittifak ilişkisinin tam olarak kurulup kurulamayacağı gibi noktaların karara bağlanması gerekmektedir.

Daha detaylı bir genellemeyle güvenlikleştirme, caydırma ve kurumsallaşma teorileri kapsamında siber çatışmaların gerçekleştiği olguların temeli ortaya

çıkarılarak gelecekte bu silahlar kullanılarak oluşabilecek bir dünya savaşının önlenmesi gerekmektedir. Bu çerçevede; güvenlik ve strateji boyutunda uluslararası arenada dengelerin değişimi ele alınarak anarşik sistemde çıkarların, çatışmaların ve çakışmaların ortasında bu savaşın önlenebilmesi için denetleyici, düzenleyici ve kontrol edici uluslararası bir örgütün kurulması zorunluluktur.

Özellikle dijital dönüşüm kavramlarıyla birlikte "küresel risk" ve "risk toplumu" etkilenmekte bu da toplumların geleceğini güvensizleştirmektedir. Bu ihtimale karşı da modern (güvenlik) kurumlarını yeniden düşünmek ve hukukun rolüne odaklanmak zorunlu olmuştur. Bu hesapta, küresel siber güvenlik politikası ve güç ilişkisi ile uluslararası hukuk arasındaki bağlantı karmaşık ve çelişkilidir. Bu karmaşıklık ve çelişki içinde kurumsalcı bakış çerçevesinde siber uzay alanında nasıl bir üst otorite kurulabileceği ile ilgili iki alternatif bulunmaktadır. Bunlardan birincisi, Birleşmiş Milletler 'in tabi olduğu sözleşmelere bu alanında eklenerek sistemin kontrol edilmesinin sağlanmasıdır. Bir diğeri ise; 1865 te Paris'te düzenlenen toplantıda kurulan ITU(Uluslararası Telgraf Birliği)nin sistemi uygulayıcı ve denetleyici bir noktaya getirilmesidir.[404] ITU'ya verilecek bu yetkilendirme sayesinde siber saldırıları, siber tehditleri ve siber savaşları öngörerek tespit etme yeteneğinin geliştirilmesi amaçlanmaktadır.

Neoliberal kurumsalcı teori çerçevesinde önerdiğimiz ITU(Uluslararası Telgraf Birliği)'nün uygulayıcı ve denetleyici kurum olarak nasıl oluşturulabileceğini kendi kuruluş anlaşmasındaki maddeler çerçevesinde kısaca incelersek;

ITU anlaşması;[405] ''ulusların devlet güvenliğinin tehlikede olduğunu değerlendirdiklerinde veya ulusal yasalar, kamu düzeni veya ahlakından herhangi birinin ihlali durumunda tüm iletişimi durdurma hakkı saklıdır.'' Şeklinde bir madde içeriyordu. Telgrafın hayata girmesiyle birlikte ITU yeni bir küresel iletişim çağına yardım etmiş ancak devlet kontrolünü de bu alanın üstünde tutulmasını sağlamıştır. Teknolojik gelişim ve değişimler sonucunda iletişimde telgrafın öneminin yerini zaman içinde internetin almasıyla birlikte telgraf eskisi kadar iletişimde öncü bir araç olmamıştır. Böylece günümüzde internet'in telgrafın yerini almasıyla birlikte

[404]International Telecommunication Union, About International Telecommunication Union (ITU), https://www.itu.int/en/about/Sss/default.aspx, ET.30.01.2020.
[405]Bilgi Teknolojileri ve İletişim Kurumu, Uluslararası Telekomünikasyon Birliği-ITU, 16.04.2018, https://www.btk.gov.tr/itu, ET.30.01.2020.

devletler bu değişimi kabullenmeyerek kontrolü ellerinde tutmuştur. ITU'nun doğuşunda olduğu gibi siber uzay ile ilgili teknik koordinasyon ve yanlış kullanılma ile ilgili bir koordinasyon oluşturulması gerekmektedir. Her ne kadar ITU telgraf, telefon, telsiz işinden günümüzdeki internet sürecine giriş yapmaya çalışsa da devletler bu duruma izin vermemiştir. Sonuç olarak da günümüz Soğuk Savaş'ın dijital versiyonu olarak adlandırılan gerilimli bir siber savaş alanına dönüştü. Peki, Soğuk Savaş döneminde bile ITU anlaşmalarında bir fikir birliği varken siber uzay hakkında devletler neden anlaşamamaktadır? İşte buda siber uzayın sahip olduğu bilinmezlik ve etki gücünde saklıdır.[406] Bu etki gücü "Siber" sözcüğü ve "Savaş Meteforu"nu birlikte açıklamamıza yol açmaktadır. Siber savaşla birlikte siber uzayın bugünkü önemine gelmesini sağlayan konvansiyonel veya nükleer bir savaşa girmeden, büyük kayıplar yaşamadan kazanma imkânını devletlere sağlamış olmasıdır.

Sonuç olarak; devletlerin uluslararası hukuk kuralları çerçevesinde siber ortama yönelik ortak bir dil oluşturması ve bu dili takip edecek bir üst otorite kurması gerekmektedir. Günümüzde olduğu gibi devletler rakiplere karşı siyasi durumu değiştirmek için siber şiddet yollarını kullanmaya devam edip bunu gerçekleştirmek için terör gruplarına destek vermeye devam ederlerse bu durum ilerde çok ciddi güvenlik açıklarına yol açacaktır. Çünkü siber güvenlik açısından her zaman saldırgan bir adım öndedir. Hedef bellidir. Saldırganlar işlerini iyi yaparak en zayıf halkayı bulurlar. Bu sebeple her ne kadar tamamen riski ortadan kaldırmak imkânsız olsa da iletişim sektörüyle bağlantılı bir şekilde uzun yıllardır Birleşmiş Milletlerin alt çatısı altında görev yapan ITU'ye siber alanında verilecek üst bir otorite yetkisi ile bu risk azaltılabilir.

c) ***Modeli Destekleyecek Bakışlar***

Bu önerinin gerçekleşmesinde en büyük sıkıntı bir ülkede meşru olduğu düşünülen internet faaliyetlerinin başka bir ülkede yasa ihlali olarak görülmesidir. Siber uzay ile ilgili bu durum ülkelerin tek başına çözüm bulmalarını etkisiz kılmaktadır. Bu yüzden bu küresel soruna verilebilecek en güzel cevap Birleşmiş Milletlerin kuruluşu olan ITU'nün kontrolü altında yeni bir yapılanma sürecine girilmesi, sahip olunan üyelik ve kabiliyet gücünün uluslararası siber güvenlik

406Sınger ve Fnedman, a.g.e. , ss.244-249.

girişimlerini bir araya getirmek ve standartları korumak için siber meseleleri içerecek şekilde yaptırım veya cezai yetkinin tanınmasıdır. Bu bağlamda tezimizde ortaya koyduğumuz bu modele hem Schmit yasası hem de Stanford teklifi destekleyici bir bakış sunmuştur.

Siber operasyonların daha kapsamlı değerlendirilmesi ve karakterize edilmesi yönünde bir yaklaşım sunan Schmitt Analizi, siber silahlarla kuvvet kullanımındaki nicel ve nitel boşluğu kapatmaya çalışmaktadır. Bu yönden tezimizde önerdiğimiz modeli destekleyen Schmitt Analizi Madde 2 (4) çerçevesinde daha tutarlı, öngörülebilir ve nispeten siber uzayda kuvvetin nesnel karakterizasyonuna bağlılığı ortaya çıkaracak bir çerçeve sunarak siber saldırın daha kapsamlı değerlendirilmesini sağlayabilir.

1999 yılında, Profesör Michael N. Schmitt tarafından ortaya atılan Schmitt Analizi, bir siber saldırının BM Şartı açısından bir kuvvet kullanım gücüne eşit olup olmadığını değerlendirmiştir. Saldırı senaryolarında yedi nitel faktörü değerlendirerek toplam güçlülük düzeyini, fiziksel yaralanmayı veya hasarı ölçen şiddeti belirlemeyi temel alan Schmitt Analizi, 2003 yılında bir araştırmacı ekip tarafından teröristlerin yazılımı vurmak için uzaktan kötü amaçlı kod kullandığı bir saldırı senaryosuyla kavramsal bir siber sisteme uygulanmıştır. Böylece Profesör Schmitt'in analitiği siber operasyonları karakterize etme yaklaşımında ve Stuxnet'in analizini ortaya çıkarmada önemli bir model sunmuştur. Daha da önemlisi, bu analiz modeli Madde 2 (4) çerçevesinde daha tutarlı, öngörülebilir ve nispeten siber uzayda kuvvetin nesnel karakterizasyonuna bağlılığı ortaya çıkaracak bir çerçeve sunmuştur.

Ayrıca Schmitt Analizi Estonya, Gürcistan ve İran'daki olaylar çerçevesinde siber uzayda kuvvet kullanımı ve yasal sonuçlar hakkında tartışma eksikliği üzerinden devletlerin yakın zamanda siber güç kullanımını neyin oluşturduğu konusunda fikir birliğine varması olası gözükmemektedir. Bu olası olmayan durum sonucunda gelişen normların, Madde 2 (4) 'ün kuvvet kullanımındaki dar yasağı ile siber uzayın yıkıcı sonuçlarının ve uluslararası toplumun güvenlik açıklarının kısıtlanmasının muhtemel olmadığı sonucuna ulaşır.[407] Peki Schmitt Analizi ne sunar? Yada ne kadar doğrudur?

[407]Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate, ndupress", JFQ sayı 67, 2012, ss.40-48.

Bir ülkede meşru olduğu düşünülen internet faaliyetleri başka bir ülkede yasaları ihlal etmektedir. Bu yüzden siber uzay ile ilgili tek başına ülkeler çözüm bulmakta etkisiz kalacaktır. Bu yönden Schmitt Analizi aslında doğru sonuç vermektedir. Fakat bu küresel soruna küresel bir etkisi olacak olan BM, uluslararası siber güvenlik girişimlerini bir araya getirmek ve standartları korumak için siber meseleleri içine alacak ITU'nün kontrolü altında bir yeniden yapılanma sürecine sokulursa sahip olduğu üyelik ve kabiliyet gücü uygunsuzluk için yaptırımlar veya cezai eylemler ortaya koyarak bu sorunun çözülmesine yönelik bir fırsat sunabilir.

Modeli destekleyecek bir diğer önemli bakış 2000 yılında Stanford Üniversitesi tarafından hazırlanan "Siber Suç ve Terörizmle İlgili Uluslararası Bir Sözleşme Önerisi"dir. Bu sözleşme önerisi daha büyük bir uluslararası işbirliğinin sağlanabilmesi için siber saldırılara karşı mücadelede çeşitli argümanlar sunmuştur.[408]

Stanford Önerisine göre; siber suçlular yasalardan veya icra uygulamalarındaki zayıflıklardan yararlanmaktadır. Aynı zamanda; siberlerin hızı ve teknik karmaşıklığı yüzünden tehditlere ve saldırılara yanıt verecek faaliyetlerin araştırılmasında önceden belirlenmiş ve üzerinde anlaşmaya varılmış işbirliği prosedürleri gerekmektedir. Bu bağlamda; Stanford Taslağı, Taraf Devletlerin 6. ve 11. Maddelerde belirtilen karşılıklı hukuki yardım ve kolluk hükümleri aracılığıyla soruşturmada işbirliği yapmasını gerektirmektedir. Bu maddeler uyarınca taraf devletler bilgi alışverişi, kanıt toplama ve koruma konusunda yardım, iddia edilen suçluları tutuklama, kovuşturma veya iade etme, güvenlik ve yasa uygulama ile ilgili olarak kabul edilmiş uluslararası standartları uygulamalıdır. Stanford Teklifinin 12. Maddesi de uluslararası bir kuruluşun kurulmasını savunmaktadır. Hoover Enstitüsü, oluşturulacak bu kuruluş önerilerinin içerisinde Uluslararası Telekomünikasyon Birliğini de sayarken yetkilendirilmiş bu kurumun temel endişeyi gidereceğinden bahsetmiştir.

Ancak, Stanford Önerisinin tek eksiği devlet davranışını hariç tutarak yalnızca bireylerin veya grupların davranışlarını ele almasıdır. Bu yüzden bu öneri bizim model önerimizden ayrılmaktadır. Tezimizde bahsettiğimiz sponsor devletler

[408]Stanford University, "A Proposal for an International Convention on Cyber Crime and Terrorism", Ağustos 2000, http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm ET. 25.01.2020.

konvansiyonel veya nükleer saldırıların maddi ve manevi zorluklarından dolayı bu saldırıların sayısını azaltarak, maliyeti ve karmaşıklığı endişe verici oranlarda artan siber saldırılarda bireyleri (hackerları) ve terör gruplarını kullanmaktadır. Çünkü siber uzayın kullanım alanının artmasıyla birlikte bilgi altyapısı siber suçlular tarafından giderek daha fazla saldırı altına girmektedir. Fakat artan bu saldırılara karşı hem özel sektör hem de kamu sektörü tarafından bugüne kadar alınan önlemler yeterli düzeyde güvenlik sağlamamıştır. Bu yüzden yeni saldırı yöntemleri uzmanlar tarafından doğru bir şekilde öngörülmüş ve erken aşamalarda bazı büyük saldırılar tespit edilmiş olsa da, bunları önleme veya caydırma çabaları büyük ölçüde başarısız olmuş ve giderek daha fazla zarar verici sonuçlar doğmuştur. Böylece saldırılarla mücadele için gerekli bilgiler zamanında paylaşılmamıştır. Soruşturmalarsa yavaş ve koordine edilmesi zor bir hal almıştır.

Modelimizi destekleyecek bu öneriler var olsa da günümüzde hala siber alanda yaşanan siber çatışmaların arttığı ve uluslararası işbirliğine gönüllüğün yetersiz kaldığı unutulmamalıdır. Bazı saldırılar, yeterli yasalara sahip olmayan devletlerden kaynaklanmaktadır. Bu yüzden siber kelimesinin ulus ötesi niteliğe sahip olan özü gereği birden fazla devletin yargı beyanlarını içerecek şekilde suçlar tanımlanmalıdır. İhtilaflı iddialardan kaçınmak için yargı yetkisi ve icra anlaşmaları geliştirilmelidir. Bu bağlamda; siber suç ve terörizmle mücadele kavramını devletlerden ayrı sadece özel sektörü içerecek şekilde tek boyutlu olarak kesinlikle düşünmemeliyiz.

SONUÇ

İnternetin ortaya çıkmasıyla beraber tüm dünya yeni bir düzene geçmiş, internetin kullanım yaygınlığının ve sıklığının artmasıyla da büyük bir dönüşüm başlamıştır. Tüm dünyada birbirine bağlı ağlar oluşturan internet, teknolojik bir devrim niteliğiyle küresel düzeyde rakiplerle mücadele şeklini değiştirmiş, yeni tür silahları ortaya çıkarmış ve tüm kritik alanların iç içe geçmesiyle güvenlik kapsamını genişletmiştir. İnternete her geçen gün erişilebilirliğin artması ile bilgilerin depolanması, saklanması, korunması ve doğru kişilerle paylaşılması gibi sorunları da beraberinde getirmiştir.

Endüstri 4.0 ve Toplum 5.0 kavramlarının konuşulduğu günümüzde siber ortamda faaliyet yürüten kullanıcı sayısının artması, her türlü aktör profilinin kullanıcılar arasında bulunması, karşıdaki kişinin kim olduğunun sanal ortamda tespit edilememesi ve sahte hesaplar gibi sebepler siber tehditleri ortaya çıkarmıştır.

Bilgi çağı olarak adlandırılan bu dönemde güvenlik, tehdit, risk ve caydırıcılık kavramlarıyla birlikte kronikleşen sorunlar ortaya çıkmıştır. Bu sorunların çözümü hızlı analiz ve aksiyonların alınmasını zorunlu kılmış, uluslar arası düzeyde ülkeler için yapay zekaya, siber güvenliğe ve dijital dönüşüm araçlarına ihtiyaç doğmuştur. Bunları elinde bulunduran ya da bunlara yatırım yapan aktörler yeni küresel düzendeki yerini almış ve uluslararası alanda 'gücü ellerinde bulunduranlar' konumuna gelmiştir. Bu güç değişimindeki asıl nedense siber uzayın içinde barındırdığı karakteristik özelliklerden gelmektedir.

Siber uzay; karşı tarafın zayıf yönlerini hedef alarak rakipleri korkutmayı, etkilemeyi veya caydırmayı hedefleyen asimetrik ve hibrit bir tehdit ortamıdır. Siber saldırıların en önemli özelliğinin ne zaman, nereden ya da kim tarafından gerçekleştirileceğinin bilinmemesi siber uzayın içinde barındırdığı bilinmezlik, öngörülemezdik ve tahmin edilemezlik gibi karakteristik özellikleri risk unsurunu arttırmaktadır. Artan risk korkuyu, artan korku tehdidi, artan tehdit güvensizlik hissini, artan güvensizlik hissi silahlanmayı, artan siber silahlar güvenlik ikilemini, artan güvenlik ikilemi güç dengesi arayışlarını ve çatışmaları, artan çatışmalarsa savaşları doğurmaktadır.

Savaş kavramı ise güvenlik ve strateji kavramlarından ayrı düşünülemez. Dolayısıyla, güvenlik ve tehdit, karşılıklı ve sürekli olarak birbirlerini etkileyen

anarşik bir yapıdadır. Ayrıca siber alanda tehdit belirleme ve güvenlik stratejisi oluşturma ihtiyacının ana sebebi uluslararası sistemin anarşik bir yapıya sahip olmasıdır. Bu doğrultuda, siber güvenlikte herkes güvende olmadan hiç kimse güvende olamaz. Bu durumda devletler askeri güçlerine güvenmek ve bu alanda askeri güçlerini yeterli düzeyde tutmak amacıyla askeri yapılarının içerisinde siber ordu birimleri kurarak bu güç boşluğunu doldurmak istemektedirler.

Siber uzayın kapsama alanı ve etki boyutu henüz tam olarak bilinmemektedir. Buna ilave olarak siber savaşın nasıl olacağının canlandırmasının ilk aşamasında olduğumuz bugünlerden 21. yüzyılın sonlarına gittiğimizde siber uzaya hâkim olanın yeni stratejik zeminin hakimiyetini elinde bulunduracağı gerçektir.

Siber uzay küreseldir fakat devletsiz değildir. Boyut ve ölçeği sürekli evrim geçirmektedir. Siber uzayın coğrafyası fiziki değildir. Bir tuşla değişebilir. Buda risk ve tehdidi arttırmaktadır. Risk ve tehditlerin önlenmeside siber güvenliği sağlamaya bağlıdır. Bu yüzden siber güvenlik, 21. yüzyılda ulusal güvenliğin en yeni sorunudur. Nasıl sanayi devrimi'nin yarattığı büyük değişiklikler tüm dünyayı ve 20. yüzyılın savaş alanını dönüştürdüyse, 21. yüzyılın ilk çeyreğinde gerçekleşen bilişim teknolojileri ve biyoteknolojideki gelişmeler de siber uzay alanı içinde kullanılan siber silahlarla aktörleri yeni bir savaş alanına dönüştürmüştür. Bu yeni soruna karşı siber güvenliği sağlamak ve siber saldırılara karşı koymak için hazırlanacak stratejinin üç hedefi olmalıdır. Bunlar; savunma, tespit ve caydırmadır. Bunun düzgün bir şekilde sağlanabilmesi için ise siber güvenlik duvarları oluşturmak yeterli değildir. Oluşturulan bu siber güvenlik duvarlarının milli imkânlarla oluşturulması ve milli yapay zekâ ile makinelerin bu stratejiyi öğrenmesi sağlanmalıdır.

Aynı zamanda; siber saldırıların öncelikle bilgisayar veya sunuculara yönelik düzenlenmesinin anlık ve hızlı bir yayılma etkisi göstermesinden küresel etkiler yaratması kaçınılmazdır. Küresel anarşik bu yapı içerisinde dünyanın en önemli askeri ve siber gücüne sahip olan Amerika Birleşik Devletleri aynı zamanda en fazla tehdit riskine sahip ülke konumundadır. Bu ters orantılı fırsat/tehdit paradoksunda Rusya, Çin ve Amerika'nın dış politikasında uyguladıkları çatışma/işbirliği dinamiklerinde siber uzayın rolü bu ülkelerin uluslararası sistemdeki ana siber güçler oldukları görülmektedir. Ayrıca, teknoloji cephesinin günümüzdeki yansımalarına baktığımızda Çin ve Rusya gibi ülkelerin birbirleriyle askeri, ekonomik ve ticari

ilişkilerini geliştirmelerini siber alanda da sürdürmektedirler. Bu işbirliği çabaları ABD ve AB gibi batı ekseninde endişe yarattığından ABD ve NATO'nun da karşı düzlemde siber ittifak yaratma çalışmalarını devam ettiği görülmektedir. Çünkü bu mücadeleler sürerken günümüzde Çin'in ABD ekonomisini zayıflatmak için kendi siber uzay gücünü kullandığı, Rusya'nın eski coğrafyasına yönelik hâkimiyetini tekrar kazanmak için geleneksel savaş yöntemlerinin yanında siber saldırıları kullandığı, ABD'nin yüz yüze kaldığı siber güvenlik risklerinden dolayı NATO içerisinde özellikle Estonya örneğinde de olduğu gibi bir ittifak sistemi oluşturmaya çalıştığı örnek vakalar üzerinde açıklanmıştır.

Özellikle 2000 ve 2014 yılları arasında yaşanan gelişmeler ışığında uluslararası sistemde ana aktör olan devletler tarafından gerçekleştirilen zorlama yaklaşımının bir parçası olarak siber çatışmaların ve tehditlerin sonucunda siber teknolojiler hayatın her alanını bütünleştirmiştir. Bu bütünleşme çerçevesinde Soğuk Savaş döneminde tecrübe edilen askeri rekabet ve uzay yarışının günümüzde ABD ve Rusya arasında yaşanan siber uzay temelli teknoloji çatışmalarının temelini oluşturduğu ve Güvenlik ittifaklarına bakıldığı zamanda, AB'nin siber savunma işbirlikleri ve NATO'nun kolektif savunma anlayışında sistemin değişen şartlarıyla birlikte siber savunma ve siber güvenlik ortamına uyum sağladığı görülmektedir. Fakat şuana kadar küresel olarak dengeleri değiştirecek boyutta bir siber saldırıyla karşılaşılmamıştır. Bu yönde alınması gereken ciddi önlemlerin varlığı kabul edilerek bugün bir değişim ve dönüşüm içinde olduğumuz unutulmamalıdır.

Bu tezde yapılan araştırma ve incelemeler sonucunda ulaşılan tespitlerden ilk ve önemlisi siber savaş, siber güvenlik, siber silah kavramları ile küresel düzende tehdit, caydırıcılık, güvenlik ve strateji konularının bir arada analiz edilmesinin gerektiğidir. Bu sebeple siber ortamda gerçekleşen çatışma sürecine stratejik olarak yaklaşılmalıdır. Bunun için de siber güvenlik stratejileri belirlemek gerekmektedir. Bu stratejiler belirlenirken bazı temel ilkelere dikkat edilmelidir. Bu temel ilkeler, temel hak ve hürriyetlerin korunması, demokratik toplum düzeninin gereklerine uyulması, ölçülülük ilkesine uyulması, karar alma süreçlerine tüm paydaşların katılımının sağlanması, bütüncül bir yaklaşımla hukuki, teknik, idari, ekonomik, politik ve sosyal boyutların ele alınması, güvenlik ile kullanılabilirlik arasında denge

kurulması, diğer ülke mevzuatlarının göz önünde bulundurulması ve uluslararası işbirliğinin sağlanması şeklinde sıralanabilir.

Strateji kavramı güç, tehdit, caydırıcılık, çatışma, güvenlik ve savaş kavramları ile doğrudan bağlantılıdır. Siber strateji oluşturma sürecini tek bir teori, model veya bilim dalı ile açıklamak mümkün değildir. Çünkü siber güvenliği sağlama yönünde strateji oluşturma sürecini etkileyen birçok farklı faktör bulunmaktadır. Bunlardan bazıları; siber ortamın kara, hava, deniz ve uzay dâhil tüm boyutları kapsaması, probaganda yürütme, lobicilik, rakiplere karşı zorlama, bozma, casusluk gerçekleştirme, tehdit etme ve caydırma gibi birçok stratejik sebep için kullanılmasıdır. Ayrıca saldırgan tarafa kazanç sağlaması, düşük işletme maliyeti ve avantajları nedeniyle rekabet ilişkisinde sık sık kullanılması siber savaşı tercih edilebilir kılmaktadır. Böylece 21. yüzyılda siber uzayda hayatta kalmanın ve gelişmenin temel yolunun büyük strateji kavramının "siber güvenliğin sağlanması" olarak konumlandırılması gerekli hale gelmiştir.

Bu ilkeler çerçevesinde uzmanlaşma ve entegrasyon olmadan uluslararası anarşik sistemde ulusal güvenliğin sağlanmasının imkansız olduğu, güçlü bir milli savunma teknoloji alt yapısının oluşturulabilmesi için kritik savunma konularının enerjiden finansa, ulaşımdan sağlığa, askeri alandan nükleer tesislere kadar bir arada değerlendirilmesi gerekmektedir. Siber güvenliğin sağlanmasına yönelik farkındalığı arttırma yönünde faaliyetler geliştirilmesi, yerli ve milli ürünlerin kullanılması gibi siber güvenlik çalışmalarına hız verilmesi hayati öneme sahiptir. Ayrıca siber güvenlik kavramı her ne kadar teknoloji içerse de siber güvenlikte en önemli halkanın insan faktörü olduğu unutulmamalıdır.

Siber savaş kavramı siber uzay özelinde değerlendirildiğinde klasik bir savaşta kullanılan taktik ve stratejilerle; günümüzde gerçekleşen siber savaşlar arasında amaçlanan hedefler yönünden benzerlikler olduğu görülmektedir. Siber savaşın klasik savaş konsepti ile eşgüdümlü bir halde kullanılması halinde etkisi çok daha büyük olacaktır. Ayrıca geleneksel muharebelerdeki gibi savaş meydanının olmaması ve düşman ülkenin savunma sistemi ve kritik altyapısının kolaylıkla uzaktan imha edilebilmesi mümkün olacaktır. Bu sebeple 20. yüzyılın son döneminde yaşanan şiddet ve baskının içerdiği faşist, komünist ve kapitalist savaşlar yerlerini insanlar, bulgular, sayılar, denklemler, görüntüler ve bilgiler gibi 21.

yüzyılın yeni hedeflerine bırakmıştır. Bu yeni hedefleri içeren siber savaşlar savaş kavramının bir alt kümesi olarak ufak tefek çatışmalarda savaş öncesi bir ilk hamle olarak kullanılmaktadır. Bu sebeple siber ortamda kontrollü barışın var olduğu, teknolojik gelişmelerin savaşları değiştirip dönüştürdüğü ama teknolojik üstünlüğün savaşların kazanılması için zaferi garantileyen bir faktör olmadığını söyleyebiliriz. Ayrıca savaş maliyetlerinin artması ve savaş sonunda elde edilecek kazanımların aktörler tarafından siber yöntemler vasıtasıyla savaş olmadan elde edilme fırsatı bazı değişimleri ortaya çıkaracaktır. Bu değişimlerle birlikte siber çatışmalar artacak, temiz üniformalı ve ekran başından savaşları idare edecek askerleri içeren siber ordular yaygınlaşacaktır. Bu sebeple uluslararası hukukta herhangi bir silahlı çatışma eyleminin savaş sayılıp sayılmayacağı hususundaki temel ölçütün ilgili devletlerin amacı (isteklerini diğer bir ulus ve devletler topluluğuna zorla kabul ettirmek amacıyla giriştikleri bir mücadele) olarak değerlendirilmesi gerekmektedir. Zaten bugüne kadar Estonya, Gürcistan, Ukrayna, Venezuela ve İran'a karşı gerçekleştirilen saldırıların siber savaşın ciddiyetini ortaya koymada etkili olmuştur.

Bir ülkede meşru olduğu düşünülen internet faaliyetleri, başka bir ülkede yasaları ihlal ediyor olabilir bu durumda yeterli yasal düzenlemeleri olmayan ülkelerden diğer ülkelere karşı saldırılar gerçekleşebilir. Günümüzde konvansiyonel veya nükleer bir savaşın gerçekleşmiyor olması mutlak bir barış olduğu anlamına gelmemektedir. Nasıl soğuk savaş barış içinde sonuçlandıysa, günümüzde yaşanan siber çatışmalar, korkular ve tehditler de bir barış ortamı içerisinde gerçekleşmektedir.Bu yüzden siber savaş kavramı siber silah özelinde değerlendirilmelidir.

Siber silahlar bir ülkedeki hayatı yok edebilecek güce sahiptir. Ciddi bir güç aracı olarak kullanılan siber silahlar son yılların en önemli askeri yeniliğidir. Siber silahlar kullanılarak gerçekleştirilen saldırıların başlangıcıyla etkisi arasındaki zaman aralığı ışık hızında gerçekleşmektedir. Ayrıca saldırıların öncelikle bilgisayar veya sunuculara yönelik gerçekleşmesinden dolayı anlık ve hızlı bir yayılma etkisi gösterdiği bu yüzden de küresel olduğu açıktır. Bir diğer yandan siber silahlar cephelerde değil, doğrudan bir devletin, milletin kritik alt yapılarını, ekonomilerini ve unsurlarını hedef almaktadır. Bu durumun önüne geçmek içinde kritik savunma

konularının hepsinin (enerjiden, finansa, ulaşımdan sağlığa, askeri alandan nükleer tesislere kadar) bir arada değerlendirmesi gerekmektedir.

Silah sistemlerinin geliştirilmesi ve kullanılması disiplinler arası bir çalışma gerektirdiğinden siber silahlara yönelik uzmanlaşma ve entegrasyon olmadan uluslararası anarşik sistemde ulusal güvenliğin sağlanmasının imkansız olduğuna ulaşılmıştır. Bu bağlamda; kurumsal çerçevede siber güvenlik sürecini yönetebilmek için siber silah tehditlerinin azaltılması veya siber silah kullanımının sınırlandırılmasına yönelik uygulamaların geliştirilmesi gerekmektedir.

Neorealist çerçevede gerçekleştirilen vurgu çerçevesinde siber uzayda ki anarşik yapının dünyayı ilerleyen süreçte elektronik Pearl Harbor gibi beklenmedik bir anda siber alanda yaşanabilecek bir "World Wide Web War" savaş tehdidini tetikleyebileceği düşünülmektedir. Siber savaşlarda karşılıklı olarak gerçekleşmesi beklenen yıkım ve kimin nasıl misilleme yapacağının bilinmezliği caydırıcılığı arttırmış, aktörler arasında siber silahlara yönelik teknolojik üstünlük mücadelesiyle bir silahlanma yarışının olduğunu göstermiştir.

Siber tehdidi doğru ölçebilmek ve strateji geliştirebilmek için öncelikle gözlem, takip, analiz ve tahmin kapasitesi olan birimlerin arttırılmasının gerekliliği, savaş kavramı evrensel olduğundan siber silahların kötü amaçlı kullanımına yönelik çözümünün de evrensel olması gerektiği düşünülmektedir.

Nitekim, dünyayı derinden etkileyen ve değiştiren Sovyetler Birliğinin dağılması, komünizmin çökmesi, iki Almanya'nın birleşmesi gibi olayların kansız ve savaşsız gerçekleşmiş olduğu dönemler alternatif bir çatışma durumu olarak görülmüş, bu yaşananlar barış dönemi şeklinde algılanmamıştır. Bu sebeple günümüzde yaşanan siber çatışma dönemi klasik savaş gibi yaşanmadığından kesin olarak barış dönemi şeklinde de açıklanamayacaktır.

Neorealist çerçevede ulaşılan bu çıktılar çerçevesinde küresel anarşik yapının içerisinde gerçekleşen çatışmaların azaltılarak risk ve tehditlerin önlenmesi, barış ve işbirliğinin geliştirilmesi yönünde süreç hakkında bazı küresel öneriler ortaya konmuştur. Kısaca bunlardan bahsedersek; hem ulusal hem de küresel düzeyde konuyla ilgili uzman sayısı arttırılmalı, aktörler arasında işbirlikleri geliştirilerek hep beraber mücadele edilmeli, küresel cezaların eksik olmasından kaynaklı olarak cezaların caydırıcılığı arttırılmalı, güvenliğe ayrılan paydan siber güvenliğe ayrılan

pay arttırılmalı, siber ortamdaki korku fırsata dönüştürülerek güven arttırıcı etkinlikler, mücadele stratejileri, eylem planları ve çalışmalar yapılmalı, küresel düzeyde siber güvenlik eko-sistemi oluşturulmalı, siber silahların sürekli güncellenmesinden dolayı iç hukuk kuralları sürekli güncellenmelidir. İç hukuk kurallarının yanında silahlı çatışma hukuku, Cenevre Sözleşmesi, uluslararası hukuk kuralları vb. savaş kuralları ile uluslararası normlar, kurallar, kriterler, cezai yaptırımlar ve kaidelerin siber uzay özelinde güncellenmesi gerekmektedir. Hem iç hukuk hem de uluslararası hukuk kurallarındaki güncellemeler gerçekleştirildikten sonra uluslararası anarşik yapı içerisindeki rakipler arasındaki siber güç mücadelesinin savaşa dönüşmesi yerine işbirlikçi bir temelle barışçıl kullanımı için sanal mülkiyet kavramı ortaya çıkarılmalıdır. Sanal mülkiyetin oluşmasıyla birlikte saldırıların arkasında olan, kışkırtma yaptığına yönelik kanıtlar bırakan, sorumluluktan kaçmak için ortaya çıkmayan ve siber uzayın gizemiyle kimliğini saklamaya çalışan devletler "sponsor devlet" özelinde incelenebilir. Böylece sanal mülkiyet kavramıyla birlikte küresel standartlar ve normlar üzerinden yasal sorumluluğu kabul eden devletlere gerçekleştirdikleri tüm faaliyetlerin yükümlülükleri vekaleten devredilebilir.

Siber silah üretiminin, kullanımının, tedariğinin ve yayılmasının sınırlandırılmasına yönelik uluslararası anlaşmaların imzalanması gerekmektedir. Çünkü artan siber silah kullanımıyla birlikte ilerde ortaya çıkabilecek siber dünya savaşının önlenebilmesi için denetleyici, düzenleyici, kontrol edici ve siber güvenlikten sorumlu kurumlar arasında hızlı bilgi paylaşımı sağlanması yönünde kurumlar arası işbirliğini sağlayacak uluslararası bir üst otorite örgütünün kurulması gerekmektedir. Çünkü siber meselelerde ülkelerin küresel anlamda birbirlerine danışmaları ve bazen de işbirliğine girmeleri için etkili bir mekanizma bulunmamaktadır.

Neoliberal kurumsalcı teoriler çerçevesinde ortaya koyduğumuz öneri de bu örgüt için en uygun kurumun uluslararası alanda hukuki kuralların ve cezai mueyyidelerin oluşturulmasıyla birlikte yeniden yapılandırılacak ve yetkilendirilecek Birleşmiş Milletlerin alt kurumu olan Uluslararası Telgraf Birliği(ITU) olduğu düşünülmektedir. Avrupa Siber Suçlar Sözleşmesinden yola çıkarak hazırlanacak kapsamlı evrensel siber hukuk kuralları saldırganlığın reddedilemez kanıtını ortaya

çıkaracaktır. Böylece her devletin siber saldırılara ve yaklaşmakta olan tehlikelere karşı kendini savunma hakkı veya her türlü misilleme gerçekleştirme sınırı çizilerek üzerlerine düşen sorumluluğu yerine getirecekleri düşünülmektedir.

Bu tez teknik bir konu olarak görülebilecek siber uzay alanını sosyal bilimler alanında açıklayarak dünyanın 21. yüzyılda, ulusların dış politika ilişkileri açısından ne gibi çatışmalarla karşılaşabileceği, nasıl gelişmeler yaşanabileceği, diplomatik dengelerde nelerin etken olabileceği sorunlarına "siber uzay" sorunsalıyla ışık tutmayı amaçlamış ve siber uzayın gelecekte kullanılacak hakim anlayış olacağı yönünde literatüre farklı bir bakış açısıyla katkı yapmayı hedeflemiştir. Bu iddia ortaya atılırken; teknolojik gelişmelerin tarih boyunca savaşları, güvenlik algısını ve tehdit parametrelerini değiştirmesinden yola çıkılarak kronolojiye önem verilmiştir. Güvenlik modellemelerinde siber güvenliği önceliğe alarak dijital unsurlara yönelik bir farkındalık yaratmak hedeflenmiştir. Çünkü günümüzde yaşanan mücadelenin adı siber savaş, aracı internet ve bilgisayar, ganimeti ise bilgiye ulaşma veya sahip olunan imkânların rakiplerce kullanılmasını engellemedir. Tezimizde ayrıntılarıyla belirttiğimiz örnek çatışma vakalarında da görüldüğü üzere, siber ortamda tüm altyapılar (iletişim hizmetleri, finans piyasaları, bankacılık sistemleri, havacılık hizmetleri, acil hizmetler vb.) domino etkisiyle durma tehdidi altındadır. Bu risk siber güvenliğin önemini ortaya koymaktadır. Siber güvenlik ise tüm bu değişim ve dönüşümdeki bilgilerin gizlilik ve bütünlüğünün bozulmaması ile kritik altyapı sistemlerinin korunmasında ayrılmaz bir parça olmaya devam edecektir. Bunun asıl sebepleriyse şunlardır; bilginin temel meta olması, mücadelelerin bilgi üzerine kayması, savaş maliyetlerinin artması ve savaş sonunda elde edilecek kazanımların aktörler tarafından siber yöntemler vasıtasıyla savaş olmadan elde edilme fırsatıdır. Artık şiddet ve baskı eskisi kadar konvansiyonel alanda yaşanmamakla birlikte fikirlerin ve malların küresel ticarete dönüşmesi, arge çalışmalarının gizliliği ve stratejik konuların elektronik ortama taşınmasıyla birlikte siber güvenlik hayati bir konuma yükselmiştir.

Dünyada nasıl bugüne kadar her yüzyılda büyük bir dönüşüm yaşamışsa şuanda da yaşamaktadır. Bu sebeple, 21. yüzyıl itibariyle yaşanan temel mücadele milli yazılıma sahip olma, büyük veriyi kontrol etme, en az maliyet ve kayıpla rakiplere karşı üstün gelme, caydırıcılık yaratarak gücünü kabul ettirme, dijital

dünyanın sınır güvenliğini sağlama, dijital dönüşüm araçlarını (büyük veri, nesnelerin interneti, yapay zeka, bilgi teknolojileri, bulut, siber silah vb.) elinde bulundurma, siber ordular oluşturarak güç ve tehdit unsurlarını kontrol etme gibi durumlar yeni alanlara odaklanmayı mecbur kılmıştır. Yani, dijitalleşmeyle birlikte hayatın her alanı dijitalleşerek siber tehdit ve risklerin önemi artmıştır.

Yukarıda ayrıntılarıyla ortaya koyduğumuz neorealist ve neoliberal teoriler çerçevesinde ortaya koyduğumuz sorunsallar, tespitler, öneriler, değerlendirmelerle birlikte elde ediler veriler ışığında siber ortamda güvenli bir uluslararası ilişkiler ortamı sağlamak için donanım, yazılım ve sistemlerin güvenliğinin tüm ülkelerin problemi olduğunu açıkca söyleyebiliriz. Yaşanan çatışmalara ve dünyanın geldiği noktaya baktığımızda yapılacak çok işin olduğu açıktır. Bunun çözülebilmesi için disiplinler arası çalışma ile ulusal ve uluslararası işbirliği gerekmektedir. Küresel düzeyde bilgi paylaşım platformları geliştirilmesine yönelik yeni çözümlere ihtiyaç bulunmaktadır. Ulusal kapasitenin arttırılmasına yönelik milli bütçelerden ciddi bir ekonomik kaynak aktarılması gerekmektedir. Birlikte çalışılabilecek yapılar kurulmalıdır. Hem yazılım hem de cihazlar özelinde güven arttırıcı, milli ve kendi çözümlerimiz geliştirilmelidir. Ayrıca en önemlisi geleceğimizin teminatı olan gençlerin konuya ilgisinin ve farkındalığının arttırılması bir zorunluluktur.

Tezin son noktasında sıralanan bu noktaların asla unutulmaması gerekliliğinin ısrarla vurgulanmasının asıl sebebi ise günümüzde hala uluslararası rekabet ortamında kullanılan siber kavramlar üzerinde aktörler arasında, küresel bir uzlaşma sağlanmasına yönelik bir niyet olmamasıdır. Neoliberal değerler çerçevesinde siber uzayın barışçıl kullanımı için tüm bu maddeler baştan kabul edilerek küresel standartlar ve normlar üzerinde uluslararası işbirliğinin oluşturulması gereklidir. Çünkü siber saldırılara karşı yapılacak mukabelenin şeklinin ve sınırlarının nasıl çizileceği, karar alma sürecinin nasıl olacağı, uluslararası iş birliğinin ne şekilde sağlanabileceği, ortak savunma ve ittifak ilişkisinin tam olarak kurulup kurulamayacağı gibi noktaların karara bağlanması gerekmektedir. Bu çerçevede; neorealist çerçevede güvenlik ve strateji boyutunda uluslararası arenada siber güç dengelerinin değişimi ele alınarak anarşik sistemde çıkarların, çatışmaların ve çakışmaların ortasında bu savaşın önlenebilmesi için denetleyici, düzenleyici ve kontrol edici uluslararası bir örgütün kurulması zorunluluktur.

KAYNAKÇA

Kitaplar

Aksu, B**. Big Data Bilginin Gücü**, Pusula Yayınları, İstanbul, 2017.

Altunok, T. ve Çakmak, H. **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, Barış Platin Kitapevi, Ankara, 2009.

Arı, T. **Uluslararası İlişkiler ve Dış Politika**. Alfa Yayınları İstanbul,2006.

Arı, T. **Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği**. Alfa Yayınları İstanbul, 2004.

Arıcak, T. **Siber Alemin Avatar Çocukları İnternet ve Gençlik İlişkisinin Bugünü ve Geleceği**, Remzi Kitapevi, İstanbul, 2015.

Armaoğlu, F. **20. Yüzyıl Siyasi Tarihi 1914-1995**, Ayraç Yayınları, https://stratejikoperasyon.files.wordpress.com/2014/05/prof-dr-fahir-armaoglu-20-yzyl-siyasi-tarihi.pdf ET.06.02.2021.

Asimov, I. Çeviren Topçugil, E**. Bilim ve Buluşlar Tarihi**, İmge Kitabevi Yayınları, Ankara, 2006.

Aydın, N. **Türkiye'nin İç ve Dış Tehditlerine Stratejik Bakış**, Parola Yayınları, İstanbul, 2014, ss.137-150.

Bauman, Z. Çev: Abdullah Yılmaz, **Kureselleşme-Toplumsal Sonucları**, Arıntı Yayınları, İstanbul, 2010, ss.63.

Barnet. R. ve Cavanagh, J. Çev. Gülden Şen, **Küresel Düşler: İmparator Şirketler ve Yeni Dünya Düzeni**, Sabah Yayınları, İstanbul, 1995.

Başaran, A. **Yaklaşan felaketin habercileri Siber kıyamet**, Arion Yayınevi, İstanbul, 2017.

Bayraktar, G. **Siber Savaş ve Ulusal Güvenlik Stratejis**i, Yeni Yüzyıl Yayınları, İstanbul, 2015.

Black, J. **Introductıon To Global Mılıtary Hıstory 1775 To The Present Day**, Routledge, 2005.

Booth, K. **Theory Of World Security**, Cambridge University Press, Uk, 2007.

Booth, K. **Realizm and World Politics**, Routledge Journal, 2011.

Bonaparte, N. Çeviren, Gündüz, E. **Savaş ve Strateji ile ilgili Görüşlerim**, Q-Matris Yayınları, İstanbul, 2003.

Burchill S. ve Linklater A. Çeviren; Aslan, A. **Uluslararası İlişkiler Teorileri**. Küre Yayınları, 2013.

Buzan. T. ve Buzan, B. Çevr. Tercanlı, G. **Zihin Haritaları**, Alfa Yayınları, İstanbul, 2019.

Buzan, B. and Hansen, L. **The Evolution Of International Securıty Studies**, Cambridge University Press,2009.

Buzan, B. "**People, States And Fear",** Wheatsheaf Book, 1983.

Brzezinski, Z. Çeviren, Türedi, Y. **Büyük Satranç Tahtası: Amerika'nın Küresel Üstünlüğü ve bunun Jeostratejik Gereklilikleri**, İnkılap Yayınları, ss.36.

Carr, J. İnside **Cyber Warfare Massing The Cyber Underworld**,O'Reilly, USA,2012.https://books.google.com.tr/books?id=5LIyXzpKhYsC&printsec=copyright&hl=tr#v=onepage&q&f=false E.T:08/12/2019

Christen, M. Gordijn, B. Loi, M. **The Ethics of Cybersecurity**, Springer Open, The International Library of Ethics, Law and Technology 21, Switzerland,2020.

Carter, A. B. Perry, W. J. ve Aidekman, D. "**Countering Asymmetric Threats", Keeping the Edge Managing Defense for the Future,** the Mit Press, Cambrigde,2001,ss.120-121. https://books.google.com.tr/books?id=hduWZJ3j_KEC&pg=PA1&lpg=PA1&dq=Keeping+the+Edge:+Managing+Defense+for+the+Future&source=bl&ots=lMtpNzU_4h&sig=ACfU3U0TNlwVxK1ocsGvmICr0pfH2ZbuFg&hl=tr&sa=X&ved=2ahUKEwj4ruSvg4XkAhVWhlwKHewwAeY4ChDoATABegQICRAB#v=onepage&q=Keeping%20the%20Edge%3A%20Managing%20Defense%20for%20the%20Future&f=trueET. 06.02.2021

Clausewitz, C. Çev. Koçak, S. **Savaş Üzerine**, Doruk yayınları, 2015.

Clarke, A. R. ve Knake, R. K. Çeviren Erduran, M. **Siber Savaş,** İstanbul Kültür Ünüversitesi Yayınları, İstanbul, 2011.

Clarke, R. A. and Knake, R. K. **Cyber War The Next Threat to National Security and What to Do About It**, Harper Collins e-books

Chomsky, N. Çeviren Süreyya Evren**, Halk Üzerinden Kazanç Neoliberalizm ve Küresel Düzen**. Everest Yayınları İstanbul, 2014.

Çifci, H. **Her Yönüyle Siber Savaş,** Tubitak Yayınları, Ankara, 2013.

Dağı, İ.D. ve Eralp, A. **Devlet, Sistem ve Kimlik Uluslararası İlişkilerde Temel Yaklaşımlar**. İletişim Yayınları, İstanbul, 2007.

Davutoğlu, A. **Stratejik Derinlik**, Küre Yayınları, İstanbul,2016.

Deibert, R. Palfrey, J. Rohozinski, R. and Zittrain, J. **Access Contested: Security, Identity, and Resistance in Asian Cyberspace**, The MIT Press, Cambridge, England, 2012.

Dedeoğlu, B. **Uluslararası Güvenlik ve Strateji**, Yeni Yüzyıl Yayınları, 2014.

Dyer, N. Çeviren Çakıroğlu, A. **Siber Marx Yüksek Teknoloji Çağında Sınıf Mücadelesi**, Aykırı Yayıncılık, İstanbul, 2004.

Eren, M. **Avrupa Birliği'nin Siber Güvenlik Politikası**, Beta Yayınları, İstanbul, 2017.

Eslen, N. **Tarih Boyu Savaş ve Strateji,** İstanbul, Q-Matris Yayınları, 2003.

Fassi, E. Lucarelli, S. and Marrone, A. **What NATO for what threats?** Warsaw and Beyond, Belgium,2015.

Field, J. **Dünya'nın Kanlı Tarihi**, Maya Kitap, İstanbul, 2015.

Freedman, L. Çeviren Belkıs Çorakçı Dişbudak, **Strateji**, Alfa Yayınları,2014.

Fukuyama, F. Çeviren Zülfü Dicleli, **Tarihin Sonu ve Son İnsan**, Gün Yayıncılık, İstanbul, 1999.

Fromm, E. Çeviren Sayın, A. **İtaatsizlik Üzerine Denemeler**, Yaprak Yayınları, İstanbul,1987.

Geers, K. Strategıc **Cyber Securıty, NATO Cooperative Cyber Defence Centre of Excellence**, June 2011.

Gözkaman, A. ve Paksoy, P. **Arap Baharı Üzerine Değerlendirmeler**, Detay Yayınları, 2001.

Gözen, R.(Eds.) **Amerikan Dış Politikası**, Anadolu Ünüversitesi yayın numarası: 2609 ss.146.

Gözen, R. **Uluslararası İlişkiler Teorileri**, İletişim Yayınları. Ankara, 2014.

Gözen, R. **Uluslararası İlişkiler Sonrası Çoğulculuk, Küreselleşme ve 11 Eylül,** Alfa Yayınları, İstanbul, 2004.

Gray, C. Çeviren Öz, H. **Modern Strateji**, Truva Yayınları,2008.

Gray, C. **Strategy and History**, Routledge Yayınları, 2006.

Greene, R. ve Elffers, J. Çeviren Doruker, F. **33 Stratejide Savaş**, Altın Kitaplar Yayınevi, İstanbul, 2018.

Griffiths, M. Roach, S. C. And Solomon, M. Scott. **Fifty Key Thinkers İn İnternational Relations**, Routledge Journal, 2009.

Hall, L. Çeviren. Koçak, S. **Stratejik Dolaylı Tutum**, Doruk Yayınları, 2015.

Harari, Y. Çeviren. Siral, S.. **21. Yüzyıl için 21 Ders**, Kolektif Kitap Yayınları, İstanbul, 2018.

Hart, G. Çeviren. Karabaşoğlu, İ. **Dördüncü Güç 21. Yüzyılda Amerikan Büyük Stratejisi**, Avangard Kitap, İstanbul, 2016, ss.18-21,30-33,62-63.

Heintze, H. J. and Thielbörger, P. **From Cold War To Cyber War,** The Eciltution Of The İnternational Law Of Peace And Armed Conflict Over The Last 25 Years, Springer, Germany, 2016 ss.24.

Heywood, A. **Siyaset.** Liberte Yayınları, Ankara, 2006.

Heywood, A. Siyaset Teorisine Giriş. Küre Yayınları, İstanbul, 2014.

Heywood, A. **Global Politics,**Palgrave Macmillan Foundation, Newyork, 2011.

Kardaş, Ş. ve Balcı, A. **Uluslararası İlişkilere Giriş Tarih**, **Teori, Kavram ve Konular**, Küre Yayınları,2014.

Kaldor, M. and Rangelov, I. **The Handbook of Global Security Policy**, Wiley Blackwell Journal, 2014.

Katzenstein. P. Çeviren Efe, İ. **Milli Güvenlik Kültürü: Dünya Siyasetinde Normlar ve Kimlik**, Sakarya Üniversitesi Kültür Yayınları, Sakarya, 2014.

Keleştemur, A. **Siber İstihbarat**, Level Kitap Yayınevi, İstanbul,2015.

Kennedy, P. Çeviren; Karanakçı, B. **Büyük Güçlerin Yükseliş ve Çöküşleri**, İş Bankası Yayınları, 13. Basım, 2013.

Kennedy, P. Çeviren Fethi, A. **Savaşta ve Barışta Büyük Stratejiler**, Totem Yayıncılık, İstanbul,2014.

Keohane, R. **After Hegemony: Cooperation and Discord in the World Political Economy,**Princeton: Princeton University Press, 1984.

Keohane, R. **Power And Governance İn A Partially Globalized World**, Routledge, 2002. ss. 272.

Kissinger. H. Çeviren, Gül, S. **Dünya Düzeni**, Boyner Yayınları, İstanbul,2016 ss. 372-379.

Kumar, K. **Sanayi Sonrası Toplumdan Post-Modern Topluma Çağdaş Dünyanın Yeni Kuramları**, Dost Yayınları, Ankara, 2013, ss.19.

Kurtoğlu, R. **Küresel Para Oyunları ve Psiko-Siber Savaş**, İstanbul, Destek Yayınları,2017.

Marr, B. **Veri Stratejisi Büyük Veri ve Nesnelerin İnterneti Nasıl Kar Getirir?** Media Cat, İstanbul, 2018 ss.10.15.59.125-129,239.248-249.

Marr, B. Çeviren Gündüz, B. **Büyük Veri İş Başında 45 Yıldız Şirket Büyük Veriyi Nasıl Kullandı?** Mediacat, İstanbul, 2016, ss.11.

Mitnick, K. D. Çev. Tezcan, N. E. **Aldatma Sanatı**, Odtü Yayıncılık,2006.

Murray, W. Sinnreich, R. Lacey, J. Çeviren Baltacı, E. **Büyük Stratejinin Oluşumu**, Siyaset, Diplomasi ve Savaş, Avangard Yayınları, İstanbul, 2017,ss. 10.

NATO Office of Information and Press, **The North Atlantic Treaty Organization, Facts and Figures,** Brüksel, 1989.

Newton, K. ve Van D. Jan W. Çeviren Saraçoğlu, E. **Karşılaştırmalı Siyasetin Temelleri**. Phoenix Yayınları, Ankara, 2014.

Nye, J. **Power in the Global Information Age From realism to globalization**, Routledge Journal, 2004.

Nye, J. ve Welch, D. Çeviren Akman, R. **Küresel Çatışmayı ve İşbirliğini Anlamak**. Türkiye İş Bankası Yayınları, İstanbul, 2010.

Özkan, A. **21. Yüzyılda Abd'nin Küresel Stratejileri**, Tasam Yayınları, İstanbul,2006.

Özdağ, Ü. **İstihbarat Teorisi**, Kripto Yayınları, Ankara 2018.

Paret, P. Çeviren Doruk Can Koçak, **Modern Strateji Machiavelli'den Nükleer Çağa**, Doruk Yayınları, 2015.

Primakov, Y. **11 Eylül ve Irak Müdahelesi Sonrası Dünya**, Doğan Kitap,2004.

Primakov, Y. Ceviri: Olga Tezcan, **Ruslarin Gözüyle Ortadoğu**, Timaş Yayinlari, İstanbul, 2010.

Primakov, Y. **Rusyasız Dünya**, Timaş Yayınları, İstanbul, 2010.

Reveron, D. S. **Cyberspace and National Security Threats, Ossortunities, and Power İn A Virtual World**, Georgetown University Press, Washington Dc, 2012.

Richard L. Kugler, **Policy Analysis in National Security Affairs: New Methods for a New Era**, (Washington DC: National Defense University Press, 2006), ss.87.

Richard A. Çeviri Domaniç, N. Arhan, N. **Dünya Düzeni Nereye? Amerikan Emperyal Jeopolitikası**, Metis Yayınları, 2004, ss.38.

Rousseau, J. Çeviren. Ilgaz, T. **Toplum Sözleşmesi**, Kırmızı Yayınları, İstanbul, 2006, ss.43.

Sander, O. **Siyasi Tarih İlkçağlardan 1918'e**, İmge Yayınları, Ankara, 2003.

Sayan, S. ve Bilgin, H. **Karşılaştırmalı Siyaset Temel Konular ve Yaklaşımla**r. İstanbul Bilgi Üniversitesi Yayınları, İstanbul,2014, ss.101-113.

Schelling, T. **The Strategy of Conflict** (Cambridge: Harvard University Press, 1980.

Schweller, R. Maxwell's D**emon And The Golden Assle: Global Discord İn The New Millennium,** Johns Hopkins University Press, Baltimore, 2014.

Shimer, D. **America, Russia, and One Hundred Years of Covert Electoral Interference**, Knopf journal, ABD, 2020, ss.6-10.

https://books.google.com.tr/books?id=hbfNDwAAQBAJ&printsec=frontcover&dq=David+Shimer&hl=tr&sa=X&ved=2ahUKEwjUhvmOwZ3tAhX6CRAIHVrFBf0Q6AEwAHoECAUQAg#v=onepage&q=David%20Shimer&f=false ET.25.11.2020

Stalin, J.V. Çeviren Kor, A.F. **Strateji ve Taktik**, Kitap Yayınevi, 1. Baskı,2017.

Singhal, A. **Data Warehousing and Data Mining Techniques for Cyber Security**, Springer, United States of America, 2007.

Singer, P.W ve Friedman, A. Çeviren. Atav, A. **Siber Güvenlik ve Siber Savaş**, Ankamat Matbacılık, Ankara, 2014.

Sur, M. **Uluslararası Hukukun Esasları**, Beta Yayınları, İstanbul,2006.

Shelley E.T. Letitia, A.P. ve David, O.S. Çeviren Dönmez, A. **Sosyal Psikoloji**, İmge Yayınları, Ankara, 2007, ss.505.

Şensoy, Ü. **Dijital Dönüşüm Siber Güvenlik**, Harvard Business Review Press, Optimist Yayınları, İstanbul, 2020. ss.7, ss.13-18, ss.41-43.67.175.177.187.189

Tzu, S. **Savaş Sanatı**. Hasan Alı Yücel Klasikleri Türkiye İş Bankası Yayınları, İstanbul, 2018.

Ünal, A.N. **Siber Güvenlik ve Elektronik Bileşenleri**, Nobel Yayınları, Ankara, 2015.

Valeriano, B. Jensen. B. **Cyber Strategy: The Evolving Character of Power and Coercion**, Oxford University Press, 2018.

Vergin, N. **Siyasetin Sosyolojisi Kavramlar, Tanımlar, Yaklaşımlar**, Bağlam Yayıncılık, 2007.

Wallerstein, İ. Çeviren. Alpay, N. **Tarihsel Kapitalizm**, Metis Yayınları, İstanbul, 2006, ss.40-41.

Waltz, K.N. **Theory of Intemational Politics**, Addison Wesley Journal, 1979, ss.93.

Yalçınkaya, H. **Savaş Farklı Disiplinlerde Yeni Yaklaşımlar**, Siyasal Kitapevi, Ankara, 2010.

Yılmaz, S. **21. Yüzyılda Güvenlik ve İstihbarat**, Alfa Yayınları, İstanbul, 2006. https://www.academia.edu/6107400/21.-yy-da-G%C3%BCvenlik-ve-%C4%B0stihbarat ET.28.01.2020.

Süreli Yayınlar

Ada, M. ve Çakır H. K**uzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi,** Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 5, 2017, ss. 632-656.

Aksu, M. ve Turhan, F. **Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik**, Uluslararası Alanya İşletme Fakültesi Dergisi, C:4, S:2, Yıl:2012, ss. 69-80.

Akyazı, U. **Uluslararası Siber Güvenlik Strateji Ve Doktrinleri Kapsamında Alınabilecek Tedbirler**, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, Ankara 20-21.10.2013, ss.216-220.

Alexander, D. **Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses**, İGÜSBD Cilt: 1 Sayı: 2, October 2014, ss.1-23.

Arreguin-Toft, I. "**How the Weak Win Wars: A Theory of Asymmetric Conflict''**, International Security, Cilt. 26, No.1, 2001, ss.93-128.

Ashley, Richard "**The Poverty Of Neorealism**," International Organization, Cilt. 38, No. 2, Spring 1984, ss. 225-286.

Aslay, F. **Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi,** International Journal of Multidisciplinary Studies and Innovative Technologies Cilt: 1, Sayı:1, Yıl: 2017, ss. 24-28.

Aybay, R. **Uluslararası Antlaşmaların Türk Hukukundaki Yeri**, TBB Dergisi, Sayı:70, Cilt:1, Yıl: 2007, ss.187-213.

Barbara D., Wu N. ve Jajodia S., **Detecting Novel Network İntrusions Using Bayes Estimators.** In Proc. First SIAM Conference on Data Mining, Chicago, IL, April 2001. ss.1-17.

Bakan, S. ve Şahin, S. **Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler**, The Journal of International Lingual, Social and Educational Sciences , Cilt:4, Sayı:2, Yıl: 2018, ss.135-152.

Baldwin, D. The **Concept Of Security**, Review of International Studies, British International Studies Association, Cilt:23, Yıl: 1997, ss.5-26.

Baran, T. ve Macar, E. **Değişen Güvenlik Yaklaşımları Örneğinde Kopenhag Okulu'nun Toplumsal Güvenlik Yaklaşımı**, Uluslararası Sosyal Araştırmalar Dergisi Cilt: 10, Sayı: 54 Yıl: 2017, ss.251-258.

Baysal, B. ve Lüleci, Ç. **Kopenhag Okulu ve Güvenlikleştirme Teorisi**, Güvenlik Stratejileri, Sayı: 22, Yıl: 2011, ss. 61-90.

Baylis, J. "**Uluslararası İlişkilerde Güvenlik Kavramı**", Uluslararası İlişkiler, Cilt:5, Sayı:18,Yaz 2008, ss. 69-85.

Bıçakcı, S. **Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu**, Uluslararası İlişkiler, Cilt:9, Sayı:34, Yaz 2012, ss. 205-226.

Bıçakcı, S. **NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik**, Uluslararası İlişkiler, Cilt 10, Sayı 40, Kış 2014, ss. 101-130.

Birdişli, F. **Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım**: **Galler Ekolü**, Güvenlik Stratejileri, Sayı: 20, Yıl: 2010, ss.229-250.

Bozoklu, O. ve Çil, C. Z. **Yazılım Güvenlik Açığı Ekosistemi ve Türkiye'deki Durum Değerlendirmesi.** Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:1, 2017, ss.6-26.

Brauch, H. "**Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü"**, Uluslararası İlişkiler, Cilt 5, Sayı 18, Yaz 2008, ss. 1-47.

Bull, H. International Theory: **The Case for a Classical Assroach World Politics**, The Johns Hopkins University Press , Cilt.18, Sayı.3, Yıl. 1966, ss. 361-377.

Buzan, B. From **International System to International Society: Structural Realism and Regime TheoryMeet the English School**, The MIT Press, International Organization, Cilt. 47, Sayı.3, Yıl. Yaz 1993, ss. 327-352.

Buzan, B. **"Askeri Güvenliğin Değişen Gündemi**", Uluslararası İlişkiler, Cilt 5, Sayı 18, Yaz 2008, ss.107-123.

Buzan, B. **New Patterns Of Global Security İn The Twenty-Frst Century** International Affairs, Royal Institute of International Affairs, Cilt. 67, Sayı.3, Yıl.1991, ss. 431-451.

Buzan, B. **New Patterns of Global Security in the Twenty-First Century**, International Affairs (Royal Institute of International Affairs 1944-), Cilt. 67, Sayı.3, Yıl.1991, ss.431-451.

Cha, V. "**Globalization and the Study of International Security**", Journal of Peace Research, Cilt. 37, Sayı.3, Yıl.2000, ss. 391-403.

Cullen, P. J. **MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare MCDC** Ocak 2017, ss.7-30.

Choucri, N. Madnick, S. and Ferwerda, J. **Institutions for Cyber Security: International Responses and Global Imperatives,** Information Technology for Development, Cilt.20, Sayı.2, Yıl.2014, ss. 96-121.

Çatal, B. **Diplomaside Değişim ve Dönüşüm: Siber Diplomasi**, Medeniyet Araştırmaları Dergisi, Cilt: 2 Sayı: 3 Yıl: 2015, ss. 43-53.

Çelik, S. ve Çeliktaş, B. **Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar**, Cyberpolitik Journal Cilt. 3, Sayı.5, Yıl.2018, ss.105-128.

Çelik, Ş. "**Stuxnet Saldirisi ve Abd'nin Siber Savaş Stratejisi: Uluslararasi Hukukta Kuvvet Kullanmaktan Kaçinma İlkesi Çerçevesinde Bir Değerlendirme**", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 15, Sayı: 1, Yıl.2013, ss.137-175.

Cumali, A. Ç. **Siber Uzay ve İnsan Hakları,** Cyberpolitik Journal Cilt. 3, Sayı. 5 ss. 133-145.

Daban, C. **Siber Güvenlik ve Uluslararası Güvenlik İlişkisi**, Cyberpolitik Journal Cilt. 1, No. 1 ss. 84-98.

Darıcılı, Ö. R**usya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi**, sayı 83, Güz, 2017, ss. 121-139.

Davenport, T. H. Barth, P. And Bean, R. **How 'Big Data' Is Different, Mitsloan Management Review**, Cilt. 54, No. 1, 2012, ss.22-24 https://pdfs.semanticscholar.org/e726/e02d793c15551be92e6aa2d00ce439a229ff.pdf?_ga=2.153140600.1575586772.1582809115-982778214.1582809115 ET.2702.2020.

Darıcılı, A. **Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi,** Uluslararası Çalışmalar Dergisi, Cilt.1, No.1, Yıl.2017, ss.1-24.

Darıcılı, A. B. ve Özdal, B. E**nformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi**, İGÜ Sos. Bil. Derg., Cilt.4, No.1, Yıl.2017, ss. 19-40.

Dedemen, F. **Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi** Güvenlik Bilimleri Dergisi, Cilt.1, Sayı.5, Yıl.2016, ss.141-176.

Demirdöğen, Ü.D. **Soğuk Savaş Sonrasında NATO ve Yeni Stratejisi**, 1993, ss. 155-160.

Devlen, B. ve Özdamar, Ö. **"Uluslararası İlişkilerde İngiliz Okulu Kuramı: Kökenleri, Kavramları ve Tartışmaları"**, Uluslararası İlişkiler, Cilt 7, Sayı 25, Bahar 2010, ss.43-68.

Dursun, S. **İç Tehditler ve Dış Politika: Gürcistan Dış Politikası Örneği** (1991-2003), AÇÜ Uluslararası Sosyal Bilimler Dergisi, Cilt: 3, Sayı:2, Yıl: 2017, ss. 24-49.

Dinstein, Y. '**Computer Network Attacks and Self-Defense'**, International Law Studies, Cilt.76, Yıl.2002, ss.103.

Erendor, M. E. **"Silahlı Çatışma Hukuku İlkelerinin Değerlendirilmesi: Askeri Gereklilik, Gereksiz Acı ve Istırabın Önlenmesi ve Onur"**, Manas Sosyal Araştırmalar Dergisi, Cilt.8, Sayı.2, Yıl.2019, ss. 1991-2009.

Ertoz L., Eilertson E., Lazarevic A., Tan P., Dokes P., Kumar V., Srivastava J., **Data Mining for Network** Intrusion Detection, Computer Science Department University of Minnesota, The United State Of America, ss.21-30. https://pdfs.semanticscholar.org/8bac/ad4990b3dd0ced614e596eb1a6d98865d693.pdf ET:24.01.2020.

Ergüven, N. S. **Uluslararası Hukuk Açısından Güvenlik Kavramının Teorik Temelleri**, Ankara Üni. Hukuk Fak. Dergisi, Cilt.65, Sayı.3, Yıl.2016, ss. 771-835.

Falk, R. War, **War Crimes, Power and Justice: Toward a Jurisprudence of Cons**cience, The Asia-Pacific Journal, Cilt.10, Sayı.4, Yıl.2012, ss.1-12.

Foltz, A. C. **Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate,** ndupress, JFQ sayı 67, Yıl.2012, ss.40-48.

Gaddis. J. **İnternational Relations Theory And The End Of The Cold War**, İnternational Security, Cilt. 17, No. 3, Winter 1992/93, ss. 5-58.

Gartzke, E. **The Myth of Cyberwar Bringing War in Cyberspace** Back Down to Earth International Security, Cilt. 38, No. 2, Fall 2013, ss. 41–73.

Gerson, M. S. **Conventional Deterrence in the Second Nuclear Age**, Parameters, 2009, ss.32-48.

Glenny, M. and Kavanagh, C. **800 Titles but No Policy,Thoughts on Cyber Warfare**, American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy, Cilt.34, No.6, Yıl.2012, ss.287-294.

Gülboy, B. S. **Pax Britannica'dan Pax Americana'ya**, Academia, https://www.academia.edu/5416592/Pax_Britannica_dan_Pax_Americana_ya ET.14/12/2019.

Güreşçi, R. **Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi,** Savunma Bilimleri Dergisi, Cilt.18, Sayı.1, Yıl.2019, ss.87.

Greathouse, C. B. **Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?**, Cyberspace and International Relations, Springer-Verlag Berlin Heidelberg, 2014, ss.21-38.

Gözkaman, A. **Avrupa Savunma Topluluğu'nun Reddi Üzerine Bir Analiz**, Beykent Üniversitesi Sosyal Bilimler Dergisi, Cilt.7, Sayı.2, Yıl.2014, ss.6-19.

Gök, A. **11 Eylül Sonrası Savaşın Değişen Doğası**, Sosyal Bilimler Dergisi, Cilt.4, Sayı.11, Yıl. Haziran 2017, ss. 726-743.

Guay T. and Callum R. **The Transformation and Future Prospects Of Europe's Defennce İndustry**, İnternational Affairs, Cilt.78, No.4, Yıl.2002, ss.757-776.

Gündoğdu, E. **Uluslararası İlişkilerde Caydırma Teorisi**, Marmara Üniversitesi Siyasal Bilimler Dergisi, Cilt.4, Sayı.2, Yıl. Eylül 2016, ss.1-22.

Güler, A. **İnsani Müdahale Aracı Olarak Siber Uzay**, Medeniyet Araştırmaları Dergisi, Cilt. 2 Sayı. 4 Yıl. 2015, ss.139-147.

Güntay, V. **Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu**:**Siber Savaş Örneği**, Güvenlik Bilimleri Dergisi, Cilt.6, Sayı.2, Yıl. Kasım 2017, ss. 81-108.

Harold, S. W. Libicki, M. C. and Cevallos, A. S. **The "Cyber Problem" in U.S.-China Relations**, RAND Corporation, 2016, ss.1-17.

Hekim, H. ve Başıbüyük, O. **Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları**, Uluslararası Güvenlik ve Terörizm Dergisi, Cilt.4, No.2, Yıl.2013, ss. 135-155.

Holsti, K. J. **The Concept of Power in the Study of International Relations**, Published by: Wiley on behalf of The International Studies Association, Cilt. 7, No. 4, Yıl. Şubat 1964, ss. 179-194.

Howard, M. **Threat or Ossortunity?** Managing Risk Through R&D, Epri Journal, Kasım/Aralık 2015, ss.1-2.

Hughes, R. **NATO In Cyberspace: Digital Defences, Royal Institute Of International Affairs**, The World Today, Cilt. 65, No. 4, Nisan 2009, ss. 19-21.

İsmayıl, T. ve Tatlı, **U. Uluslararası İlişkilere Rusya'nın Gözüyle Bakmak,** Trakya Üniversitesi Sosyal Bilimler Dergisi Cilt 20 Sayı 1, Haziran 2018. ss.113-127.

Karabulut, A. N. **Eski Savaş, Yeni Strateji: Rusya'nın Yirmibirinci Yüzyıldaki Hibrit Savaş Doktrini ve Ukrayna Krizi'ndeki Uygulaması** Uluslararası İlişkiler, Cilt 13, Sayı 49, Yıl.2016, ss. 25-42.

Katzenstein, P. **Protean Power And Uncertainty: Exploring The Unexpected İn World Politics**, International Studies Quarterly, Cilt.62, Sayı.1, Yıl.2018, ss.80-93.

Katzenstein, P. **Small States and Small States Revisited**, Carfax Publishing, New Political Economy, Cilt. 8, No. 1, 2003, ss. 9-27.

Katzenstein, P. **The Culture of National Security: Norms, Identity, and Culture in World Politics** , Columbia University Press, New York, 1996. ss.1-27.

Katzenstein, P. and Sil, R. **Analytic Eclecticism in the Study of World Politics: Reconfiguring Problems and Mechanisms across** Research Traditions Perspectives on Politics, Cambridge University Press, Cilt.8, Sayı.2, Yıl.2010 ss.411-431.

Katzenstein, P.J. **Introduction: Alternative Perspectives On National Security,** The Culture Of National Security, Columbia University Press, New York, 1996,ss 1-27.

Katzenstein, P. **Regionalism İn Comparative Perspective. Cooperation And Conflict,** Cilt.31,Sayı.2, Yıl.Haziran 1996, ss.123-59. Reprinted İn Philisse De Lombaerde And Frederki Söderbaum, Eds., Regionalism. Los Angeles: Sage Publications, 2013. https://pkatzenstein.org/publications/show_list/start/0

Katzenstein, P. **Conclusion: National Security in a Changing World**, in, ed., The Culture of National Security, Columbia University Press, New York, 1996.

Kaldor, M. **In defence of new wars**, International Journal of Security and Development, 2013, ss.1-16.

Keohane, R. and Martin, L. **The Promise of Institutionalist Theory**, International Security, Cilt. 20, No. 1. Yıl.Yaz 1995. ss. 39-51.

Korhan, S. **Uluslararası İlişkilerde Siber Caydırıcılık**, Cyberpolitik Journal Cilt. 1, No. 1, Yıl.2016, ss.153-167.

Körpe, Ö. **Stratejik Kültür ve Güncel Kuramsal Tartışmalar**, Security Strategies Sayı: 24, Yıl. 2012, ss. 147-175.

Kurnaz, İ. **Siber Güvenlik ve İlintili Kavramsal Çerçeve**, Cyberpolitik Journal Cilt. 1, No. 1 ss. 62-83.

Kozlowski, A. **Comparatıve Analysıs Of Cyberattacks On Estonıa, Georgıa And Kyrgyzstan**, European Scientific Journal cilt.3, ISSN: 1857 – 7881, February 2014, ss. 237-240.

Krahmann, E. '**From State To Non-State Actors: The Emergence Of Security Governance'**, New Threats And New Actors İn International Security, Palgrave Macmillan, New York, 2005, ss.3-19.

Kshetri, N. **Pattern Of Global Cyber War And Crime: A Conceptual Framework**, Journal of International Management, cilt.11, Yıl.2005, ss.541–562.

Korchenko, O. Vasiliu, Y. and Gnatyuk, S.**Modern Quantum Technologies Of İnformation Security Against Cyber-Terrorist Attacks**, Aviation, Cilt.14, No.2, Yıl. 2010, ss.58-69.

Korns, S.W. and Kastenberg, J.E. **Georgia's Cyber Left Hook**, Army War College Carlısle Barracks Pa Strategıc Studıes Instıtute, 2009, ss.60-73.

Luukas K. Tımothy J. Frank J. and Alec A. **European Union and NATO Global Cybersecurity Challenges: A Way Forward, Institute for National Strategic Security**, National Defense University, Cilt. 6, No. 2, Yıl. 2016, ss. 126-141.

Mearsheimer, J. "**The False Promise Of International Institutions,"** International Security, Cilt. 19, No. 3, Yıl. Kış 1994-1995, ss. 7-11.

McMullan, J.L. and Perrier, **D.C. Controlling Cyber-Crime and Gambling: Problems and Paradoxes in the Mediation of Law and Criminal Organization**, Police Practice and Research: An International Journal, Cilt.8, No.5, Yıl.2007, ss.431-444.

Nil, Ş. ve Özpek, B. B. **"ABD ve Türkiye'de Geçmişten Günümüze Güvenlik Çalışmaları",** Ortadoğu Etütleri, Cilt 2, Sayı 2, Yıl. Ocak 2010, ss. 75-114.

Ning P., Xu D., **Learning Attack Strategies from Intrusion** Alerts, Proc. ACM Computer and Communications Security Conf, 2003, ss.1-17. http://discovery.csc.ncsu.edu/pubs/ccs03-ids-full.pdf ET:24.01.2020

Nye, J. and Keohane, R. **Transnational Relations and World Politics**, International Organization, Cilt. 25, No. 3, Yıl. Yaz-1971, ss.329-349.

Nye J. **Nuclear Lessons for Cyber Security?** Strategic Studies Quarterly, Kış-2011, ss.19-35.

Nye, Jr. J. S. **Cyber Power**, Harvard Kennedy School Belfer Center for Science and International Affairs, Mayıs-2010 ss.1-30.

Oğuzlu, T. **Güvenlik Kültürü ve Türk Dış Politikası**. Bilig Yayınları, sayı 72, Kış 2015, ss.223-250.

Öğün, M. N. ve Kaya. A. **Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler** Güvenlik Stratejileri Yıl: 9 Sayı: 18, ss. 145-170.

Örmeci, O. **21. Yüzyılda ABD-Çin Rekabeti**, SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi, Sayı:29, Ağustos 2013, ss.1-14.

Özer, Y. **Savaşın Değişen Karakteri: Teori ve Uygulamada Hibrit Savaş**. Güvenlik Bilimleri Dergisi, Cilt.1 Sayı.7, Yıl.2018, ss.29-56.

Öztürk, M. **Uluslararası Liderlik Meselesi ve Rusya'nın Büyük Güç Unsurları: Bir Değerlendirme**, Avrasya Etüdler, Cilt.49, Sayı.1, Yıl.2016, ss. 55-75.

Perkovich, G. and Levite, A. E. **Cyber War and Information From Understanding Cyber Conflict: Fourteen Analogies Editors**, Blank, S. Published by Georgetown University Press, Kasım 2017, ss. 81-89.

Powell, R. **"Anarchy in International Relations Theory: The Neorealist-Neoliberal Debate**," International Organization Cilt.48, No.2, Yıl. Bahar 1994, ss.313-44.

Rid, T. and McBurney, P. **Cyber-Weapons**, The RUSI Journal, Cilt. 157, No.1, Yıl. 2012, ss. 6-13.

Rid, T. **Cyber War Will Not Take Place**, Journal of Strategic Studies, Cilt.35, No.1, Yıl.2012, ss. 5-32.

Sancak, K. **21.Yüzyılda Güvenlik Sorunları: Bir Tehdit Unsuru Olarak Nükleer Silahlar**, The Journal of Academic Social Science Studies, Cilt.6, Sayı 8, Yıl. Ekim 2013, ss.499-510.

Scheinman, L. **The Non-Proliferation Treaty: Ont He Road To 1995**,Special Reports, IAEA Bulletin,Sayı.1, Yıl.1992, ss.33-40.

Scott J. Shackelford, F**rom Nuclear War to Net War: Analogizing Cyber Attacks in International Law**, Berkeley Journal of International Law, Cilt.27, No.1, Yıl. 2009. ss.195.

Sertçelik, A. **Siber Olaylar Ekseninde Siber Güvenliği Anlamak**, Medeniyet Araştırmaları Dergisi, Cilt: 2 Sayı: 3 Yıl: 2015. Ss.25-42.

Shafqat, N. and Masood, **A. Comparative Analysis of Various National Cyber Security Strategies**, International Journal of Computer Science and Information Security, Cilt. 14, No. 1, Ocak 2016, ss.129-135.

Singer, J. D. "**Uluslararası İlişkilerde Analiz Düzeyi Meselesi",** Uluslararası İlişkiler, Cilt 3, Sayı 11, Güz 2006, ss. 3-24.

Sinovets, P. **From Stalin to Putin: Russian Strategic Culture in the XXI Century**, Its Continuity, and Change, Philosophy Study, July 2016, Cilt. 6, No. 7, ss.417-423.

Shackelford, S.J. **From Nuclear War to Net War: Analogizing Cyber Attacks in International Law**, Berkeley Journal Of Internatıonal Law, Cilt.27, No.1, Yıl.2009, ss.191-250.

Streeten, P. **Globalisation: Threat Or Ossortunity**?, The Pakistan Development Review Cilt.37, No. 4, Yıl. Kış 1998, ss.51-83.

Smeets, M. and Healey, J. **Cyber Conflict History**, Columbia Cyber Conflict Studies Association, Cyber Conflict State of the Field Series: Economic Dimensions of Cyber Conflict, 2017, ss.1-10.

Sun, X. **The Dilemmas of the Rise of China**, Elcano Royal Institute Asia Pasific. Madrid, 07.02.2012, ss.1-13

Sümer, Gültekin, "**Amerikan Dış Politikasının Kökenleri ve Amerikan Dış Politik Kültürü",** Uluslararası İlişkiler, Cilt 5, Sayı 19, Güz 2008, ss. 119-144.

Şeker, E. **Siber Savunma Tatbikatları**: Planlama, Uygulama ve Değerlendirme, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, Yıl.2017, ss.33-41.

Şenol, M. **Siber Güçle Caydırıcılık Ama Nasıl**? Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:2, Yıl. 2016, ss.10-17.

Şentürk, H. Çil C. Z. ve Sağıroğlu Ş. **Siber Güvenlik Yatırım Kararları Üzerine Literatür İncelemesi,** Politeknik Dergisi, Cilt.19, No.1, Yıl.2016, ss. 39-51.

Tanrıverdi, E. G. **Giddens ve Küresel Demokrasi**, Uluslararası İnsan Bilimleri Dergisi, Cilt:6 Sayı:1 Yıl:2009, ss.858-870.

Tunç, H. **Milletlerarası Sözleşmelerin Türk İç Hukukuna Etkisi ve Avrupa İnsan Hakları Mahkemesinin Türkiye İle İlgili Örnek Karar İncelemesi**, Anayasa Yargı Sempozyumu, 2000, ss.174-193.

Türkay, Ş**. Siber Savaş Hukuku ve Uygulanma Sorunsalı**, İühfm C. Lxxı, S. 1, 2013, ss.1177-1228.

Toft, I. A. **How theWeak WinWars A Theory of Asymmetric Conflict,** International Security, Cilt. 26, No 1, Yıl. Yaz 2001, ss.93–128.

Ünal, A.N. Yarman, B.S.B. **Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü**, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ISC Turkey, İstanbul, 17-18.10.2014.

Ünver, G. N. **Siber Çatışmaların Tanımlama Sorunu**, Cyberpolitik Journal Cilt. 3, No. 5, 2017, ss. 23-39.

Walt, S. **Alliance Formation and The Balance Of World Power**, The Mıt Press, International Security, Cilt. 9, No. 4, Spring, 1985, ss. 3-43.

Waltz, K. **Uluslararası Politikanın Değişen Yapısı**, Uluslararası İlişkiler, Cilt 5, Sayı 17, Bahar 2008, ss. 3-44.

Waewer, O. "**Toplumsal Güvenliğin Değişen Gündemi**", Uluslararası İlişkiler, Cilt 5, Sayı 18, Yaz 2008, ss. 151-178.

Wirtz, J. J. **Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy,** NATO Publications, Tallinn, 2015, ss.29-37.

Wohlforth, W. **Gilpinian Realism and International Relations**, Sage Journal, International Relations, Cilt.25, No.4, Yıl.2011, ss.499-511.

Wohlforth. W. **Realism and the End of the Cold War**, The MIT Press, International Security, Cilt. 19, No. 3, Kış 1994-1995, ss. 91-129.

Yayla. M. **Hukuki Bir Terim Olarak Siber Savaş**, TBB Dergisi 104, 2013 ss. 184-185.

Yayla, M. **Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı**, Hacettepe HFD, Cilt.4, No.2, Yıl.2014, ss.181–200.

Yılmaz, S. **Yumuşak Güç ve Evrimi,** Turan Stratejik Araştırmalar Merkezi Dergisi, Cilt: 3, Sayı: 12, Sonbahar 2011, ss.31-36.

Yiğittepe, L. **NATO ve Rusya Arasında Türkiye'nin Güvenlik Algılaması: S-400 Krizi Örneği,** Cilt.16, Özel Sayı, Eylül 2018, ss. 276-289.

Yükselen, H. **Strateji Kavramını Çalışmak**, Milli Savunma Üniversitesi Güvenlik Stratejileri Dergisi, Sayı: 27, Yıl: 2014.

Zhigang, Y. **Cyber Variants of Traditional Crimes and Criminal Law Responses**, Social Sciences in China, Cilt.32, No.1, 2011, ss.66-79.

İnternet/Kurum

Bilgi Teknolojileri ve İletişim Kurumu, **Uluslararası Telekomünikasyon Birliği**-ITU, 16.04.2018, https://www.btk.gov.tr/itu, ET.30.01.2020.

Bilgi Teknolojileri ve İletişim Kurumu, **Siber Güvenlik Tatbikatları**,2017, https://www.btk.gov.tr/siber-guvenlik-tatbikatlari, ET.28.01.2020.

Bilgi Güvenliği Derneği, **Ulusal Siber Güvenlik Stratejisi**, 2012, http://www.bilgiguvenligi.org.tr/wpcontent/uploads/2016/03/Ulusal_Siber_Guvenlik_Stratejisi.pdf, ET.28.01.2020.

Bilgi Güvenliği Derneği, **Kritik Enerji Altyapılarının Korunması ve Siber Güvenlik Sempozyumu Sonuç Bildirgesi**, 2015, https://www.bilgiguvenligi.org.tr/wp-content/uploads/2016/03/KEBAK_Sonuc_bildirgesi_08.12.2015_Son.pdf, ET.28.01.2020.

Bilgi Teknolojileri ve İletişim Kurumu, Uluslararası Telekomünikasyon Birliği-ITU, 16.04.2018, https://www.btk.gov.tr/itu, ET.30.01.2020.

Charter of the United Nations, Chapter VII — Action with respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression and Chapter VIII-**Regional arrangements Article 39,40,41,42 and 52**, https://legal.un.org/repertory/art52.shtml , ET:20.01.2020.

Council of Europe, **Convention on Cybercrime, European Treaty Series - No. 18, Budapest**, 23/11/2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, ET:20.01.2020.

Cronin, C. **The Growing Threat of Cyberterrorism Facing the U.S. American Security Project**, Jun 25, 2019 https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/, ET:10.01.2020.

Çukurova Ünüversitesi, **Internet Nedir?-Türkiye'de Internet,** http://ekinoks.cu.edu.tr/Css/bolum2.html , ET.17.09.2020.

Dor, D. **These will be the main cybersecurity trends in 2020**, Weforum Organizasion, 07 Jan 2020, https://www.weforum.org/agenda/2020/01/these-will-be-the-main-cybersecurity-trends-in-2020/ , ET.28.02.2020.

Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, **Birleşmiş Milletler Sözleşmeleri,** http://www.diabgm.adalet.gov.tr/arsiv/sozlesmeler/coktaraflisoz/bm_yeni.html ET.29.01.2020.

DHS, **Cybersecurity**, U.S. Department of Homeland Security, October 23, 2019, https://www.dhs.gov/topic/cybersecurity , ET.28.02.2020.

Enisa, **Cybersecurity is a key enabler for Industry 4.0 Adoption**, Enisa News, November 19, 2018,https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption , ET.28.02.2020.

Franke, T. **Sosyal medya: siber savunmanın ön cephesi mi?,** NATO Yayınları, 22 Mart 2011, https://www.nato.int/docu/review/tr/articles/2011/03/22/sosyal-medya-siber-savunmanin-oen-cephesi-mi/index.html ET.12.02.2020.

Havelsan, **Siber Güvenlikte Yerli Ürünleri HAVELSAN Geliştirecek**, 13.01.2017, http://www.havelsan.com.tr/tr/news/siber-guvenlikte-yerli-urunleri-havelsan-gelistirecek ET.30.01.2020.

Haberleşme Genel Müdürlüğü, **Sektörel SOME Kurulum ve Yönetim Rehberi,** https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/sektorel-some-reh.pdf, ET.28.01.2020.

Milli Güvenlik Kurulu Genel Sekreterliği, **Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı** (Uluslararası Siber Güvenlik Hukuku), https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku ET.29.01.2020.

OrtaDoğu Teknik Ünüversitesi Bilgi İşlem Daire Başkanlığı, **İnternet Tarihi**, http://www.internetarsivi.metu.edu.tr/tarihce.php , ET.17.09.2020.

UN General Assembly, **Agreement Between The Governments Of The Member States Of The Shanghai Cooperation Organization On Cooperation, İn The Field Of İnternational İnformation Security**, 61st PlenaryMeeting,02.12.2008,ss.202-213, https://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf, ET.06.02.2021

United Nations Charter, **Purposes and Principles of the United Nations Article 2(4),**https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter , ET. 17.01.2020.

United Nations **Convention on the Law of the Sea**, **Breaking or injury of a submarine cable or pipeline, Article 113, ss.**64 https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf, ET:20.01.2020.

Ulaştırma ve Altyapı Bakanlığı, **Türkiye 2016-2019 Ulusal Siber Güvenlik Stratejisi,**https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, ET.28.01.2020.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı,** https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf , ET.28.01.2020.

International Telecommunication Union, A**bout International TelecommunicationUnion(ITU),** https://www.itu.int/en/about/Pages/default.aspx , ET.30.01.2020.

Information Office of the State Council of the **People's Republic of China, The InternetinChina,**08.06.2010,http://www.china.org.cn/government/whitepaper/node_7093508.htm, ET:24.01.2020.

İnternational Telecominication Union, **Making an IMPACT on global cybersecurity**, İTU News, October 2009, https://www.itu.int/net/itunews/sayıs/2009/08/22.aspx ET.05.02.2020.

Ministry of Foreign Affairs of Georgia, "**Cyber Attacks Disable Georgian Websites,"** 11.08.2008, http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html. ET:08.01.2020.

NATO, Active Engagement, **Modern Defence, Summit Meeting of NATO Heads of State and Government** Lisbon, Portugal, 19.12.2010, www.nato.int/cps/en/natolive/official_texts_68580.htm. ET: 20.01.2020.

NATO, **Defending against Cyber Attacks**, 6.10.2019, https://www.nato.int/cps/en/natohq/topics_78170.htm? ET: 20.01.2020.

NATO, **4 April 1949 The North Atlantic Treaty**, Washington D.C., 10.04.2019,https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=en, ET.24.11.2020.

NATO **Defence Ministers Adopt New Cyber Defense Policy**, NATO, 08.06.2011, www.nato.int/cps/en/natolive/news_75195.htm. ET: 20.01.2020.

Ramadass, S. A **Study on the IPv6 Address Allocation and Distribution Methods**,International Telecommunication Union, Geneva, 2009, https://www.itu.int/dms_pub/itu-t/oth/3B/02/T3B020000020001PDFE.pdf ET:24.01.2020.

Stanford University, **A Proposal for an International Convention on Cyber Crime and Terrorism**, IWS The İnformation Warfe Site August 2000, http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm , ET. 20.01.2020.

Tübitak Ulusal Akademik Ağ ve Bilgi Merkezi, **Ulaknet Tarihçesi**, https://ulakbim.tubitak.gov.tr/tr/kurumsal/ulaknet-tarihcesi ET:17.09.2020.

Türkiye'nin Endüstri 4.0 Platformu, **Endüstri Tarihine Kısa Bir Yolculuk**, https://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/ ET:24.11.2020.

The JRC in Seville, **The European Commission's science and knowledge service**,07.07.2016,https://ec.europa.eu/jrc/en/about/jrc-site/sevilleET.03.02.2020

İnternet Kaynakları

Computer History Museum, **A History of the Internet 1962-1992,** https://www.computerhistory.org/internethistory/ , ET.17.01.2020.

BBC. **Google ' May Pull Out of China after Gmail Cyber Attack,** BBC News, 13 Ocak 2010, http://news.bbc.co.uk/2/hi/business/8455712.stm ,ET. 24.01.2020.

BBC. **Estonya'ya Siber Saldırı**, BBC Türkçe, 17.05.2007, http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml ET.31.01.2020.

Bond, S. **Iran Conflict Could Shift To Cyberspace**, Experts Warn, NPR Organization,21.01.2020,https://www.npr.org/2020/01/21/797449708/iran-conflict-could-shift-to-cyberspace-experts-warn ET.28.02.2020.

Brinded, L. **Ranked: These will be the 32 most powerful economies in 2030**, Business İnsider UK, Reuters, 2017 https://www.businessinsider.com/ranked-pwc-predicts-the-most-powerful-economies-in-2030-2017-2?r=UK#11-france-3377-trillion-22 ET:09.04.2020.

Browne, R. **US and UK Accuse Russia Of Major Cyber Attack On Georgia**, CNN, 20.02.2020, https://edition.cnn.com/2020/02/20/politics/russia-georgia-hacking/index.html ET.28.02.2020.

Brunt, R. **Cyber Security at Civil Nuclear Facilities: Understanding the Risks**,Chathamhouse,05.10.2015, https://www.chathamhouse.org/2015/10/cyber-security-civil-nuclear-facilities-understanding-risks ET.30.01.2020.

Brent, L. **NATO'nun Siber Uzaydaki Rolü**, NATO Dergisi,2019, https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/TR/index.htm ET.29.01.2020.

Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, articles 1 to 3, 18 October 1907, 36 Stat. 2310, Treaty Series 540, Manchester, U.K: Manchester Univ. Press, 2000, 1.ss.654-666 https://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0654.pdf ET.06.02.2021.

Committee to Protect Journalists, **Burma's Exile Media Hit by Cyber-attacks,** 27.09.2010, http://cpj.org/2010/09/burmas-exile-media-hit-by-cyber-attacks.php ET. 23.01.2020.

Tech Accord News, **Cybersecurity Tech Accord returns to the World Economic** Forum, 24.01.2020, https://cybertechaccord.org/cybersecurity-tech-accord-returns-to-the-world-economic-forum/ ET.28.02.2020.

Cronin, K. **American Security Project**, 25.06.2019, https://www.americansecurityproject.org/the-growing-threat-of-cyberterrorism-facing-the-us/ ET:10.01.2020.

Çavuş, M. **Siber Saldırılara Karşı 7 Etkin Savunma**, BT Günlüğü, 27.06.2018, https://www.btgunlugu.com/siber-saldirilar-a-karsi-7-etkin-savunma/ ET.30.01.2020.

Dorothy E. **Denning."Cyber Terrorism**" Testimony before the Special Oversight Panel on TerrorismCommittee on Armed Services U.S. House of Representatives,GeorgetownUniversity,23.05.2000,https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm, ET. 09.09.2020.

Denning, D. E**. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy**, Networks and Netwars: The Future of Terror,CrimeandMilitancy,ss.239-288. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf , ET.09.09.2020.

Dikmeci, O. **Cumhurbaşkanlığı İkinci 100 Günlük Eylem Planında Savunma Sanayii**,18.12.2018,http://sahipkiran.org/2018/12/18/savunma-sanayii/ ET.30.01.2020.

Erdogan, İ. **Uluslararası Bilgisayar Şebekesi İnternet ve İletişimin Kontrolu**, BilimveUtopyaDergisi,13.07.1995,http://www.irfanerdogan.com/makaleler1/internet.htm, ET.31.01.2020.

Forrest, C.**Understanding The Military Buildup Of Offensive Cyberweapons**,ZDNet,01.09.2016,https://www.zdnet.com/article/understanding-the-military-buildup-of-offensive-cyberweapons/ ET.28.02.2020.

Fulghum, D.A. Wall, R. and Butler, A. **Israel Shows Electronic Prowess,** Warsclerotic,2010. https://warsclerotic.com/2010/09/28/israel-shows-electronic-prowess/ ET. 09.01.2020.

Galeotti, M. **I'm Sorry for Creating the 'Gerasimov Doctrine'**, Foreign Policy, 05.03.2018,https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ ET.30.01.2020.

Gross, M.J. **A Declaration of Cyber-War**, Vanity Fair, Mart 2011, https://www.vanityfair.com/news/2011/03/stuxnet-201104 ET.03.02.2020.

Guest Blogger for Net Politics, **Cyber Deterrence Is Dead. Long Live Cyber Deterrence**!, Council on Foreign Relations, 18.02.2020, https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence ET.28.02.2020.

Gjelten, T. **Seeing the Internet as an Information Weapon**, National Public Radio,23.09.2010,https://www.npr.org/templates/story/story.php?storyId=130052701 ET:23.01.2020.

Halthen, E. **The Role of Hardware Security to Meet Industry 4.0 Aspirations**, Analog Devices, ss.1-3. https://www.analog.com/media/en/technical-documentation/tech-articles/The-Role-of-Hardware-Security-to-Meet-Industry-4.0-Aspirations.pdf , ET.28.02.2020

Heacock, R. **China shuts down Internet in Xinjiang region after riots**, OpenNet Initiative Blog, 06.07.2009, http://opennet.net/blog/2009/07/china-shuts-down-internet-xinjiang-region-after-riots ET.23.01.2020.

Hersh, S.M. **The Online Threat: Should We Be Worried about Cyber War?,** NewYorker,Ekim 2010, https://www.newyorker.com/magazine/2010/11/01/the-online-threat ET.31.01.2020.

Internet World Stats, **İnternet Users in the Top 20 Countries**, 30.06.2019, http://www.internetworldstats.com/top20.htm ET:17.01.2020.

Krasavin, S.**What is Cyber-terrorism?,** Computer Crime Research Center, 2001-2002,http://www.crime-research.org/library/Cyber-terrorism.htm, ET.09.09.2020.

Korzak, E. **Is This China and Russia's Nonaggression Pact for Cyberspace?,** 21.08.2015,https://nationalinterest.org/blog/the-buzz/china-russias-nonaggression-pact%E2%80%9D-cyberspace-13654 ET.06.02.2021.

Koltuksuz, A. **Siberuzayda Savunma ve Güvenlik,** Yaşar Üniversitesi, https://ce.yasar.edu.tr/wp-content/uploads/2013/04/koltuksuz_3_siberuzayda_savunma_ve_guvenlik.pdf ET. 30.01.2020.

MacKinnon, R. **Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom,** a paper presented at Liberation Technology in Authoritarian Regimes Conference, sponsored by the Hoover Institution and the Center on Democracy, Development, and the Rule of Law (CDDRL),StanfordUniversity,11–12Ekim2010, http://rconversation.blogs.com/MacKinnon_Libtech.pdf ET:24.01.2020

New York Times/Guardian, **Pentagon'dan tarihi adım,** Hürriyet, 01.06.2011, http://www.hurriyet.com.tr/gundem/pentagondan-tarihi-adim-17925614 ET.31.01.2020.

Nye, J.J.S**. Is Cyber the Perfect Weapon?**, Project Syndicate, 05.07.2018, https://www.project-syndicate.org/commentary/deterring-cyber-attacks-and-

information-warfare-by-joseph-s--nye-2018-07?barrier=accesspaylog ET.13.12.2019.

Personel Writer, **SA ranks as 31st worst country at cyber security**, İTWeb, Johannesburg,04.03.2020, https://www.itweb.co.za/content/5yONPvEg2YkMXWrb ET.09.04.2020.

PTI, **COVİD-19: CERT-In flags spurt in cyberattacks on personal computers since 'work from home' protocol began**, Yeni Delhi, 27.03.2020, https://www.deccanherald.com/national/Covid-19-cert-in-flags-spurt-in-cyberattacks-on-personal-computers-since-work-from-home-protocol-began-818277.html ET.09.04.2020.

Pokorny, Z. **What Is Threat Intelligence? Definition And Examples**, 30.04.2019, https://www.recordedfuture.com/threat-intelligence-definition/ ET. 30/01/2020.

Poulsen, K. **Slammer Worm Crashed Ohio Nuke Plant Nework**, Security Focus, 19.08.2003, https://www.securityfocus.com/news/6767 ET:17.01.2020.

Poulsen, K. **Cyberwar and Estonia's Panic Attack**, WIRED, 22.08.2007, https://www.wired.com/2007/08/cyber-war-and-e/ ET:06.02.2021.

Reuters, **Why we urgently need a Digital Geneva Convention**, Weforum, 29.11.2017, https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention , ET.30.01.2020.

Reuters. **Threats To The Cybersecurity Of Nuclear Weapons**, World Econic Forum,11.02.2018, https://www.weforum.org/agenda/2018/02/nuclear-weapons-and-cybersecurity-threats-vulnerabilities-and-consequences ET.30.01.2020.

Rhoads, C. **Politics and Economics: Cyber Attack Vexes Estonia,** Poses Debate,TheWallStreetJournal,18.05.2007,https://www.wsj.com/articles/SB117944513189906904 ET:17.01.2020

Reuters. **Dijital Dünyada Kaos Yaşanıyor: 3. Dalga Başladı**, Sputniknews, 22.10.2016, https://sptnkne.ws/c4W4 , ET.30.01.2020.

Robinson, N. **Başarılı Bir Siber Savunma İçin Harcama Yapmak**, NATO Dergisi,2017https://www.nato.int/docu/review/tr/articles/2017/04/06/basarili-bir-siber-savunma-icin-harcama-yapmak/index.html, ET: 29.01.2020.

Sarah C. **CISA Sayıs Chinese Hacking Groups Warning**, İnfo Security Magazine,https://www.infosecurity-magazine.com/news/cisa-sayıs-chinese-hacking-groups/ ET: 17.09.2020.

Savtürk Güvenlik Sistemleri, **Milli siber güvenlik kalkanı 'Ahtapot' yaygınlaştırılacak**, 27.11.2018, https://savturk.com/tr/siber-guvenlik-kalkani-ahtapot-yayginlastirilacak ET.30.01.2020.

Siber Bülten, **Küresel Siber Güvenlik Endeksi açıklandı, Türkiye ilk 10'a giremedi,**19.07.2017, https://siberbulten.com/sirket-haberleri/kuresel-siber-guvenlik-endeksi-aciklandi-turkiye-ilk-10a-giremedi/ ET:30.01.2020.

SSM, **Yerli Siber Güvenlik Teknolojileri için Kümelenme Faaliyetleri Tamamlandı,**DefenceTurkey,28.06.2018,http://www.defenceturkey.com/en/content/yerli-siber-guvenlik-teknolojileri-icin-kumelenme-faaliyetleri-tamamlandi-3084#.XDxbPk0UnIU , ET:29.01.2020.

Talbot, D. **China: Our Internet Is Free Enough**, MIT Technology Review, 16.06.2010,http://www.technologyreview.com/web/25592/page1/ET:24.01.2020.

Taylar, H. **What Are Cyber Threats and What to Do About Them,** preyproject, 22.01.2020, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/ ET.31.01.2020.

Tehrani, H. **Iran: Cyber Islamic Militarism on the March**, Global Voices,19.02.2010,http://globalvoicesonline.org/2010/02/19/iran-cyber-islamic-militarism-on-the-march ET:23.01.2020.

Vijayan, J. **Report Sounds Alarm on China's Rerouting of US Internet Traffic,**Computerworld,18.11.2010,https://www.computerworld.com/article/2514493/update--report-sounds-alarm-on-china-s-rerouting-of-u-s--internet-traffic.html ET:20.01.2020.

Yuxi W. **China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty**, The Henry M. Jackson School Of İnternational Studies, University OfWashington,21.06.2016, Https://Jsis.Washington.Edu/News/China-Russia-Cybersecurity-Cooperation-Working-Towards-Cyber-Sovereignty/ ET:24.02.2020.

Yazıcı, M. **İlk Modern Siber-Atak: Estonya**,2TUIC Akademi, 04.09.2015, http://www.tuicakademi.org/ilk-modern-siber-atak-estonya/ ET:30.01.2020.

Zehir, E.Ö. **Milli Yazılımda İlk Mesaj İletildi: 'Merhaba Tarihi An'**, Webtekno,https://www.webtekno.com/milli-yazilimda-ilk-mesaj-iletildi-merhaba-tarihi-an-h60835.html ET:30.01.2020.

Gazete

AA, **Milli Siber Güvenlik Ürünleri DMO Kataloğuna Girecek**, TRT Haber, 07.11.2018,https://www.trthaber.com/haber/ekonomi/milli-siber-guvenlik-urunleri-dmo-kataloguna-girecek-392883.html ET:30.01.2020.

AA. **Siber Güvenlik Yazılımlarına Ayrılan Bütçe Artıyor**, Yeni şafak, 09.03.2017,https://www.yenisafak.com/ekonomi/siber-guvenlik-yazilimlarina-ayrilan-butce-artiyor-2625667 ET:30.01.2020.

AA. **2017'de Siber Güvenlik İçin 86 Milyar Dolar Harcandı**, Sigortacı Gazetesi, 29.08.2018, http://www.sigortacigazetesi.com.tr/2017de-siber-guvenlik-icin-86-milyar-dolar-harcandi/ ET:30.01.2020.

AA, **İllerde Seçim Koordinasyon Merkezleri Kurulacak**, Anadolu Ajansı, 11.01.2019,https://www.aa.com.tr/tr/turkiye/illerde-secim-koordinasyon-merkezleri-kurulacak/136188630.01.2020 ET:30.01.2020.

AA. **Nato'dan Rusya'ya Tatbikat Misillemesi**, Hürriyet, 28.09.2018, https://www.hurriyet.com.tr/dunya/natodan-rusyaya-tatbikat-misillemesi-40970195 ET:30.01.2020

Alkan, H. **ABD'nin Siber Güvenliği İçin 19 Milyar Dolar**, Tech İnside, 10.02.2016, https://www.techinside.com/abdnin-siber-guvenligi-icin-19-milyar-dolar/ ET:30.01.2020.

Akal, D. **ABD Ordusunda Yapay Zeka Devri**, Deutsche Welle Türkçe, 16.01.2020, https://p.dw.com/p/3WGJu ET:28.02.2020.

Alkan, M. **Siber Güvenlik Önlemi Almayan Ülkelerin Geleceği Çok Ciddi Tehdit ve Risk Altında**, Milliyet, 02.11.2017, http://www.milliyet.com.tr/prof-alkan-siber-guvenlik-onlemi-almayan-mersin-yerelhaber-2377954/ ET:28.01.2020.

Alvarado, I**. Venezuela'da Darbe Girişimi**, Sputniknews, 08.03.2019, https://sptnkne.ws/kTjW ET:26.02.2020.

Arthur, C. **That Cyberwarfare By Russia On Estonia? It Was One Kid İn Estonia**,TheGuardian,25.01.2008,https://www.theguardian.com/technology/blog/2008/jan/25/thatcyberwarfarebyrussiaon ET:30.01.2020.

Bakanlar Kurulu, **İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun,** Resmi Gazete, 29.07.2020 https://www.resmigazete.gov.tr/eskiler/2020/07/20200731-1.htm, ET:02.10.2020

Bakanlar Kurulu, **Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun,** Resmi Gazete, 22.04.2014, http://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm ET:29.01.2020

Bakanlar Kurulu, **Ulusal Siber Güvenlik Stratejisi Ve 2013-2014 Eylem Planı Dair Kanun**, Resmi Gazete, 25.03.2013, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm, ET:29.01.2020.

Bakanlar Kurulu, **Elektronik Haberleşme Kanunu**, Resmi Gazete Sayı 27050, 10.11.2008, https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm ET:10.02.2020.

Bozkurt, Ö.B. **Siber Dünya'da; Tanımlar, Ulusların Politikaları, Saldırılar ve Stuxnet Virüsü,** Beynelmilelpost, 13.10.2019, https://beynelmilelpost.com/siber-dunyada-tanimlar-uluslarin-politikalari-saldirilar-ve-stuxnet-virusu/ ET:29.01.2020.

Chalabov, K. **Askeri Stratejisini Yenileyen Çin 'Beyaz Kitap'la Okyanusa Açılıyor**,Sputnik News,26.05.2015, https://sptnkne.ws/ufcb ET:30.01.2020.

Davis, J. "**Hackers Take Down The Most Wired Country İn Europe,"** Wired Magazine,21.09.2007.http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia ET:17.01.2020.

D.W. **Rusya, Gürcistan'ı Sanal Alemde De Vurdu**, Deutsche Welle, 18.08.2008, https://p.dw.com/p/F09O, ET:30.01.2020.

D.W. **Huawei'nin Sahibinin Kızı Kanada'da Gözaltına Alındı**, Deutsche Welle, 06.12.2018, https://p.dw.com/p/39YfO ET:29.01.2020.

Denning, D.**How Iran's Military Outsources İts Cyberthreat Forces**, Times Of Israel, 22.01.2020, https://www.timesofisrael.com/how-irans-military-outsources-its-cyberthreat-forces/ ET.28.02.2020.

Demirci, M.C. **Yapay Zekâ Teknolojisi Savaşın Karakterini Nasıl Değiştirecek?,**Euronews,28.12.2018, https://tr.euronews.com/2020/02/23/yapay-zeka-teknolojisi-savasin-karakterini-nasil-degistirecek ET:30.01.2020.

Dpa, G. **Alman Hükümetinden Siber Saldırı Açıklaması**, Deutsche Welle Türkçe, 04.01.2019, https://p.dw.com/p/3B253 ET:30.01.2020.

Dpa, **ABD'den Çinli Askerlere Siber Saldırı Suçlaması**, Deutsche Welle Türkçe, 10.02.2020, https://p.dw.com/p/3XZf1 ET:28.02.2020.

Doğru, İ. **Çin'de Üretilen Bilgisayar Ekipmanlarında Casus Çip İddiası,** Anadolu Ajansı, 04.10.2018, https://www.aa.com.tr/tr/dunya/cinde-uretilen-bilgisayar-ekipmanlarinda-casus-cip-iddiasi/1273175 ET:28.01.2020.

Doomsday Fears Of Terror Cyber-Attacks, BBC NEWS, 11.10.2001, http://news.bbc.co.uk/2/hi/science/nature/1593018.stm ET:07.02.2020.

Gözütok, A. **Savunma Sanayiinde Siber Güvenlik Milat Projesine Emanet Ediliyor**,Donanım Haber, http://dhbr.co/bitj ET:30.01.2020.

Graham, B.B. **Orders Guidelines For Cyber-Warfare; Rules For Attacking Enemy Computers Prepared As U.S. Weighs Iraq Options**,The WashingtonPost,07.02.2003,https://www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber-warfare/dd8b4a18-140c-4690-88a5-0041d4ce1b1c/ ET:08.01.2019.

Guardian, **İngiltere'den Gizli Siber Silah,** Hürriyet Gazetesi, 01.06.2011, http://www.hurriyet.com.tr/gundem/ingiltereden-gizli-siber-silah-17916922 ET:10.10.2019.

Hollis, D.B. **Rules Of Cyberwar**? Los Angeles Times, 08.10.2007 https://www.latimes.com/archives/la-xpm-2007-oct-08-oe-hollis8-story.html ET:17.01.2020.

Hacısalihoğlu, D. **ABD'den Rusya'ya Seçim ve Siber Saldırı Yaptırımları**, Euronews, 20.12.2018 https://tr.euronews.com/2018/12/20/abd-den-rusya-ya-secim-ve-siber-saldiri-yaptirimlari ET:30.01.2020.

Haberler.com, **Erdoğan'dan 'Yerli Ürün, Milli Yazılım' Vurgusu**, 06.02.2018, https://www.haberler.com/erdogan-dan-yerli-urun-milli-yazilim-vurgusu-10534621-haberi/ ET:30.01.2020.

Habertürk, **Türkiye'nin Siber Ordusu BTK Yarışması**, 16.04.2017, https://www.haberturk.com/ekonomi/teknoloji/haber/1463070-turkiyenin-siber-ordusu ET:30.01.2020.

Habertürk, **F-35 Savaş Uçağı Verileri Çinliler Tarafından Hacklendi**, 16.10.2017,https://www.haberturk.com/f-35-hacklendi-1674633-ekonomi, ET:14.12.2019.

Haberturk, **Erdoğan'dan "Bilgi Ve İletişim Güvenliği Tedbirleri" Genelgesi**,07.07.2019,https://www.bloomberght.com/erdogan-dan-bilgi-ve-iletisim-guvenligi-tedbirleri-genelgesi-2227997 ET:29.01.2020.

Hürriyet İnternet Gazetesi, **Aktivist Ne Demek? Aktivist Nedir? Aktivist Tdk Kelime Anlamı** , 29.03.2020, https://www.hurriyet.com.tr/gundem/aktivist-ne-demek-aktivist-nedir-aktivist-tdk-kelime-anlami-41480920, ET:24.11.2020

İHA, **Savunma Sanayi Başkanı Demir: "Siber Güvenlik Alanında Seferberlik Gerek",** Milliyet, 01.10.2018, http://www.milliyet.com.tr/savunma-sanayi-baskani-demir-siber-guvenlik-ankara-yerelhaber-3066883/ ET:30.01.2020

İHA, **Siber Ordunun Gücüne Güç Katacak Proje Start Aldı**, Haberler.com, 11.07.2017, https://www.haberler.com/siber-ordunun-gucune-guc-katacak-proje-start-aldi-9816838-haberi/ ET:30.01.2020.

İHA, **BTK Bu Yarışmayla, Yetenekli Kişileri İstihdam Edecek**, Memurlarnet, 24.01.2019https://www.memurlar.net/haber/804817/btk-bu-yarismayla-yetenekli-kisileri-istihdam-edecek.html ET**:**30.01.2020.

Kholoosi, A. **İranlı Komutan: ABD'den Karşılık Gelseydi Daha Fazla Saldırı Düzenleyip Binlerce Can Kaybı Verdirecektik**, Sputniknews, 09.01.2020, https://sptnkne.ws/AWU9 ET:28.02.2020.

Kabakçı, F. **Çin'den ABD'nin 'Siber Casusluk' Suçlamalarına Tepki**, Anadolu Ajansı, 21.12.2018, Çin'den ABD'nin 'siber casusluk' suçlamalarına tepki https://www.aa.com.tr/tr/dunya/cinden-abdnin-siber-casusluk-suclamalarina-tepki/1345331 ET:30.01.2020.

Krebs, B. "Report: **Russian Hacker Forums Fueled Georgia Cyber Attacks**," TheWashingtonPost,16.10.2008,http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?nav=rss_blog ET:07.01.2020.

Kılınç, Ş. **Milli Savaş Uçağı Projesine 'Yerli Süper Bilgisayar' Desteği Geldi!,** Webtekno, https://www.webtekno.com/milli-savas-ucagi-projesine-yerli-super-bilgisayar-destegi-geldi-h43012.html ET:30.01.2020.

M. Erdoğan: **'Ahtapot' Siber Saldırıyı Engelledi, Gerçekleşecek Bir NATO Tatbikatına Dahil Edildi**, Sputniknews, 26.12.2018 https://tr.sputniknews.com/turkiye/201812261036814345-erdogan-tubitak-tuba-odul-toreni-bilim/ ET:30.01.2020.

Memurlar Net, **Maliye'nin Web Sitesi Hacklendi**. 10.11.2011, https://www.memurlar.net/haber/209719/maliye-nin-web-sitesi-hacklendi.html ET.29.01.2020.

Mynet, **Telefonlarına Gelen Mesajı Görenler Şoke Oldu! PKK'dan Toplu SMS,** 16.08.2018, https://www.mynet.com/telefonlarina-gelen-mseaji-gorenler-soke-oldu-pkk-dan-toplu-sms-110104335942 ET.29.01.2020.

Nakashima E. ve Pomfret, J. **''China Proves To Be An Aggressive Foe İn Cyberspace,''**WashingtonPost,11.11.2009www.washingtonpost.com/wpdyn/content/article/2009/11/10/AR2009111017588_pf.html. ET:20.01.2020.

Ordumanset, **Ordu Valiliği Sitesine Pkk Saldırısı**, 16.02.2014, http://www.ordumanset.net/m-haber-4017.html ET:29.01.2020.

Sancak, M. **5 Trilyon Dolarlık Siber Savaş Daha Da Kızışacak**, Haber Türk Gazetesi,21.11.2015,https://www.haberturk.com/ekonomi/savunma-sanayi/haber/1156360-5-trilyon-dolarlik-siber-savas ET:29.01.2020.

Sanger, D. E. **Obama Order Sped Up Wave Of Cyberattacks Against Iran,** thenewyorktimes,01.06.2012https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html ET:10.10.2019.

Staples, D. **İngiltere, Rusya'yla İlişkilerde Soğuk Savaş Stratejisine Geri Dönüyor,**Sputnik,19.12.2018, https://sptnkne.ws/kr82 ET:30.01.2020.

Superhaber, **Teröristbaşı Abdullah Öcalan Öldü Mü?** 12.01.2019, https://www.superhaber.tv/teroristbasi-abdullah-ocalan-oldu-mu-haber-167086 ET:29.01.2020.

Sputnik, **Rusya: ABD Nükleer Silahlar Alanında Gerilimi Tırmandırmaya Yönelik Adımlar Atıyor,** Sputnik News, 21.01.2020, https://sptnkne.ws/Bd66 ET:28.02.2020.

Sözcü Gazetesi, **PKK Müftülük'ü Hack'ledi**, 11.11.2012, https://www.sozcu.com.tr/2012/gunun-icinden/pkk-muftuluku-hackledi-111761/ ET:29.01.2020.

STM, **Savunma Sanayii Başkanlığından Kritik Hamle! Milli siber güvenlik sistemi CyDecSys tanıtıldı,** Yeni Akit Gazetesi, 31.10.2018, https://www.yeniakit.com.tr/haber/savunma-sanayii-baskanligindan-kritik-hamle-milli-siber-guvenlik-sistemi-cydecsys-tanitildi-538585.html ET:30.01.2020.

T24 Haber, **Devletin Sirlarini Çalan Pkk Kuryesi Cikti**, 19.11.2008, http://t24.com.tr/haber/devletin-sirlarini-calan-pkk-kuryesi-cikti,17138 ET:29.01.2020.

TRT haber, "**Çinli Hacker'lar ABD'ye ABD'nin Siber Yazılımıyla Saldırdı",** 05.05.2019, https://www.trthaber.com/haber/dunya/cinli-hackerlar-abdye-abdnin-siber-yazilimiyla-saldirdi-414599.html ET:28.01.2020.

Türkiye Gazetesi, **NATO Gözünü Kararttı! Büyük Tehdit.** https://www.turkiyegazetesi.com.tr/fotogaleri/nato-gozunu-karartti-buyuk-tehdit-16610.aspx?O=6, ET:29.01.2020.

Jamil N.J. **The Best (Cyber) Defense Is A Good (Cyber) Offense**, Opinion, Newsweek, 14.09.2020 https://www.newsweek.com/best-cyber-defense-good-cyber-offense-opinion-1531606 ET:16.09.2020.

Johnson, B. **US Asks China To Explain Google Hacking Claims**, Theguardian, 31.01.2010, https://www.theguardian.com/technology/2010/jan/13/china-google-hacking-attack-us ET:14.12.2019.

Waterman, S. **Georgia Hackers Strike Apart From Russian Military,** The WashingtonTimes,19.08.2008,http://www.washingtontimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military ET:07.01.2020.

Washington Post, **ABD Savunma Bakan Yardımcısı: Bütün Askeri Sırlarımız Çalındı**,Hürriyet,26.08.2010, https://www.hurriyet.com.tr/gundem/abd-savunma-bakan-yardimcisi-butun-askeri-sirlarimiz-calindi-15630544, ET:12.02.2020.

Yönak, R. **2016'da Gerçekleştirilen Siber Saldırılar**, BBC, 03.01.2017, https://www.bbc.com/turkce/haberler-38489376 ET:30.01.2020.

Raporlar

Arı, T. ve Özdal, B. "Uluslararası Sistemde Yeni Düzen Arayışları", VII. Uludağ Uluslararası İlişkiler Kongresi Raporu, Bursa,2016.

Arı, T. ve Aydın, K. Çiğdem. "Dünya Politikasında Kriz ve Değişim", Uluslararası IX. Uludağ Uluslararası İlişkiler Kongresi Raporu, Bursa,2017.

Archick, K. "Cybercrime: The Council of Europe Convention," CRS Report for Congress RS21208, 28.09.2006.

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights, Web Page: www.cyberpolitikjournal.org, Cilt.2, No.3, Yıl. 2017.

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights, Web Page: www.cyberpolitikjournal.org,Cilt. 1, No. 1, Yıl. 2016.

Beehner, L. Collins, L. ve Ferenzi, S. Person, R. and Brantly, A. Analyzing the Russian Way of War Evidence from the 2008 Conflict with Georgia A Contemporary Battlefield Assessment by the Modern War Institute, 20.03.2018, ss.1-90https://mwi.usma.edu/wp-content/uploads/2018/03/Analyzing-the-Russian-Way-of-War.pdf ET.06.02.2021.

Bıçakcı, S. Ergun, D. Çelikpala, M. Türkiye'de Siber Güvenlik ve Nükleer Enerji, Ekonomi ve Dış Politika Araştırma Derneği (EDAM), İstanbul, ss.29-73 http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf

Bush, G.W. National Strategy to Secure Cyberspace, Washington DC, Şubat 2003,https://uscert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf ET.06.02.2021.

CSIS Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace for the 44th Presidency, Aralık 2008, ss.49-65. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf ET:20.01.2020.

Center For Strategic and İnternational Studies(CSIS), Global Cyber Strategies Index,2020https://csis-website-prod.s3.amazonaws.com/s3fspublic/Cyber%20Regulation%20Index%20V2%20%28002%29.pdf ET.06.10.2020

Connell, M. and Vogler, S. Russia's Assroach to Cyber Warfare CNA Analysis Solution Report, Eylül 2016.

Cisco, Cisco 2018 Annual Cybersecurity Report, https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf ET.30.03.2020.

Clement, C. Proposed budget of the U.S. government for cyber security in FY 2017to2020, Statista, Mart 2019, https://www.statista.com/statistics/675399/us-government-spending-cyber-security/ ET:31.01.2020.

Clement, C. Countries with the highest commitment to cyber security based on the Global Cybersecurity Index (GCI) in 2018, Statista, Mart 2019, https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/ ET:31.01.2020.

Downin, L. Why We Need To Measure Military Cyber Power, Weforum, 29.03.2018,https://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power ET:31.01.2020.

Delpech, T. Nuclear Deterrence İn The 21ST Century Lessons From The Cold War For A New Era Of Strategic Piracy, Rand Cooperation, 2012 ss.6,141-151

Earl Zmijewski,Accidentally Importing Censorship**,** Renesys Blog, 30.03.2010, http://www.renesys.com/blog/2010/03/fouling-the-global-nest.shtml ET:24.01.2020.

Enisa, Industry 4.0 Cybersecurıty: Challenges And Recommendatıons, The EU AgencyForCybersecurıty,Mayıs2009, https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport ET:28.02.2020.

European Network And Information Security Agency, Cyber Europe 2010 EvalutionReport,2011.

Ermarth, F. W. Russıa's Strategıc Culture: Past, Present, And… In Transıtıon? Defense Threat Reduction Agency Advanced Systems And Concepts Office, 31.10.2006

European Parliment Dırectorate-General For External Polıcy Department. Russia's National Security Strategy And Military Doctrine And Their İmplications For The EU, Ocak 2017, ss.1-28

Geers, K. Cyberspace And Changing Nature Of Warfare, NATO Talin Office Raport,https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf ET:29.01.2020

Giles, K. Russia's 'New' Tools For Confronting The West Continuity And Innovation İn Moscow's Exercise Of Power, Russia And Eurasia Programme, Chatham House The Royal İnstitute of İnternational Affairs, Mart 2016.

Gouré, D. A Competitive Strategy To Counter Russian Aggression Against NATO, Lexington Institute, Mayıs 2018.

Hartwig, R. P. Cyberrisk: Threat And Ossortunity, İnsurance information instute, New York, Ekim 2016.

Harris, B. These Countries Spend The Most On Defence, 04.05.2018,https://www.weforum.org/agenda/2018/05/india-worlds-biggest-defence-military-spender/ ET:29.01.2020.

IBM ve Ponemon Enstitüsü, 2019 Cost Of Data Breach Study By Ponemon, https://www.ibm.com/security/data-breach ET:30.03.2020.

İTU, Global Cybersecurity Index, 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf ET:15/12/2019.

Karaca, M. İnsanlaşan Makinalar ve Yapay Zekâ, İTÜ Vakfı Dergisi Yayınları, Sayı 75, Ocak-Mart 2017, https://www.ituvakif.org.tr/dergi/sayi_75.pdf ET:30.01.2020.

Kasapoğlu, C. Siber Güvenlik: Beşinci Boyutu Anlamak, EDAM Siber Politikalar Kâğıtları Serisi, Haziran 2017.

Kemp, S. Global Digital Report 2018, We are social, 30.01.2018, https://digitalreport.wearesocial.com/ ET:15/12/2019.

Küçükşahin, A. T.C. Genelkurmay Başkanlığı Harp Akademileri Komutanlığı Saren, Türkiye' Ye Yönelik Dış Kaynaklı Risk ve Tehditler Sempozyumu, 05-06 Nisan 2007, ss.45

Matai, D. K. The World Beyond 11 September Focus On Asymmetric Warfare, 1 Whitehall,RTC,22 October 2001, ss.2-4

Libicki, M. Cyberdeterrence And Cyberwar, CARAND Corporation, Santa Monica, 2009.

Marten, K. Reducing Tensions Between Russia And NATO, Council Special Report No. 79, Mart 2017.

Ministry of Foreign Affairs within Estonian Development Cooperation, National Cyber Security Index 2018, https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf ET.29.01.2020

Nojonen, M. and Moshes, A. Introduction: Adjusting To The Great Power Transition. In Russia –China Relations. Current State, Alternative Futures, and Implications for the West, Finnish Institute of International Affairs Fia Report 30, Helsinki, 2011. ss.17-18

Nichol, J. Russia-Georgia Conflict İn South Ossetia: Context And Implications For US Interests, Congressional Research Service Report for Congress, 13.08.2008. ss.1-16

Nyu Tandon School Of Engineering, The Index Of Cybersecurity, Aralık 2019, https://wp.nyu.edu/awm1/ ET:15.12.2019.

International Telecommunication Union, A Comparative Analysis Of Cybersecurity Initiatives Worldwide, WSIS Thematic Meeting on Cybersecurity, Geneva,10.06.2005 https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf ET.03.02.2020

Oliker, O. McNerney, M. J. and E. Davis, L. NATO Needs A Comprehensive Strategy For Russia, Rand Corporetion perspective, 2015, ss.1-20.

Perrier, E. M. The Key Principles Of Russian Strategic Thinking, Laboratoıre De L'ırsem, 2014, ss.1-50.

Portland, The Soft Power 30, A Global Ranking Of Soft Power 2019**,** pp.40 https://softpower30.com/wp-content/uploads/2019/10/The-Soft-Power-30-Report-2019-1.pdf ET.05.02.2021.

Rid T. and Hecker, M. The Terror Fringe, Policy Review, No.158, Aralık-Ocak 2010, ss.3–19.

Sağıroğlu Ş. Akleylek S. Canbay Y. Bildiriler Kitabı, 12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı ISCTURKEY 2019, Ankara, 16-17 Ekim 2019https://www.iscturkey.org/bildiriler/2019/ISCTurkey-2019-Bildiriler-Kitabi.pdf ET:29.01.2020.

Siber Tehdit Durum Raporu**,** STM Teknolojik Düşünce Merkezi, Ekim-Aralık 2018,https://thinktech.stm.com.tr/uploads/raporlar/pdf/1712019155627260_stm_siber_tehdit_durum_raporu_ekim_aralik_2018.pdf ET.29.01.2020.

Schwab, K. The Global Competitiveness Report, World Economic Form, 2017–2018,http://www3.weforum.org/docs/GCR2017-2018/05FullReport/TheGlobalCompetitivenessReport2017%E2%80%932018.pdfET :15/12/2019.

Świątkowska, J. NATO Road To Cybersecurity**,** The Kosciuszko Institute, 2016.ss.5-70.

Touré, H. I. The Quest For Cyber Peace**,** International Telecommunication Union, January 2011, ss7-16 https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf ET:19.02.2020.

Türkiye İstatistik Kurumu, Küresel Rekabet Endeksi, 23.10.2019. http://tuik.gov.tr/UstMenu.do?metod=istendeks ET:09.04.2020.

The United States Commission on National Security, New World Comıng: Amerıcan Securıty In The 21st Century Sussortıng Research And Analysıs, 15.09.1999 https://govinfo.library.unt.edu/nssg/NWR_A.pdf ET:31.01.2020.

Unal, B. and Lewis, P. Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences, Chatham House International Security Department, Ocak 2018, ss.1-23.

United Nations Office On Drugs And Crime, The Use Of The Internet For TerroristPurposes,NewYork,2012,https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf ET:31.01.2020.

U.S.–China Economic and Security Review Commission (USCESRC), 2010 Report to Congress of the U.S.–China Economic and Security Review Commission at the 11th Congress, Second Session, Kasım 2010. https://www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf ET:24.01.2020.

Yüksel, M. Ülkeler ve Siber Güvenlik Bütçeleri, Netcom Bilgisayar A.Ş. https://www.netcom.com.tr/siber-guc-kapasitesi/ ET:29.01.2020.

Sözlük

Anonim, **Bilgisayar ağı (Network),** http://www.egitim.com/ ET: 10.12.2019.

Department of Defense Dictionary of Military and Associated Terms, **Cyberspace and Cyber Counterintelligence**, USA, 09.06.2004, ss.138 https://www.cia.gov/library/abbottabad-compound/B9/B9875E9C2553D81D1D6E0523563F8D72_DoD_Dictionary_of_Military_Terms.pdf ET:06.02.2021.

Sönmezoğlu, F. Uluslararası İlişkiler Sözlüğü, (**kararalma yaklaşımı** ss.386, **sınırlı savaş** ss. 584, **sözleşme** ss.598, **Kuzey Atlantik Anlaşması** Örgütü ss. 429, **stratejik kavram** ss.601,), DER Yayınları, İstanbul, 2005.

TürkDilKurumuSözlükleri,**SiberSavaş**,http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5cbd798e8c87c4.76321916, ET:30.01.2020.

UNTermPortal,**CyberWar,**https://unterm.un.org/unterm/search?urlQuery=cyber+war ET:30.01.2020.