T.C.
DÜZCE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TOPLAM KALİTE YÖNETİMİ ANABİLİM DALI

SİBER GÜVENLİK VE TERÖRİZMİN EVRİLİŞİ: TÜRKİYE ÜZERİNE ETKİLERİ

YÜKSEK LİSANS TEZİ

Dilaver GEDİK

Düzce
Haziran, 2018

T.C.

DÜZCE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TOPLAM KALİTE YÖNETİMİ ANABİLİM DALI

SİBER GÜVENLİK VE TERÖRİZMİN EVRİLİŞİ: TÜRKİYE ÜZERİNE ETKİLERİ

YÜKSEK LİSANS TEZİ

Dilaver GEDİK

Danışman: Doç. Dr. Zafer Akbaş

Düzce
Haziran, 2018

Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Bu çalışma jürimiz tarafından Toplam Kalite Yönetimi Anabilim Dalında oy birliği / oy çokluğu ile YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan Doç. Dr. Gökhan TELATAR .....

Üye Doç. Dr. Zafer AKBAŞ .....

Üye Dr. Öğr. Üyesi Ahmet Hüsrev ÇELİK .....

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

05/07/2018

Doç. Dr. Ali ERTUĞRUL
Enstitü Müdürü

ÖZET

SİBER GÜVENLİK VE TERÖRİZMİN EVRİLİŞİ:
TÜRKİYE ÜZERİNE ETKİLERİ

GEDİK, Dilaver

Yüksek Lisans, Toplam Kalite Yönetimi Anabilim Dalı

Tez Danışmanı: Doç. Dr. Zafer AKBAŞ

Haziran 2018, 102 sayfa

Günümüzde siber ortamda yapılan eylem ve saldırılar sonucunda ortaya çıkan büyük zararlar, siber güvenliğin önemini artırmaktadır. Siber alanda sadece terör örgütleri değil, devletlerde bu alanda faaliyet yürütmektedirler. Siber ortamda devletlerin önemli kritik altyapılarına yapılan saldırılar ile büyük maddi kayıplar ve toplumsal alanda huzursuzluk ve korku yayarak çöküntüler hedef alınmaktadır. Bu faktörler, önümüzdeki dönemde devletler arasında yaşanacak savaşlar ve mücadelelerin siber ortamda oluşmasına neden olacaktır.

Klasik Uluslararası İlişkiler, reel dünyayı ve bu dünyadaki ilişkileri incelemekte olup, siber alan ve bu alandaki uluslararası ilişkiler genel olarak gözardı edilmektedir. Bu maksatla, bu çalışmada temel olarak siber alan ve bu alandaki faaliyetlerin önemi anlatılmaktadır. Siber alandaki gelişmeler uluslararası ilişkilere farklı bir yönden bakılmasını sağlayacaktır. Bu çalışmanın ilk bölümünde, güvenlik kavramı ve dönüşümü, siber alan, siber terörizm ve siber savaş ile ilgili kavramsal bilgiler anlatıldıktan sonra, ikinci bölümde siber terörizm ve güvenlik unsurları, üçüncü bölümde siber alanda kullanılan siber silah türleri örneklerle açıklanmakta olup, dördüncü bölümde ise siber terörizmle mücadele ve alınacak tedbirler ile Türkiye'nin siber güvenlik politikaları değerlendirilmektedir.

Anahtar Sözcükler: Siber Alan, Siber Güvenlik, Siber Terörizm, Siber Saldırı, Siber Savaş, Küreselleşme.

ABSTRACT

CYBER SECURITY AND TERRORISM EVOLUTION: EFFECTS ON TURKEY

GEDİK, Dilaver

MASTER THESIS

Total Quality Management Department

Supervisor: Assoc. Prof. Dr. Zafer AKBAŞ

June 2018, 102 Pages

Nowadays, big damages caused by actions and attacks in the cyber environment increase the importance of cyber security. The cyber field is not just a terrorist organization, it is in this state in the states. In the cyber environment, attacks on important critical infrastructures of states are being targeted with massive financial losses and collapse by spreading fear and anxiety in the public arena. These factors will cause the battles and fights that will take place among the states in the coming period to occur in the cyber environment.

Classical International Relations examines the real world and its relations in the world, and the cyber space and international relations in this area are generally overlooked. For this purpose, this study mainly focuses on the area of cyberspace and the importance of the activities in this area. The developments in the cyber area will lead to a different view of international relations. The first part of this work is primarily concerned with the concept and transformation of security, the concept of cyber space, cyber terrorism and cyber warfare in the second part, cyber terrorism and security elements, in the third chapter, cyber weapon types using cyber area are explained with examples, in the fourth part of the fight against cyber terrorism and measures to be taken by Turkey's cyber security policies are evaluated.

Key Words: Cyber Space, Cyber Security, Cyber Terrorizm, Cyber Attacks, Cyber Warfare, Globalization.

İTHAF

Bu çalışmanın hazırlanmasında engin tecrübeleri ve değerli yönlendirmeleri ile bana yol gösteren danışmanım Sayın Doç. Dr. Zafer AKBAŞ'a, yardımlarından dolayı Dr. Öğr. Üyesi Ahmet Hüsrev ÇELİK ve Dr. Öğr. Üyesi Şahin ÇAYLI'ya teşekkürlerimi ve minnettarlığımı sunarım.

Bu tezi, çalışma süresince gösterdikleri maddi ve manevi fedakârlıkları her şeyin üstünde olan, anlayışlarını ve desteklerini tüm akademik hayatım boyunca hep yakınımda hissettiğim sevgili eşim Behiye ve biricik kızım Beril Su GEDİK'e ithaf ediyorum.

Dilaver GEDİK

İÇİNDEKİLER

KISALTMALAR

AB : Avrupa Birliği

NATO : North Atlantic Treaty Organization

ABD : Amerika Birleşik Devletleri

BM : Birleşmiş Milletler

İHA : İnsansız Hava Aracı

ARPANET : Advanced Research Projects Agency Network

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi

SGE : Siber Güvenlik Enstitüsü

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

BOME : Bilgisayar Olaylarına Müdahale Ekibi

SCADA : Supervisory Control And Data Acquisition

DDoS : Distributed Denial of Service

Dos : Disk Operating System

EMEA : Europa, Middle East, Africa

www : word wide web

vb. : ve benzeri

vd. : ve diğerleri

bkz. : bakınız

GİRİŞ

Yeni yüzyılda meydana gelen gelişmeler sonucunda, internet, haberleşme, iletişim ve bilgi teknolojileri günlük yaşantımızın her alanına girerek hayatımızın doğal bir parçası olmuşlardır. Hayatımızda çeşitli kolaylıklar sağlayan bu gelişmeler yaşamımızın değişmez ve vazgeçilmez bir parçası haline gelmiştir. Yaşanan bu gelişmeler kişisel ihtiyaçlarımızı karşılamada bize yardımcı olmakta, ayrıca iş hayatımızda olabilecek sorunlara çözüm bulmada kolaylıklar sağlamaktadır.

Yeni dünya düzeni ve yeni teknolojilerin insanlara sunduğu fırsatlar beraberinde riskleri de getirmektedir. Siber saldırı, siber suç, siber terörizm ve nihayetinde siber savaşlar, siber uzayda etkisini günbegün artan ölçüde hissettirmektedir. Siber savaşta kullanılan bu yöntem ve araçlar bazı kimseler ve organize suç örgütleri tarafından kullanıldığı gibi devletler tarafından da kullanılan yeni savaş teknolojileri haline gelmiştir. İçerisinde bulunduğumuz yeni yüzyılın ilk on yılı "siber savaş" olgusunun ortaya çıktığı ve geleceğe yönelik derin tesirlerin evrimleştiği sıradışı bir zaman olarak tarihe geçecektir. Bilgi güvenliği, bilişim güvenliği ve siber güvenlik gibi kavramlar tüm ülkelerin ve toplumların en önemli ve öncelikli konusu haline gelmiştir. Bu kapsamda kişisel, kurumsal ve toplumsal anlamda bilgi ve bilinç düzeyinin oluşturulması toplumun tüm kesimlerinde farkındalığın artırılması son derece önem arz etmektedir (Çiftçi, 2012;6).

Bugünün dünyasında güvenliğin ulaştığı çok boyutlu ve sadece askeri önlemlerle sağlanmayacak kadar karmaşık olan yapısı, aynı zamanda bireysel, ulusal ve uluslararası güvenlik ve istikrarın giderek daha fazla iç içe geçmekte olduğuna da işaret etmektedir. Bu nedenle güvenlik her zaman olduğundan daha kaygan ve küreselleşme ile yerelleşmenin aynı anda etkisi ve tehdidi altında Soğuk Savaşın sona ermesinden sonra ve kesinlikle 11 Eylül saldırının takiben, eskiden birbirinden ayrı politikalarla yönetilmeye çalışılan bireysel, ulusal ve uluslararası güvenlik sorunları arasındaki sınır artık ortadan kalkmış durumdadır (Bıçakçı, 2013;10).

Elde edilen bilgiler her gün dünyadaki birçok ülkede kamu ve özel sektör ile evlerde kullanılan bilgisayarların büyük çapta kayıplara neden olan siber saldırılara maruz kaldıklarını göstermektedir. Aynı durum ulusal seviyede de mevcuttur. Ulusal ağlar ile sistemleri etkilemektedir. Tek bir güvenlik stratejisi siber uzay açıklıklarının ve bununla ilgili tehditleri yok etmekle yeterli değildir. Ülkeler risk sorumluluklarını yönetmek için çaba göstermeli ve meydana gelen saldırılardan oluşan hasarları azaltmak için imkân ve kabiliyetlerini artırmak gayreti içerisinde olmalıdırlar. Siber güvenliğin önemi ile ilgili artan bilinçlenme ve önlemlere rağmen siber riskler ulusal bilgi ağları ve kritik sistemleri de hala devam etmektedir. Böyle bir riskin azaltılması kamu ve özel kurum ve kuruluşlar, hatta silahlı kuvvetler ve kişiler arasında büyük çapta aktif ortaklık ve küresel işbirliğini gerektirmektedir (Yılmaz ve Salcan, 2008;14).

Bu araştırma nitel bir araştırma olup, literatür taraması ile verilerin toplanması, çözümlenmesi ve yorumlanması aşaması izlenmiştir. Konuya dair yayımlanan kitaplar, makaleler, dergiler, tez ve çeşitli internet kaynaklarından yararlanılmıştır.

Bu çalışmada; siber alan ve bu alandaki faaliyetlerin önemi, siber güvenlik terörizmin gelişimi ve küresel boyutu, Türkiye'nin milli güvenliğini tehdit eden siber saldırıların önlenmesi amacıyla siber alanda alınması gereken önlemler, siber alanda bulunan tehditler hakkında farkındalık oluşturulması amaçlanmıştır. Tezin hipotezleri ise;

1. 21. Yüzyılda değişen güvenlik anlayışı kapsamında siber tehdit, siber saldırı ve siber terörizm küresel boyutta bir tehdittir.

2. Siber ortam, kara, hava, deniz ve uzayın ardından beşinci savaş ortamı olarak yerini almış durumdadır.

3. Siber saldırı ve siber terörizm faktörleri Türkiye'nin milli güvenliğini önemli derecede tehdit etmektedir.

BİRİNCİ BÖLÜM

1. KURAMSAL VE KAVRAMSAL ÇERÇEVE

1.1. Güvenlik Kavramı

Güvenlik kavramı bireyden uluslara kadar bütün aktörler için önem taşıyan, her seviyede farklı anlam kazanan ancak özünde her biri için hayati gereksinimleri ifade eden bir tanımdır. Bu nedenle güvenlik ihtiyacını, varlığı koruyan ve sürdürme amacı taşıyan davranış biçimlerinin bütün olarak görmek mümkündür. Güvenlik, Latince bir kelime olan Securitas kökeninden gelmektedir. Türk Dil Kurumu (2009) sözlüğünde toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyeti şeklinde tanımlanmıştır (Bayraktar, 2015: 25). Güvenlik, genel olarak insanların herhangi bir tehdit altında olmadan yaşayabilmeleri durumu ve emniyet hali olarak tanımlanır. Benzer şekilde, "zarar veya tehlikeye karşı emniyette olma veya hissetme", "tehditlerin olmaması durumu" ya da "güvensizlik derdinin bulunmaması hali" ifadeleri de güvenlik kelimesinin mahiyetini ortaya koymaktadır (Açıkmeşe, 2014: 241).

Güvenlik kavramı genel olarak savunma, kapsamı biraz daha daraltılacak olursa askeri savunma anlamına gelmektedir. Son dönemlerde yapıldığı gibi en geniş anlamda ele alınacak olursa da iklim koşullarından, kişisel hak ve özgürlüklere kadar genişletilebilmektedir. Geniş bir spektrumun üzerinde güvenliğe herhangi bir anlam verilmesi mümkündür. Tarih içinde bu kavrama farklı anlamlar yüklenmiş ve sonuç

olarak “tehditten korunmak” anlamına gelen kavram kabul edilmiştir (Yalçın, 2017: 59).

Uluslararası ilişkilerin en önemli araştırma konularından biri olan güvenlik kavramı, özellikle 1980’lerden itibaren başlayan ve 1990’lı yıllarda dünya siyasi coğrafyasını da etkileyerek siyasi, ekonomik, sosyo-kültürel ve çevresel gelişmeler ile bunların uluslararası ilişkilerin teorik çerçevesine etkileri açısından yeniden incelenmesi gerekmektedir. Geleneksel/Ortodoks uluslararası ilişkiler yaklaşımları güvenlik kavramını temelde ortaya çıkan değişim ve dönüşümü tanımlamakta yetersiz ve ilgisiz kalmaktadır. Özellikle soğuk savaş sonrası dönemde, güvenliği yeni boyutları, aktörleri ve seviyeleri dikkate alarak çok yönlü ve eleştirel olarak derinlemesine inceleyen yeni teorik yaklaşımlarda büyük bir ilerleme sağlanmıştır (Öztürk, 2014: 149).

Güvenlik, uluslararası ilişkiler alanında sorunsuz bir kavram gibi değerlendirilen, önceden tarifi yapılan sağduyu terimlerinden biri olmuştur. Soğuk Savaş döneminde güvenlik, devletler arasında bulunan stratejik ilişkilere ve ülkelerin askeri gücüne bağlı olduğu kabul edilirdi. Güvenliğin anlamı ve önemi ancak güvensizlik durumunda ortaya çıkacaktır. Güvensizlik, bir veya birçok tehditten kaynaklanan tehlikelerle, korku ve endişe içinde yaşamayı içermektedir. Bu unsurlar doğrudan şiddet tehditleri ya da yapısal etkilerden doğan yoksulluk gibi dolaylı tehditler olabilir. Meydana gelen bu güvensizlik seviyesi ne kadar artarsa yaşam üzerine etkileri o kadar artacaktır (Booth, 2012: 122-128).

Güvenlik, önceden belli bir noktaya getirilmiş olan değerlerin koruma altına alınmasıdır. Walter Lippmann’ın ifadesiyle, bir millet savaşmadığı dönemlerde kendi temel değerlerini kaybetmek zorunda kalmadığı sürece veya bir savaş halinde zafer kazanarak bu değerleri korumasını bildiği sürece güvenlidir. Bu kapsamda bir ulusun güvenliği, herhangi bir saldırı durumuna karşı caydırıcılık imkân ve kabiliyeti veya herhangi bir savaş halinde zafer kazanma kabiliyetine göre artar ve azalır. Ülkelerin güvenlik için uzun vadede harcayacakları gayretin miktarını belirlemekte özgür olmadıkları gerekçesiyle buna itiraz edebilir (Wolfers, 2013: 45-48).

Güvenlik kavramı kullanımda olan ancak günümüze kadar farklı anlam değişimlerini uğramış bir kavramdır. Ancak güvenliğin günümüzdeki hâkim anlamına yakın ilk kullanımları Thomas Hobbes'la beraber yaygınlaşmıştır. Tüm topluma korku salan İngiliz iç savaşı şartlarında yaşamış olan Hobbes, güvensizliğin en büyük nedeni olarak değerlendirdiği savaşı önleyebilecek bir "***süper devlet***" fikrini ortaya çıkarmıştır. Bu genel kabul görmüş anlam realist uluslararası ilişkiler ekolünün güvenliği devletle bağlantılı bir kavram olarak pazarlaması ile uluslararası ilişkilere taşınmıştır. Güvenlik kavramı 1980'lere kadar imparatorlukların yıkılmasını durdurmak veya iç savaşı önlemek amacında olduğu gibi hep devlet merkezli bir yaklaşım içinde olmuştur (Kardaş, 2014: 228).

1.1.1. Realizm ve Neorealizm Açısından Güvenlik Anlayışı

Realizm özellikle bilginin bilimsel bakış ve pozitivist yöntemler ile elde edilebileceğini savunan bir akademik dünyada kendisine geniş bir alan açmıştır. İkinci Dünya Savaşı sonrası uluslararası ilişkiler alanında temel teori olmuştur. Realizmin disiplini içindeki etkisi o kadar güçlü olmuştur ki diğer bütün teoriler realizme referansla disiplin içindeki kendi konum ve farklılıklarını tanımlamak zorunda kalmışlardır. Bu kapsamda, genellikle insan doğasının kötü olduğu ve insanın çevresindekileri hâkim olmak istediği varsayımından hareket eden realizm devletleri uluslararası siyasetin temel aktörleri olarak kabul etmektedir (Kardaş, Balcı, 2014: 85).

Realizme göre devletler dünya siyasetindeki temel aktörlerdir. Devletler var olma, güvenlik ve/veya dünya hâkimiyeti peşinden koşan rasyonel aktörlerdir. Diğer bir ifadeyle realizm devlet merkezli bir teori olup, uluslararası sistemindeki temel aktörlerin üniter ve rasyonel devletler olduklarını öngörmektedir (Uzer, 2008: 60).

Realizm; düşünce tarihindeki etkili tüm teori gelenekleri gibi verdiği cevapların gerçekliğinden ziyade sorduğu soruların gerçekçiliği ile önem kazanmış ve önemini muhafaza eden uluslararası ilişkiler teorilerinin hâkim geleneğini oluşturan teorileri, insanlık tarihi boyunca gerçekleşen tüm politik ekonomik askeri ve sosyal dönüşümlere karşı insanoğlunun mütemadiyen karşı karşıya kaldığı meseleleri ele almaktadır (Ersoy, 2014: 159).

Devletler arası ilişkiler bir dünya hükümetinin yokluğunda meydana gelmektedir. Realizme göre bu durum uluslararası sistemin anarşik olduğunun anlamıdır. Uluslararası İlişkiler, en iyi, ülkeler arasındaki güç dağılımına odaklanarak anlaşılabilmektedir. Ülkelerin hukuk önündeki eşitliğine rağmen, gücün dengesiz dağılımı uluslararası ilişkileri bir tür "güç politikası" alanı yapmaktadır. Gücün devletler arasındaki dağılımı zaman içinde farklılık göstermekte, nasıl dağıtılması gerektiği konusunda da fikir birliği bulunmamaktadır. Bu durum gücün ölçülebilirliğini kısıtlamaktadır. Dolayısıyla, uluslararası ilişkiler bir zorunluluk ve süreklilik alanı olmaktadır. Gerçekçiler uluslararası sistemde değişikliği düşündükleri zaman, ülkeler arasında güç dengesi değişikliklerine odaklanmakta ve sistemin dinamiğinde olası temel değişiklikleri önemsiz saymaya yönelmektedirler (Griffiths, Roach ve Salamon, 2011: 2).

Uluslararası ilişkiler kapsamında birçok akademik personel "güvenlik" terimi hakkında hem fikir oldukları tek konu, "güvenlik" teriminin "*temelinde tartışmalı bir terim"* olduğudur. Kabul edilmiş en geniş ifadeyle "güvenlik", "unsurların temel değerlerine yapılan tehdit ve risklerden uzak durma hali" olarak tanımlanmaktadır. Soğuk Savaş döneminin en önemli analiz odağı olan ulusal güvenlik kavramı, öncelikle Realist/Neorealist teorisyenlerin askeri güvenlik çerçevesinde devletlerin saldırı ve savunma kapasitelerini artırmaları ve bu yolla devletin bekasının sağlanması ve ulusal çıkarların korunması temelinde tanımlanmaktadır (Öztürk, 2014: 150).

Realizm kısa bir genelleme ile insan doğasının siyaset üzerindeki kontrolü ve uluslararası bir otoritenin olmaması üzerine varsayımlar yapmaktadır. Böylelikle realizm açısından "Güç" ve "Çıkar" kavramlarının altının çizilerek incelenmesi kaçınılmazdır (Sevim, 2013: 34). Çağdaş uluslararası politika değerlendirilmelerinde realizme göre devlet dünya siyasetinin en önemli aktörüdür. Çünkü yeryüzünde hesap vereceği başkaca bir egemen siyasi otorite yoktur. Devlet egemenliği demek bu siyasi yapının toprakları ve yönettiği nüfus üzerinde mutlak güce sahip olması demektir. Uluslararası İlişkiler kuramı açısından devletin dışında meşruiyete ve zor

kullanma imtiyazına sahip başka bir aktör bulunmamaktadır (Kegley ve Blanton, 2015: 36).

Realizm, uluslararası sistemin en temel unsuru olarak ulus-devleti kabul etmektedir. Uluslararası politikanın ana esası olarak devleti gören realistlere göre, devletlerarasında çatışmalar kaçınılmaz ve doğaldır. Realistler devleti yönetenleri ve karar mekanizmalarını rasyonel davranan kişiler olarak kabul etmektedirler. Onlara göre devlet adamının temel amacı anarşik bir yapıda devletin varlığını devam ettirmektir. Bu amaca ulaşmak için olabildiğince güçlü olması gerekir. Liberalizm bireyi sosyal düzenin, temel sivil hakların, ekonomik ve siyasal yaşamın temel birimi olarak kabul etmektedir (Çalık, 2013: 22-28).

Ulusal güvenlik konuları, realistlere göre uluslararası ilişkilerin ana gündemini oluşturmaktadır. Realistlerin düşünce yapısına göre devletler ulusal çıkarı en üst seviyeye çıkarmak maksadıyla gayret gösterirler. Realistler tarafından devletin varlığının devamını sağlamaya yönelik olan ulusal güvenlik konusu yüksek politika olarak; mali, ticari, parasal, çevresel ve sağlıkla ilgili konular ise alçak politika olarak adlandırılmaktadır (Arı, 2013: 27).

Neo-realizm terimi bir bakıma çelişkilidir, çünkü birçok realist neo-realizmin ifade ettiği fikirleri incelediğinde "yeni" ötekini hak edecek bir içeri olmadığını düşünür. Bununla birlikte çok gözlemci bir fikre katılmaz ve çoğulcu meydan okumaya karşılık realizmde gerçekten bazı değişikliklerin bulunduğuna ve neo-realizmin bu değişikliği göstermenin bir yolu olduğuna inanmaktadır (Brown ve Kirsten, 2008: 36).

Devlet-merkezli bir güvenlik analizi yapan Neo-realist teorisyenler, devletin devamının ve ulusal çıkarların savunulmasının uluslararası sistemin yapısından kaynaklanan güç ilişkileri çerçevesinde işlediğini ileri sürerler (Öztürk, 2014: 150).

Neo-realist yaklaşıma göre uluslararası sistemin yapısı uluslararası aktörlerin davranış ve güvenliklerini belirlemektedir. Bu yönüyle Neo-realizm klasik realizmden farklı olarak güvenliğin kavramsal boyutunu genişletmiş ve güvenlik kavramı içine ulus-devlet yapılarının ile birlikte uluslararası sistemin güvenliği

bulgularını da ilave etmiştir. Realist çalışmalar ile ortaya çıkan klasik güvenlik yaklaşımları neo-realist analizlerle olgunlaşıp şekillenmiştir (Darıcılı, 2017: 25).

Neo-realistlere göre uluslararası sistemin anarşik yapısının yol açtığı güvensizlik ortamı uluslararası ilişkilerin temelini oluşturmaktadır. Bu güvensizlik ortamı içerisinde her devletin öncelikli amacı egemenliğini ve güvenliği korumaktır. Bu kapsamda realistler gücü uluslararası politikanın bir amacı olarak görmekte iken neo-realistler gücü devletin varlığını sürdürmesinin ve güvenliğini sağlamasının bir aracı olarak değerlendirilmektedir (Bayraktar, 2015:46).

1.1.2. Soğuk Savaş Dönemi ve Sonrası Güvenlik Yaklaşımları

İkinci Dünya Savaşı ardından dünyada meydana gelen siyasi gelişmeler 1990'lı yıllara kadar sürecek olan ve "Soğuk Savaş" diye tanımlanacak yeni bir dönemin başlamasına neden olmuştur. Bu dönem ile beraber aynı zamanda Sovyetler Birliği'nin doğu bloğunun, Amerika'nın ise batı bloğunun önderliğini yaptığı "iki bloklu" bir yapı meydana gelmiştir (Arı, 2013: 209).

1899'da bazı düşünürler, 20. yüzyılın tüm dünyaya küresel barış getireceğini, devletlerin bir bütünlük içerisinde yaşayacağını ve savaşların sona ereceğini değerlendiriyordu. Fakat 20. yüzyıl insanlık tarihinin en çok savaşılan, en kanlı çarpışmaların yaşandığı yüzyılı olmuştur. Endüstri Devriminin sonucunda ortaya çıkan büyük boyutlardaki silah endüstrisi sektörü, zamanla daha etkili ve pazar payı artan silahlar üretmiştir. Nitekim silah sektörü savaşlarla dolu, istikrarsız ve güvensiz bir dünyada daha fazla kar elde edecekti. Geleneksel güvenlik anlayışı tüm alanlara hâkim olan bir devlet kavramına dayanmaktadır. Bu yaklaşıma göre büyük olgu devlet topraklarının (fiziksel olarak) korunmasıdır; toplumun ekonomik refahı da buna bağlı olarak artacak ve önemli bir düzeye gelecektir. Savunma ise, ülke sınırlarının dış tehditlere karşı korunması olarak değerlendirilmekte, bu kapsamda, ülkelerin kıyı sularının uzunlukları da top atışı mesafesine göre tespit edilmişti. Bu geleneksel güvenlik anlayışı ülkelerin menfaatlerine göre genişletildiği zamanlarda, dış kaynaklarının ve ticaret yollarının savunulması, ya da tek ulus yerine ittifak çıkarlarının korunması anlamına gelmiştir. Soğuk savaş dönemi, geleneksel güvenlik politikalarının birçok örneğini bulundurmaktadır (Tuna, 2003, 163-164).

Birinci Dünya Savaşı sonrası Cemiyet-i Akvam ile öz-çıkar merkezli güvenlik anlayışı yerine önerilen kollektif güvenlik sistemi uzun süreli olmamış, İkinci Dünya Savaşı sonrası ABD'nin uluslararası ilişkiler disiplinindeki hegemonyası ulusal güvenlik kavramı ve anlayışını küresel ölçekte alanda meşrulaştırmıştır. İkinci Dünya Savaşı'ndan Soğuk Savaş döneminin sonuna kadar stratejik çalışmalar adı altında askeri güvenlik konuları hâkim araştırma konusu olmuştur. İki kutuplu uluslararası sistem içerisinde sert ideolojik mücadele ve özellikle nükleer savaş tehlikesi analistleri silahsızlanma ve caydırıcılık gibi iki büyük güvenlik stratejisinin çalışılmasına ağırlık verilmiştir. Bu dar tanıma karşılık 1970'lerin sonundan başlamak üzere genişletilmiş bir kavramı kullanılmaya başlanmıştır (Kardaş, 2007: 227).

Güvenlik çalışmalarının erken dönemi ve belki de en önemlisi olarak değerlendirilen Soğuk Savaşın ilk yıllarında bu kavramın ne anlam ifade ettiği hem akademik çevreler hem de hükümet çevrelerinde çok tartışma konusu değildi. Soğuk Savaşın devletlerarası düzeyi ve bunun içerisindeki askeri rekabet göz önünde bulundurulduğunda güvenlik çalışmalarının askeri alana odaklanması şaşırtıcı olmamıştır. Erken dönemdeki birçok eser dönemin koşullarına uygun olarak nükleer silahlar ve onların yazılması ve kullanılması gibi konulara odaklanmıştır. Güvenlik denilince akla nükleer silahlar caydırıcılık NATO ve savaş gibi konular gelmektedir (Yalçın, 2017: 60).

Soğuk savaşın bitmesiyle birlikte ülkelerin tehdit algılamalarında ve uluslararası sistemin temel karakteristiklerinde bazı değişimler gerçekleşmiştir. Bu değişimler uluslararası politik yapıda farklı boyutlarda yeni güç dengelerinin ve yeni aktörlerin ortaya çıkması şeklinde gerçekleşirken, değişimin en önemli boyutu tehdit algılamasının değiştiği güvenlik anlayışında ortaya çıkmıştır. Soğuk Savaş sonrasında meydana gelen yeni dinamik ortam içerisinde ülkenin güvenliği için tehdit ve risk unsurları değişmiştir. Ortaya çıkan yeni tehdit unsurları, terör eylemleri, uluslararası grupların icra ettiği illegal faaliyetler ve siber terör gibi unsurlar yeni bir güvenlik anlayışının ortaya çıkmasına neden olmuştur (Bayraktar, 2015: 36).

1990 Ağustos'unda Kuveyt'in işgali ile meydana gelen Körfez krizi eski ve yeni yapı arasındaki geçişi simgelemektedir. İlk defa Başkan Bush tarafından kullanılan lakin pek çok kişinin ne olduğunu anlayamadığı "Yeni Dünya Düzeni" kavramı bu kriz sonrasında sıkça kullanılmaya başlanmıştır. Bu krizde tüm dünya bir saldırganın karşısına çıkarak güç kullanma yoluyla sınırlarının değiştirmesine izin verilmeyeceği mesajını vermiştir. Sonuçta Irak kuvvetleri çıkarılmış ve Birleşmiş Milletler çatısı altında kollektif güvenlik başarılı sağlanmıştır. Yeni ortaya çıkan uluslararası sistemin daha barışçı ve uzlaşmacı problemlerin ise uluslararası hukuk ve örgütler kapsamında çözümleneceği, buna karşılık sınırların güç kullanma yolu ile değiştirilemeyeceği bir yapı olacağı düşünmeye başlamıştır. Uluslararası barış ve adil bir düzen egemen kılınabilir ve bu kurumsallaştırılabilirdi. Uluslararası barışın korunmasının başlıca büyük devletler tarafından garanti altına alınacağı bir uluslararası güvenlik sisteminin kurulabileceği olasılığı üzerinde durulmaya başlandı. Fakat yaşanan gelişmeler bu olasılığın gerçekleşmeyeceğini tüm dünyaya göstermiştir (Arı, 2004: 521).

Soğuk Savaş'ın sona ermesiyle birlikte bölgesel düzeydeki güvenlik yapılanmaları uluslararası politikayı artan bir şekilde etkilemeye başladı. Bu eğilim Soğuk Savaş'ı tanımlayan süper güç odaklı katı ve iki kutuplu yapıdan farklı olarak yeni bir uluslararası ilişkiler modeli inşa etmekteydi (Yavaş, 2013: 202).

Soğuk Savaş'ın son 10 yılı güvenlik oluşumunun devletlerin askeri problemler karşısında kuvvet artırmaları ve güç kullanmaları dışında tanımlanması, yani Stratejik Çalışmaların kavramsal çerçevesinin sorgulanması gayretleri büyük ölçüde artmıştır. Bu dönüşümün temelinde, Soğuk Savaş'ın son zamanlarında askeri tehditlerin öneminin azalması ile birlikte daha önceleri kapatılan ekonomik, çevresel, toplumsal, siyasi vb. diğer sorunların güvenlik ilişkilerini etkilediği gerçeğinin anlaşılması yatmaktadır (Açıkmeşe, 2014: 247).

Soğuk Savaş'ın sona ermesiyle birlikte Avrupa ve dünya coğrafyası beraberinde birçok yeni olgu ve problemlerin doğmasına sebep olmuştur. Siyasî, iktisadî ve sosyal yansımalarıyla yepyeni bir döneme girildiğinin ilk sinyalleri 1990'lı yılların başında verilirken, bu yeni kurulmakta olan ve pek çok belirsizliği de içinde barındıran yeni düzeni (kimilerine göreyse düzensizliği) tanımlayan yeni bir isim

bulmak henüz mümkün olmamıştır. Halen “Soğuk Savaş Sonrası Dönem” diye adlandırdığımız içinde bulunduğumuz dönemin, özü itibarîyle yapılandırılma aşamasında olduğu ve bir geçiş dönemini ifade ettiği düşünülmektedir (Bakan, 2007: 36). Güvenliğin yeniden tanımlanması ve güvenlik çalışmalarının uluslararası ilişkiler disiplini içerisindeki yeri, soğuk savaş sonrasındaki akademik gündemi oldukça meşgul etmektedir (Öztürk, 2014: 160).

Önceki dönemlerde güvenlik, daha ziyade sınırların ve ülke bütünlüğünün korunması anlamında kullanılıyordu. Bir ülkenin dış politika amaçları denildiğinde klasik anlamda var olmaya ilişkin amaçlardan sonra güvenlik ve hayati çıkar gibi amaçlar gelmektedir. Ancak günümüzde özellikle küreselleşmenin ve teknolojik gelişmelerin etkisiyle ülkeler arasındaki sınırların coğrafi olarak olmasa bile ekonomik ve siyasal açılardan netliğini yitirdiğini göz önünde bulundurduğumuzda, güvenlik denilince akıllara sadece sınırların korunmasının gelmeyeceği de açıktır (Bayır, 2013: 174).

1990’lardan itibaren insan güvenliği, güvenliğin değişen tanımı içinde merkeze oturdu, devletlerden uluslar arası kuruluşlara ve küresel sivil toplum hareketlerine kadar geniş bir yelpazede kabul gördü., benimsendi. Kavramın çıkış noktası güvenliğin ulusal güvenlikle bir tutulamayacağı, devletin çıkarlarının silah gücüyle korunmasına indirgenemeyeceği düşüncesidir. Buna göre, güvenliğin referans noktası “insan” olmalıdır; güvenlik siyasetinde devletlere değil, bireylerin refahına öncelik verilmelidir (Çalkıvık, 2014: 297).

Soğuk Savaş'ın sona ermesiyle klasik güvenlik anlayışı değişerek askeri gücün önceki dönemlere göre (özellikle de Avrupalı devletlerarasında) önemini yitirdiği vurgulanmıştır. Devlet-merkezli güvenlik anlayışı sorgulanarak birey-odaklı güvenlik tanımları yapılmaya başlanmıştır. Ulusal sınırlarına direkt bir askeri tehditten yoksun olan Avrupa'da yeni güvenlik gündemi, etnik-milliyetçiliğin körüklediği bölgesel çatışmalar, nükleer silahların yaygınlaşması sorunu, göçler ve ulus ötesi suçlar gibi çeşitli risk ve sorunlarla yoğrulmaktaydı. Devlet merkezli bir analizin gerekliliğini savunan Buzan'a göre devlete yönelen tehditler artık sadece askeri tehditler değildir. Devlet için üç temel tehdit vardır: devlet fikrine yani ulus-devletin ideolojik varlığına yöneltilen tehditler; devletin fizikî varlığına yani

vatandaşlarına ve temel kaynaklarına yöneltilen tehditler; devletin 3 kurumsal kimliğine ve yapısına yani siyasî sistemine yöneltilen tehditler (Bakan, 2007: 40).

1.1.3. Aberystwyth Okulu'nun Güvenlik Yaklaşımları

Soğuk Savaş sonrasında güvenliğin yeniden tanımlanması ve yeni teorik yaklaşımlarla yeniden tartışılması süresince güvenlik kavramı, geleneksel Uluslararası ilişkiler teorilerinin kavramı sıkıştırdığı devlet merkezli ve askeri güvenlik temelli kısır tartışmalardan birey güvenliğine kayan ve referans aktörleri, boyutları seviyeleri ve amaçları bağlamında hem genişleyen hem de derinleşen yeni bir güvenlik anlayışı ortaya çıkmıştır. Yeni güvenlik kavramı, güvenliğin sadece teorik olarak yeniden düşünülmesi ve tartışılmasından dolayı dönüşen bir kavram değildir. Aynı zamanda yeni güvenlik Soğuk Savaş sonrası dönemde küresel sorunlar, riskler, belirsizlikler ve potansiyel çatışmalar içeren dünya politikasının gündemine oturan birtakım ekonomik, siyasi, kültürel, çevresel vb. gelişmelerle şekillenen teori-pratik arasındaki ilişkinin varlığının da bir sonucudur. Bu bağlamda güvenlik kavramı, dünya politikasındaki gelişmeler ve Uluslararası İlişkiler teorilerinin içinde bulunduğu Dördüncü Büyük Tartışmanın teorik ve metodolojik yönelimleriyle şekillenmeye ve dönüşmeye devam etmektedir (Öztürk, 2014: 173).

Aberystwyth Ekolü'ne göre, problemlerin güvenlik algısı dışına çıkarılması bir çözüm değildir. Yapılması gereken "güvenliğin siyasiliğinin farkına varılması"dır. Aberystwyth Ekolü bu tezini üç temel esasa dayandırır. Bunlardan ilki, eğer sorunlar güvenlik meselesi olmaktan çıkarılırsa, güvenlik, insanların güvenliğine duyarlılık göstermeyen güvenlik elitlerinin tekeline bırakılmış olur. Siyasiliğini ortaya koymak ise, güvenlik politikalarının sorgulanmasını gerektirir. İkinci gerekçe, "etik-politik"dir. Geleneksel olarak güvenlik devlet ve devletin kaygıları ile ilgili olmuş olsa da, bu hep böyle kalacak değildir. Güvenliği insanların endişesini içerecek şekilde ele alma yoluna gidilerek ve tartışma, müzakere ve diyalog süreci yaratılarak ortak bir zeminde güvenlik kaygıları ele alınabilir. Burada analistin görevi ise, "sesi duyulmayanların sesinin duyulmasına yardım etmek" olmalıdır. Üçüncü argüman analitiktir. Yani "sorunu güvenlik dışına çıkarmak mı, yoksa siyasi boyutunu ortaya koymak mı" insanların ve devletlerin güvensizlik sorununu gidermek için çaredir. Bu husus ancak, sorunun "ampirik, tarihsel,

söylemsel olarak" ele alınması ile anlaşılabilir. Örneğin HIV/AIDS'in küresel güvenlik sorunu olarak ele alınması olumlu sonuçlar verirken, göç sorununun güvenlik söylemine yerleştirilmesiyle "tehlikeli yabancılar" olgusunu ortaya çıkarmıştır (Miş, 2011; 352)

1.1.4. Liberal Kuramların Güvenlik Yaklaşımları

Liberalizm batı siyasal düşüncesinde önde gelen ideolojilerden biri olarak siyaset biliminde önemli bir yere sahiptir. Bireyin kutsallığına ve hür teşebbüsün önündeki engellerin kaldırılması sonucunda toplum refahının artacağına dair olan inanç, liberalizmin en önemli özelliğidir. Liberalizm insanı odak noktasına alan akılcılığı ön plana çıkaran ve özel hayatın serbestliğinin ve kamusal alana sınırlı bir devlet müdahalesini öngören felsefi bir yaklaşımdır (Oğuzlu, 2014: 96).

Uluslararası alanda çatışmaların varlığına işaretle güç peşinde koşmayı meşru göstermektense insanların yaşadıkları kötü koşullara odaklanmak gereklidir. Liberaller bu kötü koşulları düzeltmek yoluyla barışın alt yapısının sağlanacağı ön görmektedir (Kegley ve Blanton, 2015: 36).

Felsefi düzlemde Avrupa kökenli ve aydınlanma düşüncesinin bir ürünü olan liberalizmde, temel aktörün kökeni "birey" olarak kabul edilmektedir. Bireyi toplumun bir faktör olarak gören liberaller, devleti tamamen dışlamayarak devletin ve her türlü siyasal iktidarın sınırlandırılması ve bireysel ham ve özgürlüklerin savunulması taraftarıdırlar. Sınırlı bir devlet anlayışına sahip olan liberalizm; özgürlük, bireysellik, eşitlik ve rasyonellik değerlerini temel almaktadır (Akgül, 2014: 43).

Uluslararası hukukçu R.Falk realist jeopolitikacı bakışın yol aştığı katliam ve kitlesel yoksulluğa dikkat çekmekte ve devlet düzeyinde güvenlik yerine daha az devletçi bir güvenlik anlayışı önermektedir. Günümüzde ulusal güvenlikten insan güvenliğine doğru bir anlayış değişikliğine geçiş yapılmaktadır. Devlet merkezli jeopolitik bakıştan insan refahı ve güvenliğe dayalı çoğulcu bir bakış açısına yönelim dikkat çekmektedir (Yılmaz, 2012: 150-151).

Liberal kurama göre iç meselelerde kullanılan çatışma-çözümü pratikleri uluslararası sorunlarda da kullanılabilir. Demokratik kültür içinde sosyalizasyon sürecini deneyimleyen siyasi liderler ortak bir hayat görüşüne sahip olmaktadır (Kegley ve Blanton, 2015: 44). Liberal yaklaşımlar gücü, en son başvuracak çare olarak algılamışlar ve uluslararası işbirliği, örgütlenme ve hukuk vasıtasıyla güvenliğin sağlanabileceğini öngörmüşlerdir (Demir ve Varlık, 2013: 85).

Liberal anlayışa göre, savaşın sebepleri; otokratik liderlerin egoist, kısa vadeli ve yanlış hesaplamalara göre hareket etmelerinde yatmaktadır. Demokratik kurumların bağlayıcılığından yoksun olan Almanya ve Avusturya'nın askeri sektörlerin baskısı ile savaşa girdiklerini, İngiltere ve Fransa'nın ise askeri ittifaklar sisteminin içine girmeleri ile savaşa çekildiklerini ileri süren liberal görüşün barış önerileri, Wilson'ın savaş sonrası düzene dair önerilerinde somutlaşmıştır. Uluslararası alanda yaşanan değişimlere uyum sağlayarak değişim gösteren liberal yaklaşımların Uluslararası İlişkiler'e dair en temel tanımlayıcı unsurlarının çıkarların uyumu ve işbirliği olduğu görülmekte ve bu unsurlar çeşitli liberal yaklaşımlar tarafından farklı şekillerde vurgulanmaktadır (Akgül, 2014: 68).

1.1.5. Marksist Kuramların Güvenlik Anlayışı

Uluslararası İlişkiler disiplini içerisinde Marksizm'in bir ferdi olarak ele alınması belirli sorunlar barındırmaktadır. Marksist düşünce çerçevesinde teorik üretimde bulunan okullardan hangilerinin "Uluslararası İlişkiler Teorisi" başlığı altında alınacağı tartışmalı ve o kadar da belirsizdir. Bu nedenle Marksist yaklaşımlar, doğrudan uluslararası ilişkilerin ana akım yaklaşımları ile ortaklık taşıyan ve genellikle devletlerarası ilişkileri merkezine alan teorisyenlerin çalışmaları ile sınırlandırılma eğilimindedir. Gerçekte, Marksist kuramın ortaya çıktığı tarihsel koşullarda dahi, Marx ve takipçileri kapitalizmi küresel bir sistem olarak görmekteydi. Bu nedenle Marksizm, ulusal sınırlar ve uluslararası ilişkiler arasında kökten bir ayrım yapmayı reddederek kapitalizmin dinamiklerini bu ikisi arasındaki geçişlilik ve karşılıklı etkileşim üzerinden ve ekonomi politik bir yaklaşımla analiz etme gayretini taşımaktadır (Uğurlu, 2014: 89).

Marx'a güre üretim araçların elinde bulunduran ve maddi güce sahip olan sınıf aynı zamanda tinsel güce de egemendir. Yani yükselen her sınıf kendi çıkar ve beklentilerini toplumun çıkar ve beklentileri gibi sunar. Bu durumda kendi çıkarlarına yönelik tehditleri yaygın bir tehdit gibi göstererek ya da kendi çıkarlarının güvenliğini toplumun güvenliği gibi sunarak kolektif güvenlik politikaları içinde aslında sınıfsal çıkarların güvenliği güdülecektir. Yine bu durumda devlete getirilen tanım ve görevde son derece önemlidir. Çünkü devleti sınıflar üstü toplumsal çatışmaların ötesinde bağımsız bir varlık olarak sunmak ekonomik ilişkiler kökenini silip ortadan atmak demektir. Devleti bu şekilde tanımladığınızda tarafsız devletin algıladığı tehditler ya da bu tehditlere yönelik geliştirilen güvenlik siyasalarının toplumun tümüne ait yaygın korumacılık politikaları gibi görülmesi sonucunu çıkartır. Oysaki Marx'a göre devlet egemen sınıfın egemenliklerini devam ettirmelerinin bir aracı olmaktan başka bir şey değildir. Hatta bu durumda devletin ve hukukun bağımsızlığı iddiaları arttıkça devletin ve hukukun belli bir sınıfın organı olması da artar (Birdişli, 2011;164).

1.1.7. Kopenhag Okulu'nın Güvenlik Yaklaşımları

Kopenhag Okulu'nun temeli 1985'te Kopenhag Üniversitesi bünyesinde kurulan "Barış ve Çatışma Araştırma Merkezi'nde Avrupa Güvenliği çalışma grubunun "Avrupa Güvenliği'nin Askeri-Olmayan Boyutları" başlıklı projesinin oluşturulmasıyla atılmıştır. İşlevsel açıdan, Kopengah Okulu sektörel bir analiz çerçevesi oluşturarak, güvenliği askeri, ekonomik, çevresel, toplumsal ve siyasi sektörde ele almakta, yani güvenlikleştirme teorisini bu beş sektöre uygulamaktadır (Açıkmeşe, 2014: 251).

Uluslararası güvenlik tanımını askeri açıdan değerlendirilmemiş, daha farklı alanlarda değerlendirme yapılmıştır. Bu kapsamda politik, ekonomik, çevresel etkenler dikkate alınarak çalışmalar yapılmıştır. Güvenlik anlayışı sadece devletlerin değil bireysel anlamda güvenlikte gözden geçirilmiş ve devlet dışında bir güvenlik anlayışının da olması gerektiği açıklanmıştır. Devletin dışındaki unsurlara yer verilmiştir (Çoşkun, 2014: 181).

Kopenhag Okulu, ilk çalışmalarında geleneksel güvenlik anlayışını sorgulamaya çalışmıştır. Bu durumu en iyi özetleyen satırlar Wæver‟a ait olarak şu şekilde özetlenmiştir: Kopenhag Okulu klasik ve güce dayalı, devlet merkezli güvenlik anlayışının ötesinde, devlet dışı aktörleri de içine alacak bir güvenlik anlayışı ile güvenlik kavramının geleneksel sınırları dışına çıkmaması gerektiğini savunan, tutucu bir güvenlik anlayışına ek ve üçüncü bir yol olarak doğmuştur. Kopenhag Okulu‟nun en belirgin yönü "güvenlik" kavramını daha geniş ve sosyal bir tabana yaymasıdır. Kopenhag Okulu‟nun güvenlik çalışmaları üç temel nokta üzerinden yükselmektedir. Bunlardan ilki güvenliğin alanını belli kıstas ve sınırlara göre daraltmaya yarayan (aynı zamanda toplamda bize daha geniş bir güvenlik alanı sunan) "sektörler" olarak karşımıza çıkar. İkinci olarak ise bölgesel güvenlik kompleksleri ve son olarak ise güvenlikleştirmedir (Zora, 2015:118).

1.1.8. Eleştirel Kuramın Güvenlik Anlayışı

Uluslararası ilişkiler alanında siyaset bilimi alanında olduğu gibi diğer güvenlik anlayışlarından biride eleştirel yaklaşımdır. Klasik yaklaşım objektif güç ve güç kaynakları konularının yanına güç kimin için, güce ilişkin amaçlar nelerdir, ne tür bir yapı söz konusu ve bu yapıda özendiriciler ve sınırlamalar nelerdir ve benzeri sorularına ağırlık vermektedir (Yılmaz, 2012: 155).

Uluslararası siyaseti ancak uluslararası ilişkiler olarak ele almanın mümkün olabileceğini savunan yaklaşımların çoğunun temelinde, uluslararası ilişkileri sadece ülkeler arasındaki bir ilişkiden ibaret olmayıp ülkelerin iç yapılarındaki iktidar ve sivil toplum ilişkilerini de kapsadığı varsayımı vardır. Günümüz uluslararası siyaset literatüründeki hâkim anlayışa karşı eleştirel bir nitelik taşıyan, uluslararası sorunlara sosyolojik yaklaşım ya da uluslararası ilişkiler sosyolojisi, dünyanın, ulusal kültür kadar homojen olmasa da bir küresel kültüre sahip olduğu varsayımından hareket etmektedir (Sönmezoğlu, 2002: 22).

1995'ten günümüze dördüncü evresinde olan Güvenlik Çalışmalarını tanımlarken Eleştirel Güvenlik Çalışmaları başlığını kullanmak daha doğru olur. Eleştirel Güvenlik Çalışmaları, Mayıs 1994'de Kanada'nın Toronto kentinde düzenlenen uluslararası bir konferansta Soğuk Savaş sonrası dönemde güvenlik

çalışmalarını eleştirel bir yaklaşımla ele alan bir grup akademisyenin entelektüel yolculuğunun neticesinde ortaya çıkmıştır. Krause ve Williams'ın topladığı ve 1997 yılında basılan Critical Security Studies: Concepts and Cases başlıklı kitap disiplinde farklı bir dönemin açılmasını sağlamıştır. Buzan, Waever, Booth, Ayoob, Walker ve Erikson gibi teorisyenlerin çalışmaları ile genişleyen eleştirel güvenlik yaklaşımı, devlet-merkezli olmayan, eleştirel teoriye yaslanan ve post-pozitivist metodolojik yaklaşımı esas alan bir yaklaşımdır (Bakan, 2007: 41).

Eleştirel Güvenlik Çalışmaları, güvenliğin sadece genişletilmesi değil, aynı zamanda güvenlik kavramının derinleştirilmesi amacını da taşımaktadır (Öztürk, 2014: 170-171). Eğer eleştirel güvenlik kuramının egemen terimi *eleştirel* ise onun yönetimi altındaki coğrafya da *güvenlik*'tir (Booth, 2012: 122).

Eleştirel kuramın önemli isimlerinden Robert Cox'un "teoriler birileri içindir ve bir amaca hizmet eder" önermesi, güvenlik yaklaşımlarının da öznel ve göreceli bir doğaya sahip olduğunu ortaya koymaktadır. Eleştirel kuramcılar, güvenliğin "kimin için olduğu" ve "hangi çıkarlara dair bir tehdit algısıyla şekillendirildiği" sorularını yönelterek kavramın göreceliliğine vurgu yapmaktadır. Onlara göre klasik güvenlik anlayışı, güvenliği sadece belirli özneler, çıkarlar ve tehdit algıları ile ilişkilendirmekte ve kavramı sınırlı bir perspektifte ele almaktadır.51 Örneğin neo-realist kuram, devlet ve uluslararası sistemi özne olarak belirlemekte; ulusal çıkar kavramını devletin bekası ve prestijiyle özdeşleştirerek devlet merkezli bir güvenlik perspektifi sunmaktadır. Eleştirel bir düzlemde düşünüldüğünde neo-realizmin ortaya koyduğu bu yaklaşım güvenliği sadece devlete özgü kılarken hem tek-tip bir güvenlik kavramı yaratmış, hem de kavramın sübjektif olması nedeniyle çatışma ve güvenlik ikilemini kalıcı hale getirmiştir (Sandıklı ve Emeklier, 2014:24).

1.1.9. Postmodern Kuramın Güvenlik Anlayışı

Postyapısalcılık, Uluslararası ilişkiler kapsamında 1990'ların başından beri etkisi altına aldığı ve günümüze kadar etkisini taşımış, dünya politikasını süregelen doğal yapısı ve düzenin dışında güvenlik, devlet, dış politika gibi ana temalarının yeniden değerlendirmesi gerektiğini savunan bir yaklaşım olmuştur (Kardaş ve Erdağ, 2014: 379).

Postmodern kuramın öncülerinden olan Ashley ve Walker günümüz uluslararası ilişkilerinin teori ve pratiğinde bilgi ve gücün birbirinden ayrılmaz bir şekilde bağlı olduğunu belirtmektedir. Onlara göre uluslararası ilişkiler araştırmacıları hep ulaşılamayan bir idealin peşinde, devlet idaresi pratiklerini açıklayabilecek ve yenilik önerebilecek, güç oyununun ötesinde bir felsefi temel arayışındadırlar. Ashley ve Walker'e göre teori ve pratik arasındaki model ayrımın yerini "söylem" almış ve bu terim gerçeklik ve onun metinsel temsili arasındaki ikilemliği bulanıklaştırmıştır (Griffiths vd., 2011: 250).

Post-yapısalcılığın yapısalcılığa getirdiği en temel eleştiri, yapısalcı yazarların aydınlanma düşüncesinin ve yapı kavramının sınırlarını yeterince zorlamamalarıdır. Post-yapısalcılar a göre Saussure'ün dil ile arasında kabul ettiği bağlayıcı ilişkiyi yalnızca dil biliminin sınırları içerisinde tutmak anlamsızdır. Zira toplumsal olan her şeyin dil, kültür, pratik, öznellik ve bizzat toplum nedensiz ve uzlaşımsal olduğu post-yapısalcıların temel iddiasıdır. (Ongur, 2014: 180).

Postmodern kuram, küreselleşme ile eş zamanlı biçimde yaşanan kavram ve olgulardaki dönüşüme dikkat çekmektedir. Küreselleşmenin etkisiyle karşılaşmaların sıklaşması, zıtlıkları birbirine yakınlaştırırken çatışmaları da artırmaktadır. Örneğin klasik dost-düşman ayrımı, geçmişte belirli sınırlar içinde algılara yerleştirilmişken, bugün dost düşman tanımının yapılması daha zorlaşmaktadır. Risk ve tehditlerin daha karmaşık hale geldiğini ve belirsizliklerin kesin yargıların önüne geçtiğini söylemek mümkündür. Klasik güvenlik yaklaşımları, günümüz kriz ve kaoslarını yorumlamada ve kronikleşmiş sorunlara çözüm üretmede yetersiz kalmış; klasik paradigmanın temel araçları ise güvenliğin tesisi ve mevcut düzenin korunmasında işlevselliğini kaybetmeye başlamıştır. Kısacası postmodern düşünürler; zaman-mekân sıkışması neticesinde farklı kimliklerin artan bir ivmeyle çatıştığını, kimliksel farklılıklar arasında bir uzlaşma zemini aranmasına rağmen yaşanan iletişim devrimiyle ötekileş(tir)menin ve önyargıların giderek belirginleştiğini ve bu belirsizlikler dünyasında realist söylem ve imgelerin klasik güvenliği sağlamak adına otoritesini korumaya çalıştığını belirtmektedir (Sandıklı ve Emeklier, 2014:33-34).

1.1.10. Feminist Kuramın Güvenlik Anlayışı

Toplumsal cinsiyetin uluslararası ilişkiler teori ve pratiğindeki rolü, feminizmin sosyal bilimlerin diğer dallarındaki baskın konumuna rağmen 1980'lere kadar görmezlikten gelinmiştir. Bir grup feminist düşünür eleştirel görüşlerini bu zamana kadar cinsiyet körü olan bu alana yönelttiklerinden bu durumu artık geçerli değildir. Bununla birlikte, feminist devlet eleştirilerinin ve feminist siyaset teorisinin cinsiyetleştirilmiş doğasının kendilerini uluslararası ilişkiler alanında göstermeleri de kaçınılmazdı. Soğuk savaşın bitişi "kimlik politikaları"nın geri dönüşüm ve 1980'ler boyunca uluslararası ilişkiler alanında pozitivizmin sürekli eleştirilmesiyle, toplumsal cinsiyetin uluslararası ilişkilerdeki rolünü inceleme fırsatı birçok feminist düşünür tarafından değerlendirilmiştir (Griffiths vd., 2011: 279).

Feminizmin kuramsal birikiminin karmaşıklığı ve feminizm çatısı altında toplanan yaklaşımların çeşitliliği feminizmin genel bir tanımının yapılmasını zorlaştırsa da temelde toplumda erkeğin lehine olan güç ilişkilerinin kadını ezdiğini ve ikincilleştirdiğini savunur (Egbatan ve Şahin, 2014: 251). Feminist teorisyenler güvenlik başta olmak üzere aslında uluslararası ilişkiler teorilerinin tanımladığı tüm temel kavramlarının (güç, egemenlik, insan doğası, ulusal çıkar, devlet, siyaset vb.) birey toplumsal yapı olduklarını ve eril değerler temelinde tanımladıklarını ileri sürmektedirler. Bu bağlamda, Feminist teoriye göre savaş ve şiddet ile şekillenen uluslararası güvenlik anlayışı aslında özünde toplumsal cinsiyet temelli bir önyargı içermektedir. Güvenliğin eril temelde yapılandırılması sonucunda hegemon olan güçler güvenliği diğerlerinden ayrı ve özerk olmak diğerlerine zarar verebilme kabiliyetine sahip olmak ve güvende olmak olarak tanımlamaktadır (Öztürk, 2014: 166).

Tüm feminist kuramcılar (radikal ekol hariç) sabit bir kadın doğasıyla ilgili varsayımlara meydan okur. Ataerkil toplumda annelik ideali ne kadar şerefli olursa olsun, bu, yine de onu mutfak ve beşiğe bağlı halde şerefli olursa olsun, bu, yine de onu mutfak ve beşiğe bağlı halde bırakmanın bir başka yoludur. Maddi unsurları vurgulayan feminist bakış açıları "kadın" terimini kullanma bir sorun görmezken, post-yapısalcılar kendilerini düğümlerle bağlayabilirler (Booth, 2012: 270).

Enloe'nin feminist bir merakla sorduğu "Kadınlar nerede?" sorusunu uluslararası ilişkiler disiplininin en temel kavramlarından olan güvenlik ve onunla bağlantılı olarak barış, savaş ve şiddet kavramlarını yeniden düşünmek açısından önemli bir yol açar. Kadınların hem güvenlikten etkilenen hem de bu alanı etkileyen aktörler olarak göz ardı edilmesi güvenlik alanının erkek egemen oluşunun bir göstergesi olarak kabul ediliyor. Feministler, güvenlik alanındaki ataerkil yapıyı sorgulayarak daha kapsamlı bir güvenlik ve barış anlayışı geliştirmek için çabalarlar (Egbatan ve Şahin, 2014: 261).

1.2. KAVRAMSAL BOYUTTA SİBER

Tarihçiler, tarih öncesi dönemleri insanoğlunun aletleri/araçları (teknolojiyi) kullanma durumuna göre adlandırmışlardır: Yontma Taş Devri, Cilalı Taş Devri, Maden Devri gibi. Tarihsel devirleri de dünyanın kaderini değiştiren veya şekillendiren olaylarla isimlendirmişlerdir: İlkçağ, bulunuşuyla başlarken, Yeniçağ, İstanbul'un fethiyle başlamıştır. En son tanımlanan Yakınçağ, Fransız İhtilali'nden bugüne dek geçen sürenin adıdır. Henüz resmi olarak tanımlanmamış olsa da 20. yüzyılın son çeyreğinden itibaren farklı bir çağa girdiğimizi söylemek yanlış olmayacaktır: "internet çağı" (Arıcak, 2015: 13).

İnsanlık tarihini incelediğimizde, 21'inci yüzyılda geldiğimiz nokta, akıl almaz bir hızla sürmekte, ürün pazara sunuluncaya kadar güncelliğini yitirebilmektedir. Bu sürecin gelişimindeki en temel etken ise doğru bilgiye zamanında erişim ve bu bilginin etkin kullanımıdır. Donanım ve yazılımlar vasıtasıyla cihazların birbirine bağlandığı alana siber ortam veya siber uzay (cyberspace) olarak adlandırılmaktadır. Geçmiş dönemde sadece bilgisayarların bağlı olduğu siber uzay, mobil cihazların daha fazla kullanılmasıyla birlikte daha geniş bir alana yayılmıştı. Artık hemen hemen her kullanıcı, siber uzayda tüm gün boyunca farkında olmadan güvenlik tehlikesiyle karşı karşıya kalmaktadır. Bir başka ifadeyle, siber uzay daha geniş alanlara yayıldıkça, yapılan saldırıların sayısı ve şiddeti de aynı şekilde daha da büyümektedir (Keleştemur, 2015: 128).

Bir ulusun güvenliği daima, o dönemde mevcut askeri teknolojinin türüne ve seviyesine bağlı kalmıştır. Teknolojiyi değiştirdiğiniz takdirde bir ülkenin kendisini korumak için yapması gereken şeyleri de değiştirmiş olursunuz. Modern Avrupa'nın kurulduğu ilk dönemlerde toplar, büyük egemen krallıkların, küçük Ortaçağ prensliklerini nasıl yok edebildiğini gösteriyordu. Kale duvarları artık yıkılıp yok edilebiliyordu. Modern çağda barutun ortaya çıkmasıyla birlikte iki yeni askeri kol olan topçu sınıfı ve piyade sınıfının oluşmasını sağladı. Toplar taş duvarları yıkarak, piyadelerin içeriye girmesine yardımcı oluyordu. Devletlerin gücü artık, nüfuslarının ne kadar kalabalık, ekonomilerinin ne kadar sağlam olduğuna bağlıdır. Monarjiler arasında rekabet, Asya ve Amerika kıtaları dâhil başka yerlere yayılıp o bölgelerin keşfedilmesini sağladı. Günümüz çağında nükleer silahların, haberleşme ve ulaşım teknolojilerinin, özellikle savaşlar üzerinde büyük etkileri olmuştur. Buna askeri işlerde devrim adı verildi (Roskin ve Berry, 2014: 278).

İnternet içerisinde fazla sayıda güvenlik üzerine yazılmış makale bulunmasına karşın, internet kullanıcıları üzerinde yeterli bilinç oluşmamıştır. Bunun en büyük nedeni, internetin denetimsiz bir şekilde büyüyor olmasıdır. Bundan dolayı internete bağlanmış her bilgisayar, başka cihaz ve sistemlere saldırı yapmak için köle (kurban) bilgisayar olarak kullanılabilmektedir. Bu durum, milli güvenlik açısından da önemli bir tehdit oluşturmaktadır. Bulunduğumuz dönemde klasik olarak kara, deniz, hava ve uzay dışında "siber uzay"da birinci sınıf dünya ülkeleri tarafından yeni bir savaş alanı olarak kabul görmüş durumdadır (Keleştemur, 2015: 128).

Körfez Savaşları'nda kara ve hava sahalarında meydana gelen silahlı çatışmaların tümü elektronik hale gelmiştir. Kullanılan insansız hava araçları, hassas güdümlü mühimmat, küresel konum belirleme sistemleri, haberleşme ağları, bilgisayar dönemin teknolojik olarak en üst düzeydeki cihazlarıydı. Bazıları tarafından Amerika Birleşik Devletleri'nin yapması gereken tek şey 20 yıl boyunca teknoloji önderliğini devam ettirmek, böylece bir daha asla saldırıya uğramayacağını değerlendirilmektedir. Bu tehlikeli varsayımdır. 11 Eylül'de Amerika, kendi teknolojinin nasıl kendisine karşı kullanılabildiğini öğrenmiştir. Teknolojiler, devletlerin kendileri korumak için kullandıkları stratejileri de kullanırlar. Ulus-Devletlerin varlıklarını sürdürebilmeleri, etrafı duvarlarla çevrili şehirlerin yaptığı

gibi, kendini koruma yetenekleriyle doğru orantılıdır. Artık kendini koruyamadığı zaman, ulus-devlet yok olacaktır (Roskin ve Berry, 2014: 278).

1.2.1. Siber

Bilim dünyasındaki gelişme bilgiyi, fiziksel dünyadan elektronik dünyaya doğru hızlı bir şekilde taşımaktadır. Siber sözcüğü "sibernetik" sözcüğünden kısaltılmıştır. Amerika'da Weiner isimli bir bilim adamı hayvanlarda ve makinalarda iletişim ve kontrol bilimini tanımlarken "sibernetik"i kullanmıştır. Gelişen teknoloji ve iletişim unsurlarının etkisiyle iletişimi kontrol edebilme ve yönlendirme, internet ve bilgisayarla ilgili olarak "sibernetik" kullanılmıştır. Türkçe'de bu tanımın karşılığı "bilişim" sözcüğü ile ifade edilmiştir (Çakmak ve Altunok, 2009: 25-26).

1.2.2. Siber Ortam

Siber ortam; internet, iletişim ağları, gömülü prosesler, bilgisayar sistemleri ve kontrol birimlerini de kapsayan ve kendi aralarında bağımlı olan bilgi teknolojisi altyapıları tarafından meydana gelen küresel ortam olarak tanımlanmaktadır (Ünal, 2015: 134).

Dünyanın içinde yer aldığı sonsuz boşluk olan uzay siber ortam terimi ilk defa ABD'li yazar Gibson tarafından ifade edilmiştir. Bu terim 1982 yılında yayımlanan "Burning Chrome" adlı hikâye kitabında kullanılmıştır. Gibson, siber uzayı; tasarladığı karakterler için şifre maksadıyla "çağrışım yapan ve özellikle anlamsız" bir terim olarak tanımlamıştır. Bu kelimeleri yazarken "şifre, sıfır, önemsiz şey" anlamına gelen "cipher" kelimesi ile "cyber" kelimesinin okunuşundaki benzerlik dikkat çekmektedir. Siber ortamın tanımı da diğer birçok kavramın tanımında olduğu gibi farklı zamanlarda farklı şekillerde yapılmıştır. Beyaz Saray'ın 2003 yılındaki tanımı "Siber ortam kritik alt yapılarımızın çalışmasını sağlayan birbirine bağlı yüzbinlerce bilgisayar sonucu yönlendirici, anahtar ve fiber optik kablolardan oluşur." ABD Savunma Bakanlığı'nın 2006 yılındaki tanımı "İletişim ağı ile birbirine bağlanan sistemlerde veri saklama değiştirme ve iletme amacıyla elektronik ve elektromanyetik spektrumun kullanıldığı alanlar." ABD Savunma Bakanlığı'nın 2013 yılındaki tanımı "internet iletişim ağları

bilgisayar sistemleri gömülü işlemci ve kontrol bilimlerin içeren bilgi teknolojileri ve alt yapılarından meydana gelen birbirine bağımlı ağların oluşturduğu bilgi ortamdaki küresel bir alandır.” AB Komisyonu'nun 2013 yılındaki tanımı “Dünya çapında kişisel bilgisayarların elektronik verilerinin dolaştığı sanal ortamlar.” NATO'nun 2015 yılındaki tanımı ise “bilgisayar ağları kullanarak veri saklama değiştirme ve takas etme amacıyla bilgisayarların ve elektromanyetik spektrumun kullanıldığı fiziksel ve fiziksel olmayan bileşenlerden oluşan ortamdır” (Çiftci, 2017: 3).

İnsanoğlu tarihinden günümüze kadar ülkeler birçok alanda savaşmıştır. Kara, deniz, hava ve 1957 yılının başlarında dördüncü savaş ortamı “uzay” olarak kabul edilmiştir. Bu dört savaş sahasının her birinin kendi özellikleri ve gerekleri bulunmaktadır. 21. Yüzyıla girildiğinde bu dördüne beşinci savaş ortamı eklenmiştir, “siber ortam” (Yayla, 2013: 183).

Siber kelimesi Türkçeye Fransızcadan geçmiş olup, eski Yunancadaki “Kübernetes” sözcüğünden türetilmiş sibernetik kavramından gelmektedir. Sibernetik kavramı ise “ teknolojik, biyolojik, sosyolojik ve ekonomik sistemler de, kumanda uç iletişim sistemlerini incelemeye dayanan bir amaca doğru yönlendirilmiş etki bilimi” şeklinde adlandırılmıştır (Bayraktar, 2015: 13).

İngilizcede genellikle siber uzay (cyberspace) olarak kullanılan kavram Türkçede siber ortam olarak karşılığını bulmuştur. Siber uzay, “verinin elektronik ortamda hazırlanması ile başlayan ve dünyanın her alanına yayılmış olan iletişim unsurlarıyla erişim sağlanan alanın tamamı” olarak tanımlamıştır. Amerikan Hava Kuvvetleri’ne göre siber ortam, “ağ sistemleri ve fiziksel yapılar üzerinde veri depolamak, değiştirmek ve geliştirmek maksadıyla elektronik ve elektromanyetik spektrumun kullanılması” olarak tanımlanmıştır (Çakmak ve Altunok, 2009: 27).

Siber uzay ilk olarak ve en başta bir bilgi ortamıdır. Yaratılan saklanan ve en önemlisi paylaşılan dijital verilerde oluşmaktadır. Bu durum onun sadece fiziki bir yer olmadığından fiziksel olarak ölçülmesine karşı durmaktadır. Siber uzay sadece sanal olarak değil verileri saklayan bilgisayarlara ilave olarak bunların yayılmasını sağlayan sistem ve alt yapılarını birleştirmektedir. İnterneti genellikle dijital dünya için kısaltma olarak kullanılırken siber uzay ayrıca bilgisayarların arkasındaki

kişilerin ve onların bağlantılarının toplumu nasıl değiştirdiğini de kapsamaya başlamıştır (Singer ve Friedman, 2015: 18-28).

Amerika'nın Savunma Bakanlığının terimler sözcüğünden siber alan: "işlemci ve kontrollerin yer aldığı internet telekomünikasyon ağları ve bilgisayar sistemlerinde içine alan birbirine bağlı bilgi teknolojileri altyapıların bulunduğu küresel bir ortam" olarak tanımlanmaktadır (Gürkaynak ve İren, 2011: 265).

Siber uzayın objesel, hibrit bir yapısı da vardır. Siber uzay sadece internetle sınırlandırılamayacak bir yapıdır. Bu standart protokoller kullanarak birbirleriyle haberleşen küresel bilgisayarlar, alanı bulunduran internet sadece birbirini tanıyan bilgisayarların haberleştiği kapalı internetler, hücresel teknolojiler, fiber optik kablolar, uzay temelli telekomünikasyon ve hatta kablolu telefon ağları ve televizyonlarda siber uzayı oluşturan bir bütünün parçası olarak karşımıza çıkmaktadırlar. Siber uzayın geçmişi insan-makine temelli haberleşme araçlarının kullanımı kadar eski bir tarihe dayandığı da belirtilmektedir. Uluslararası ilişkilerde realist bir bakış açısıyla "Güç, istediklerini elde edebilmek için başkalarını etkileme yeteneğidir. Bu yetenek zor güç kullanımı (hard power) ile de yumuşak güç (soft power) ile de gerçekleştirilebilir. Siber uzay bunu gerçekleştirmek için yeni bir alan yaratmaktadır. Siber güç siber uzayda kullanabileceği gibi siber enstrümanlar siber uzayın dışında da kullanılabilmektedir" (Demircioğlu, 2014: 40).

Siber uzay; bilginin adlandırılması, kaydedilmesi, ulaştırılması amacıyla ağ merkezi sistemler ve elektromanyetik spektrumun kullanılması suretiyle oluşturulan, internet ve benzeri haberleşme ağlarında kapsayan bir ortam olarak adlandırılmaktadır. En geniş anlamıyla siber uzay bilişim ve iletişim ağlarını şekillendiren uzayı ifade etmektedir. Siber uzay bilginin tanımlanması, kaydedilmesi, iletilmesi maksadıyla ağ merkezli sistemler ve elektromanyetik spektrumun kullanılması suretiyle oluşturulan internet ve benzeri haberleşme ağlarını da kapsayan bir ortam olarak adlandırılmaktadır. En geniş tanımıyla siber uzay bilişim ve iletişim ağlarını şekillendiren uzayı ifade etmektedir (Bayraktar, 2015: 13).

Siber alan için genel anlamda herkes tarafından kabul edilen bir tanımlama yapılamamıştır. Haberleşme ve iletişim teknolojilerinde gelişmiş ülkelerin önünde yer alan Amerikanı'nın Savunma Bakanlığı tarafından yayınlanan terimler sözlüğünde siber alan; "işlemci ve kontrolörlerin bulunduğu internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan" olarak tanımlanmaktadır. Aslında belirtilen bu alan fiziki ve somut bir alan değildir. Kısaca stenografik yazım şekliyle gösterilen siber alan; birlikte işleyerek bilgi akışı sağlayan bilgisayar ağları ve telekomünikasyon sistemlerinin bulunduğu w*orld wide web* (www.) olarak tanımlanabilir. Başka bir tanım ise ABD Kongre Araştırma Merkezi tarafından yapılmıştır. Buna göre siber alan; "insanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumudur" (Gürkaynak, İren, 2011: 265)

Siber uzay; içerisinde bilginin çevrim içi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağlarının (ve arkalarındaki kullanıcıların) âlemidir. Siber uzay ilk olarak ve en başta bir bilgi ortamıdır. Yaratılan, saklanan ve en önemlisi paylaşılan dijital verilerden oluşmaktadır. Bu durum onun, sadece fiziki bir yer olmadığından fiziksel olarak ölçülmesine karşı durmaktadır. Siber uzay bilgisayarların internetini, kapalı intranetleri, hücresel teknolojileri, fiber-optik kabloları ve uzay tabanlı iletişimi kapsamaktadır. 2008'de yılında Pentagon siber uzayın tanımında onu interneti de içeren bilgi teknolojileri altyapılarının bağımsızlık telekomünikasyon ağı bilgisayar sistemleri ile gömülü işlemciler ve yöneticileri içeren bilgi ortamı dâhilindeki küresel alan olarak tanımladılar (Singer ve Friedman, 2015: 18-28).

1.2.3. Siber Güvenlik

Siber güvenlik siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi, yaklaşımları, faaliyetler, eğitim ve teknolojiler bütün olarak açıklanmaktadır. 2016-2019 Ulusal Siber Güvenlik Stratejisi Belgesinde, siber güvenlik, "Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını ve ortamda işlenen bilgi/verilerin gizlilik, bütünlük ve iş birliğinin güvence altına alınmasını, saldırıları ve siber güvenlik olaylarının tespit edilmesini,

bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşını, siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder" şekilde tanımlanmıştır. Siber güvenlik kurumunun amacı kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik güçlerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesinin sağlanmasıdır. Siber tehditler/riskler birçok gelişmiş ülke tarafından milli güvenliğe karşı en büyük tehditler arasında görülmeye başlanmıştır. ABD eski başkanı Barack Obama; siber tehdidi millet olarak karşı karşıya kalınan en ciddi, milli ve ekonomik güvenlik tehditlerinden biri olarak nitelendirilmiş ve siber güvenliğin önemini vurgulamıştır. Siber güvenlik kurum kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlar (Çiftci, 2017; 8).

1.2.4. Siber Saldırı

Siber saldırılar bilgilere veya komuta sistemlerine yönelik olmak üzere iki şekilde yapılmaktadır. En sık karşılaşılan eylem türleri bilginin çalınması ya da bozulmasına yönelik yapılan işlemlerdir. Komuta/kontrol sistemleri ile ilgili olarak kullanılan fiziksel alt yapıyı yok etme, çalışamaz durumu getirme maksadıyla yapılmaktadır. Siber saldırılar kendi içerisinde belli başlıklar altında değerlendirildiğinde; E-postaların eklerine virüs yerleştirilerek yapılan saldırılar, kamu hizmetlerinin görülmemesini sağlama, iletişim araçlarına aşırı yükleme yaparak çalışamaz bir hale getirme, propaganda yapmak maksadıyla devletlerin veya ticari kuruluşların internet sayfalarının çalışamaz hale getirme, bilgisayar sistemlerine yetkisiz girişler yapılarak kişisel bilgilerin elde edilmesi olarak açıklanmakladır (Çakmak ve Altunok, 2009: 29-30).

İlk bilgisayarlar üretilmesinden itibaren bilgisayarı çok iyi kullananlara verilen bir isimdi hacker kelimesi. Değişmeyen tek şey değişimdir, sözünün bir örneği olarak zamanla değişen bu kelime günümüzde çoğu kaynak tarafından bilgisayar ve ağ sistemlerine zarar veren kişi olarak tanımlanmaktadır. Türk Dil Kurumu'nun "hacker" tabiri ise bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde kanun dışı, zarar verici işler yapmak için kullanan kişi olarak tanımlanmaktadır (Bülbül ve Bingöl, 2017: 15).

Siber saldırılar, yetkili hükümet organlarının yasal veya kanun dışı kuruluşların, teröristlerin şirketler veya şahısların, stratejik, operasyonel ve taktik gayelerini oluşturmak için siber ortamda uyguladıkları saldırı faaliyetlerdir. Siber saldırılar siber ortamda çalışan yazılım, donanım ve altyapıyı hedef almaktadır. Bir siber saldırının oluşumda temel bazı hususlar vardır. Siber saldırının en temel elemanları ise şunlardır:

Amaç; saldırganların amaçlarında bazı değişiklikler olabilir, teknik özelliği olmamasına rağmen amaç saldırının analizi için göz önünde bulundurulması gereken bir boyuttur.

Saldırı şekli; saldırılar, aktif veya pasif olabilmektedir. Aktif saldırılar, hedef sisteme nüfus etme veya onu devre dışı bırakma yöneliktir. Pasif saldırılar ise, sıklıkla hedef sisteminin davranışlarını, bilgi akışını, zamanlamasını ve diğer karakteristik özelliklerini gözlemlemeye yöneliktir. Etkiler; saldırıların etkileri tacizden hırsızla sistemin dar anlamda değişiminden büyük ölçüde bozulmasına kadar değişebilir. Ahlakilik ve yasallık; faaliyet ve etkiler mevcut yasalara göre yasal veya yasadışı olabilmektedir. Aynı zamanda hedef alınan bilginin sahibinin kişilik haklarının da ahlaki açıdan göz önünde bulundurulması gerekmektedir. Sahip olunan diğer mülklerin aksine bilgi sahibinin haberi olmadan paylaşılabilen kötüye kullanılabilen veya çalınabilen bir mülktür (Çiftci, 2017; 151).

Son zamanlarda gerek bireysel gerekse kamu kuruluşlarının bilgisayarlar ve cep telefonları başta olmak üzere diğer kurumlara ve bireylere yönelik siber saldırı olaylarında büyük artışın olduğu görülmektedir. Başka bir ifadeyle siber saldırılar, gündelik hayattaki zorbalığın online ortama taşınmış halidir. Saldırılarda temel amaç, kişi ya da kişilerin, şirketleri maddi-manevi şekilde küçümsemek, zor duruma düşürmek, şifresini ele geçirmek, virüs taşıyan mesajlar gönderilerek elektronik saldırı faaliyeti gerçekleştirmektir. Bazen de ticari amaçlı olarak saldırılar düzenlenmektedir. Geçtiğimiz dönemde Amerikalı bir perakende satış şirketinin bilişim sistemlerine bir saldırı gerçekleşmişti. Saldırıların boyutları gün yüzüne çıkarken çalınan ödeme kartı verilerinin yaklaşık 40 milyon dolar olduğu ve bilgisayar korsanlarının Amerikan vatandaşı olmadığı öğrenilmiştir (Altun, 2016: 192).

1.2.5 Siber Casusluk

Siber casusluk kişisel, ekonomik, politik veya askeri alanda bazı imkânlar oluşturmak maksadıyla iletişim ağları veya bilgisayarlara yasadışı girerek şahıslardan, rakiplerden, gruplardan, ülkelerden veya düşmanlardan onların izni olmadan sırlarını elde etme faaliyetleridir (Çiftci, 2017; 9)

Siber casusluk "siber espinoyaj" olarak da adlandırılmaktadır. İngilizce olarak "cyber espionage" ya da "cyber spying" şeklinde bilinmektedir. Siber casusluk faaliyetleri önceleri kişisel maksatları kapsamaktaydı. İlk zamanlar çeşitli trojen yazılımlar ile kullanıcıların bilgisayarlarına sızma ve onların şifrelerini ele geçirmek, masaüstlerine erişebilmek gibi yine bireysel maksatlar üzerinden gerçekleşmekte iken zamanla ekonomik, politik ve askeri avantaj sağlamak için kullanılmaya başlanmıştır. Bugün siber casusluk faaliyetleri ile rakip ülkenin internet ağlarında bulunan tüm bilgilerini ele geçirmek imkânı bulunmaktadır. Ayrıca konvansiyonel savaşlarda kullanılması planlanan strateji ve taktikleri dahi görebilmek mümkün olmaktadır. Siber casusluk siber savaş için oldukça önemli bir unsurdur. Siber casusluk faaliyetleri kanun dışı olarak yapılmaktadır. Rakip ülkenin iletişim ağları veya bilgisayarlarına yasal olmayan yollardan girerek herhangi bir izin almaksızın kişi grup ya da devlete ait gizli bilgilerin sızdırılması ile kimi zaman dijital olarak saklanan ve çeşitli bürokrat ve devlet adamlarına ait olan belge, ses ve video gibi dosyalarda siber casusluk faaliyetleri ile ele geçirilebilmekte ve karşı ülkeye farklı şantaj çeşitleri yapılabilmektedir. Bu sayede de o ülkenin hareket alanı kısıtlanabilir. İyi ve doğru şekilde yapılan bir siber casusluk faaliyeti ile siber savaşa başlamadan önce düşmana karşı üstünlük sağlayabilmektedir (Keleştemur, 2015; 162).

1.2.6. Siber Tehditler

Siber tehditler siber uzayda varolan bilginin bozulması, bilginin ortaya çıkarılması, erişebilirliğinin kopması gibi istenmeyen durumlara sebep olma potansiyelidir. Bu tehditler bilgi ve iletişim teknolojilerinden yararlanılarak üretilmiş, tamamen ilgili suç tanımları doğuran siber taarruzların yanı sıra, bilgi ve iletişim teknolojilerinin getirdiği imkânların araç olarak kullanıldığı klasik suçların siber ortama uyarlanmış hallerini de kapsamaktadır (Bayraktar, 2015: 14).

Siber uzayın insanlarda yarattığı endişe, organize siber saldırıların ulusal kritik altyapı ekonomi ve ulusal güvenliği zarar verebilecek imkâna sahip olmasıdır. Böyle bir saldırın gerçekleştirmesi için saldırganların ihtiyaç duyabilecekleri gerekli teknolojik gelişmişlik yeterli, mevcut ve temini kolaydır. Siber uzayda gözlenen olaylardan elde edilen tecrübe ve bilgi saldırganların teknolojideki gelişmelerden ve açıklıkları etkin bir şekilde yararlanarak daha yıkıcı imkân ve kabiliyetlere sahip olabilecekleri göstermektedir. Siber tehdide yönelik yapılan analizler tehdit ve açıklıkların uzun vade içerisindeki eğilimleri açıklayıcı olmalıdır. Yaşadığımız bu dünyada gelişmiş saldırı araç ve metotlarının, geniş çapta herkese açık bir şekilde kullanıma hazır hale geldiği, isteyen herkesin bunlara kolaylıkla sahip olabildiği ve e her geçen gün daha da geliştikleri gerçeğidir (Yılmaz ve Salcan, 2008:43).

Siber tehditler bilgi ve iletişim teknolojilerinden faydalanarak türetilmiş tamamen yeni suç tanımlarını doğuran siber saldırıların yanısıra bilgi ve iletişim teknolojilerinin getirdiği imkânların araç olarak kullandığı klasik suçların siber ortama uyarlanmış hallerini de kapsar. Siber tehditleri şu başlıklar altında toplamak mümkündür; siber casusluk, veri hırsızlığı, hizmet dışı bırakma, teçhizatın bozulması, kritik altyapı saldırıları ve tuzaklı donanım. Gelişmiş ülkelerde asgari iletişim altyapıları büyük çoğunlukla sivil iletişim ağları üzerinden karşılanır. Ulusal ve uluslararası iletişim altyapıların askeri ve sivil amaçlar için ortak kullanımı siber savaşı sivil birey ve örgütlerinin katılması için uygun ortam hazırlamıştır. Bu ortamda tehdit kaynakları olarak askeri personelin yanı sıra sivil toplum örgütleri, kamu ve özel kurum ve kuruluşlar, organize suç örgütleri, terör örgütleri ile profesyonel ve amatör bireyler karşımıza çıkmaktadır (Çiftçi, 2012:220).

1.2.7. Siber Suç

Bilişim teknolojilerindeki gelişmeler eğitimden kültüre, ticaretten eğlenceye, devlet sektörüne, özel sektöre kadar birçok alanda klasikleşen anlayışı değiştirmiş ve insanlara yeni bir yaşam sunmuştur. Fakat bütün bu faydaların yanında bir takım olumsuzluklarda bu gelişmelerle beraber hayatımıza girmiştir. Klasik suç tanımlarına uymayan yeni bir suç türü olarak siber suç ortaya çıkmıştır. Literatürde siber suçlarla ilgili çeşitli tanımlamalar yapılmıştır. Siber suçlar bilgisayarların kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin

kanuna ve meslek ahlakına aykırı davranışlar şeklinde yapılmıştır. Siber suçlar kavramı daha önceleri bilgisayar suçları ve bilgisayar bağlantılı suçlar kavramları ile ifade edilmektedir. Siber suç kavramı, henüz çok yeni bir kavram olmasına rağmen bilgisayar suçları kavramı yarım yüzyıldan bu yana kullanılmaktadır. Bu suçların ortak özelliği hepsinin bilgisayar aracılığıyla gerçekleştirilmesidir (Çakır ve Kılıç, 2014; 21).

Siber suçlar kredi kartı, bilgisayar veya cep telefonu gibi günlük yaşantımızın vazgeçilmez araçlarıyla işlenebilmektedir. Böyle geniş bir kapsamı içermesi birçok farklı tanımlamanın yapılmasına da sebep olmuştur. En basit tanımıyla bilgisayar suçları olarak adlandırılabileceği gibi, siber suçlar, dijital suçlar, elektronik suçlar, internet suçları, ileri teknoloji suçları gibi ifadeler de kullanılabilmektedir. Siber suçlar konusunda herkesin kabul ettiği bir tanım olmasa da "Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısında yaptığı tanımlama başlangıç noktası olarak dikkat çekicidir. Bu komisyon siber suçu; "bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlakı veya yetki dışı gerçekleştirilen her türlü davranış" olarak tanımlamıştır (Çakmak ve Altunok, 2009: 31-32).

Siber suç, siber uzay ortamında işlenen tüm suçları kapsamaktadır. Siber suçlar siber uzayda siber alanın ana yapısı olan bilişim sistemleri ile yine bu bileşenlere karşı işlenmiş suçların tamamıdır. İnternet bağlantılı herhangi bir bilgisayar sistemine ya da ağının diğer bilgisayar sistemleri ya da ağlarına karşı kötü amaçlı eylemler gerçekleştirmek maksadıyla kullanılması, klasik suçların yeni teknolojiler kullanılarak işlenmesi ve internetin ortaya çıkışı ile beraber gelişen yeni suçlarda bu kapsamda değerlendirilmektedir (Bayraktar, 2015: 14).

İKİNCİ BÖLÜM

2. SİBER TERÖRİZM VE GÜVENLİK

2.1. 21'inci Yüzyılda Siber Güvenlik

Siber uzayın teknolojisiyle birlikte ondan beklentilerimiz de benzer şekilde evrim geçirmektedir. İnterneti oluşturanın kendisi, daha önde ve önemli bir evrime uğramaktadır. Aynı zamanda çok büyük miktarda büyümekte (her gün yaklaşık 2,500,000,000,000,000,000 byte küresel dijital bilgi tedarikine eklenmektedir) ve çok fazlası kişiselleştirilmektedir. Bu çevrim içi bilginin saldırısını pasif bir şekilde karşılamaktansa bireyler kullanıcılar kendi kişisel kullanımlarına ilişkin siteler yaratıyor ve şekil veriyorlar ve sonuç olarak kendileri hakkında da fazlasını açığa vurmaktadırlar. Bu siteler Amerika'da Facebook ve Çin'de RenRen'den, Twitter ve Çinli karşılığı olan Tencent ve Sina gibi mikro bloglara kadar değişmektedir. Çin'deki mikro bloglar (isimleri Weibo), 2012'de 550 milyonun kaydolduğu bir boyuta ulaşmaktadır (Singer ve Friedman, 2015: 31).

Yeni buluşlarla beraber dünyanın hızlı değişimi insanların ve kurumların teknolojiye olan bağlılıklarını artırmıştır. Son çeyrek yüzyılda büyük bir gelişim gösteren bilgisayar bilgi sistem teknolojilerinin günlük yaşantımızda sıklıkla kullandığımız birçok işlemin altyapısını oluşturmaktadır (Bayraktar ve Demir, 2013: 23).

Siber uzay bir zamanlar sadece bir iletişim ve sonrasında e-ticaret dünyası iken (yıllık 10 trilyon dolarlık satışa ulaşan), "kritik alt yapı" dediğimiz kavramı da içerecek şekilde genişlemiştir. Bunlar günümüz medeniyetinin yürümesini sağlayan tarım ve gıda dağıtımından bankacılık, sağlık, ulaşım, su ve enerjiye kadar değişen

altta yatan alanlardır. Bunlar bir zamanlar ayrı ayrı dururlardı fakat şu anda hepsi birbirine ve siber uzaya bilgi teknolojileri vasıtasıyla ve çoğunlukla "uzaktan kontrol ve gözetleme sistemi" SCADA üzerinden bağlıdır. Bunlar izleyen, değişimleri ayarlayan ve kritik altyapının diğer süreçlerini kontrol eden bilgisayar sistemleridir. Siber uzay işte bu yüzden bir zamanlar Başkan George W.Bush'un dediği "sinir sisteminden ekonomimizin kontrol sistemi daha fazlası olan bir şeye doğru evrim geçirmektedir" Wired dergisinin editörü Ben Hammersley'in tanımladığı gibi siber uzay "21'inci yüzyılda yaşam için egemen platform" haline dönüşmektedir (Singer ve Friedman, 2015: 31).

Siber güvenlik, son kullanıcıdan internet servis sağlayıcıları (ISP), alt yapı donanım satıcıları, haber taşıyıcıları ve yazılım programcıları, tehdit ve risk analizcilerine kıdemli yönetim veya siyasi karar alıcılarına kadar çeşitli sorumluluklar ortaya koymaktadır. Şirketler ve hükümetler, mevcut iletişim teknolojisi (IT) ile ilgili risklerle baş etmeye çalışırken, güvenlik arayışındaki organizasyonlar, IT kurumları ve ağları da, var olan belgeleri, yazılımları ve güvenlik önlemlerini güncelleştirmek ve iyileştirmek için organize olmaktadır (Yılmaz ve Salcan, 2008: 28).

Bir devletin güvenliğine yönelik tehditleri geleneksel olarak iç ve dış tehdit olarak ikiye ayırmak ve suç ile terörü iç tehdit, savaşı ise dış tehdit sınıflaması içinde değerlendirmek mümkün olabilir. Bu klasik teorinin geçerliliğini kendi içinde sorgulamak mümkünken, siber ortam ve siber tehditler söz konusu olduğunda iç ve dış tehdit sınıflandırılmasının aynı rahatlıkla yapılabileceği söylenemez. Uluslararası boyutu olmayan yerel siber saldırılar yapmak mümkün olsa da genel olarak siber saldırılar için herhangi bir sınır yoktur. Ayrıca günümüzde suç ve terörizm olguları ülkelerin sınırlarını tanımamakta, organize suç örgütleri ve terörist örgütler uluslararası ortamda faaliyet gösterdikleri gibi aralarındaki ayrım da gün geçtikçe belirsiz hale gelmektedir. Öyle ki, geçmişte birbirinden tamamen ayrı olarak faaliyet gösteren bu örgütlerin birçoğu günümüzde tek bir yapı içerisinde kaynaşmış biçimde görülebilmektedir (Çakmak ve Demir, 2013: 24).

Siber güvenlik alanında devlet dışı unsurların etkisi büyük orandadır. İnternet ile ilgili teknik standartlar, uluslararası üyeleri olan özel sektör tarafından kontrol

edilen Internet Enginering Task Force tarafından geliştirmekte ve önerilmektedir. Siber güvenlik açısından önemli olan öteki elemanlar, büyük telekominasyon taşıyıcıları, internet hizmet sağlayıcıları ve diğer birçok kuruluş bulunmaktadır. Standartlar aynı işlemin, aynı şekilde yapılmasını, faaliyetlerin aynı süreçler takip edilerek gerçekleştirmesini, ürünlerin aynı süreçler içinden geçerek üretilmesini sağlamaya çalışan belgelerdir. Özellikle bilgi sistemleri ve bilgi güvenliğinde standartların takip edilmesinin önemi büyüktür (Çiftci, 2017; 249).

Siber güvenlik, çok az bir maliyetle kısa bir zaman diliminde farklı alanlara yönelik yapılan siber saldırılar sonucunda ulusların siyasi ve askeri alanlarında bulunan gizli bilgilere ulaşılarak bu bilgilerin dışarıya sızdırılması, toplumsal alanda farklı algıların oluşturulması, devlet ekonomilerinin zarar görmesi, haberleşme ve iletişim alanlarına yapılan saldırılar ile çevresel problemlerin ortaya çıkmasını sağlayan önemli bir güvenlik alanı, bir anlamda güvenlik sektörü haline gelmiştir (Ünal, 2015; 105).

2.2. Siber Terörizm

FBI, siber terörizmi "alt-ulus grupları veya gizli örgütler tarafından savaşçı olmayan hedeflere karşı şiddetle son bulan bilgisayar sistemleri, bilgisayar programları ve verilere karşı önceden planlanmış siyasi güdümlü saldırı" olarak tanımlamaktadır. Siber güvenlikte ki birçok diğer konu gibi gerçek olan ve korkulan genellikle aynı ortam içerisinde bulunmaktadır. Bu durum, terörist grupların şiddet eylemlerini gerçekleştirmek için siber teknoloji kullanmada ilgisiz olduklarına işaret etmez. Örneğin 2001'de Afganistan'da ele geçiren El Kaide bilgisayarlarında bir barajın çizimlerini ve kontrollerini ele geçirilmesini simüle eden bir mühendislik yazılımı bulunmuştur. Aynı şekilde 2006'da Guantanamo Körfezi'ndeki kötü muamelelere karşılık olarak terörist web siteleri ABD finans sektörüne karşı siber saldırılar ön ayak olmuşlardır (Sınger ve Friedman, 2015; 135).

Küçük bir terörist grup, internet sayesinde küresel ölçekli uydular ve mobil iletişim sistemleri ile bugün, büyük devletler hariç, çoğu ülkeden daha fazla komuta, kontrol, iletişim ve istihbarat imkânına sahip bulunmaktadır. İletişim ve ulaşım kolaylıkları, küreselleşmenin en önemli unsurlarından biridir ve aniden bir grup

teröristin elinde yıkıcı ve öldürücü silahlara dönüşebilmektedir. Elde edilen bilgilere göre El Kaide militanlarının arasında dünyanın birçok bölgesinde bulunan müslümanların olduğu gibi, sistem karşıtı farklı dinlere mensup üyeler de vardır. Artık terör örgütleri de küreselleşmektedir. Bunun adı da "büyük dönüşüm" olarak nitelendirilmektedir. Bu dönemde hemen hemen değişmeyen hiçbir şey kalmamıştır. Başkan Bush'un, 22 Eylül 2001'de yaptığı bir konuşmada hedefin, "küresel erişimi olan terörist gruplar" ve "terörizmi hala desteklemekte olan ülkeler" olduğunu söyleyerek düşmanı daha net bir şekilde tanımlamaya çalışmıştır. Aslında bu durum 11 Eylül sonrası oluşan yeni dönemi ifade etmektedir. Sonuç olarak küresel düşünebilen ve örgütlenen, yerel hedeflere yönelen, Soğuk Savaş'a göre değişime uğramış, esnek yapıda örgütlenmiş, hızla karar alıp uygulayabilen az maliyetli örgütler ile karşı karşıya kalmaktayız. Geldiğimiz noktada, küresel sisteme, teknolojik dönüşüme ve siyasal etnik anlaşmazlıklardan yola çıkarak buna uygun davranabilen ve kendini dönüştürme yeteneğindeki teröristlere karşı mücadele sorumluluğu olanların da, benzer hızla ve fonksiyonel olarak kendilerini dönüştürmüşlerdir (Temizel, 2011: 331).

Siber terörizm kavramı günümüzde çok sık kullanıyor olmasına karşın, basit bilgisayar suçlarının "siber terör" adı altında toplanmasının doğruluğuna ilişkin yeterince kanıt ya da ispatlanmış olay bulunmamaktadır. Popüler kullanımına karşın, aynı şekilde hangi eylemlerin "siber terör" kavramı içerisinde değerlendirilebileceği üzerinde de uzlaşı mevcut değildir. Kavram ilk olarak 1980'lerde Barry Collin tarafından ortaya atılmış ve yakın geçmişte modern dönemlerin en büyük iki korkusu, teknolojik araçlardan ve modern alışkanlıklardan mağduriyet korkusu ve bilgisayar teknolojilerine olan güvensizlik ve endişe birleşerek siber terörizm korkusunu yaratmıştır. Siber terörizm tartışmalarında iki karşıt görüş yer almaktadır. Öncelikli olarak siber terörizm kimseye zarar vermeyen bir mittir. Bu teori 11 Eylül'de ABD'de ikiz kulelere yönelik yapılan eylemlerle anlamını kaybetmiştir. İkinci görüş ise daha çok bilgisayar güvenliği konuları ile ilgilenmiş olup, siber ortamda yapılan eylem ve faaliyetlerin gerçek bir tehdit olduğudur (Özkışlalı, 2008: 69).

Siber silahlar terör örgütlerine çok düşük maliyet gerektiren, kolayca saklanabilen sistemler ile amaçladıkları etkiyi oluşturma imkânı sağlamaktadır. Hizbullah, Hamas ve El Kaide terör örgütleri bilgisayar dosyalarını, e-postaları kendi faaliyetlerini için kullanabilmektedirler. İletişim için internet dünya çapında büyük kitlelere hitap etmesi, bilgi akışının çok hızlı bir şekilde işlemesi, terör örgütleri için gereken yeni elemanları kazanabilme imkânı sağlaması, steganognafi (fotoğraf, resim ve objelerde belirtilen gizli mesajlar), fon sağlama, istihbarat toplama yetenekleri, psikolojik açıdan propaganda yaratabilirken, siber saldırılar teröristlere saklanma, gizlenme, operasyonel faaliyetleri icra etme imkânı sağlamaktadır (Çakmak ve Altunok, 2009: 94).

Siber terörizm kavramını açıklamadan önce terör ve terörizm tanımlarını yapmamız gerekmektedir. Siber terörizm kökünü latince 'terrere' kelimesinden almıştır. Genel olarak "korkudan sarsıntı geçirme" veya "korkudan dehşete düşmeye sebep olma" anlamlarına gelmektedir. Terör kelimesi ilk defa Dictionnarire de l'Academie Française'nin 1789 yılında yayınlanan ekinde görülmüştür. Terörizmi tanımlamak zordur. Bu tanımda bir fikir birliğine ulaşılamamasının temel nedeni girişilen eylemlerin suç niteliği mi taşıdığı, yoksa daha iyiyi elde etme amacına mı yönelik olduğu konusunda geniş bir ideolojik tartışma olmasıdır. Terör terimi, korku ve endişeyi belirtirken terörizm bu kavrama ise siyasi anlamda bir içerik ve devamlılık anlamı eklemektedir. Bu yönde terörizm; "Savaş ve diplomasi ile kazanılmayan sonuçları elde etmek, korkutmak ve itaat ettirmek için bir teoriye, felsefeye ve ideolojiye dayanılarak siyasi maksatlarla, iradi olarak terör ve şiddetin sistemli ve hesaplı bir şekilde kullanılmasıdır" şeklinde tanımlanabilmektedir. Terör, kısaca silahlı eylemler yoluyla kendini ve davasını geniş kitlelere duyurma; terörizm ise, bu eylemleri savunan, stratejilerini anlatan, aktaran, geliştiren bir düşünce disiplini ve akımıdır denebilir. Teröristler yeraltına girerler, gizlilik içinde çalışır, eylemlerini yaparlar ve sonuçta bu eylemlerinin amaçları doğrultusunda propagandaya yönelirler. Terörizm ise bu dönemden sonra devreye girmektedir. Yani terör stratejik eylem, terörizm ise stratejik söylemdir. Terörizm bir davaya veya siyasal anlaşmazlığa dikkat çekmeye çalışmaktadır. Bu da toplumda oluşturulan korku ile yapılmaktadır. Terörizm kitle iletişim araçlarını da kullanarak "benden olanlar" ve "benden olmayanlar" şeklinde toplumda bir bloklaşma yaratmaya

çalışmaktadır. Böylelikle insanları zorunlu bir şekilde taraf olmaya iter. Bu da toplumun birliğine ve bütünlüğüne zarar verir (Özkışlalı, 2008; 48).

Birinci terör dalgasının oluşum ve kaynağı 19. yüzyılda sanayileşme ve kentleşmesini devam ettiren Batı ülkelerindeki işçi kitlelerinin şikâyetlerinden ortaya çıkmıştır. Bunun sonucu olarak bu dönem terör olayları işçi hareketleriyle etiketlenmiş ve çoğunluk tarafından işçi direnişi veya işçi hareketleri "terör" olarak isimlendirilmiştir. 20. yüzyılda ise, durum farklılaşmış, ikinci terör dalgası ortaya çıkmıştır. Yaşanan bağımsızlık hareketleri genel olarak ayrılıkçı terör olaylarını ön plana çıkarsa da, bu gelişmelere daha baskın çıkan ve belirleyici siyasal söylemi olan Soğuk Savaş dönemi terörü olmuştur. Bu dönemde, Doğu ve Batı Blok'unda yer alan devletler karşılıklı savaşı göze alamadıklarından hasım ilan ettikleri taraflara karşı mücadele eden terör örgütlerini yoğun bir şekilde desteklemişlerdir. Soğuk Savaş Döneminin 1991'de SSCB'nin yıkılması ve ABD'nin önderliğindeki Batı Blokunun zaferiyle sonuçlanmasının ardından terörün üçüncü dalgası ortaya çıkmıştır. Kapitalist dünyanın lideri konumuna gelen ABD, uluslararası ilişkilerde ben merkezli ve dominant politikalarıyla tepkisel süreci başlatmıştır. Bu defa devletler değil, El-Kaide gibi tabandan gelen örgütler ön plana çıkmaya başlamış ve teknolojinin sunduğu avantajları kendi kazanımlarına çevirerek yeni düzenin söylemlerini mağduriyet merkezli ajite etmişlerdir. Soğuk Savaş sonrası dönemde "yeni terörizm" ve daha yaygın haliyle "küresel terörizm" olarak tanımlanan asimetrik savaş stratejisinin önemli bir tehdit olarak varlığını sürdürdüğü ve hatta artırdığı görülmektedir. Kırılma noktasının 11 Eylül 2001 terörist saldırıları olan bu dönemin en büyük özelliği, küresel teröristlerin ideolojik motiflerinin "nefret" odaklı olması ve "yok etme" ilkesine dayalı bir strateji benimseyerek bir dünya düzeni önermemesidir. Bu nedenle her tür öldürücü silahı çekinmeden kullanabilme özelliğine yatkın olmalarıdır. Dolayısıyla küresel terör, "yıldırmadan" ziyade "yok etme"yi benimseyen ve kitle imha silahları dâhil her tür öldürücü silahı kullanabilecek bir terör hareketi olarak tanımlanabilir (Özkışlalı, 2008; 52).

Her yeni teknolojinin ve gelişimin beraberinde getirdiği yeni fırsatların yanı sıra birçok tehdidi de yanında taşıdığı tartışılmaz bir gerçektir. Teknolojik alandaki hızlı gelişmeler bir taraftan toplumların sosyal, ekonomik ve siyasi hayatlarını

olumlu anlamda etkilerken diğer tarafta terör örgütleri de gelişen bu teknolojiyi yakından izleyerek, siyasi hedeflerine ulaşmakta bu teknolojiyi etkin olarak kullanmaktadırlar. Hedefine ulaşmada hiçbir sınır tanımayan terör örgütleri kriminoloji de "suçların fırsatları takip etmesi" yönünde bir gelişme kazanarak, suç tasvirlerine yeni bir oluşum sağlamıştır. Klasik terör türlerinin dışında yeni terör türlerin ortaya çıkmasına neden olan bir kavram siber terörizmindir (Bayraktar, 2015: 70).

Joshua Gren, "The Myth of Cyberterroism" başlığını taşıyan makalesinde bilgisayarlar tarafından öldürülen insanların olmadığını, devletlerin çok gizli ve güvenlik gerektiren bölgelerinde internet bağlantılarının bulunmadığını ifade ederek siber terörizm kavramının abartıldığını belirtmektedir. Gerçekten de bu kavramın yeni ve biraz da sınırlarının bilinmez olmasının büyüsüne kapılarak, içinde bilgisayarların yer aldığı en küçük bir olay bile siber terörizm olarak ifade edilmektedir. Terör örgütleri siber ortama oldukça ilgi göstermektedirler. Bu ilginin aşağıdaki sebeplerden kaynaklandığı iddia edilebilir:

Daha az mali kaynak ve personel ihtiyacı gerektirir,

Uygulama yöntemi geleneksel terörist eylemlerden daha kolaydır,

Çok ileri teknoloji kullanılmasını gerektirmez,

Geleneksel yöntemlere kıyasla faillere daha fazla anonimlik sağlar. Tespit edilebilme ve özellikle kimliklerinin ayırt edilmesi güçtür,

Muhtemel hedeflerin sayısı ve çeşidi çoktur,

Siber terör saldırıları çok uzak bir mesafeden gerçekleştirilebilir. Bu durum faillerin tespit edilmelerinde ve yakalanmalarında güçlüğe sebep olur,

Siber saldırıların çekiciliği sebebiyle teröristler medyada daha fazla yer işgal etme imkânı kazanabilirler, böylelikle terörizmin ihtiyacı olan halka ulaşma ve propaganda daha kolay gerçekleştirilebilir (Çakmak ve Altunok, 2009: 36-37).

İngilizce adıyla “Cyber terrorism” olarak da adlandırılan siber terörizmin amacı, bilgisayar ağlarını kullanılamaz hale getirmeye yönelik kasıtlı olarak yapılan, geniş kapsamlı eylemlerde dâhil olmak üzere, terör eylemlerinde internete bağlı kişisel bilgisayarları kullanmak ve internet tabanlı saldırılar yapmaktır. Buradaki tanıma göre, belli bir teknik bilgiye vakıf olmak gerektiği belirtilmiş olsa da aslında sosyal ağlar üzerinden yapılan terörü destekleyen faaliyetlerde siber terörizmin kapsamı içerisine girebilmektedir. Reel hayat da teröre destek vermek, teröriste yardım ve yataklık etmek de bir terörizm faaliyetiyse, aynı şekilde sosyal ağlar üzerinden propaganda yapmak, terörizmi desteklemek de siber terörizm faktörü olarak kabul edilmektedir. Siber terörizm, maksat olarak sadece bilgisayarları değil, insanların can ve malları tehdit eden saldırıları kapsamaktadır. Bunun dışında geniş bir spektrumdan bakıldığındaysa dini, ideolojik, politik, sosyal ve kültürel yapılarını da tehdit edici unsurlar barındırabilmektedir. Siber saldırı ve siber terörizmi birbirinden ayıran en büyük etken, etki alanının genişliğidir. Tek bir kullanıcı yahut sunucuya yapılan taarruz siber saldırı olarak kabul edilebilirken, siber terörizm olması için geniş kapsamlı bir alanı içermesi gerekmektedir. Ayrıca siber terörizmde belli bir ideolojik amaç varken, siber saldırı ego tatmini yahut intikam gibi kişisel duygular sebebiyle gerçekleştirilebilir. Her siber saldırı bir siber terörizm eylemi olmayabilir ancak her siber terörizm faaliyeti bir siber saldırıdır (Keleştemur, 2015: 161).

Siber terörizm, belirli bir politik ve sosyal hedefe ulaşabilmek için; bilgisayar veya bilgisayar sistemlerinin, bireylere ve mallara karşı bir hükümeti veya bir ulusu bıktırma, onların üzerinde baskı unsuru oluşturma olarak açıklanabilir. Stanford Üniversitesi, Uluslararası Güvenlik ve İşbirliği Merkezi (CISAC) tarafından yapılan çalışmada siber terörizmin ne anlama geldiği, neyi ifade ettiği, neleri kapsadığı gibi konulara açıklık getirilmeye çalışılmıştır. Stanford Taslağı olarak bilinen belgede siber terörizm şu şekilde anlatılmıştır: “Yasa kapsamında yetki verilmiş görevli personelin yapmış oldukları eylemler dışında, siber alt yapıya karşı yapılan saldırılar ve bunun sonucunda insanların ölümü, yaralanması, kamu düzenin yıkılması, büyük ekonomik zararların verdirilmesi ve mallara karşı yapılan önemli zararlara sebep olması muhtemel olan yıkma, bozma, engelleme ve şiddet eylemlerini kasıılı bir şekilde yapılması veya yapılacağına dair tehdit.” Stanford Taslağı’nın 3. maddesinde

suçlar başlığı altındaki tanımlamaya göre, siber terörizm, daha önce teröre karşı hazırlanan uluslararası sözleşmelerde tanımı yapılan terör eylemlerini yapmak maksadıyla siber ortamın kullanılması durumunda söz konusu olacaktır. İlgili uluslararası sözleşmeler şunlardır: 1963 tarihli Tokyo Sözleşmesi (Uçaklarda İşlenen Suçlar), 1970 tarihli Hague Sözleşmesi, 1971 tarihli Montreal Sözleşmesi, 1979 tarihli Rehine Alınmasına Karşı Uluslararası Sözleşme, 1988 tarihli Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi, 1988 tarihli Denizlerde Terörizm Sözleşmesi, 1997 tarihli Terörist Bombalamaları Sözleşmesi'dir. Siber terörizmi açıklarken en temelinde terörizm olgusunun özellikleri değil, terör olgusunun nasıl faaliyete geçirildiği önemli bir nokta olarak öne çıkmaktadır. En basit şekliyle siber terörizmi terör eylemlerinin iletişim ve bilgisayar sistemleri üzerinden yapılması durumunda tanımlayabiliriz. Fakat yaygın iletişim sistemlerindeki son gelişmelerin oluşturduğu "siber" kelimesi "terör" sözcüğü ile yan yana geldiği takdirde ortaya yeni bir olgu çıkmaktadır. Avrupa Konseyi tarafından hazırlanan 'Siber Suçlar Sözleşmesi'nin II. Bölüm I. Kısımda dokuz ayrı siber suçtan bahsedildiği halde siber teröre ilişkin bir düzenleme bulunmamaktadır. Bu nedenle öncelikle siber suç ile eş anlamlı olarak kullanılan bilgisayar suçları ve bilişim suçları kavramlarına açıklık getirilmesi gerekmektedir (Özkan, 2006; 81).

"Siber terörizm" ile "hacker" arasındaki farkın anlaşılması güçtür. Kurumsal sistemler veya kişisel bilgisayarlara zarar veren, kayıtlı bilgileri ortadan kaldıran h saldırıları, siber terörizmde olduğu gibi politik maksatlarla motive olmamaktadır. Protesto amacı taşımazlar, öldürmek ya da yaralamak gibi amaçları yoktur. Ancak, hekırlık siber terörizmin tehlike potansiyeli hakkında bilgi vermektedir. Teröristler, hekırların kullandığı yöntemlere benzeyen yöntemler kullanarak büyük yıkımlara neden olabilirler (Özkışlalı, 2008: 70).

Siber terör, bir bilgi devriminin karanlık yüzü olarak ifade edileceğinden bu faktörler teknolojinin kötü amaçlar için kullanılması olarak tarif edilebilir. Siber terörün tercih edilmesini sağlayan faktörler dört başlık altında toplanabilir. Bunlar, küresel bağlanabilirlik, teknolojiye olan bağlılık, hukuksal bütünlüğün olmaması ve düşük maliyet (Topal, 2004: 38).

Teröristlerin internetten genel olarak iki amaçla faydalandığı söylenebilir. Birincisi, internet teröristler için etkin bir iletişim ve eğitim ortamı sağlamaktadır. Teröristler ve sempatizanları böylelikle haberleşebilmekte, örgüt propagandası yapabilmekte, talimatlar örgüt üyelerine aktarabilmekte ve hatta internet sanal eğitim amacıyla kullanılabilmektedir (Çakmak ve Altunok, 2009: 38).

Dünya, siber terörist eylemler kapsamında sayılabilecek pek çok örneğine şahit olmuştur. Örneğin Endonezya polisi, Bali'de 2002 yılında yaşanan bombalama olayları ile ilintili olarak teröristlere bilgisayar teknolojileri aracılığıyla yardım ettikleri gerekçesiyle Agung Prabowo ve Agung Setyadi adlı iki kişiyi tutuklamıştır. Bali'de 2002 yılının Ekim ayında gece kulüplerinde çok sayıda bomba patlamış ve çoğunluğu yabancı turistlerin oluşturduğu 202 kişi hayatını kaybetmiştir. İmam Samudra bu terörist eylemin başı olarak 2005 yılında idam edilmek üzere cezaevine konmuştur. Tutuklanan teröristlerden Agung Setyadi'nin, İmam Samudra'ya hücresinde dizüstü bilgisayar sağladığı ve bu sayede Samudra'nın aylarca internette diğer teröristlerle iletişime geçtiği ve eylemler için para transferi yaptığı saptanmıştır. Bu görüşmeler sonrasında da 2005 yılının Ekim ayında Bali'de üç bomba daha patlamıştır. Bunun üzerine, Samudra ve tutuklanan iki terörist ölüm cezasına çarptırılarak, yüksek güvenlikli cezaevine nakledilmişlerdir. Profesyonel bir hekır olarak nitelendirilen Agung Prabowo ise oluşturulmasına yardım ettiği web sitesinde Bali'deki yabancıları katletmek için onları vurmanın en iyi yol olduğunu söylediği için suçlanmıştır. Bali'deki bombalamalardan Güneydoğu Asya İslami militan örgüt Jemaah Islamiah sorumlu tutulmuş olup, yetkililer olayların El-Kaide ile de bağlantılı olduğunu belirtmişlerdir (Özkışlalı, 2008: 79).

2.3. Siber Savaş

Siber savaş terimi tam olarak açıklanmış değildir. Siber savaş temelinde geniş bir kavram ifade etmektedir. İki isimden oluşmaktadır. Siber kelimesi aslında ikinci sözcüğün yani savaşın türünü, dalını ve yönünü ifade etmektedir. Siber savaş terimi ingilizce karşıtı "Cyber War" olarak Türkçeye çevrilmiştir. İngilizcede "Cyber" kelimesi siber, "War" kelimesi ise savaş anlamında kullanılmaktadır (Yayla, 2013: 179).

Devletin kuruluş maksadının temel niteliğinin güvenlik olduğunu böylece bireylerin tehlikelerden korunmuş, korkmadan hayatlarını sürdürebildiği, toplumsal yaşamın gereksinimleri doğrultusunda sürekli biçimde işlediği, herkesin kendisini emniyet içinde hissettiği bir ortamı ifade etmektedir. Bilgi çağında bilgiye sahip olmak tek başına yeterli değildir. Tıpkı istihbarat biliminde olduğu gibi bilginin işlenmesi yorumlaması gerekmektedir. Böylelikle bilgiye hâkim olunur ve güç bu noktadan sonra kişiye/örgüte/kuruma/devlete geçer. Yeni savaş alanı olarak kabul edilen siber uzay da yalnızca bilgiye erişim değil, ayrıca bilgiyi geliştirme manipüle etme siber istihbarata karşı koyma bilgiyi çarpıtma koruma gibi tam manası ile bir mücadele söz konusudur. Siber uzay kendisinden önceki savaşlar gibi olur ve biter vaziyette değildir. Bir muharebe alanının ve sınırlarının olmayışı siber uzayın savaş ortamından çok bir mücadele ortamı olarak ortaya çıkmasını zorunlu kılmıştır (Kurgan, 2018: 68).

21'inci yüzyılda yaşanan inanılmaz gelişmelerle birlikte, bilgi teknolojileri günlük hayatımızın her anına girerek hayatımızın doğal bir parçası olmuştur. Hayatımızı oldukça kolaylaştıran bu teknolojiye gittikçe daha bağımlı hale gelmekteyiz. Bilgi teknolojileri özel hayatımızı kolaylaştırmakla birlikte, iş yaşamında da görevlerin icrası için kullanılması kaçınılmaz olan uygulamaları içermektedir. Hayatımızın bu kadar içerisine girmiş ve artık bir yaşam ortamı olan siber ortamı insanoğlu olarak kısa sürede bir çatışma ve savaş ortamı haline getirmeyi "başardık"! Artık siber ortam kaçınılmaz bir şekilde, kara, hava, deniz ve uzayın ardından beşinci savaş ortamı olarak yerini almış durumdadır (Kara, 2013: 40).

Dijital şifrelemenin yazılımlarının siyasi terminolojideki imaları 1990'larda ABD hükümet çevrelerince "munitions" (cephane) olarak sınıflandırılmaya başlamıştır. Gelecek bilimci Bruno Guissani'nin ifadesiyle siber savaş "rakibinizin kim olduğundan hiçbir zaman emin olamadığınız yedi boyutlu bir satranç oyunu gibi". ABD için Google sadece özel bir kuruluş değil aynı zamanda Beyaz Saray'ın nezdinde çok önemli bir milli varlıktır. ABD başkentinin mesajı açık ve nettir. Google'a saldırırsanız ABD'ye de saldırmış olursunuz. Google Facebook'la birlikte yeryüzündeki en geniş veri deposudur. Bu özelliği ile karlı bir iş sağlamaktadır.

Bunun yanında reklamcılar bu verinin açığa çıkaracak bireysel alışkanlıklarla alakalı gizli hususları öğrenmek için para ödemeye hazırdırlar. Benzer şekilde bu özelliği ile hem kendileri, hem gizli teşkilatlar, hem sektör, hem de rakip devletler için çalışan bilgisayarlar korsanları için kutsal kase niteliğindedir (Kurtoğlu, 2017; 103).

Devletler kendilerini kısıtlı bir tarihten veya gerginliğin artmasından sonra bir siber savaş içinde bulabilirler. Siber saldırı kullanan devletler diğer devletler üzerinde baskı ve üstünlük sağlayacağını düşünerek bu tür faaliyetler içerisine girmektedirler. Siber savaşın dâhili ve harici olmak üzere iki amacı vardır. Harici amacı; siber savaş asıl amacıdır. Karşı tarafa boyun eğdirmek, bilgilerini çalmayı, sistemleri belli bir süre devre dışı bırakmayı veya tamamen bozma içerir. Dâhili amacı ise; siber savaş uygulamalarının nasıl yapılacağını (saldırıları durdurmak, kapsamı sınırlandırmak, karşı tarafın sağlıkla ilgili sistemlerine saldırmama vb.) ve gerginliğin tırmandırılmasından nasıl kaçılacağını içermektedir (Çiftci, 2017; 10).

Gerçek bir savaş durumu ile savaş konseptinin daha sık olan kullanım ve yanlış kullanımları arasındaki kopukluğu “siber savaş” gibi bir terimi tartışırken akılda tutulması çok önemlidir. Savaş, uluslararasındaki silahlı çatışmalarda sembolü çekişmelere kadar çok çeşitli durum ve davranışlar kümesini tanımlamak için kullanılmaktadır. “Siber savaşa” gelince, terim bir siber barbarlık ve bozulma kampanyasından gerçek bir siber araçlardan faydalanan savaş durumuna kadar her şeyi tanımlamak için kullanmıştır. Aslında 2010'da The Ekonomist; askeri çatışmadan kredi kartı dolandırıcılığına kadar tasvir ettiği siber savaş hakkında bir kapak hikâyesi yapmıştır. Siber savaşı tanımlamak bu kadar karışık olmak zorunda değildir. Siber uzaydaki savaşın ana elemanlarının diğer alanlardaki savaşta karşılıkları ve bağlantıları vardır. İster karada savaş olsun ister denizde veya havada ya da şimdi siber uzay da savaşın her zaman siyasi bir amacı ve biçimi vardır ve her zaman bir şiddet unsuru içerir. Şu anda Amerikan hükümetinin tutumu kuvvet kullanımının bir tanımını karşılamak için siber saldırının yaklaşık olarak ölüm, yaralanma veya önemli yıkım ile sonuçlanmak zorunda olmasıdır. Diğer bir değişle siber vasıtalarla yapılmış bile olsa etkisi fiziksel hasar veya yıkım olmalıdır. Bir örnek gerekirse bomba bırakan bir uçak hava savaş aracı olarak görülür, broşür bırakan ise o kadar değildir. Fakat siber savaşının ne zaman başladığını ve bittiğini

bilmek onu tanımaktan daha zor olabilir. Kore savaşının gerçekte 2. Dünya Savaşının olduğu gibi açık başlangıç tarihi ve anlaşmalı bitiş tarihi yoktur. Bunun yerine başlangıç ve bitişleri bulanıktır. Örneğin ABD 1950'de Kuzey Kore'ye savaş ilan etmemiş olabilir, fakat 5.3 milyonun öldüğü bir çatışmanın Başkan Turuman'ın zamanında adlandırıldığı gibi sadece bir "Polisiye Eylem" olduğunu tartışmak zordur. Onu takip eden tarih kitaplarının belirttiği gibi Kore Savaşı resmi olarak bir barış antlaşması ile hiçbir zaman sona ermediği halde, gerçek çatışma 1953'te durmuştur (Singer ve Friedman, 2015; 164).

İnternetin doğru ve güvenli kullanımı yaşam standardını yükseltmektedir. Ancak kötü niyetli kullanımı ise hayatı kaosa dönüştürmektedir. Bu kaotik durum siber savaş kavramının oluşmasına neden olmuştur. Siber savaş kavramının ulusal bir hedefi gerçekleştirmek ya da devam eden savaşı desteklemek maksadıyla bir ülke tarafından veya insiyatifinde diğer bir ülkenin askeri ve sivil her türlü bilişim sistem ve altyapısının işlevselliğini engellemek imha etmek ve kendi çıkarlarımız doğrusunda kullanmak için siber savaş yöntemlerinin kullanılması ve buna karşı koyacak tedbirler veya süreçler şeklinde tanımlamak mümkündür. Gerçekleştirmek istenen amaçlar dikkate alındığında siber savaş askeri, ekonomik, politik ve psikolojik gayeler için hedef seçilen ulusa yönelik bilgi ve iletişim sistemleri üzerinde gerçekleştirilen organize saldırılar bütün olarak tanımlanmaktadır. Siber savaşlar stratejik, operatif ve taktik olmak üzere her seviyede uygulanabilir olma özelliğine sahiptir. Bu nedenle her seviyede istenen etki elde edilebilmektedir. Hedef olarak ise siber savaşlar temel olarak ülkelerin kritik bilgi sistemi altyapılarını hedef almaktadır. Siber savaş sayesinde bu altyapıların hizmet dışı bırakılmasının yanısıra, ülkelerin sivil ve askeri hassas kıymetli bilgilerine ulaşılabilmektedir. Söz konusu bilgiler çalınabilir, hatta silinebilmektedir. Ayrıca saldırıya maruz kalan ülke halkının ve yönetimini siber ortamda dezenformasyon ile psikolojik olarak etkilemek de mümkün olmaktadır. Bu nedenle toplumun her kesimini etkileyebilmek de, çatışma ve rekabet ortamı yaratabilmektedir (Bayraktar, 2015; 48).

Siber uzayın sanal olması ordu yapısının da kısmen sanal çalışmasına imkân sağlamaktadır. 1900'lü yıllarda iyice konuşulmaya başlanan siber saldırılar medyada "cyber war" olarak ifade edilmeye başlandı. Time dergisi 1995 yılının Ağustos

sayısında konuyu kapağına taşımış ve konuyu manşet ile takipçilerine duyurmuştu. Ülkelerin oluşturduğu söz konusu kuvvetleri istihbarat toplamak, fiziksel operasyonlara elektronik destek vermek, gelebilecek taarruzlara karşı bilgisayar sistemleri ile tam zamanlı savunma yapmak, uluslararası politikanın gidişatına göre tavır almak gibi çeşitli faaliyetlerde bulunarak internet ile bilişim sistemlerini etkin kullanmak üzere yapılandırılmışlardır. Barış, savaşın başka metotlarla devamı ve silahlı savaşa hazırlanmanın ayrı bir şeklidir. Aynı durum siber uzay için de geçerlidir ve barış zamanında ülkeler başka ülkelere daha sonra "ziyaret" etmek üzere arka kapılar bırakmaktadırlar. En basiti orijinal yazılımları crackleyerek internete sızdırmak bunların en bilinen yöntemlerden biridir (Kurgan, 2018: 137)

1978 Washington mutabakatı ile başlayan deregülasyon politikaları neoliberalizm ile başlayan süreçte 2008 krizi dünya tarihinde yaşanan ilk küresel kriz olma özelliğini taşır. 2008 krizini diğer krizlerden ayırıp onu küresel bir kriz durumuna dönüştüren sebep ise sermaye hareketlerinin tam serbestliğe sahip olmasıdır. Tarihin hiçbir döneminde küresel sermaye bu denli rahat hareket edememiştir. Bunda internetin olağanüstü katkısını belirtmeliyiz. Kendisi de muhasebeci olan Karl Marx, "Para İsrailoğullarının kıskanç tanrısıdır. Yahudi Tanrısı dünyevileştirilip, yeryüzünün Tanrısı haline getirildi." demişti. Gerçekten artık onlar küresel finans endüstrisine hükmediyorlar. İnternet akıl almaz yoğunlukla veri ve bilgi depolanmıştır. Bunların çoğu paha biçilmez, yorumlanamaz özellikte olup, küçük bir oranı sahtelik konusunda tekliğe arz etmektedir. Ağ sistemleri üzerine suç, sinai casusluk ve siber savaş arasında gidip gelen bilgisayar korsanları ile istihbarat ajanları gibi epeyce uzmanlaşmış grupların sağladığı birbirine bağlantılı daha fazla bağımlı olmaya başladık. İnternet ve finans endüstrisi "bilgi asimetrisi" dediğimiz bankalar ve diğer finansal kurumlarla sıradan yatırımcılar arasındaki bilgi eksikliği bir tarafa internet ve finans endüstrisindeki inovatif uygulamalar her iki alanda bayağı bilgi sahibi olanların bile ters köşe yatıracak analistler korsanlar elinde tam manasıyla şirketlerden şirketlere ve devletlerden devletlere saldırı ve yıkım silahına dönüşmüş durumdadır (Kurtoğlu, 2017; 104).

Estonya 1989 yılında Sovyetler Birliğinin dağılması sonrasında bağımsızlığını ilan etmiştir. Estonya 50 yıl süren Sovyetler Birliği baskısının simgesi

haline gelmiş “kızıl ordu askeri heykelini” ortadan kaldırmak maksadıyla “Bronz Gecesi” denilen 26 Nisan 2007 tarihinde Rus etnik kökenli insanlarla gerginlik yaşamışlardır. İnternet sisteminden yapılan siber saldırı sonrasında en çok kullanılan kamu ve özel sektörleri ait siteler çökmüştür. Estonya’ya yapılan saldırı DDoS saldırısıydı. On binlerce zombi bilgisayar tarafından Estonya siber saldırının esiri olmuştur. Siber saldırıya maruz kalan Estonya’da 27-29 Nisan 2007 tarihleri arasında devletin internet sayfaları, çeşitli gazetelerin web siteleri kullanılamaz hale gelmiştir. 30 Nisan-18 Mayıs tarihleri arasında ise saldırıların hedefini daha organize hale getirilmiş ve internet hizmet sağlayıcıları ve ulusal bilgi sistemleri büyük zararlar görmüştür. Ülkenin en büyük bankası olan Hansabank tamamen kullanılamaz hale getirilmiştir. Ülke içerisinde iletişim ve ticari faaliyetler durmuştur. Alınan tedbirler sayesinde zombi bilgisayarlar ana bilgisayarlar tarafından yeniden programlanarak bu önlemlere adapte olmuştur. Ana bilgisayarların Rusya’da olduğu ve programın Kril alfabesiyle yazıldığı tespit edilmiştir. Fakat Rusya siber saldırıları inkâr etmiştir. Estonya devleti “e-devlet”in kullanılması açısından gelişmiş ve öncü ülkelerin başında gelmektedir. Bundan dolayı “e-devlet” sistemi içerisinde bulunan tüm alt yapı tesisleri etkilenmiştir (Kara, 2013; 47).

2.4. Siber Silahlar

Siber silahlar elektromanyetik ya da fiziksel bir etki olmaksızın doğrudan siber sistemleri bozmak ve tarih tahrip etmek maksadıyla kullanılmakta olan yazılım veya kullanılan yöntemleri denilmektedir. Genel olarak siber silah denildiğinde akla zararlı yazılımlar gelmektedir. Bu yazılımları örnek olarak virüsler, bakteriler, solucanlar, truva atları, arka kapılar, botlar gelmektedir. Yöntemler ise daha farklıdır sahte e-posta göndermek sahte web sitelerine yönlendirme yapmak da siber silahlar arasında yer almaktadır (Keleştemur, 2015; 221).

Terörist grupların siber savaş kabiliyetine sahip olup olmadıkları veya ne kadar kabiliyetleri oldukları açık değildir. Ancak son zamanlarda bazı terörist grupların siber saldırıları bir silah olarak kullanmaya başladıkları görülmektedir. Teröristlerin plan yapmak, mali işlemlerini yürütmek, propagandaları yaymak ve güvenli haberleşmelerini yapabilmek için yoğun olarak bilgi teknolojileri ve interneti kullandıkları bilinmektedir. Örneğin 1993 yılında Dünya Ticaret Merkezinin ilk

bombalanmasının planlanmasından sorumlu olmaktan hüküm giymiş terörist Remzi Yusuf'un diz üstü bilgisayarında kriptolu olarak saklanmış dosyalarında Pasifik'te 12 adet değişik Hava Yolları'na ait bombalama planlarını kapsayan gelecekteki terörist hedeflerin detaylarını bulunduruyordu. Dünya Ticaret Merkezi ve Pentagona yapılan saldırılarla İngiliz Güvenlik Kuvvetlerinin İrlanda Kurtuluş Ordusu İRA'nın Londra civarında bulunan elektrik santrallerini tahrip etme planlarını ortaya çıkarması gibi örnekler terörist grupların kritik alt yapı tesislerine saldırılar düzenleme arzularının her geçen gün daha da arttığını göstermektedir. Dünya Ticaret Merkezine yapılan saldırılar yalnızca can ve mal kaybına yol açmamış, pazarların kapanmasına ve New York şehrinin mali bilgi altyapısının yok olmasına neden olmuştur. Böylece teröristlerin bilgi teknolojisini kritik altyapı hedeflerine karşı bir silah olarak kullanmaya eğilimleri açıkça görülmektedir (Yılmaz ve Salcan, 2008; 54).

ÜÇÜNCÜ BÖLÜM

3. SİBER SALDIRI ÇEŞİTLERİ

3.1. Oltalama (phishing)

Oltalama insanlara ait özel bilgileri kopyalamak maksadıyla yapılan yöntemlerin başında gelmektedir. İnternet kullanıcılarının kandırılması ve ikna edilmesi yöntemi ile gerçek ya da tüzel kişilerin kendine özel verilerinin bankacılık gibi bilgilerinin elde edilmesine imkân veren bir internet dolandırıcılığı yöntemidir. Oltalama genellikle e-posta aracılığıyla yapılan bir siber saldırı tekniğidir. Kişilerin kullanmakta oldukları sosyal medya hesapları ve mail hesapları aracılığı ile kişinin müşterisi olduğu bir bankadan ya da üyesi olduğu bir kuruluştan mail geliyormuş gibi bir mail atılır ve mail içerisine yerleştirilen yönlendirme linkinin tıklanması ile bilgileri elde etmek isteyen kişinin belirlemiş olduğu yere link aracılığı ile girilen bilgiler kaydedilir ve bu bilgiler yetkisiz kişilerin eline geçmiş olur. Oltalama yönteminin en sık kullanıldığı alan olarak ise karşımıza finans sektörü ve resmi kuruluşlar çıkmaktadır. Nitekim bu kuruluşlar aracılığı ile gönderilen e-postaların kopyası yapılarak anlaşılması çok zor bir hale dönüştürülmektedir. Bu yönteme maruz kalan kişilerin kişisel bilgilerine ulaşan kişiler bu bilgiler aracılığı ile kişilerin hesaplarına yetkisiz erişim ve yetkisiz işlem yapma yetkisine sahip olabilmektedirler. Kötü niyetli üçüncü kişilerin bu yöntemlerle haksız kazanç elde etme olasılığı da artmaktadır. Oltalama yapan kişiler genellikle sunucusu farklı ülkelerde bulunan web siteleri tasarlayarak bu sitelere yönlendirilen linkler aracılığı ile bilgileri elde ederek amacına ulaştıktan sonra bu sitelerin ya sunucularını değiştirerek ya da kapatarak ulaşılabilir olmaktan çıkarlar. Özellikle bilişim hukukunda gelişmemiş ülkelerde bu

sitelerde bağlantı kurulan yerlerin ve kullanan kişilerin tespit edilmesi çok zordur (Eren, 2017: 37).

3.2. Kötücül Yazılım (Malware)

Kötücül yazılım bilgisayar kullanıcılarının haberi olmaksızın kullandıkları bilgisayarlara sızmak ve bu bilgisayarlara zarar vermek amacıyla kodlanmış yazılımların genel adıdır. Bilişim ağlarına yetkisiz erişim sağlamak için ve kullanıcıların iradesi dışında farklı işlerde kullanılmak üzere yerleştirilir kötücül yazılım bulundurulduğu ülkeler bakımından uzak doğu ülkeleri miktar bakımından daha yoğun bölgeler olarak karşımıza çıkarken, Avrupa ülkelerinde bu oran daha az olmaktadır. Bunun sebebi olarak hukuki alt yapının oluşturulmuş olmasını ve önleme çalışmalarının daha yoğun olarak uygulanmasını söyleyebiliriz. Çin başta olmak üzere Türkiye ve Tayvan'da bilgisayarlara bulaşan kötücül yazılım oranlarının daha yüksek olduğunu söylemek mümkündür (Eren, 2017: 39).

3.2.1. Truva Atı (Trojan Horse)

Truva atı internet kullanıcıları için faydalı gibi görünen ancak içinde barındırdığı zararlı kodlar sebebiyle bilişim güvenliğine zarar veren bir program türüdür. Truva atları bilgisayarları kullanıcılarının isteğinin dışında yönetmek ve bilgisayarlara erişim sağlamak için kapı açan programlardır. Özellikle lisanslı ve ücretli yazılımların ücretsiz olarak sunulduğu siteler aracılığı ile indirilen programların çalıştırılması ile bilgisayarlara bulaşır. Farkında olmadan kullanıcı kendi faydasına olacak ücretsiz bir yazılım indirdiğini düşünürken arka planda bir truva atı da yüklenmiş olabilir ve kullanıcısının bilgisi dışında hatta çoğu zaman haberi bile olmadan çalışmayı sürdürmektedir. Truva atının kullanıcı bilgisayarına yerleştiren bilgisayar korsanları arka kapılar aracılığı ile kullanıcının bağlı olduğu sistemlere erişim sağlayarak kullanıcının bilgilerini kullandığı şifreleri ele geçirebilir (Eren, 2017: 42).

Truva atı genel olarak internetten indirilen müzik, dosya ve programlara iliştirilmiş olarak bilgisayarınızın içerisine girmekte veya e-posta yoluyla ulaşmaktadır. Truva atı sunucu ve istemci kısmı olarak iki kısımdan oluşur. Sunucu

kısmı hedefteki bilgisayara yüklenmiş olan program, istemci kısmı ise bu yazılımı kullanarak hedefe erişen kullanıcının bilgisayarına kurulan karşı taraftaki bilgileri çekmeye ve hedef bilgisayarı komut vermeye yarayan programlardır (Benzer, 2014; 28).

Trojen olarak da bilinen truva atları tıpkı tarihte olduğu gibi iyi niyetli zararsız gibi kendini gösterip sisteme girerler. Ancak arka planda hiç istenmeyen faaliyetler sevgilerle bu zararlı yazılım türünü ismi Yunanlılar tarafından truva hediye olarak gönderilen tahtadan inşa edilmiş at figüründen gelmektedir. Truva atlarının en önemli özelliği yazılımcı ile sürekli iletişim halinde olması böylelikle hedef sistemi her türlü erişim hakkını sağlayabilmesidir. Virüsün aksine bir başka bilgisayara kendisini kopyalamaktadır. Kimi zaman kurbanın bilgisayarında çalıştıktan sonra sanki eğlenceli bir programmış gibi kendisini gösterir. Bu basit bir bilgisayar oyunu olabileceği gibi havai fişek patlaması gibi bir animasyon da olabilir. Bir kere çalıştırdığı anda, artık sistemde yerini alır ve bilgisayar çalıştığı, internete bağlı olduğu sürece yazılımcı tarafından kontrol edilebilir. Saldırganlar truva atlarını kullanarak toplu saldırılar düzenleyebilecek gibi tekil bilgisayarlar üzerine çalışma yapabilmektedir. Truva atlarının çalışma prensipleri genel olarak aynı olmakla birlikte görev bakımından farklılıklar gösterebilmektedir (Keleştemur, 2015; 223).

3.2.2. Virüs (Virus)

Virüsler en eski ve en tehlikeli kötücül yazılım olarak bilinmektedir. Nitekim bilgisayar belleğine yerleştirilen yerleştiği zaman programlarda değişikliklere yol açan en önemlisi de kendi kendini çoğaltılabilen bilme özelliği bulunan zararlı yazılımlardır. Virüsler çoğaldıkları bilgisayarlarda bilgisayardaki verilere zarar vermenin yanında sisteme de zarar vererek sistemin çökmesine neden olabilir (Eren, 2017: 43).

Bilgisayar virüsleri tıpkı biyolojik virüsler gibi çalışmaktadır. Başka programlara bağlıdırlar ve içlerine kızdıkları yapıda hızlı bir şekilde çoğalabilmektedirler. Sızma işleminin ardından içten içe görevine başlayan virüs sonuç olarak sistemi kullanılamaz hale getirebilmektedir. Virüsler mevcut sistem içerisinde kendini çoğalabildiği için ev sahibini taşıyıcı olarak da kullanabilmektedir.

Genellikle içine gizlendiği programı çalıştırılması ya da sistem içerisindeki bir aksiyonun faaliyete geçmesiyle birlikte yayılmaya ya da çalışmaya başlarlar. Kimi virüs kendini kopyalamak için internet ve yerel ağlar kullanabileceği gibi kimisi USB, diskler, CD ve DVD'ler gibi harici depolama araçlarında kullanabilmektedir (Keleştemur, 2015; 222).

3.2.3. Solucan (Worm)

Solucan bağımsız, kendi kendine çoğalabilen, ağda bir bilgisayardan diğerine yayılma yollarını araştıran ve yayılan bir programdır. Kurt olarak da adlandırılır. Solucan işletim sistemleri ve programların güvenlik açıklarını kullanarak önce bir bilgisayardan başlar, sonra ağdaki diğer bilgisayarları ile iletişim kurduğu anda kendini o bilgisayara transfer eder. Saniyeler içinde milyonlarca bilgisayara bulaşma kabiliyeti vardır. İnternet aracıyla dağılan ve o ana kadar ki en büyük hasara neden olan en eski solucan Morris Internet Worm'dur. Boston Bilim Müzesi'nde sergilenen bu solucanın kaynak kodunun yer aldığı disket bulunmaktadır (Çiftci, 2017; 169)

İngilizce Worm olarak bilinen solucanlar Türkçe'de aynı zamanda kurt olarak da kullanılmaktadır ve virüslere nazaran daha zararsız bir yapıya sahiptir. Solucanlar veri kaybı ya da sistem hasarı oluşturmazlar. Ancak virüslere göre çok daha hızlı ve sistematik bir yayılma gücüne sahiptirler. Hiçbir uygulamaya bağımlı olmaksızın kendi kendine çoğalabilen ve bağlı olan aracılığıyla diğer sistemlere de kolayca ulaşabilmektedirler. Sistemin açıklarından faydalanan solucanlar çoğalma ve yayılma süreci içerisinde sistemin yavaşlamasına sebep olmaktadırlar. Solucanların sadece birkaç saniye içerisinde milyonlarca bilgisayara ulaşabilme yetenekleri bulunmaktadır. Gelişmiş yapıdaki solucanlar e-posta listeleri veya sohbet uygulamalarınızdaki kişi listelerini tarayarak bu kişilerin bulunduğu sistemleri doğrudan yayılma kapasitesine sahiptirler (Keleştemur, 2015;226).

3.2.4. Reklam İçerikli ve Casus Yazılımlar (Creative Content and Spyware)

Reklam içerikli ve casus yazılımlar bilgisayar kullanıcılarının istekleri dışında sürekli reklam içerikli mail gelmesini ve bilgisayarlara yerleştirilen yazılımlar

aracılığı ile kullanıcı bilgilerinin karşı tarafın eline geçmesini ifade etmektedir. Reklam içerikli yazılımlar web tarayıcıları aracılığı ile bilgisayara yerleşerek sürekli kullanıcının isteği dışında sayfaların açılmasını ve reklamı yapılan sayfalara yönlendirmelere sebep olmaktadır. Tarayıcının varsayılan ayarları bilgisayarlara bulaşan reklam içerikli yazılım aracılığı ile değiştirilmektedir. Örneğin kullanıcının ayarlamış olduğu arama motoru ya da ana sayfa olarak belirlediği web sayfası bu şekilde değiştirilmiş olabilir (Eren, 2017: 45).

3.3. Botnet

Botnet kullanıcıların bilgisi dışında bilgisayarlarına yerleşen kötücül yazılımlar aracılığı ile merkezi bir yerde çok sayıda kötücül yazılım ulaştırılmış bilgisayarlar kümesini ifade etmektedir. Kullanıcısının iradesi dışında kötücül yazılım bulaşmış olan bilgisayarlar terminolojide zombi olarak nitelendirilmektedir. Botnet tek bir noktada genellikle bir kişi tarafından kontrol edebilme yeteneği sağlamaktadır. Bir zombiye dönüşmüş olan bilgisayarlar bu kişiden gelecek komutlar doğrultusunda farklı amaçlara hizmet etmek için kullanılabilmektedirler. Bu ağ sistemini yönetmek için tasarlanmış kötücül yazılımlara ise bot adı verilmektedir. Bu sayede botnet sahibi kötü niyetli kişi verecek komutlarla dünyanın farklı yerlerindeki çok sayıda bilgisayarı amaçları doğrultusunda işlem yaptırabilmektedir. Kullanıcısının haberi olmadan gizlice bilgisayara yerleşmiş olan kötücül yazılımlar aracılığı ile binlerce bilgisayar botnet sahibi tarafından yönetilmekte ve kontrol edilebilmektedir (Eren, 2017: 48)

Botlar yazılan kodlar doğrultusunda otomatik işlemler yapan ve birtakım yönetimsel araçlar ele geçiren yazılımlardır. Özellikle toplu saldırılar için kullanılan botlar sayısını hedefteki sistemlerin çalışması engellenmektedir. Son cümleden de anlaşılacağı gibi botlar sistemlere zarar vermek yerine çalışmalarını engellemek veyahut yavaşlatmak maksatlı kullanılmaktadır. Köle bilgisayarlar tarafından devamlı surette saldırı silah olarak kullanan botlar, günümüzde ayrıca web sitelerine otomatik olarak zararlı yazılım indirilmesi şeklinde kod toplu olarak da görev almaktadırlar (Keleştemur, 2015; 228).

3.4. Hizmeti Engelleme (Dos/DDoS) Saldırıları (Service Blocking (Dos/DDoS) Attacks)

Hizmeti engelleme saldırıları günümüzde bilişim sistemlerinin erişilebilirliğine yönelik gerçekleştirilen en yaygın saldırı türü olarak karşımıza çıkmaktadır. Dos/DDoS saldırılarının kullanıldığı birçok yöntemdeki temel amaç, gerçekleştirilen siber saldırılar ile resmi bir kuruluşun ya da şirketin bilgi iletişim ağlarını kilitlemek ve verdiği hizmetleri engellemeye çalışmaktır. Günümüzde hizmeti engelleme saldırıların büyük çoğunluğu birden çok bilgisayar kullanılarak gerçekleştirilebilmektedir (Eren, 2017: 51).

2018 yılının başlarında Reddit başta olmak üzere birçok platform üzerinde milyarlarca kişiye ait e-posta adresi ve parola bilgileri yayınlandı. Artık siber suçların yanı sıra bu işe yeni başlamış kişiler bile yeraltı olarak tabir edilen platformlar üzerinden hassas bilgileri rahatlıkla erişebilmektedir. Siber suç saldırıları katlanarak devam etmektedir. Sızdırılan veriler bugüne kadar ki en büyük sızıntı olarak kabul edilecek cinsten. Toplamda 1 milyarın üzerinde kişinin e-posta adresi ve parola bilgisi yayınlanmış görünmektedir. 41 GB boyutuna sahip liste 5 Aralık 2017 tarihinde bir forum sitesinde yayınlanmıştır. Listenin son olarak 29 Kasım 2017 tarihinde güncellendiği gözlenirken toplamda yayınlanan kullanıcı adı ve parola bilgisi sayısının 1 milyar 400 milyon 5536 bin 869 olduğu görülmektedir. Veriler daha hızlı artırılabilmesi amacıyla parçalanmış ve alfabetik olarak ağaç yapısına dönüştürülmüştür. Bugüne dek yaşanan veri sızıntıları arasında bu sonuncunun en büyük veri sızıntısı olduğunu rahatlıkla söylenebilmektedir. Bundan önce gerçekleştiren en büyük sızıntı yaklaşık 797 milyon olan Exploit.in Combo listesine aitti. Yeni gerçekleştiren sızıntı ise neredeyse bu sızıntının iki katı büyüklüğündedir (Altınkaynak, 2018: 13).

3.5. Mantık Bombaları (Logic Bombs)

Mantık bombaları, iletişim ve haberleşme sistemlerinde öncelikli olarak herhangi bir zarar vermeyen, ancak istenilen şartlar oluştuğunda veya belirlenen zamanın geldiği durumlarda ortaya çıkarak zarar veren virüs programlarıdır. Truva atlarına benzer özellik taşıyan mantık bombaları önceden belirlenmiş özel şartlar

oluştuğunda ortaya çıkarak zarar verir ve kendisini sürekli açığa çıkarmayan Truva atları programlarından bu noktada ayrışmaktadır. İstenilen ortam oluşana kadar faydalı bir program gibi gözüken temelinde ise zarar vermek geliştirilen programlardır. Mantık bombalarının tek amacı içerisine yerleştirilen sistemleri yok etmek, çalışamaz duruma getirmek olduğundan dolayı, dönüşüm geçirdikleri sistem için yıkıcı olmaktadırlar. Mantık bombası örnek olarak 1999 yılında ortaya çıkan "Çernobil Virüsü" gösterilebilir (Çakır ve Kılıç, 2014; 29).

3.6. Köle Bilgisayarlar (Zombie)

Bilgisayarlar yüklenen bir program vasıtası ile uzaktan kontrol edilebilir. Uzaktan kontrol edilebilen ve saldırganın her türlü amacı için kullanabilen bilgisayarlara köle bilgisayar adı verilir. Köle bilgisayar oluşturmak için gerekli çeşitli yöntemler kullanılmaktadır. Zararlı kod içeren bir web sitesinin ziyaret edilmesi sonucu zararlı kod çalışır ve kullanılan web tarayıcısına tarayıcı eklentisine veya güncel olmayan işletim sistemine ait bir zafiyet istismar edilerek kullanıcı farkına varmadan arka planda zararlı yazılım yüklenir. Ekinde zararlı bir yazılım ya da zararlı kod içeren bir dosya bulunan e-posta gönderilerek ekteki zararlı yazılımlara dosyanın kullanıcı tarafından çalıştırması sonucu zararlı yazılım yüklenir. Zararlı yazılımlar internette genellikle ücretsiz veya cüzi bir fiyata satılan korsan yazılımlar yoluyla bilgisayara yüklenir. Kullanıcısı bilgisayarına gizlice yüklenen ve saldırgan hedef sistemi internet bağlantısı üzerinden uzaktan kontrol etmesine imkân sağlayan programlar aracılığıyla köle bilgisayarlar kontrol edilir. Kullanıcısının haberi daha olmadan uzaktan kontrol edilebilen bu bilgisayarlar her an saldırı için kullanılmaya hazır ve tehlikeli olduğundan "köle" olarak adlandırılır (Çiftci, 2017; 172).

DÖRDÜNCÜ BÖLÜM

4. SİBER TERÖRİZMLE MÜCADELE

4.1. Siber Saldırılara Karşı Alınacak Tedbirler

Siber güvenlik; "Siber ortamda 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." Bilgi güvenliğinde siber ortamda bulunan kurum, kuruluş ve kişisel kullanıcıların bilgi güvenliğinin sağlanması maksadıyla üç ana unsura dikkat edilmelidir. Bunlar, erişebilirlik, bütünlük ve gizliliktir. En önemli unsurların başında gelen gizlilik iş hayatında değil kişisel verilerin korunması anlamında değerlendirilmelidir. Olabilecek herhangi bir siber saldırıda kişisel bilgilerin yetkisiz insanların eline geçmesi durumunda varlığın gizliliğinin ihlal edilmesine neden olacaktır. Siber ortamda saklanan verilerin bütünlüğünün korunmasındaki gaye ise yetkisiz kişiler tarafından bilginin bütünlüğünün değiştirilmemesi ve bozulmamasını sağlamaktır. Varlığın bilgi güvenliği bileşenlerinden biri olan erişebilirlik ile de anlatılmak istenen bilgiye ihtiyaç duyduğunda erişebilmesidir. Yapılacak olan siber siber saldırılar sonucu bilgiye, veriye olan erişim engellenebilmekte kişi, kurum ve kuruluşları zor duruma düşebilmektedir (Gökçe vd., 2014: 215).

Şirketler ve kurumlar bilişim sistemlerinde "firewall" adı verilen güvenlik duvarı yazılımları bulundurarak yetkisiz erişimlerin önüne geçmeli ve bilişim sistemlerine anti-virüs yazılımları yükleyerek ve bu yazılımları internet üzerinden sürekli güncelleyerek yeni virüslerin bilişim sistemine girmesin önlemeli, girenleri ise temizlenmeye çalışılmalıdır Özellikle büyük kurumların bilgi işlem

merkezlerinde ancak yetkisi olan ve güvenilir personelin alıştırılmasının sağlanmasıdır Son olarak ise, özellikle genç kuşak "siber etik" denilen sanal âlemde davranış kuralları konusunda eğitilmelidir (Özkışlalı, 2008; 102).

2009 yılında ABD Başkanı Barack Obama (25 Mayıs 2009) yapmış olduğu değerlendirmede siber tehditleri Amerika için en önemli ekonomik ve ülke genelinde güvenlik problemi olarak göstermiştir. Ülkenin huzur ve refah ortamının siber güvenlikle doğru orantıda olduğunu belirtmiştir. Amerika'nın 21. Yüzyıldaki huzur ve refahının siber güvenliğe dayandığını belirtmiştir. İngiltere'nin 2010 yılında yayınlanan ulusal güvenlik stratejisinde siber saldırılar uluslararası terörizm ve uluslararası askeri krizlerle aynı kategoride değerlendirilmiştir. Stratejinin önsözünde Başbakan Cameron siber saldırıların Britanya'ya ölümcül hasarlar verebileceğini belirtmiştir. 2011 yılında NATO Güvenlik Konferansı'nda Almanya Başbakanı Merkel (5 Şubat 2011) klasik askeri tehditlerin "geçmişe ait bir şey" olduğunu söyleyerek, NATO'nun yeni stratejik konseptinde her şeyin siber savunma ve siber saldırılar üzerine kurulduğunu ilan etmiştir (Demircioğlu, 2014: 39).

Bilişim suçlarını kovuşturan ve yargılayan makamların az da olsa teknik bilgiye sahip olmaları gerektiğinden özel ihtisas mahkemelerine ihtiyaç vardır. Ancak bu mahkemeler, bilişim sistemleri konusunda eğitimli ve bu konuda özel olarak görevlendirilmiş kolluk görevlilerinin kovuşturmaya katılmasıyla anlamını bulacaktır. İnternet süjelerinin hak ve sorumlulukları açıkça belirlenmeli ve suç teşkil eden içerikten dolayı kimin sorumlu olacağının net bir şekilde ortaya konulması gerekmektedir. Sanal suçun failini, zamanını ve yerini tespit etmek açısından, trafik verilerinin kayıt altına alınması sağlanmalıdır. Bu alanda eğitilmiş devlet örgütlerinin yanı sıra özel sektörün de yardımı ve hatta uluslararası işbirliğinin sağlanması da gerekmektedir. Adli Tıp ya da üniversite bünyesinde, haksızlığa yer vermemek için bilirkişilik hizmeti alma amacıyla bilişim ihtisas daireleri kurulmalıdır. Polisin ve diğer kolluk birimlerinin bilişim suçları konusunda eğitilmesi gerekmektedir. Kollukça yapılan kovuşturmalar için özel hayatın gizliliğini ve temel özgürlükleri koruyucu düzenlemeler yapılmalı, hukuka uygun deliller elde edilmesi sağlanmalıdır. İnternet kafe işletmecileri meslek odası şeklinde örgütlenmeli, internet kafeler kollukça değil, STK düzeyinde kuruluşlarca ve eğitimcilerle denetlenmelidir.

İnternet kafelerden bilişim suçu işlenememesi için program indirmeye ve yüklemeye izin vermeyen yazılımlar kullanılmalı, bu yazılımların işletilmesi ve kullanılması meslek kurulacak meslek odasınca zorunlu tutulmalıdır (Özkışlalı, 2008; 102).

4.2. Siber Terörizm ile Mücadelede Karşılaşılan Zorluklar

Sunulan bilgiler ışığında ve Castells'in "ağ toplumu" kuramından yola çıkıldığında bu binyıl dönümünde dünyanın yeniden şekillendiği görmekteyiz. Üç bağımsız sürecin bir araya gelmesi enformasyon teknolojisi devrimi, kapitalizmin ve devletçiliğin ekonomik krize girmesi ve yeniden yapılanması ve kültürel ve toplumsal hareketlerin yeşermesi yeni dünyanın köklerini oluşturmaktadır. Bunun sonucunda kapitalizmin yeniden inşası, teknolojinin çok hızlı gelişmesi, küreselleşmenin olumsuz etkileri ve mikro milliyetçiliğin yükselmesi yeni bir küresel terörizm, yani siber terörizmi yaratmıştır (Özkışlalı, 2008: 103).

Dijital dünyada yaşamaya devam ettikçe siber suçluların sömürmek için fırsatları artmaya devam edecektir. Siber suçlar en hızlı büyüyen suç şekliyle her gün 1 milyondan fazla insan siber suça maruz kalmaktadır. Bu suç şebekeleri her gün daha yanıltıcı ve karmaşık işlemeye devam etmekte ve bunlarla mücadele için daha güvenilir, sağlam araçlara ihtiyaç duyulmaktadır. Siber suçlular bazı riskleri ve büyük parayla çalışmaktadırlar. Bu da bu alanı klasik suçlardan daha çok tercih edilen bir yöntem olarak kullanmaya teşvik etmektedir. Bu bağlamda siber suçları azaltmak için güçlü ve etkili bir yasamanın varlığı büyük önem arz etmektedir (Eren, 2017; 85).

Soğuk savaşın bitmesi ile birlikte siber ortam gerçek ve tüzel kişilikler tarafından yoğun bir şekilde kullanılan bir alan olmuştur. Siber uzay yoğun şekilde paylaşılan ve geniş kullanıcı kitlesine sahip bir alana dönüştü. Ülkeler kamu alanlarında bulunan birçok hizmeti siber alan içerisinde kullanıcılar için sunmaya başlamıştır. Diğer taraftar her geçen gün hızlarını artıran işlemciler verilen hizmetlerden faydalanmak istenilen kullanıcıların artmasına neden olmuştur. Başlıca, gaz, elektrik, su dağıtım işleri ile kara, deniz ve hava yollarının kontrolleri işletim sistemleri ile sağlanmaya başlanmıştır. Bulunduğumuz dönemlerinde bu kritik alt yapılara yapılacak saldırılar için bir tehdit oluşturmaktadır. Siber ortamın

hayatımızın içerisine girdiği bu dönemde 1994 yılının Aralık ayında Rus askeri birlikleri Çeçenistan'ın başkenti olan Grozni'ye girdiler. Rus birliklerinde bulunan gelişmiş ağır silahlarla Çeçen direnişinin çok fazla sürmeyeceği planladılar. Ancak çatışma alanındaki asıl gerçeklerle uyuşmadı. Soğuk savaş sonrasında ilk defa askeri bir çatışma siber ortama taşındı. Çeçenler ellerinde bulunan tüm medya unsurları ve özellikle internet ortamını çok iyi bir şekilde kullanmaya başladılar. Böylelikle bilgi savaşlarının ilk örneklerini vermeye başladılar. Çeçenler çatışmalardan ölü olarak ele geçirdikleri Rus askerlerin görüntülerini internet ortamından tüm dünyaya yansıttılar. Bunun üzerine bölgede bulunan Rus askerlerin anneleri çocuklarını kurtarmak amacıyla hareke geçtiler. Yapılan bu bilgi ve propaganda internetin savaş alanı olarak kullanıldığı ilk örneklerden birisiydi. Bu yeni dönemde internet sadece iletişimin yapıldığı bir ortam olmaktan çıkıp korunması gereken bir alan haline gelmeye başlamıştır. Rus-Çeçen çatışmasında internetim kullanılması ister istemez alternatif tehditleri akla getirince uluslararası sistemin güçlü ülkeleri muhtemel saldırılara karşı hazırlık yapmaya başladılar. Ulus-devlet düzeyindeki hazırlıklar bütün aktörler açısından yeterince etkin olamayınca uluslararası yapılar devreye girmeye başladı. Bunun öncülerinden olan NATO daha 1999'da üyelerini askeri haberleşme sistemlerine karşı yapılabilecek saldırılar hakkında uyarmış ve hazırlıklı olmalarını istemişti (Aydın, 2013; 29).

Terörizmle mücadele, yurtiçindeki ve yurtdışındaki mücadeleyle beraber, bir bütündür. Özellikle, terörizmin genel kabul gören bir tanımının yapılması gerekmektedir. Çünkü bir ülkenin terörist olarak tanımladığı kişi bir başka ülke tarafından siyasal suçlu olarak nitelendirilirse terörle mücadelenin bundan olumsuz etkilenmesi kaçınılmaz olur (Özkışlalı, 2008: 92).

Başkan George Bush Dünya Ticaret Merkezi ve Pentagon'a yönelik 2001'de yapılan saldırılardan sonra terörizme karşı savaş ilan etmiştir. Kongrenin birleşik oturumunda ki bir konuşmasında 'Özgürlüğün düşmanları ülkemize karşı savaş açtı" diyordu. Başkanın sözcük seçimi hukuk dilinden, savaş diline doğru dramatik bir değişimi temsil ediyordu. Başkanın terörizme karşı savaşı Bush doktrini olarak adlandırılan kavramının ortaya çıkmasını sağladı. "Bugünden itibaren diyordu" Bush ülkesine terörizmi barındırmaya ve ona destek olmaya devam eden her ülke ABD

tarafından düşman bir rejim olarak algılanacaktır. Bush doktrini teröristler için sığınak sağlayan devletlerin egemenlik ilkesini hükümsüz kılıyordu. Egemenliğin dokunulmazlığı 1648 yılında 30 Yıl Savaşları'nın bitirerek ulus devletlerin uluslararası ilişkilerin temel aktörü haline getiren ve Wesphalia Anlaşması ile kurulan uluslararası sistemin temel direği olmuştu. 300 yıl sonra bu uluslararası düzen modeli Birleşmiş Milletler yasasında "devletleri iç işlerine müdahale edilmemesi" olarak ifade edilerek yeniden farklı bir boyut kazanmıştır (Allison, 2006: 153).

Dünya üzerinde devletlerarası meydana gelebilecek herhangi bir saldırıda başvurulacak temel kurum BM'dir. Birleşmiş Milletler Sözleşmesi madde 51. "Bu anlaşmanın hiçbir hükmü Birleşmiş Milletler üyelerinden birinin silahlı bir saldırı hedef olması halinde Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve konseyin iş bu anlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir şekilde etkilemez şeklinde olup, herhangi bir çatışma anında ilk yapılması gerekenleri açıklamaktadır. Ancak bu ifade klasik fiili anlamda bir çatışmadan bahsedildiği görmek nedir bu ifade herhangi bir şekilde siber saldırı ifadesi yer almamaktadır. Siber güvenlik kavramının gelişmesi siber tehditlerin etkileriyle kapsamlarının genişlemesi ve sınırlar üstü bir savunma zafiyeti haline gelmesi siber savaş hukuku hakkında çalışmasını gerekli kılmıştır. Bu kapsamda yapılan uluslararası ilk çalışmalardan biri NATO Siber Savunma Mükemmeliyet Merkezi uluslararası bağımsız uzmanlar grubunca hazırlanan siber savaşa uygulanacak hukuk hakkında Talin El Kitabı olmuştur. Tallinn el kitabı savaşa girmenin haklı nedenleri savaş sırasında uyulması gereken kurallar devletlerin ulusal politikaların bir aracı olarak kuvvete başvurmak konusunu düzene uluslararası hukuk silahlı kuvvetleri yönetimi ve düzenli uluslararası hukuk savaş hukuku silahlı çatışma okulu, uluslararası insanlık hukuku da dâhil konularını içermektedir. El kitabı bağımsız uzman grubun görüşlerini ibaret olup resmi bir nitelik taşımamaktadır. Mükemmeliyet merkezinin destekli ülkelerinin ve NATO'nun görüşlerini temsil etmemektedir. El kitabı

Cambridge Üniversitesi tarafından 2013 yılı Mart ayında yayınlanmıştır (Ünal, 2015: 123).

Siber suçlarda suçun gerçekleşme süresi, klasik suçların aksine, bilgisayarların işlem hızları ile yani mil saniye, mikro saniye ve nano saniye gibi değerler ile ölçülmektedir. Teknoloji aynı anda birden çok suçun birden çok kişiye karşı ve mağdurlarla temasa gerek kalmadan işlenebilmesine imkân sağlamaktadır. Klasik yöntemde suçla mücadelede var olan tepkisel strateji siber suçlar söz konusu olduğunda yarar sağlamamaktadır. Çünkü tepki genellikle suç işlendikten ve izler soğuduktan oldukça sonra başlamaktadır. Siber suçlarda saldırganın nadiren suç mahallinde bulunması nedeniyle, klasik suçların aksine suç hazırlığı, icrası ve kaçış esnasında yakalanma olasılığı da ortadan kalkmaktadır. Böylece siber suçlular çok hızlı bir şekilde suçu işlemeyi müteakip, gerçek kimlik ve yer bilgilerini açığa vurmadan kaçabilmektedirler. Siber suçların elektronik ortamda oluşması nedeniyle bu suçlara ait deliller varsa elektronik ortamda bulunmakta ve çok kolay yok edilebilmektedir. Siber suçlular suçu gerçekleştirdikten sonra sıklıkla izlerini saklamak, kaybettirmek ya da izlerini sürenleri yanlış yönlendirmek için elektronik ortamdaki sistem kayıtlarını değiştirmekte veya yok etmektedirler. Bunun için çok gelişmiş program ve araçları da kullanmaktadırlar. Dolayısıyla bazen takip edilecek bir iz bulmak, doğru izi takip etmek veya var olan izleri takip ederek gerçek suçluya ulaşmak güçleşmekte ve bu sayede siber suçlular klasik suçlulara nazaran mükemmel bir şekilde kendilerini gizleme olanağına sahip olabilmektedirler. Siber suçlar nispeten çok daha yeni bir alandır ve bu nedenle birçok ülke bu konuda yetişmiş yeterince personele sahip değildir. Ayrıca, bu personelin eğitimi uzun süreli bir yatırım ve yüksek maliyet gerektirmekte, özel sektörde daha yüksek gelir imkânı nedeniyle yetişmiş personelin elde tutmasında güçlükler yaşanmaktadır. Bir diğer problem de sürekli gelişen teknoloji ve suç teknikleri karşısında personelin bilgilerinin güncel tutulmasındaki zorluktur Dolayısıyla bu durum kolluk güçlerinin siber suçlarla mücadelesini olumsuz yönde etkileyebilmektedir (Özkışlalı, 2008; 93).

4.3. Türkiye’de Siber Güvenlik

24 Kasım 2015 tarihinde Türk Hava Kuvvetlerine ait F-16'ların Türk hava sahasını ihlal eden bir Rus SU-24 uçağını düşürmesi haberi tüm dünyanın gündemine

girmiştir. Yaşanan bu olay kısa sürede büyüyerek Türkiye ve Rusya Federasyonu arasında gelişen siyasi gerginliğin başlangıcı olmuştur. Bu gelişmelerden sonra 14 Aralık 2015 tarihinde ülkemize yönelik olarak "DDoS" saldırıları yapılmıştır. Yapılan bu saldırılar durumu iyice çıkılmaz hale getirmiştir. Yapılan saldırılar ".tr" uzantılı ağın genişliğini hedef almıştır. Böylelikle ülkemizin özel sektör ile kamu kurum ve kuruluşlarına yönelik yapılan saldırılar sonucunda kritik alt yapılara zarar vermek istenmiştir. Yapılan bu siber saldırılarla ulaşılmak istenilen adreslerle bağlantı sağlanamamıştır. Saldırıları "Anonymous hacker grubu" tarafından üstlenilmiştir. Saldırı nedenlerini ise yayınladıkları bir videoda Türkiye'nin Irak Şam İslam Devleti (IŞİD)'e verdiğini iddia ettiği destekten dolayı yaptıklarını belirtmişlerdir. Ayrıca finansal destek sağlandığı, IŞİD militanlarının ülkemizde tedavi gördükleri iddia edilmiş olup, saldırıların devam edeceği anlatılmıştır. Belirtilen açıklamaların "sahte bayrak (false flag)" operasyonun bir parçası olduğu değerlendirilmektedir. Saldırılar, Türkiye'nin siber güvenlik alanında belli bir mesafe aldığını göstermiştir. Ancak siber savunma direncinin zayıf ve dağınık olduğu görülmüştür. Saldırılar konusunda yeterince bilgilendirme yapılmamış, saldırıların ne kadar sürdüğü, nereleri hedef alındığı, ne kadar zarar verildiğine dair herhangi bir bilgi paylaşımı olmamıştır. Siber saldırılar sonucunda Türkiye'nin finans sektöründe meydana gelen zararlar açıklanmamıştır. Yapılan bu saldırı sorucunda ülkenin alması gereken tedbirler masaya yatırılmış ve incelenmiştir. Yapılan saldırılar toplumsal alanda ciddi deformasyonun oluşmasına neden olmuştur (Darıcılı, 2017: 228).

Sun Tzu der ki "*savaş yeteneği olanlar düşmanının ordusunu savaşmadan bastırır şehirlerini saldırmadan ele geçirir ve devletleri operasyonlar olmadan devirir*." Tzu'nun uzun asırlar önce ki bu sözü 1990'larda Amerika'da ortaya çıkan yumuşak gücün 21 Yüzyıl'a uydurulmuş haliyle uygulanmaya devam edilmektedir. Dünyada sistemine sızılmamış neredeyse hiçbir kurum yoktur. 1992'de kaleme alınmış bir eser Approachin Zero: Data Crime and the Computer Underworld'de Byan Clough ve Paul Mungo'nun ifadeleri de bunu güçlendiriyor. Pentagon, NATO ve NASA gibi kurumların yanında üniversiteler, askeri ve endüstriyel araştırma laboratuvarlarının bilgisayar sistemlerine bilgisayar korsanları misafir oldular. Bu davetsiz misafirlerin bedeli ise 1992 yılında Amerika ve İngiltere her yıl için 2 milyar pound olduğu belirtilmektedir. Raporda bilişim suçlarının %85 gibi ciddi bir

boyutu da kayıtlarda yer almadığı tahmin edilmektedir. Güvenli liman olarak görülen Apple cihazlarda yer yer eden İCloud'un veritabanlarına girilmesi de hiçbir zaman %100 güvenliğin olmayacağını göstermektedir. Öyle ki ülkemize dönüp baktığımızda da 2010'da yaklaşık 50 milyon Türkiye Cumhuriyeti vatandaşının kimlik bilgilerinin devletin kurumlarından ele geçirilerek internette paylaşıldığı bilinmektedir (Kurgan, 2018: 16).

Siber saldırılara maruz kalan Türkiye'de siber güvenlik olaylarına karşı mücadelesine devam etmektedir. Dünya genelinde siber ortamda meydana gelen saldırılarda bir önceki döneme göre %81 artış meydana geldiği Symantec'in yayınladığı İnternet Güvenliği Tehdit Raporunda belirtilmiştir. Bu dönemde Türkiye'ye yapılan saldırılarda da aynı oranda artış meydana gelmiştir. Türkiye'nin de bulunduğu EMEA (Avrupa, Orta Doğu ve Afrika) bölgesinde kötü amaçlı yazılım saldırılarına en çok maruz kalan 10 ülke arasında 4. sıradadır. Türkiye'de internet kullanımı her geçen gün artmaktadır. Türkiye, yaptığı çalışmalar ile AB direktifleri kapsamında çalışmalarını sürdüren diğer ülkeler ile aynı seviyede sürdürmektedir (Kara, 2013: 70).

Bilgi teknolojilerinin kullanımının geniş bir alana yayılması ve bulunduğumuz dönemde kurumlara ait bilgi ve verilerinin büyük oranı siber ortamda bulunması nedeniyle oluşan siber tehditler giderek artmaktadır. Giderek artan sosyal paylaşım ağları ve kullanıcılarının artması, birçok ülkenin hizmetlerini siber ortamda sunması internet ortamındaki bilgilerin artmasına sebep olmuştur. Ortaya çıkan durum birçok devletin yönünü bu alana çevrilmesine neden olmuştur. Çünkü ülkeler arasında yapılan klasik savaşlarda olduğu gibi siber güvenlik alanında da daha önceden alınan güvenlik tedbirleri, yapmış olduğunuz denemeler, yaşadığınız tecrübeler, kurumlar arasındaki uyum ve en önemlisi ortaya çıkardığınız durumsal farkındalıklar siber alanda sistemlerinizi korumaya yardımcı olacaktır. Siber alanda en önemli unsur bu ortamda çalışan personelin farkındalığının ve konu hakkında yeterli bilgi ve tecrübesinin bulunmasıdır. İçerisinde bulundurduğu önemli bilgiler nedeniyle farkındalığın en üst seviyede olması gereken yerlerin başında kamu kurum ve kuruluşları bulunmaktadır. 2010 yılı içerisinde yapılan bir çalışmada siber alanında güvenlik algısının ne derecede olduğu araştırılmış ve kamu kurumlarında

güvenliğin sadece sistemlerin güvenliği anlamında değerlendirildiği görülmüştür. Bu alanda yapılan en büyük çalışma güvenlik duvarları olarak dikkat çekmektedir. Sadece güvenlik duvarları ile siber alanda güvenli olunamayacağı kesindir. Türkiye'de bu konuda özellikle kamu kurum ve kuruluşlarının idari, teknik, hukuksal, bilişim, yönetimsel ve benzeri alanlarda eksik yönlerini tespit etmek, bunlara çözüm bulmak ve daha güvenli bir siber ortamın tesis edilmesi maksadıyla ulusal çapta politika stratejisi ve eylem planlarında oluşan 2013 yılının Haziran ayında yayımlanan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda siber güvenlik alanında özellikle insan kaynaklarının yetiştirilmesi ve bilinçlendirme faaliyetleri başlığı altında siber güvenlik farkındalığı ele alınmıştır (Akın vd., 2016).

Ülkemizde yetkililer uzunca bir süre siber tehditler sadece siber suç seviyesinde değerlendirdi. Yapılan siber saldırılar terörle mücadele kapsamında değerlendirilmiştir. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından siber güvenlik farkındalığının artırılması ve oluşturulması için çalışmalar yapılmıştır. 2010 yılında Milli Güvenlik Kurulu'nda ülkemize yönelik yapılan siber saldırılar değerlendirilerek siber tehditlerin Milli Güvenlik Siyaset Belgesi'ne girmesi kararı alınmıştır. Ocak 2011 yılında TUBİTAK ile Bilgi Teknolojileri ve İletişim Kurumu ortaklığı ile ülkemizde Birinci Ulusal Siber Güvenlik Tatbikatı icra edilmiştir. Yapılan tatbikat sonrasında Türkiye'nin siber saldırılara açık hedef olduğu bu konuda çalışmaların yetersiz olduğu tespit edilmiştir (Aydın, 2013; 45).

Türkiye'nin kan dolaşımı yani enterkonnekte sistemi sabah 10.30 sularında 31 Mart 2015'te çöktü. Ülkemizin tarihinde ilk kez yaşanan bu olay sebebiyle ülke genelinde 10-18 saat elektrik kesintisi yaşandı. Hayat durdu. En kuvvetli ihtimal ülkemizin enterkonnekte sistemine siber saldırıda bulunularak test edildi. 31 Mart saat 10.36 itibaren Türkiye karanlığa görünürken TEİDAŞ'ın Ankara Gölbaşı'ndaki ana kontrol odası ve TEİDAŞ'ın Sakarya Adapazarı'ndaki yedek ana kontrol odasındaki bilgisayarlar aynı anda alarm sesleri verdi ve saliseler içinde Türkiye'nin dört yanını kaplayan hatlardaki elektrik frekansı sistemi çöktü (Kurtoğlu, 2017: 198).

Türkiye'de uzun yıllardan beri yaşanan terör olayları ile ilgili olarak, bulunduğumuz dönemde terör örgütlerine siber ortamda destek veren dış merkezli bilgisayar sistemleri ile ülkemize yapılacak saldırıların olabileceği ve bu saldırılara

karşı alınacak tedbirler kapsamında kamu kurum ve kuruluşları arasında gerekli koordine kurularak, işbirliği yapılmasının önemi her geçen gün artmaktadır. Yapılacak siber saldırılara karşı acil eylem planları ile gerekli hazırlıklar yapılmalıdır. Türkiye aleyhine faaliyet içerisinde bulunan yaklaşık 8000 adet internet sitesi bulunmaktadır. Söz konusu internet sitelerinden 150 tanesi aktif olarak bulunmakta olup, her gün ortalama 900-1000 kişi ziyaret etmektedir. Bu siteler genel olarak net, org, com uzantılıdır. Belirtilen siteler Hollanda, Amerika ve Almanya ile Batı Avrupa ülkelerinden yayın yapmaktadırlar[1] (Özkışlalı, 2008: 89).

Diyarbakır'ın Bismil ilçesinde terör örgütü PKK/KCK'ya ait bir mezarlık bulunduğuna dair internette haber ve fotoğrafların kullanıldığı ve bunlar e-mail yoluyla basına yollandığı anlaşılmıştır. Aslında gerçek dışı olan bu haberlerin PKK terör örgütü veya sempatizanları tarafından yayınlandığı şüphesizdir. Maksat Türk halkının hassasiyetlerini tahribat yaparak büyük bir hayal kırıklığı yaratmak ve devletin otoritesi üzerine şüphe oluşturmaktır. Buna karşılık olarak da http://pkk.kongragel.com. adresli PKK terör örgütünün sitesi hack edilmiştir. Siteye girmek isteyenler Atatürk'ün kalpaklı resminin içinde yer aldığı ay yıldızlı bayrağımız ile karşılaşmaktadırlar. Sayfanın alt bölümünde ise "Bu siteye Devlet-i Ebed müddet ülküsüne gönül veren ve burada gül bahçesine girercesine kara toprağa düşen aziz şehitlerimizin adına el konulmuştur" ifadesi yerleştirilmiştir. Bankalar ve mali kuruluşlara yönelik yapılacak siber terör saldırısında meydana gelen zarar geleneksel terör saldırıları ile verilecek zararın çok ötesinde olabilir. Geleneksel terörizmle zarar verme bir araç iken siber terörizme bir araç olmaktan daha çok öteye giderek amaç olmuştur (Yılmaz ve Salcan, 2008; 54).

Ülkemizde terör örgütleri siber ortamı öncelikli olarak eğitim ve propaganda amaçlı olarak kullandıkları görülmektedir. Bölücü örgütlerden özellikle PKK/KCK, yapılan başarılı operasyonlar nedeniyle sıcak terör eylemlerini yapamayacak duruma geldikten sonra "siyasallaşma" dönemine girmeye çalışmış özellikle bu alanda yoğun

[1] İnternet üzerinden yayın yapan terör örgütü sitelerinden bir kısmı şunlardır; www.pkk.org, www.ibda-c.org, www.ozgurpolitika.org, www.kurd.gr, www.partizan.org, www.atilim.org, www.evrensel.net, www.hilafet.org, www.tkp-ml.org, www.mlkp.net, www.kurtulus.com, www.hizb-ut-tahrir.org.

bir gayret göstermektedir. “Siyasallaşma” alanında kullandıkları en önemli araç ise internet ortamıdır. Aktif olarak kullandıkları yüzlerce web sitesinden ve sosyal paylaşım sitelerinde yoğun bir propaganda faaliyeti yapmaktadırlar. Türkiye’de faaliyet gösteren terör örgütlerinde olduğu gibi uluslararası faaliyet yürüten terör örgütleri de internet ortamını etkin bir şekilde kullanmaktadırlar (Özkışlalı, 2008: 90).

2011 yılında Bakanlar Kurulu Kararı ile Bilişim Suçlarla Mücadele Daire Başkanlığı Emniyet Genel Müdürlüğü'nde kurulmuş ve çalışmalarına başlamıştır. Belirtilen dönemde alınan mahkeme kararlarıyla YouTube ve Blogspot gibi internet sayfalarına erişiminin engellenmesi nedeniyle Anonymous grubu Türkiye’nin kamu kurum ve kuruluşlarının internet siteleri hedef alarak bir siber saldırı düzenlemiştir. Yapılan bu saldırılar sonucunda Türkiye’de siber güvenlik alanında bir bilincin oluşması başlamıştır. Diğer taraftan 2012 yılı içerisinde Redhead isimli grubun önemli kamu kuruluşlarına yapmış olduğu saldırılar basında geniş yer bulmuştur. Bu olaylardan sonra Bakanlar Kurulu kararı ile Ekim 2012 ayında Ulaştırma Denizcilik ve Haberleşme Bakanlığı Başkanlığınca Siber Güvenlik Kurulu’nun oluşturulmuştur. Bu kuruluş kamu kurumlarının hizmetlerini sağladığı ağ bağlantılarının güvenliğinin sağlanması, gizliliğin korunmasına yönelik gerekli tedbirlerinin alınmasını sağlamak, tüm internet kullanıcılarının uyması gereken kuralları belirlemek, gerekli yasal düzenlemeleri hazırlamak olarak belirlenmiştir. Türkiye’ye yönelik gelişen siber tehditler ve riskler göz önüne alınarak 2. Ulusal Siber Güvenlik Tatbikatı icra edilmiştir. NATO'nun tarafından siber güvenliğin sağlanması için alınan kararlar çerçevesinde Türk Silahlı Kuvvetleri Ocak 2013 ayında Siber Savunma Merkezi Başkanlığını kurduğunu açıklamıştır. Kurulan bu yapı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile koordineli çalışacak ve NATO tatbikatlarına katılacağı da belirtilmiştir (Aydın, 2013; 45).

Siber güvenlikle ilgili gerekli önlemleri almalı, siber saldırılara karşı sistemler vatandaşları korumalıdır. Türkiye'de siber faaliyetlerle ilgili birçok önemli çalışma yapılmaya başlanmış, yeni kurumlar meydana getirilmiştir. Her geçen gün daha fazla siber güvenlik uzmanı yetiştirilmekte ve uzmanlar devletin önemli kurumlarına görev almaktadır. Türkiye'de siber güvenlikle ilgili Ulaştırma,

Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Siber Güvenlik Kurumu, TÜBİTAK, TSK Siber Savunma Merkezi Başkanlığı, önemli çalışmalar yapmaktadır. Bunların dışında çeşitli dernek ve sivil toplum örgütleri de siber güvenlikle ilgili çalışmalar yapmakta, internet kullanıcılarını bilinçlendirmek maksadıyla birçok faaliyetlerde bulunmaktadır (Keleştemur, 2015:171).

4.3.1 Türkiye'de Siber Güvenlik Alanında Faaliyet Yürüten Kurumlar

4.3.1.1 Bilgi Teknolojileri ve İletişim Kurumu (BTK)

Bilgi Teknolojileri ve İletişim Kurumu, Türkiye Cumhuriyeti'nde telekomünikasyon sektörünü düzenleyip denetleyen kurumlardandır. 10 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile kurulmuş Türkiye'nin ilk sektörel düzenleyici kurumudur. Bünyesinde bulunan Siber Güvenlik Kurumu sayesinde siber saldırılara karşı mücadele kapsamında önemli çalışmalara imza atılmaktadır. Bilgi Teknolojileri ve İletişim Kurumu tarafından siber güvenliğin sağlanmasına yönelik olarak son yıllarda yürütülmekte olan çalışmalar uluslararası çalışmalarla paralellik göstermekte, ulusumuzun siber uzaydaki güvenliğini en üst seviyede korumayı amaçlamaktadır (Keleştemur, 2015:175).

4.3.1.2 Telekomünikasyon İletişim Başkanlığı (TİB)

Telekomünikasyon İletişim Başkanlığı Türkiye'de telekomünikasyon yoluyla yapılan iletişimin içeriğini kontrol etmekle yükümlü devlet kurumudur. 2005 yılının Ağustos ayında kurulmuş olan kurum internet için izlenmesi ve denetlenmesinden sorumludur. Hâkim, mahkeme ve Cumhuriyet Savcıları tarafından verilmiş erişim engelleme kararlarının uygulanmasına da yine TİB sorumluluğundadır. Türkiye dışında barındırılanın içeriğe erişimi, idari kararla engelleme yetkisine de sahip olan TİB ve BTK'ya bağlıdır (Keleştemur, 2015:175).

Türkiye'de bilinçlendirme faaliyetleri internet kullanımını hızlı artışının paralelinde BTK kontrolünde TİB tarafından yürütülmektedir. İnternet yasasında yapılan son değişiklik ile birlikte interneti güvenli kullanması sağlama ve bilişim şuurunu geliştirmeye yönelik çalışmalara ayrıca yer verilmiştir. TİB tarafından

yapılan bilinçlendirme faaliyetleri internetin bilinçli güvenli ve etkin kullanımı başlıklarında başka çocuk ve ailelere yönelik araştırma yayınları eğitim faaliyetleri ve çeşitli projeler çerçevesinde yürütülmektedir (Çakır ve Kılıç, 2014:85).

4.3.1.3 USOM ve SOME

Ülkemizin siber güvenliğe karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi muhtemel saldırı ve olayların etkilerinin azaltılması ve ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması için ulusal ve uluslararası düzeyde çalışmak üzere Telekomünikasyon İletişim Başkanlığı bünyesinde oluşturulmuştur. Başkanlık bünyesinde kurulan USOM ulusal ve uluslararası seviyedeki siber tehditler ile ilgili kendisi ulaştırılan ihbarları da değerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için kamu kurumları özel kurumlar ve kişiler ile koordinasyon sağlamaktadır. Bu USOM'a bağlı olarak çalışan sektör ve kurum bazında kurulmakta olan siber olaylara müdahale ekipleri de SOME olarak adlandırılmaktadır. Sektörleri yönetecek SOME'lere sektörel SOME, kurumları yönetecek SOME'lere kurumsal SOME denilmektedir (Keleştemur, 2015:176).

Mayıs 2013'te kurulan USOM ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da değerlendirerek söz konusu tehditlerin tespit ve bertaraf edilmesi için kamu kurumları ve özel kuruluşlar ile koordinasyonu sağlamaktadır. Aynı zamanda ulusal ve uluslararası siber güvenlik tatbikatları düzenleyerek kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalık ve hazırlığın arttırılması faaliyetleri ile bilinçlendirme ve yönlendirme faaliyetleri de USOM'un görevleri arasındadır (Çiftçi, 2012:400).

4.3.1.4 TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü

Ulusal siber güvenlik kapasitesinin arttırılmasına yönelik çalışmalar gerçekleştirmek amacıyla kurulan Siber Güvenlik Enstitüsü'nün faaliyetleri 1997 yılında Bilişim Sistemleri Güvenliği Birimi adı ile TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü altına başlamıştır. 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesine ayrı bir enstitü olarak faaliyetlerini sürdürmektedir.

Siber güvenlik alanında araştırma ve geliştirme faaliyetlerini yürütmekte, askeri kurumlara, kamu kurum ve kuruluşları ve özel sektöre, çözüme yönelik projeler geliştirmektedir (Keleştemur, 2015:177).

Siber Güvenlik Enstitüsü etkinlikleri üç başlık altında toplanmaktadır; ileri siber güvenlik araştırma geliştirme çalışmaları, siber güvenlik stratejisi belirleme çalışmaları, siber güvenlik çözüm projeleri. Siber Güvenlik Enstitüsü siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte, askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştirmektedir (Çiftçi, 2012:403).

4.3.1.5 Siber Güvenlik Kurulu

Siber Güvenlik Kurulu, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın başkanlığında, kamu kurum ve kuruluşlarının temsilcilerinin katılımı ile oluşturulmuştur. Türkiye'nin Siber güvenlik ile ilgili olası tehditlere karşı nasıl önlemler alması gerektiğini belirlemek hazırlanan plan program ve raporları belirli usuller ve standartlar çerçevesinde oluşturmak için onay, uygulama ve koordinasyon sağlamakla görevlidir (Keleştemur, 2015:177).

Siber Güvenlik Kurulunun görevleri; siber güvenlik ile ilgili politika strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararlar almak, kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak, siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek, kanunlarla verilen diğer görevleri yapmaktır (Çiftçi, 2012:398).

4.3.1.6 TSK Siber Savunma Merkezi Başkanlığı

Türk Silahlı Kuvvetleri kara, deniz, hava ve uzay hareket alanlarına birlikte siber ortamda da harekât kapasitesini arttırmak için 2012 yılında TSK Siber Savunma Merkezi Başkanlığını oluşturmuştur. Başkanlığın görev ve sorumluluğu Türk Silahlı Kuvvetleri'nin kullanmakta olduğu sistemlerin siber savunmasından oluşmaktadır. Siber tehditleri önlemek, gelişmiş bir siber savunma ikaz ve püskürtme sistemleri oluşturulmasını sağlayan başkanlık Ulaştırma, Denizcilik ve Haberleşme Bakanlığı,

TÜBİTAK ve diğer kamu kurumları ile koordinasyon içerisindedir (Keleştemur, 2015:177).

TSK'nın kullandığı siber ortamda bulunan tüm sistemlerin siber savunmasını yapmak, siber olaylara 7/24 esasına göre müdahale etmek, ulusal olarak ve NATO tarafından icra edilen tatbikatları katılım sağlamak, TSK çapında bilinçlendirme ve eğitim faaliyetlerini sürdürmek, TSK tarafından kullanılan ağlarda düzenli olarak siber güvenlik denetleme ve testleri yapmaktır (Çiftçi, 2012:400).

4.3.1.7 Türkiye'de Siber Güvenliğe Yönelik Çalışmalar

Türkiye'de yetkililer uzunca bir süre siber tehditleri sadece siber suç seviyesinde değerlendirdi. Hatta önemli güvenlik kurumlarına yapılan saldırılar terörle mücadele çerçevesinde ele alındı. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) bünyesinde kurulan birimler ve ulusal bilgi güvenliği kapısıyla devlet kurumlarındaki siber güvenlik bilinci arttırmaya çalışıldı. 27 Ekim 2010'da toplanan Milli Güvenlik Kurulu'nda siber tehditler tartışılarak, Milli Güvenlik Siyaset Belgesi'ne girmesini karar verildiği ilan edildi (Bıçakcı, 2013:45).

Bu kapsamda, ülkemizde siber güvenlik ile ilgili yapılan başlıca çalışmalar;

2003/10 sayılı Başbakanlık Genelgesi (2003)

E-Dönüşüm Türkiye Projesi (2003)

E-Dönüşüm Türkiye Projesi Eylem Planı (2005)

Bilgi Toplumu Stratejisi ve Eylem Planı (2006)

Ulusal Bilgi Güvenliği Programı (2007)

Ülkemizdeki İlk Siber Tatbikatı (2008)

Ulusal Sanal Ortam Güvenlik Politikası (2009)

MGK Bildirisi (2010)

Ulusal Siber Güvenlik Tatbikatı (2011)

Siber Güvenlik Çalıştayı (2011)

Siber Güvenlik Hukuku Çalıştayı (2012)

Siber Kalkan Tatbikatı (2012)

Türkiye Siber Güvenlik Organizasyonu ve Yol Haritası (2012)

Ulusal Siber Güvenlik Strateji Çalıştayı (2012)

Türkiye Büyük Millet Meclisi Meclis Araştırma Komisyonu Raporu (2012)

Türk Silahlı Kuvvetleri Siber Savunma Merkezi Başkanlığının Kurulması (2012)

TÜBİTAK Siber Güvenlik Enstitüsü'nün Kurulması (2012)

Siber Güvenlik Kurumu'nun Kurulması (2012)

Ulusal Siber Güvenlik Tatbikatı (2013)

Ulusal Siber Olaylara Müdahale Merkezi USOM (2013)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı (2013)

Kurumsal SOME'lerin Kurulması (2013)

Siber Güvenlik Faaliyetlerin Yasalaşması (2014)

Uluslararası İlk Siber Anlaşmamız (6533 Sayılı Kanun) (2014)

Uluslararası Siber Kalkan Tatbikatı (2014)

Bilgi Toplumu Stratejisi ve Eylem Planı 2015-2018

Elektronik Ticaretin Düzenlenmesi (6563 Sayılı Kanun) (2015)

Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı (2016)

Kamu Kurum ve Kuruluşların KamuNet'e Dâhil Edilmesi (2016) (Çiftçi, 2014:404)

SONUÇ

1985 yılında kullanılmaya başlayan internet kelimesi kendi aralarında bağlantılı ağlar anlamına gelen “Interconnected Networks” teriminin kısaltması olup, günümüz itibariyle tartışmasız bir şekilde yaşamımızın ve güvenlik yaklaşımlarımızın ayrılmaz bir öğesi olmuştur. Diğer bir deyişle internet dünya üzerinde bulunan tüm dengeleri alt üst etmiş, siber ortamda saldırıları ve ülkeler arasında siber savaşlara neden olabilecek şekilde temel taş haline gelmiştir. İnternet ve ağ teknolojilerinde yaşanan gelişmeler ile birlikte siber uzay kaynaklı saldırılar devletlerin ruhsal ve ekonomik güvenliğini tehdit etmeye başlamıştır. Gelecek on yıllar içerisinde de internet ve ağ teknolojileri merkezli gelişmelerin ticari, kültürel, askeri, siyasal ve finans gibi sektörleri de içine alacak şekilde tüm dünyayı derinden etkileyici açıktır. Bilgisayarların taşınabilir bir hale gelmesi akıllı cep telefonu teknolojisinin ve internet erişiminin yaygınlaşması ile birlikte internetin yarattığı imkânlar ve kolaylıklar günlük yaşamın ötesinde siyasal, askeri, ekonomik yaşamda da yeni bir güç faktörünün ortaya çıkmasına sebep olmuştur. Bu durum ayrıca güvenlik tartışmalarında ve analizlerinde siber uzay ve siber güvenlik şeklinde tanımlanan yeni kavramlarının tartışılmasını da yol açmıştır. Ağ teknolojileri temelli gelişmeler ile birlikte devletlerin savaş, saldırı ve savunma teknikleri de farklılıklaşmaya başlamıştır. İnternetin 90’lı yıllar ile birlikte hızla ticarileşmesi ve yaygınlaşması hem devletler hem de bireyler için yeni bir tehdit kaynağının oluşmasına da sebep olmuştur. Bu kapsamda bireysel veya devlet destekli hackerlar internetin gizemli dünyasını aralamış ve internet aracıyla network güvenlik risklerinin yaratabileceğini devletlere ve sıradan insanlara göstermişlerdir.

Ülkelerin teknoloji alanında özellikle bilgisayar ve iletişim teknolojilerine ihtiyaç duyması gelebilecek siber saldırılara karşı tehdit durumunun artmasına neden olmaktadır. Dünya üzerinde hızla yayılan bilişim alanındaki gelişmeler ve internetin yayılmasıyla birlikte terör örgütlerinin siber ortamı kullanmalarını sağlamış, ülkelerin güvenlik algılarını değiştirmiştir. Siber terör internet ortamını iki amaç için kullanmaktadır. Bunlardan birincisi şiddet içermeyen eylemlerdir. Genellikle propaganda, interneti kötüye kullanma yönünde eğitim ve iletişim-haberleşme ağlarına yönelik eylemler şeklinde gerçekleşmektedir. Şiddet içermeyen terör

eylemlerinin amacı hedefin alt yapısını etkileyerek zayıf düşürme, güvenilirliğini kaybettirme ve maddi kazançlar sağlamaktır. Siber alanda diğer terör çeşidi ise, içerisinde şiddet bulunan eylemlerdir. Buradaki amaç ise hedefi yıpratma ve yok etmektir. Yapılan eylemlerde kullanılan yöntemler büyük maddi kayıplara, (iletişim alt yapısına yönelik) ve toplumsal alanda huzursuzluk ve korku yayarak çöküntüler hedef alınmaktadır. Siber terör olaylarında fiziksel anlamda bir alana bağlı kalmaksızın yapılabilmesi, ülkelerin birlikte hareket etme gerekliliği artırmıştır. Bundan dolayı uluslararası yapılacak işbirliği çalışmaları ile sağlanabilir. Bu nedenlerden dolayı, tezin hipotezlerinden biri olan "21. Yüzyılda değişen güvenlik anlayışı kapsamında siber tehdit, siber saldırı ve siber terörizm küresel boyutta bir tehdittir." varsayımı doğrulanmış olup, siber terörün oluşmaması ve engellenmesi için ülkelerin, uluslararası kuruluşların bir bütün olarak işbirliği yapmaları gerekmektedir.

Ülke olarak haberleşme, iletişim ve internete olan bağlılığımız her geçen artmakta ve siber ortamda oluşacak riskleri artırmaktadır. Siber alanda bulunan siber tehditleri tespit edebilmek için öncelikle olarak gözlem, takip, analiz ve tahmin alt yapısı olan kurumlara ihtiyaç bulunmaktadır. Siber güvenlik sadece internet güvenliği anlamında değil, tüm haberleşme ve iletişim yapısını kapsayan bir alan olması nedeniyle ulusal bir güvenlik politikası benimsenmelidir. Türkiye'nin büyük bir boyutta siber saldırıya maruz kalmamış olması, terör örgütlerinin böyle bir potansiyelinin olmadığı anlamına gelmemelidir. Bundan dolayı siber ortamda pasif savunma önlemlerinin yanında aktif savunma yöntemlerinin de geliştirilmesi gerekmektedir. Siber güvenlik alanında yapılacak çalışmalarda bazı hususlara dikkat etmek gerekmektedir. Güvenlik-demokrasi, fayda-maliyet dengelerinin gözetilmesi mutlaka yapılmalıdır. Kurumsal alanda alınacak bazı tedbirler ulusal siber güvenliğin oluşmasında önemli katkılar sağlayacaktır. Kamu ve kuruluşlarında yapılan bilişim projelerine güvenlik algısının yerleştirilmesidir. Bunların yanında kurumların işletim sisteminden faydalanan kişisel kullanıcılar ile kurumlarda çalışan personeli için standart çalışma şartları belirlenmeli ve belirlenen standartların hangi derece uygulandığını denetlemek sistemler için tehdit oluşturan birçok riski ortadan kaldırmasına yardımcı olacaktır. Yapılacak denetimlerin periyodik ve düzenli bir şekilde yapılması ulusal anlamda siber güvenlik bilincinin yayılmasını sağlayacaktır.

Kurum ve kuruluşların kendi içlerinde yapılacak olan bir iç denetim mekanizması veya dışarıdan yapılacak denetimlerle sistemlerin ne derece güvenli oldukları test edilmiş olacaktır. İç ve dış denetim sonucunda kurum ve kuruluşa yapılacak herhangi bir saldırıda hizmetlerin ne kadar aksayacağı, saldırı altındaki bir sistemin ne kadar sürede eski haline döneceği gibi konulara ilişkin tedbirlerin alınması sağlanacaktır. En önemli unsur ise kamu kurum ve kuruluşlarında kullanılan/kullanılacak olan donanım ve yazılımların test edilmiş ve güvenlik açısından sorunlu olan noktaların tespit edilmesi gerekmektedir. Aksi takdirde donanım ve sistemlerde olabilecek herhangi bir açıklık alınacak bütün önlemleri başarısız kılacaktır. Diğer önemli bir husus ise kurumlar arasında yapılacak olan işbirliğidir. Özellikle siber güvenlik alanında faaliyet gösteren kurumların kendi aralarında hızlı bir bilgi paylaşımı yapmaları ve koordine olmaları kurumların gücünü artıracaktır. Yapılacak olan işbirliğinin sadece kamu kurum ve kuruluşları arasında değil, özel sektör arasında da sağlanması gerekmektedir. Bu işbirliği kamu kurumlarının güçlenmesini sağlayacaktır. Çünkü kamu kurum ve kuruluşlarının bilişim alt yapılarının çoğunu özel sektör işletmektedir.

Siber güvenlik alanında yaşanan gelişmeler çok hızlı bir şekilde gelişmektedir. Bulunan yasal mevzuat bu gelişmelerin çok gerisinde kalmaktadır. Bundan dolayı yasal düzenlemeler hemen geliştirilmeli ve günlük hayata geçmelidir. Yapılacak siber saldırılarının faillerinin tespit edilmesi maksadıyla kanun yapıcılar kanıtlanabilirlik ve geriye dönük iz takibi yapılabilecek şekilde hizmet veren sektör unsurlarına verilerin saklanması ve erişim konularında bazı yükümlülükler getirilmesi zorunludur. Ancak faaliyet gösteren özel sektör unsurları maliyet ve gizlilik sorunları taşımaktadır. Özel sektöre endişe duydukları konularda kolaylıklar sağlanmalı verilerin saklanması kapsamında bilginin güvenliği garanti altına alınmalıdır. Kamu ve özel sektör arasında ayrıca güven sorunu yaşanmaktadır. Bu önemli sorunun ortadan kaldırılması için gerekli çalışmaların yapılması ve bunun ortadan kaldırılması gerekmektedir. Siber alandaki tehditlerin en aza indirilmesi ve yok edilmesi için yapılması gereken en önemli yollardan biri de eğitimdir. Siber alandaki tehditlerin fazla olması nedeniyle hem kendimizin hem de kurumun kullandığı bilgisayarlarda gerekli güvenlik önlemlerinin alınması şart olmuştur. Bunların yanında bilgisayarlar teknolojik alt yapısı ve güvenlik yazılımları ile

donatılmalıdır. Kurum ve kuruluşlarda gerekli tehdit değerlendirilmeleri yapılmalı ve olabilecek saldırı ve sorunlar karşısında yapılacak olan işlemler belirlenmelidir. Kurum için yedek planlar oluşturulmalıdır. İşletilen sistemlerin aksatılmadan yürütülmesi, ülke açısından hem ekonomik hem de sosyal açıdan büyük önem taşımaktadır. Sistemin açık ve çalışır durumda iken müdahale edilerek devamının sağlanması gerekmektedir. Müdahale edilirken kurumlar arası koordinasyon önemlidir. Ülke açısından kritik öneme sahip alanların güvenliğinin alınması için gerekli yasal düzenlemelerin yapılması gerekmektedir. Ayrıca önemli görülen işletim sistemlerinin alt yapısının tamamen milli olması büyük önem taşımaktadır.

İcra edilmekte olan siber güvenlik ile ilgili konferans ve çalıştaylarda ortaya çıkarılan faydalar siber güvenlik alanında alınacak tedbirler kapsamında önemlidir. Yapılacak olan buna benzer çalışmalara devlet desteği artırılmalı katılımlar sağlanmalıdır. Kamu kurum ve kuruluşlarında alınan ulusal güvenlik önlemleri için oluşturulan birimler özel sektörlerde de oluşturulmalıdır. Siber ortamda yapılan saldırılar bir alanda kaydedilmeli ve bir veri tabanı oluşturulmalıdır. Bu veri tabanına hem kamu hem de özel sektör unsurların erişebilirliği sağlanmalıdır. Yapılacak bu veri tabanı saldırıların önceden tespit edilmesi ve zaman kaybının ortadan kaldırılması için büyük önem taşımaktadır. Siber tehditlerin fazla olması, çeşitliliği, türleri ve verdiği zararlar göz önüne alındığında geniş katılımcılı bir koordinasyona ihtiyaç duymaktadır. Ayrıca herşeyden önemlisi bilişim alanında bilinçli kullanıcı yetiştirmektir.

Modernleşme ile birlikte teknolojinin gelişmesi ve kullanımının artması yeni risk ve tehditleri beraberinde getirmiştir. Klasik savaş kapsamında geçmişte ezilen, yıkılan ve uluslararası ortamın dışına itilen ülkeler asimetrik savaş olguları bağlamında denge kurabilmek amacıyla teknolojinin getirmiş olduğu yeniliklerden ve etkilerden faydalanmış ve sistem içerisinde etkili olmaya çalışmışlardır. Risk toplumu ve refleksif modernleşme olgusu içerisindeki bumerang etkisi bir anlamda kendi üreticilerini vurmuş ve Soğuk Savaş sonrası dönemde büyük devletlerin ekonomik anlamda zarara uğramalarına sebep olmuşlardır. Ayrıca son dönemlerde Hibrit Savaş ya da diğer adıyla Karma Savaş içerisinde de önemli bir yer edinen

siber saldırılar günümüz modern dünyasına şekil vermekte ve devletlerarasında ya da terör örgütlerinin devletler üzerindeki etkisinde önemli roller oynamaktadır.

Diğer taraftan, ülkelerin siber tehditlere, siber saldırılara ve terör olaylarına yaklaşımları farklı hatta aynı devletin değişik ve tutarsız yaklaşımları olabilmektedir. Siber ortamda daha az işlemleri olan ülkeler siber alanda daha duyarsız kalmaktadırlar. Bazı ülkeler siber alanı bir savaş alanı olarak değerlendirmekte ve bu alan içerisinde yapılacak faaliyetleri daha çok önemsemekte ve diğer ülkelerin siber güvenlikteki eksik yanları tespit etmeye gayret göstermektedirler. Bu tür ülkeler uluslararası koordinasyona sıcak bakmamakta, diğer ülkelerin işbirliği içinde olarak siber alandaki eksik yönlerin tespit edilmesi ve çözüm bulunmasını istememektedirler. Ancak ülkeler uluslararası ortamda siber alanda yapılabilecek saldırı ve savaş gibi terimleri tanımlamak ve aralarında bir uzlaşı sağlamak zorunda kalacaklardır. Herhangi bir savaşı kazanmak için sadece savunma yeterli değildir. Aslında siber kelimesinin yanına saldırı kelimesi gelince birçok kişi konuya mesafeli yaklaşmaktadır. Öte yandan ülkelerin birçok harp silahı araç ve gereçleri var, ülke orduları düzenli olarak savunma ve saldırı eğitimleri yapmaktadır. Yani saldırı kabiliyetinin olması bu kabiliyetini mutlaka kötü kullanacağı anlamına gelmemektedir. Bunun yanında siber saldırılar barış ortamında da uygulandığı için saldırı kelimesinin fazla vurgu yapılmamasını daha çok aktif siber savunma gibi bir ifadenin kullanılmasına faydalı olabilir. ABD Siber Komutanlığının 12 Mart 2013 tarihinde yaptığı açıklamada, ilk kez siber saldırıya yönelik ekiplerin teşkil edileceği duyurulmuştur. Daha sonra birçok ülke tarafından savunma ve saldırı kabiliyetlerinin yer aldığı siber harekâta yönelik yapılanma ve pratik çalışmalar başlatılmıştır. Bu kapsamda, tezin hipotezlerinden biri olan “Siber ortam, kara, hava, deniz ve uzayın ardından beşinci savaş ortamı olarak yerini almış durumdadır.” varsayımı doğrulanmış olup, bu açıdan ülkemizde de siber saldırı kabiliyetlerinin kazandırılmasına yönelik adımların atılması angajman kurallarının belirlenmesi göz önünde bulundurulmalıdır. Ayrıca bu kabiliyetin ulusal ve uluslararası hukuk kurallarına uygun bir şekilde kullanılması esas olmalıdır.

Siber güvenlik alanında yapılacak çalışmalarda dikkat edilmesi gereken en önemli husus bu sistemleri kullanacak olan vatandaşlar unutulmamalıdır. Alınan tüm güvenlik önlemlerine rağmen, siber alan sunmuş olduğu geniş ve kontrolsüz ortam saldırıyı düzenleyen güçlerin ortaya çıkarılmasında zorlukların yaşanmasına ve zararın çok büyük olduğu eylemlere sebep olmaktadır. Saldırıların ve eylemlerin verdiği zararlar ve alınan hedefler dikkate alındığında yapılan bu eylem/saldırıların arkasında devletlerin olduğunu tahmin edilmektedir. Ancak siber uzayın kendine has özellikleri nedeniyle yapılan eylemlerin kimin tarafından yapıldığı ortaya çıkarmaya ve kanıtlanmasına müsaade etmemektedir. Diğer taraftan siber alanda fark edilmeden birçok siber casusluk eylemi gerçekleştirilmektedir. Aslında herkes tarafından görülen siber eylem ve saldırıların dışında sessizce, gizlice yapılan faaliyetler daha etkin ve korkutucudur. Önümüzdeki dönemlerde siber güvenliği etkileyecek başlıca unsurlar insan ve teknolojinin yaygınlığıdır. Gelecek nesiller küçük yaşlardan itibaren bilişim teknolojileri ile büyüdükleri için bilişim teknolojilerine daha hâkim oldukları görülmektedir. Bilişim teknolojilerinin evlerimizin ve iş yerlerimizin her noktasına artan hâkimiyeti insan unsurlarıyla birleştiğinde gelecek yıllarda nasıl bir dünyada yaşayacağımızı tahmin etmek zor olmayacaktır.

Türkiye bugün siber uzay güvenliği konusunda teknolojik gelişmişlik açısından dünyanın önde gelen ülkelerinden birisidir. Teşkilatlanma, bilinç ve eğitim açısından durum ise tam tersidir. Türkiye'nin güvenliğini etkileyen siber alt yapısının günümüz şartlarında olması gereken özellikleri taşımadığı ve ülke için gerekli olan bilişim yapısını tam olarak karşılamadığı değerlendirilmektedir. Siber alt yapının ihtiyaçları karşılamaması olabilecek siber saldırılar durumunda yetersiz kalacaktır. Bilgi güvenliği konusunda sorumluluk, koordinasyon ve yetkilerin dağınık bir yapı göstermesi de hassasiyeti daha da arttırmaktadır. Bu kapsamda; tezin hipotezleri arasında bulunan "Siber saldırı ve siber terörizm faktörleri Türkiye'nin milli güvenliğini önemli derecede tehdit etmektedir." varsayımı doğrulanmış olup, bundan dolayı ulusal güvenlik bir bütün olarak ele alınmalıdır. Bir yerde olan zafiyet, çok ciddi boyutlarda güvenlik ihlaline neden olabilecektir. Tehdidin bu kadar gelişmiş, beceri sahibi, bilgili ve teknolojik açıdan üst düzeyde olduğu bir dünyada, onunla mücadele edebilmeli en etkin yolu, ondan bir adım önde olmaktır.

Bilgi ve iletişim teknolojilerinin günlük hayattan en kritik askeri sistemlere kadar her alanda kullanılması ile birlikte siber ortamın korunması ülkeler açısından milli güvenliğin önemli unsurlarından biri haline gelmiştir. Artık günümüzde kara, deniz, hava ve uzayın yanı sıra siber ortamda yeni bir mücadele ve savaş alanı olarak ortaya çıkmıştır. Siber sistemlerin kullanımının yaygınlaşmasıyla bu sistemlere yapılan saldırıların sayısı ve karmaşıklığı da artmıştır. Yapılan siber saldırılar nedeniyle şirketlerin ve ülkelerin milyarlar tutarında maddi kayba uğradıkları ileri sürülmektedir. Teknolojik gelişmeler ışık hızıyla ilerlediği bir dönemde bu gelişmelerin getirdiği tehdit, zafiyet ve risklere karşı tedbirlerin alınması ve uygulamaya konulması büyük önem arz etmektedir. Bu maksatla siber alanda güvenliğin sağlanması, gerekli altyapının oluşturularak savunma ve saldırı kabiliyetlerinin kazanılması, başarılması gereken stratejik bir hedeftir. Sadece siber silahların kullanıldığı ülkelerarası bir siber savaşın olması çok zor görünmektedir. Öte yandan gelecekteki tüm çatışmalarda siber silahların güç çarpanı olarak geleneksel silahların yanında kullanacağı ise kesindir.

EK-1

SİBER SAVAŞTA UYGULANACAK HUKUK HAKKINDA TALLINN EL KİTABI

(ÖZET BİLGİ)

NATO Siber Savunma Mükemmeliyet Merkezi, Uluslararası Bağımsız Uzmanlar Grubu tarafından üç yıl süren bir çalışma sonucunda "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı" hazırlanmıştır. Hazırlanan kitapta mevcut uluslararası yasaların siber savaş durumunda hangi düzeyde uygulanacağına dair bir çalışma yapmışlardır. Tallinn El Kitabı, bağımsız uzman grubunun görüşlerinden ibaret olup, resmi bir nitelik taşımamakta, Siber Savunma Mükemmeliyet Merkezi'nin, destekçi ülkelerinin veya NATO'nun görüşlerini de temsil etmemektedir. El kitabı, Cambridge Üniversitesi tarafından 2013 yılının Mart ayında yayınlanmıştır. "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı"; I-"Uluslararası Siber Güvenlik Hukuku" ve II-"Siber Silahlı Çatışma Hukuku" başlıklı iki ana bölümden oluşmaktadır (www.mgk.gov.tr).

BİRİNCİ BÖLÜM: ULUSLARARASI SİBER GÜVENLİK HUKUKU

1. Devletler ve Siber Uzay:

Kural-1: Egemenlik

Bir devlet, kendi egemenlik bölgesi dâhilinde, siber altyapı ve siber eylemler üzerinde kontrol yetkisini kullanabilir.

Kural-2: Yargılama Yetkisi

Bir devlet, uygulanabilir uluslararası yükümlülükleri ihlal etmeden,

a. Kendi sınırlarındaki siber faaliyetlerle ilgili kişiler üzerinde,

b. Kendi sınırlarındaki yerleşik siber altyapı üzerinde,

c. Uluslararası hukukla uyumlu biçimde, kendi sınırı haricinde de, yargılama yetkisini kullanabilir.

Kural-3: Devletlerin Uluslararası Ortamda Yargılama Yetkisi

Uçaklar, gemiler veya uluslararası hava sahasındaki diğer platformlarda açık deniz üzerinde veya uzay boşluğu içinde yerleşik siber altyapılar, ait olduğu veya kayıtlı olduğu devletin yargılama yetkisine konu olurlar.

Kural-4: Egemenlik Muafiyeti ve Dokunulmazlığı

Nerede olursa olsun, bir platform üzerinde siber sistemlere sahip bir devletin, hareketlerinin sonuçlarından muaf olduğunu düşünerek diğer bir devleti etkilemesi, o devletin egemenliğine ihlal anlamına gelir.

Kural-5: Siber Altyapının Kontrolü

Bir devlet, kendi sınırları veya kendi münhasır kontrolü içerisinde olan bölgelerdeki siber altyapıların başka devletleri olumsuz ya da hukuksuz olarak etkileyecek şekilde kullanılmasına bilerek izin veremez.

Kural-6: Devletlerin Yasal Sorumluluğu

Bir devlet, kendisine atfedilebilen ve uluslararası yükümlülük ihlali oluşturan bir siber operasyon konusunda uluslararası yasal sorumluluğu taşır.

Kural-7: Devlete Ait Siber Altyapıdan Başlatılan Siber Harekâtlar

Devlete ait siber altyapıdan başlatılan veya bu altyapıdan kaynaklanan siber harekât, o devletin siber harekât icra ettiğine ilişkin yeterli delil teşkil etmemekte, ancak söz konusu devletin harekât ile ilişkilendirilebileceğine ilişkin emare teşkil etmektedir.

Kural-8: Bir Devlet Üzerinden Yönlendirilen Siber Harekâtlar

Bir devlette yerleşik siber altyapı aracılığıyla siber harekâtın yönlendirilmiş olması, bu devlete siber harekâtı atfetmek için yeterli delil teşkil etmemektedir.

Kural-9: Karşı Tedbirler

Uluslararası olumsuz faaliyetlerden zarar görmüş bir devlet, sorumlu devlete karşı, siber karşı tedbirler dâhil olmak üzere orantılı karşı tedbirlere başvurabilir.

2. Güç Kullanımı:

Kural-10: Tehdit veya Güç Kullanımının Yasaklanması

Bir devletin hudut bütünlüğüne, siyasi bağımsızlığına tehdit teşkil eden veya kuvvet kullanımı içeren ya da Birleşmiş Milletlerin amaçlarıyla uyumsuz olan bir siber harekât hukuksuzdur.

Kural-11: Kuvvet Kullanımı Tanımı

Bir siber harekât, çapı ve etkileri itibariyle, siber olmayan bir harekâtın çapı ve etkisine denk bir etki yaratıyor ise, o siber harekât "kuvvet kullanımı" anlamına gelir.

Kural-12: Kuvvet Tehdidi Tanımı

Gerçekleştiği takdirde hukuksuz güç kullanımı anlamına gelebilecek bir siber harekât ya da siber harekât tehdidi hukuksuz kuvvet tehdidi anlamına gelir.

Kural-13: Silahlı Saldırıya Karşı Meşru Müdafaa

Silahlı saldırı seviyesine gelmiş bir siber harekâtın hedefi olan bir devlet, doğal olarak meşru müdafaa hakkını kullanabilir. Bir siber harekâtın silahlı saldırı olup olmaması bu harekâtın çapına ve etkisine bağlıdır.

Kural-14: Gereklilik ve Orantılılık

Meşru müdafaa hakkını kullanan bir devlet tarafından siber harekâtı da içeren güç kullanımı, gerekli ve orantılı olmalıdır.

Kural-15: Kaçınılmazlık ve Acil Durum

Meşru müdafaada kuvvet kullanma hakkı, bir siber silahlı saldırı gerçekleşirse veya kaçınılmaz ise ortaya çıkar. Bu husus aynı zamanda acil bir gereksinime bağlıdır.

Kural-16: Birleşik Meşru Müdafaa

Meşru müdafaa hakkı birleşik harekât olarak da kullanılabilir. Silahlı saldırı seviyesine gelmiş bir siber harekâta karşı birleşik meşru müdafaa hakkı, yalnızca mağdur ülkenin talebi ile ve talep kapsamı doğrultusunda kullanılabilir.

Kural-17: Meşru Müdafaa Tedbirlerini Raporlama

Birleşmiş Milletler Sözleşmesi'nin 51'inci maddesi doğrultusunda, meşru müdafaa hakkını kullanmakta olan devletler, siber harekât ile ilgili almış oldukları tedbirleri gecikmeksizin Birleşmiş Milletler Güvenlik Konseyi'ne raporlamalıdır.

Kural-18: Birleşmiş Milletler Güvenlik Konseyi

Birleşmiş Milletler Güvenlik Konseyi, bir eylemin barışı tehdit veya ihlal ettiğini veya saldırı eylemi olduğunu belirlerse, siber harekât dâhil olmak üzere kuvvet kullanımı içermeyen tedbirlere izin verebilir. Eğer Güvenlik Konseyi, bu tedbirlerin yetersiz olduğunu değerlendirirse, siber tedbirler dâhil kuvvet kullanımı içeren tedbirlerin uygulanmasına karar verebilir.

Kural-19: Bölgesel Organizasyonlar

Uluslararası organizasyonlar veya bölgesel nitelikli kuruluşlar, Birleşmiş Milletler Güvenlik Konseyi tarafından yetkilendirilmeyi ya da görevlendirilmeyi müteakip, siber harekâtlara karşılık ya da siber harekât içeren yaptırım niteliğinde eylemler icra edebilir.

İKİNCİ BÖLÜM: SİBER SİLAHLI ÇATIŞMA HUKUKU

3. Genel Siber Silahlı Çatışma Hukuku:

Kural-20: Silahlı Çatışma Hukukunun Uygulanabilirliği

Silahlı çatışma kapsamında icra edilen siber harekât, silahlı çatışma hukukuna tabidir.

Kural-21: Coğrafi Kısıtlamalar

Siber harekât, silahlı çatışma sırasında uygulanan uluslararası hukukun ilgili hükümlerinden kaynaklanan coğrafi kısıtlamalara tabidir.

Kural-22: Uluslararası Silahlı Çatışma Olarak Nitelendirme

Uluslararası çatışma, iki veya daha fazla devlet arasında, siber harekâtı içeren veya siber harekâtla sınırlı savaş durumunun gerçekleşmesi halinde meydana gelir.

Kural-23: Uluslararası Olmayan Silahlı Çatışma Olarak Nitelendirme

Uluslararası olmayan silahlı çatışma, devletlerin silahlı kuvvetleri bir ya da daha fazla silahlı gruplar arasında veya böyle grupların arasında meydana gelen siber harekâtı içeren veya siber harekâtla sınırlı temdit edilmiş silahlı şiddet olaylarının mevcudiyetinde meydana gelir. Çatışma belirli bir minimum yoğunluk seviyesine ulaşmalı ve çatışmaya dâhil olan gruplar belirli bir seviyede kurumsallığa sahip olmalıdır.

Kural-24: Komutanlar ve Amirlerin Cezai Sorumlulukları

a. Komutanlar ve diğer amirlerin, savaş suçlarını oluşturan siber harekât emirlerine ilişkin cezai sorumlulukları vardır.

b. Komutanların, astlarının savaş suçu işliyor olması, işlemek üzere olması veya işlemiş olmasını bildiği veya bilmesi gerektiği durumlarda; söz konusu eylemlerin engellenmesi için mantıklı ve mümkün önlemleri almak ve sorumluları cezalandırmakta başarısız olmaları halinde cezai sorumlulukları vardır.

4. Düşmanca Davranışlar

Kural-25: Genel Katılım

Silahlı çatışma hukuku, herhangi bir kategorideki kişilerin siber harekâta iştirak etmesini engellemez. Fakat iştirakin yasal sonuçları, silahlı çatışmanın doğasından ve bireyin ait olduğu kategoriye bağlı olarak değişir.

Kural-26: Silahlı Kuvvetler Mensupları

Uluslararası silahlı bir çatışmada, çatışmaya taraf olan silahlı kuvvetlerin siber harekât esnasında harbin şartlarına uymada başarısız olan mensupları harp dokunulmazlığı ve esirlik haklarını kaybeder.

Kural-27: Kitlesel İsyan

Uluslararası bir silahlı çatışmada, işgal altında olmayan bir bölgenin kitlesel isyanın bir parçası olarak siber harekâta dâhil olmuş sakinleri, harp dokunulmazlığı ve esirliği durumundan yararlanır.

Kural-28: Paralı Askerler

Siber harekâta dâhil olan paralı askerler, harp dokunulmazlığı ve esirlik durumundan yararlanamaz.

Kural-29: Siviller

Sivillerin düşmanlık boyutundaki siber harekâta katılımları doğrudan yasaklanmamıştır, fakat katılımları süresince saldırılardan korunma haklarını kaybederler.

Kural-30: Siber Saldırının Tanımı

İster taarruz ister savunma maksadıyla olsun, nesnelerin zarar görmesi/imhasına veya insanların yaralanmasına veya ölümüne neden olması oldukça beklenen durumlardaki Siber saldırı siber harekâttır.

Kural-31: Ayrım

Ayrım ilkesi siber harekâta uygulanır.

Kural-32: Sivillere Saldırının Yasaklanması

Sivil topluluklar ve bireyler siber saldırıların hedefi olmamalıdır.

Kural-33: Kişilerin Statüsüne İlişkin Şüphe

Bir kişinin sivil olup olmadığına ilişkin şüphe oluşması durumunda, o kişi sivil kabul edilmelidir.

Kural-34: Saldırıların Yasal Hedefleri Olarak Bireyler

Aşağıdaki bireyler siber saldırıların hedefi olabilir:

a. Ordu mensupları,

b. Organize silahlı grupların mensupları,

c. Savaşta doğrudan rol alan siviller ve

ç. Uluslararası bir silahlı çatışmada, kitlesel isyan katılımcıları.

Kural-35: Saldırgan Davranışlara Doğrudan İştirak Eden Siviller

Saldırgan davranışlara doğrudan iştirak etmeyen siviller, saldırılara karşı korunma hakkından yararlanırlar.

Kural-36: Terör Saldırıları

Temel amacı sivil toplum arasında terörü yaymak olan siber saldırılar ve tehditler yasaklanmıştır.

Kural-37: Sivil Hedeflere Saldırı Yasağı

Siviller siber saldırıların hedefi olamazlar. Bilgisayarlar, bilgisayar ağları ve siber altyapı askeri amaçlı ise saldırı hedefi yapılabilirler.

Kural-38: Sivil Unsurlar ve Askeri Hedefler

Askeri amaçlı olmayan bütün hedefler sivil unsurlardır.

Kural-39: Sivil ve Askeri Amaçlar İçin Kullanılan Unsurlar

Sivil ve askeri amaçların her ikisi için kullanılan bir unsur: bilgisayar, bilgisayar ağları, siber altyapıyı içeren: askeri bir hedeftir.

Kural-40: Unsurların Durumu Hakkındaki Şüphe

Normalde sivil amaçlar için kullanılan unsurların askeri harekâta etkili bir katkı yapmasıyla ile ilgili şüphe duyulduğunda, ancak dikkatli bir değerlendirme yapılması halinde bir karar verilebilir.

Kural-41: Savaşın Araçları ve Metotlarının Tanımı

El Kitabı'nın amaçları için:

a. "Siber savaşın araçları" siber silahlar ve onlarla ilişkili olan siber sistemlerdir ve

b. "Siber savaşın metotları" siber taktikler, teknikler ve çatışmaların yürütüldüğü prosedürlerdir.

Kural-42: Aşırı Zarar Verme Gereksiz Acı Çektirme

Aşırı zarar verme veya gereksiz acıya sebep olabilecek siber savaş metot ve araçlarını kullanmak yasaklanmıştır.

Kural-43: Ayrımcı Olmayan Araç ve Yöntemler

Doğası gereği ayrımcı olmayan siber savaşın araç ve metotlarını kullanmak yasaklanmıştır. Siber savaşın araç ve metotları özel bir askeri hedefe yönlendirilmediğinde ve sivil asker ayrımı yapmaksızın saldırıldığında doğası gereği ayrımcı değildir.

Kural-44: Siber Bubi Tuzakları

Silahlı çatışma hukukunda özellikle belirtilen nesnelerle ilişkili siber bubi tuzaklarının kullanımı yasaklanmıştır.

Kural-45: Açlık

Sivillerin aç bırakılması veya açlıktan ölmelerinin siber savaşın bir metodu olması yasaklanmıştır.

Kural-46: Saldırgan Misilleme

Siber harekât yoluyla saldırgan misillemenin;

a. Savaş esirleri,

b. Gözaltındaki siviller, işgal edilmiş bölgedeki siviller, bunun dışında savaşa karşı bir tarafın elinde bulunanlar ve arazisinde bulunanlar,

c. Savaşın dışında olanlar ve

ç. Sağlık personeli, tesisler, araçlar ve aletlere karşı uygulanması yasaklanmıştır.

Kural-47: Ek Protokol: 1 Kapsamındaki Misillemeler

Ek Protokol: 1 taraf devletlerin sivil halkı, sivil bireyleri, sivil nesneleri, kültürel nesneleri, ibadet yerlerini, sivil halkın hayatı için zorunlu olan nesneleri, doğal

çevreyi ve barajları, su setlerini, nükleer elektrik üreten istasyonları misilleme yoluyla siber saldırının hedefi yapmalarını yasaklar.

Kural-48: Silahların Gözden Geçirilmesi

a. Tüm devletler sahip oldukları siber savaş vasıtalarının devleti bağlayan çatışma hukuku kurallarına uygun olarak bulundurmaya ve kullanmaya zorunludurlar.

b. Ek Protokol: 1'i imzalayan devletler için protokolde ve uluslararası hukuk kurallarıyla yasaklanmış olan faaliyetler, yeni siber savaş vasıtalarını veya metotları üzerinde çalışmada, bunları geliştirmede, tedarik etmede veya bünyesine adapte etmede de geçerlidir.

Kural-49: Ayrım Gözetmeyen Saldırılar

Yasal hedeflere yönlendirilmemiş ve sonuç olarak yasal hedeflerle birlikte sivil hedefleri de ayrım gözetmeksizin hedef alan siber saldırılar yasaklanmıştır.

Kural-50: Net Olarak Ayrılmış ve Aşikâr Askeri Hedefler

Öncelikli olarak sivil maksatlı kullanılan siber alt yapılar içerisinde aşikâr askeri hedefleri tek bir hedef olarak değerlendiren siber saldırılar korunması gereken sivil unsurlara da zarar verebileceğinden yasaklanmıştır.

Kural-51: Orantılılık

Olası sivil kayıplara, yaralanmalara veya sivil unsurların zarar görmesine neden olabilecek olan ve beklenen askeri avantajlar ile ilişkilendirildiğinde aşırıya kaçan siber saldırılar yasaklanmıştır.

Kural-52: Sürekli Olarak Dikkat Gösterme

Siber harekâtları da içeren savaş durumu süresince, sivil nüfusun, sivil bireylerin ve sivil hedeflerin ayrı tutulmasına sürekli olarak dikkat edilmelidir.

Kural-53: Hedeflerin Doğrulanması

Bir siber saldırıyı planlayanlar veya karar verenler saldıracakları hedeflerinin siviller, sivil unsurlar veya özel korumaya alınmış hedefler olmadığını doğrulamak için mümkün olan her yolu denemek zorundadırlar.

Kural-54: Vasıtaların veya Metotların Seçimi

Bir siber saldırıyı planlayanlar veya karar verenler olası böyle bir saldırı neticesinde sivil yaralanmaları, sivil hayat kayıpları ve sivil hedeflerin parçalanması veya zarar görmesini engellemek ve bu tür saldırılarda bunları asgariye indirmek maksadıyla vasıtaların ve metotların seçiminde tüm gerekli tedbirleri alacaktır.

Kural-55: Orantılılık Hakkında Tedbirler

Bir siber saldırıyı planlayanlar veya karar verenler olası sivillerin ölümlerine, yaralanmalarına veya sivil unsurların zarar görmesine neden olabilecek olan ve beklenen askeri avantajlar ile ilişkilendirildiğinde aşırıya kaçan siber saldırıları başlatmaya karar vermekten kaçınmalıdırlar.

Kural-56: Hedeflerin Seçimi

Ek Protokol: 1'i imzalayan devletler benzer bir askeri avantajı ele geçirmek için birçok askeri hedef arasında seçim yapmak durumunda kalınca, kullanacakları siber saldırının hedefi sivil yaşamlar ve sivil hedefler için en az tehlikeli olması beklenen hedef olacaktır.

Kural-57: Saldırıların İptali veya Askıya Alınması

Siber saldırıyı planlayan, onaylayan veya icra edenler aşağıdaki durumların açık bir şekilde ortaya çıkması durumunda söz konusu saldırıyı iptal edecek veya askıya alacaktır;

a. Hedeflerinin askeri bir hedef olmadığının veya özel olarak korunan bir nesne olduğunun anlaşılması,

b. Siber saldırıların olası sivil hayat kayıpları, sivillerin yaralanması, sivil hedeflerin zarar görmesi veya beklenen askeri avantajlar ile ilişkilendirildiğinde aşırıya kaçmasının öngörülmesi durumunda.

Kural-58: Uyarılar

Koşulların izin verdiği müddetçe, sivil nüfusu etkileyebilecek siber saldırılar için önceden etkili uyarılar yapılacaktır.

Kural-59: Siber Saldırıların Etkilerine Karşı Tedbirler:

Silahlı çatışmanın tarafları, kendi kontrollerinde bulunan sivil nüfusu, bireyleri veya sivil unsurları siber saldırılardan kaynaklanabilecek zararlara karşı korumak için gerekli tedbirleri azami seviyede alacaklardır.

Kural-60: Hainlik

Siber harekâtı da kapsayan düşmanca davranışlar kapsamında, hasım şahsı ihanet etmeye yönlendirmeyi müteakip öldürmek ya da yaralamak yasaklanmıştır. Müteakiben ihanet etme niyetiyle; hasım şahsın güvenini kazanarak onun silahlı çatışma hukukuna göre koruma altında olduğuna veya işbirliği yapmak zorunda olduğuna inandırmak hainlik anlamına gelir.

Kural-61: Hile

Savaş hileleri olarak nitelendirilen Siber Harekâta izin verilmiştir.

Kural-62: Koruyucu İşaretlerin Uygun Olmayan Kullanımı

Silahlı Çatışma Hukukunda belirtilen koruyucu amblem, işaret ve uyarıların uygun olmayan şekilde kullanılması yasaklanmıştır.

Kural-63: Birleşmiş Milletler Ambleminin Uygun Olmayan Kullanımı

Birleşmiş Milletlerin ambleminin siber harekâtta kullanımı (Birleşmiş Millerin yetki verdikleri hariç) yasaklanmıştır.

Kural-64: Düşman İşaretlerinin Uygun Olmayan Kullanımı

Siber taarruz dâhil taarruzda, düşman tarafından görülebilecek durumdayken düşmana ait flamaların, askeri işaretlerin, rütbe işaretlerinin veya üniformaların kullanımı yasaklanmıştır.

Kural-65: Tarafsız İşaretlerin Uygun Olmayan Kullanımı

Siber Harekâtta, tarafsız veya çatışmaya taraf olmayan devletlere ait flamaların, askeri işaretlerin, rütbe işaretlerinin ya da üniformaların kullanımı yasaklanmıştır.

Kural-66: Siber Casusluk

a. Silahlı çatışma süresince, siber casusluk veya düşmana yöneltilmiş olan diğer bilgi toplama yöntemleri Silahlı Çatışma Hukukunu ihlal etmez.

b. Düşman kontrolü altındaki topraklarda siber casusluk görevi verilmiş bir silahlı kuvvetler personeli esir olma hakkını kaybeder ve ait olduğu silahlı kuvvetlere katılmadan yakalanırsa casus olarak muamele görür.

Kural-67: Ambargonun Uygulanması ve Muhafazası

Siber yöntemler ve savaş araçları denizden veya havadan ambargo uygulanması ve muhafazası için kullanılabilir. Ancak bu yöntemlerin tek tek veya diğer yöntemlerle bütünleşik olarak kullanımı uluslararası silahlı çatışma hukukuna aykırı eylemlerle sonuçlanamaz.

Kural-68: Tarafsız Aktivitelerdeki Ambargonun Etkisi

Siber harekâtın denizden veya havadan ambargonun uygulanması maksadıyla kullanımının tarafsız topraklara erişimi engelleme etkisi olmamalıdır.

Kural-69: Bölgeler

Devletlerin barışta veya savaş süresince yasal olarak oluşturabilecekleri bölgelerde, hukuka uygun olarak gerçekleştireceği siber harekât ile bölgeye yönelik haklarını koruyabilirler.

5. Belirli Kişiler, Nesneler ve Faaliyetler:

Kural-70: Sağlık ve Din Personeli, Sağlık Birimleri ve Sağlık Kapsamındaki Nakliye İşlemleri

Sağlık ve din personeli, sağlık birimleri ve sağlık kapsamındaki nakliye işlemleri gözetilmeli, korunmalı ve özellikle de siber saldırıların hedefi yapılmamalıdır.

Kural-71: Tıbbi Bilgisayarlar, Bilgisayar Ağları ve Veriler

Tıbbi birimlerde ve bu birimlerin nakliyesinde veya yönetiminde kullanılmakta olan tıbbi bilgisayarlar, bilgisayar ağları ve veriler gözetilmeli, korunmalı ve özellikle de siber saldırıların hedefi yapılmamalıdır.

Kural-72: Tanımlama

Tıbbi birimlerde ve bu birimlerin nakliyesinde veya yönetiminde kullanılmakta olan tıbbi bilgisayarlar, bilgisayar ağları ve veriler ile ilgili elektronik işaretleme dâhil olmak üzere uygun araçlarla açık bir şekilde tanımlamak için gerekli tedbirler alınmalıdır. Tanımlama işleminde başarısız olunması bu unsurları sahip oldukları korunma hakkından yoksun bırakmaz.

Kural-73: Korumanın Kalkması ve Uyarı

İnsani fonksiyonlarının dışında düşmana zarar verici eylemlere girişmedikleri sürece Tıbbi birimlerde ve bu birimlerin nakliyesinde veya yönetiminde kullanılmakta olan tıbbi bilgisayarlar, bilgisayar ağları ve verilerin korunması durumu ortadan kalkmaz. Ancak insani fonksiyonlarının dışında yaptıkları eylemleri durdurmaları için uyarılıp makul bir süre tanınmasına rağmen kötü eylemlerini devam ettirmeleri halinde korumalı durumları ortadan kalkabilir.

Kural-74: Birleşmiş Milletler Personeli, Tesisleri, Malzemeleri, Unsurları ve Araçları

a. Silahlı çatışma hukuku kapsamında sivillere ve sivil unsurlara tanımlanmış olan korunma hakkına sahip oldukları sürece Birleşmiş Milletler personeli ile Birleşmiş

Milletler faaliyetlerini destekleyen bilgisayarlar ve bilgisayar ağları dâhil tüm tesisleri, malzemeleri, unsurları ve araçları gözetilmeli, korunmalı ve bir siber saldırının hedefi yapılmamalıdır.

b. Birleşmiş Milletler imtiyazına sahip diğer insani yardım ve barışı koruma görevi icra eden diğer personel, tesis, malzeme, unsur ve bilgisayar/bilgisayar ağları da dâhil olmak üzere araçlar da benzer şekilde siber saldırılara karşı korunmalıdır.

Kural-75: Gözaltına Alınmış Kişilerin Korunması

Savaş esirleri, etkisiz hale getirilmiş korunan kişiler ve gözaltına alınmış kişiler mutlaka siber harekâtın zararlı etkilerine karşı korunmalıdır.

Kural-76: Gözaltına Alınan Personelin İletişimi

Savaş esirleri, etkisiz hale getirilmiş korunan kişiler ve diğer gözaltına alınan kişilerin mutlak iletişim hakkı siber harekât ile engellenmemelidir.

Kural-77: Askerî Faaliyetlere Mecburi Katılım

Savaş esirleri ve etkisiz hale getirilmiş korunan kişiler doğrudan kendi ülkelerine karşı yapılan siber harekâta katılım ve destek konusunda zorlanmamalıdır.

Kural-78: Çocukların Korunması

Çocukların orduya katılımı veya siber savaşın bir parçası olmalarına izin verilmesi yasaklanmıştır.

Kural-79: Basın Mensuplarının Korunması

Siber saldırılarla ilgili savaşın içerisinde doğrudan yer almadıkları sürece, silahlı çatışma bölgesinde tehlike içinde profesyonel görev yapan basın mensupları sivil kabul edilir ve bu nedenle gözetilmelidir.

Kural-80: Taarruz Süresince Barajları, Su Bentlerini ve Nükleer Elektrik Santrallerini Koruma Görevi

Barajlar, su bentleri ve nükleer elektrik santrallerinin barındırdıkları tehlikeli gücün salıverilmesini ve buna bağlı olarak ağır sivil nüfus kayıplarını engellemek için bu tür tesislere karşı yapılacak siber taarruzlarda özel koruma tedbirleri alınmalıdır.

Kural-81: Hayatta Kalma İçin Vazgeçilmez Olan Unsurların Korunması

Siber harekâtın araçları kullanılarak sivil nüfusun hayatta kalabilmesi için zaruri olan malzemelere taarruz edilmesi, onların imha edilmesi, yok edilmesi veya kullanışsız hale getirilmesi yasaklanmıştır.

Kural-82: Kültürel Varlıkların Gözetilmesi ve Korunması

Silahlı çatışmanın tarafları, siber uzayda yer alan veya siber taarruzlardan etkilenecek olan kültürel varlıkları gözetmeli ve korumalıdır. Özellikle de sayısal ortamdaki kültürel varlıkların askerî maksatlar için kullanımı yasaklanmıştır.

Kural-83: Doğal Ortamın Korunması

a. Doğal ortamın sivil bir unsur olması nedeniyle, siber saldırı ve etkilerine karşı korunma hakkından faydalanır.

b. Ek Protokol 1'e taraf ülkelerce; siber metotları ya da diğer savaş araçlarını kullanarak doğal ortamın tümüne yayılabilecek ve etkileri uzun süre devam edebilecek ağır zararların verilmesi yasaklanmıştır.

Kural-84: Diplomatik Arşiv ve İletişimin Korunması

Diplomatik arşiv ve İletişimler daima siber harekâta karşı korunacaktır.

Kural-85: Toplu Cezalandırma

Siber araçlar kullanılarak yapılacak toplu cezalandırma yöntemi yasaklanmıştır.

Kural-86: İnsani Yardım

Siber harekât, insani yardım sağlama amacı güden tarafsız gayretleri gereksiz yere engellemek maksadıyla planlanmamalı ve uygulanmamalıdır.

6. İşgal:

Kural-87: İşgal Edilmiş Bölgedeki Korunan Kişilerin Gözetilmesi

İşgal edilmiş bölgedeki korunan kişiler, siber harekâtın zararlı etkilerine karşı korunmalı ve gözetilmelidir.

Kural-88: İşgal Edilmiş Bölgede Asayiş ve Güvenlik

İşgalci güçler kendi gücü dâhilinde mümkün olduğu kadar kamu düzeni ve güvenliğini sağlamak için ülkedeki yürürlükte olan ve siber faaliyetlere uygulanabilir kuralları da içeren yasalar çerçevesinde gerekli tüm tedbirleri almalıdır.

Kural-89: İşgalci Güçlerin Güvenliği

İşgalci güçler kendi genel güvenliğini sağlamak maksadıyla, kendi siber sistemlerinin bütünlük ve güvenilirliği de dâhil olmak üzere gerekli tüm tedbirleri alabilir.

Kural-90: El Koyma ve Kamulaştırma

Siber altyapının ve sistemin kontrol altına alınması maksadıyla, işgalci güçler tarafından el koyma ve kamulaştırma yapılabilir.

7. Tarafsızlık:

Kural-91: Tarafsız Güçlere Ait Siber Altyapının Korunması

Siber araçlar ile tarafsız güçlere ait siber altyapılara yönelik düşmanca siber faaliyetlerin uygulanması yasaklanmıştır.

Kural-92: Tarafsız Bölgede Siber Harekât

Tarafsız bölgede siber araçlar ile düşmanca siber faaliyetlerin uygulanması yasaklanmıştır.

Kural-93: Tarafsız Güçlerin Yükümlülükleri

Tarafsız bir devlet, kendi sınırları veya kendi münhasır kontrolü içerisinde olan bölgelerdeki siber altyapıların çatışan devletlere düşmanca faaliyetlerin gerçekleştirilmesine bilerek izin veremez.

Kural-94: Çatışan Taraflarca İhlallere Müdahale

Eğer tarafsız bir devlet kendi toprakları üzerinde muharip hakların uygulanmasını sonlandırmada başarısız olursa, mağdur olan taraf bu harekete karşı siber harekâtı içeren gerekli adımları atabilir.

Kural-95: Tarafsızlık ve Güvenlik Konseyi Faaliyetleri

Bir devlet, Birleşmiş Milletler Tüzüğü Bölüm 7 altında belirtilen Güvenlik Konseyinin aldığı önleyici ve zorlayıcı kararlara aykırı olarak siber harekâtı içeren bir hareketi haklı çıkarmak için tarafsızlık ilkesine güvenemez (www.mgk.gov.tr).

KAYNAKÇA

Açıkmeşe, Sinem Akgül, (2014). *Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler,* (Editör: Evren Balta) *Küresel Güvenlik*, İletişim Yayınları, İstanbul, 2014, (239-253)

Akgül, Fulya, (2014). *Uluslararası İlişkiler Teorileri/Temel Kavramlar,* (Editör: Mehmet Şahin, Osman Şen) *Uluslararası İlişkilerde Liberal Yaklaşımlar,* Ankara: Kripto Yayımları, (65-89)

Akın Osman, Çınar Işıl, Karaman Muhammer, Bilekyiğit Fatih, (2016), *Siber Durum Farkındalığını Artırmada Etkili Bir yöntem: Bayrağı Yakala (Capture the Flag,* http://www.academia.edu/6839094/SIBER_DURUM_FARKINDALIGINI_ARTIRMADA_ETKILI_BIR_YONTEM_BAYRAGI_YAKALA_CAPTURE_THE_FLAG_ 06 Ağustos 2016 tarihinde erişilmiştir.

Aktel, Mehmet ve Gürkaynak, Muharrem. *Küreselleşen Terörizm: Bir Etkileşim Çalışması,* Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, http://www.ayk.gov.tr/wp-content/uploads/2015/01/AKTEL-Mehmet-G%C3%9CRKAYNAK-Muharrem%C3%9CRESELLE%C5%9EEN-TER%C3%96R%C4%B0ZM-B%C4%B0R-ETK%C4%B0LE%C5%9E%C4%B0M-%C3%87ALI%C5%9EMASI.pdf Erişim Tarihi. 12 Haziran 2016

Allison, Graham (2006). *Nükleer Terörizm, Önlenebilir Nihai Felaket*, (Çeviren Ayas, Güneş), İstanbul: Salyangöz Yayınları

Altınkaynak Mustafa, (2018). *Her 8 Kişiden 1'İNİN Parolası Biliniyor!*, Arka Kapı Dergisi, Sayı 1, (13-17) İstanbul

Altun, İsa, (2016). *Ortam Sanal Suç Gerçek*, İstanbul: İskenderiye Yayınevi

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

Yayınları

Arı, Tayyar, (2013). *Uluslararası İlişkilere Giriş*, Bursa: MKM Yayıncılık

Arı, Tayyar, *Uluslararası İlişkiler ve Dış Politika*, İstanbul: Alfa Yayınları

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

Kitapevi

Bakan, Zerrin Ayşe, (2007). *Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye'nin Güvenlik Algılamaları*, 21. Yüzyıl Dergisi, Ekim-Kasım-Aralık 2007, Ankara, (35-50)

Bayır, Özgün Erler, (2013). *Uluslararası İlişkilerde Teorik Tartışmalar,* (Editör:Hasret Çomak, Caner Sancaktar) *Soğuk Savaş Sonrasında Güvenliğe Yönelik Teorik Tartışmalar*, Beta Basım, 2013, (171-191)

Bayraktar, Gökhan, (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi*, İstanbul: Yeniyüzyıl Yayınları

Bıçakcı, Salih, (2013). *21. Yüzyılda Siber Güvenlik, (*Editör: Mustafa Aydın*),* İstanbul: İstanbul Bilgi Üniversitesi Yayınları,

Bıçakçı, Salih, (2013). *21. Yüzyılda Siber Güvenlik*, (Editör: Aydın, Mustafa), İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Birdişli, Fikret, (2011). *Ulusal Güvenlik Kavramının Tarihsel ve Düşünsel Temelleri*, Kahramanmaraş Sütçü İmam Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi, Sayı: 31 Yıl:2011/2 (149-169 s.)

Booth, Ken, (2012). *Dünya Güvenliği Kuramı*, (Tercüme: Çağdaş ÜNGÖR), İstanbul: Küre Yayınları

Brown, Chris, Ainley, Kirsten, (2007). *Uluslararası İlişkileri Anlamak*, (Çeviren: Arzu Oyacıoğlu), İstanbul: Yayınodası Yayıncılık

Bülbül İsmail ve Bingöl Poyraz Emre, (2017). *Etik Hackerlığa Giriş, Ofansif Siber Güvenliğin ABC'si!*, İstanbul: Hayykitap Yayınevi

Coşkun, B.Balamir, (2014). *Kopengah Okulu ve Güvenlikleştirme,* (Derleyen: Tayyar ARI), *Uluslararası İlişkiler Teorileri:2, Bursa:* Dora Yayınevi

Çakır, Hüseyin, Kılıç, Mehmet Serkan (Editör), (2014), *Güncel Tehdit: Siber*

Suçlar, Ankara: Seçkin Kitapevi

Çakmak, Haydar ve Altunok, Taner (2009). *Suç, Terör ve Savaş Üçgeninde Siber Dünya,* Ankara: Barış platin Kitapevi

Çakmak, Haydar ve Altunok, Taner, (2009). *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, Ankara: Barış Platin Kitapevi

Çalık, Nuray, (2013). *Amerika Birleşik Devletleri'nin 11 Eylül Sonrası Asya Pasifik Politikası,* Yayımlanmamış Yükseklisans Tezi, Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Aydın.

Çalkıvik, Aslı, (2014). *Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler,* (Editör: Evren Balta) *Soğuk Savaş ve Sonrası Güvenlik Siyaseti*, İletişim Yayınları, İstanbul, 2014, (281-299)

Çiftci, Hasan, (2017). *Her Yönüyle Siber Savaş*, Ankara: Tübitak Popüler Bilim Kitapları

Darıcılı, Ali Burak, (2017). *Siber Uzay ve Siber Güvenlik Nedir?,* Bursa: Dora Yayınları

Demircioğlu, Cemalettin, (2014). *Siberuzayda Güç ve Güvenlik*, İdarecinin Sesi, Mart-Nisan 2014, (39-41)

Egbatan, Mine ve Şahin, Gonca, (2014). *Uluslararası İlişkiler Teorileri/Temel Kavramlar,* (Editör: Mehmet Şahin, Osman Şen) *Uluslararası İlişkilerde Feminist Yaklaşımlar, Ankara:* Kripto Yayımları, (251-281)

Eren, Mehmet, (2017). Avrupa Birliği'nin Siber Güvenlik Politikası, İstanbul:

Beta Yayınevi

Ersoy Eyüp, (2014). *Uluslararası İlişkiler Teorileri*, (Derleyen: Ramazan Gözen) İstanbul: İletişim Yayınları

Gökçe, K.G., Şahinaslan, E., Dinçel S., (2014). *Mobil Yaşamda Siber Güvenlik Yaklaşımı,* 7'nci Uluslararası Bilgi Güvenliği ve Kriptoloji ve Konferansı, (214-221)

Griffiths, Martin, Roach Steven C., Salamon, M. Scott., (2011). *Uluslararası İlişkilerde Temel Düşünürler ve Teoriler*, İstanbul: Nobel Yayınları

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

Gürkaynak, Muharrem ve İren, Adem Ali (2011). *Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler* Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Y.2011, C.16, S.2, (263-279)

Gürkaynak, Muharrem, İren Adem Ali, *Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler*, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Y.2011, C.16, S.2, (263-279), Isparta

http://readgur.com/doc/24650/-episode-2---siber-g%C3%BC%C3%A7lerin-y%C3%BCkseli%C5%9Fi-cemalettin-demi%CC%87rci... 06 Ağustos 2016 Erişim tarihi.

Hekim Hakan, Başıbüyük Oğuzhan, *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları*
https://s3.amazonaws.com/academia.edu.documents/37825457/Siber_Suclar_ve_Turkiyenin_Siber_Guvenlik_Politikalari.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1527770185&Signature=rAuqbOWYCh2uNmW4Scw31moBQns%3D&response-content-disposition=inline%3B%20filename%3DSiber_Suclar_ve_Turkiyenin_Siber_Guvenli.pdfarı Erişim Tarihi: 31.05.2018

Kara Harp Okulu, http://www.kho.edu.tr/yayinlar/cizgi/aralik2001/terorizm/index.htm (17.12.2010)

Kara, Mahruze, (2013). *Siber Saldırılar - Siber Savaşlar ve Etkileri,* Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, İstanbul

Kara, Oğuz, Aydın Üzeyir, Oğuz, Ahmet, *Ağ Ekonomisinin Karanlık Yüzü: Siber Terör*
http://kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu%20siber%20teror.pdf Erişim Tarihi: 31.05.2018

Kardaş, Şaban, Balcı, Ali., (2014). *Realizm, Uluslararası İlişkilere Giriş*, İstanbul: Küre Yayınları

Kardaş, Şaban., Balcı Ali., (2014). *Uluslararası İlişkilere Giriş*, İstanbul: Küre Yayınları

Kardaş, Tuncay, Erdağ, Ramazan, (2014). *Uluslararası İlişkiler Teorileri (Derleyen: Ramazan Gözen)* (*Postyapısalcılık ve Uluslararası İlişkiler)*, İstanbul: İletişim Yayıncılık

Kegley, Charles William ve Blanton, Shannon Lindsey (2015). Dünya Siyaseti Yönelim ve Dönüşüm, (Çeviren, Gessler, Helin Alagöz) Sakarya Üniversitesi Kültür Yayınları, Ankara

Keleştemur, Atalay (2015). *Siber İstihbarat*, Level Yayınları Kocaeli Üniversitesi, Kocaeli

Kurgan, Bilişim Güvenliği Araştırmaları ve Geliştirme Merkezi, 2018, *Siber Mücadele Giriş*, İstanbul: Kutlu Yayınevi

Kurtoğlu, Ramazan, (2017). *Küresel Para Oyunları ve Psiko-Siber Savaş*, İstanbul: Destek Yayınları

Miş, Nebi, (2011). *Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi,* dergipark.ulakbim.gov.tr/akademikincelemeler/

Ongur, H.Sevinç, (2014). *Post-Yapısalcılık, Uluslararası İlişkilere Giriş* (Editörler: Şaban KARDAŞ, Ali BALCI)*, İstanbul:* Küre Yayınları

Öğün, Mehmet Nesim, Kaya, Adem, *Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler* Güvenlik Stratejileri Dergisi, Yıl:9 Sayı:18 (146-180)

Özkışlalı, Gizem, (2008). *Küreselleşme, İnternet Ve Terörizmin Değişen Yüzü;*

Öztürk, Zerrin Ayşe (2014). *Uluslararası İlişkilerde Güvenliği Yeniden Düşünmek: Geleneksel ve Alternatif Yaklaşımlar,* (Editor: Tayyar ARI), *Uluslararası İlişkiler Teorileri:2,* Bursa, Dora, (149-178)

Özkan, Tuncay, (2006). *Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analiz,* Yüksek Lisans Tezi, Anadolu Üniversitesi, Eskişehir

Roskin, Michael G., Berry, Nicholas O. (2014). *Uluslararası İlişkiler, Uİ'nin Yeni Dünyası,* Adres Yayınları

Sandıklı Atilla, ve Emeklier Bilgehan (2012). *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri,* İstanbul, BİLGESAM Yayınları.

Sandıklı, Bilgehan (2011). *21'inci Yüzyılda Uluslararası Örgütlerin Güvenlik Yaklaşımları ve Balkanlar'ın Güvenliği,* (Editör: Hasret Çomak, Caner Sancaktar) *21. Yüzyılda Yeni Güvenlik Anlayışları ve Yaklaşımları*, Uluslararası Balkan Kongresi, Kocaeli, (21-41)

Atilla, Sandıklı ve Bilgehan Emeklier, (2014). *Güvenlik Yaklaşımlarında Değişim ve Dönüşüm,* http://www.bilgesam.org/Images/Dokumanlar/0-81-2014040746sandikli_emeklier.pdf

Singer, P.W. , Friedman Allan (2015). *Siber. Güvenlik (ve) Siber. Savaş,* Buzdağı Yayınevi, Ankara

Sönmezoğlu, Faruk., (2002). *Uluslararası İlişkilere Giriş*, İstanbul: Der Yayınları.

Temizel Metehan, (2011). *Terörizmde Yeni Milad: 11 Eylül 2001*, "Terörizmin İdeolojik Temelleri ve 11 Eylül Sonrası Terörizm" Yayımlanmamış Yüksek Lisans Tezi Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya

Temizel, Metehan, (2011). *Terörizmde Yeni Milad: 11 Eylül 2001* Sosyal Bilimler Yüksekokulu Dergisi, Cilt:14 Sayı:1-2, (330-347), Konya

Topal, Hikmet, (2004). *Siber Terör*, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara

Topal, Hikmet, (2004). *Siber Terör*, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul

Tuna, Gülgün (2003). *Küresel Ekonomik, Ekolojik ve Sosyal Tehditler: Yeni Güvenlik*, Ankara, Nobel Yayın Dağıtım.

Uğurlu, Göksel (2014). *Uluslararası İlişkiler Teorileri/Temel Kavramlar,* (Editör: Mehmet Şahin, Osman Şen) *Marksizm,* Kripto Yayımları, Ankara, 2014, 89-109

Uzer, Umut., (2008). *Uluslararası İlişkiler Teorileri*, *Değişen Dünyada Uluslararası İlişkiler*, (Editör: İdris BAL), Lalezar Kitapevi, Ankara

Ünal, A. Naci (2015). *Siber Güvenlik ve Elektronik Bileşenleri,* Nobel Yayınları, Ankara, 2015

Wolfers, Arnold (2013). *Muğlak Bir Simge Olarak "Ulusal Güvenlik"*, (Çeviren: H.Burç AKA) *Uluslararası İlişkilerde Anahtar Metinler,* (Editör: Esra DİRİ), İstanbul, Özener Matbaacılık, (43-59)

Yalçın, Hasan Basri, (2017). *Ulusal Güvenlik Stratejisi (ABD-İngiltere-Fransa-Rusya-Çin)*, İstanbul: SETA Kitapları

Yavaş, Gökçen (2013). *Uluslararası İlişkilerde Teorik Tartışmalar*, (Editör: Hasret Çomak, Caner Sancaktar) *Bölge, Bölgeselleşme ve Güvenlik*, Beta Basım, 2013, (191-201)

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

Yayla, Mehmet (2014). *Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı,* Hacettepe HFD, 4 (2) 2014, (181-200)

Yılmaz, Aytekin, (2012). *Küresel Dünyada Uluslararası İlişkiler*, Ankara: Kadim Yayınevi

Yılmaz, Aytekin., (2012). *Küresel Dünyada Uluslararası İlişkiler Teori-Temel Kavramlar-Yeni Gelişmeler*, Ankara: Kadim Yayınları

Yılmaz, Sait ve Salcan Olay (2008). *Siber Uzay'da Güvenlik ve Türkiye*, İstanbul: Milenyum Yayıncılık

Zora, Kadir, (2015). *Güvenlikleştirme: Hukuksal Meşruiyetten Siyasal Meşruiyete Evrilme ve Kopenhag Okulu*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Cilt 23, Sayı 2, Yıl 2015, http://dergipark.gov.tr/download/article-file/262896 https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku Erişim Tarihi: 29 Temmuz 2018