

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

DOKTORA TEZİ

SİBER SALDIRILARA KARŞI MEŞRU
MÜDAFAA HAKKININ ULUSLARARASI
HUKUK AÇISINDAN İNCELENMESİ

CAN BOLAT

2502160563

TEZ DANIŞMANI
PROF.DR. YAŞAR ONAY

İSTANBUL- 2020



T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

DOKTORA
TEZ ONAYI



ÖĞRENCİNİN;

Adı ve Soyadı : CAN BOLAT Numarası : 2502160563
Anabilim Dalı /
Anasanat Dalı / Programı : ULUSLARARASI İLİŞKİLER Danışmanı : PROF. DR. YAŞAR ONAY
Tez Savunma Tarihi : 06.01.2020 Saati : 11:00 / 14:00
Tez Başlığı :
" SİBER SALDIRILARA KARŞI MEŞRU MÜDAFAA HAKKININ ULUSLARARASI HUKUK
AÇISINDAN İNCELENMESİ "

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin 50. Maddesi uyarınca yapılmış,
sorulan sorulara alınan cevaplar sonunda adayın tezinin **KABULÜNE** / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF. DR. YAŞAR ONAY		KABUL
2- DOÇ. DR. HASAN DURAN		Düzeltilme
3- DOÇ. DR. ÖZGÜN ERLER BAYIR		KABUL
4- DR. ÖĞR. ÜY. ATAHAH BİROL KARTAL		KABUL
5- DR. ÖĞR. ÜY. LAMİA MAMMADOVA		KABUL

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF. DR. MİTHAT BAYDUR		
2- DOÇ. DR. HAKAN GÜNEŞ		

ÖZ

Siber Saldırlara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi

Can BOLAT

İnternet ve ağ tabanlı sistemleri kullanımına başladığından beri çok hızlı bir gelişme kaydetmiş geline aşamada hayatımızın vazgeçilmez bir parçası olmuştur. Devletlerin kritik altyapıları ve kamu hizmetlerinin çoğunluğu ve bankacılık gibi birçok özel hizmet de internet ve ağ tabanlı sistemler üzerinde çalışmaktadır. Bu hizmetlerin kesintisiz devamı için bu sistemlerin güvenliği ulusal menfaatler açısından öncelikli hale gelmiştir.

Siber alanın özellikleri nedeniyle devletlerin kritik altyapılarına saldırı yapıp yapılmadığının veya yapıldıysa kim tarafından yapıldığının tespitinde zorluklar yaşanmaktadır. Örneğin İran'ın nükleer yakıt zenginleştirme tesislerine karşı 2009 yılında yapılan siber saldırılar 2010 yılında bir siber güvenlik şirketi tarafından tesadüfen tespit edilmiştir. Saldırının hedefi tesislerdeki denetleme, kontrol ve veri toplama sistemidir. Birçok devlet tarafından, bu sistemler su, doğal gaz, kanalizasyon benzeri belediye hizmetleri ile elektrik üretim ve dağıtımının kontrol edilmesi gibi kritik siber altyapıların izlenmesi ve kontrol edilmesi için kullanılmaktadır.

Meydana gelen aksaklığın siber bir saldırı olduğunun tespitini müteakip bu saldırının kim veya kimler tarafından yapıldığının belirlenmesi de siber alanın saldırganlara sağladığı imkânlar nedeniyle oldukça zordur. Günümüzde geliştirilen tekniklerle siber saldırı saldırgana yüksek bir yüzde ile atfedilebilmektedir. Saldırgan devlet dışı bir aktör ise iç hukuk yoluyla gerekli yaptırımlar uygulanmaktadır. Ancak saldırgan bir devlet ise o takdirde durum biraz karmaşık hale gelmektedir.

Mevcut uluslararası hukuk ve teamül hukukuna göre bir devlete silahlı bir saldırı yapılması o devlete meşru müdafaa hakkı vermektedir. Siber saldırıların silahlı bir saldırı seviyesine ulaşması durumunda da meşru müdafaa hakkının doğacağına şüphe yoktur. Ancak siber saldırıların çoğu silahlı saldırı seviyesinde değildir. Bu nedenle mevcut silahlı çatışma hukuku siber alandaki sorunların çözümünde yetersiz kalmaktadır. Bunun yanında göreceli olarak yeni bir alan olan siber alanla ilgili normlar oluşmamış, oluşan normlar ise yeterince yaygınlaşıp kabul görmemiştir.

Devletlerin siber alanla ilgili yakın zamanda uluslararası bir anlaşma yapmaları mümkün görülmediğinden siber alanla ilgili normlar gelişinceye kadar devletlerin kritik siber altyapılarını ve bunlara ilişkin angajman kurallarını deklare etmeleri ve bu angajman kurallarına göre hareket etmeleri en iyi çözüm yolu olarak ortaya çıkmaktadır. Çünkü devletin hayatta kalması ve hayati çıkarlarını koruması derhal, güçlü ve saldırgan bir karşılık vermesine bağlı olabilir.

Anahtar Kelimeler: Kritik Altyapı, Siber Saldırı, Meşru Müdafaa, Atfetme.

ABSTRACT

Analysis of the Right to Self-Defense Against Cyber Attacks in Terms of International Law

Can BOLAT

Since the beginning of the use of internet and network-based systems has made a very rapid development has become an indispensable part of our lives. Many of the critical infrastructures of the state and the majority of public and private services such as banking work on the internet and network-based systems. For the uninterrupted continuation of these services, the security of these systems has become a priority for national interests.

Due to the characteristics of the cyber space, it is difficult to determine whether the critical infrastructure of the state has been attacked or who has done it. For example, cyber attacks against Iran's nuclear fuel enrichment facilities in 2009 were detected by a cyber security company in 2010. The target of the attack is the supervision, control and data collection system in the facilities. These systems, which are used by many states, are used to control and monitor critical infrastructures such as energy production and distribution, water, natural gas and sewage systems.

Because of the opportunities provided by the cyber space to the attackers if it was a cyber-attack, it is quite difficult to determine who or by whom this attack was made. Cyber-attack is attributed to the attacker with a high percentage with the techniques developed today. If the attacker is a non-state actor, necessary sanctions are imposed through domestic law. However, if it is an aggressive state, then the situation becomes a bit complicated.

According to current international law and customary law, an armed attack on a state gives it a right to self-defense. There is no doubt that the right to self-defense will arise if cyber attacks reach an armed attack level. However, most cyber attacks are not at the level of armed attacks. For this reason, the current law of armed conflict is inadequate in solving cyber problems. In addition, norms related to cyber space, which is a relatively new field, have not been formed and norms formed have not been widely accepted.

Since it is not possible for states to conclude an international agreement on cyberspace in the near future, it is the best solution for states to declare their critical cyber infrastructures and their rules of engagement and act in accordance with these rules of engagement until the norms related to cyberspace are developed. Because the survival of the state and the protection of its vital interests may depend on its immediate, strong and aggressive response.

Keywords: Critical Infrastructure, Cyber Attack, Self-Defense, Attribution.

ÖNSÖZ

Bilgi ve iletişim teknolojileri son yirmi yılda çok hızlı gelişmiş ve yaşamımızın hemen hemen her alanına entegre edilmiştir. Bu dijitalleştirmenin getirdiği dönüşüm yeni bağımlılıklar yaratmıştır. Ekonomi, devlet idaresi ve temel hizmetlerin sağlanması artık siber alanın bütünlüğüne ve onu destekleyen altyapı, kazanım ve sistemler ile verilere dayanmaktadır. Bu bütünlüğe olan güven kaybı, bu teknolojik devrimin faydalarını tehlikeye atabilir. Birbirine bağlı dijital ortamı geliştirmek için geliştirilen donanım ve yazılımların çoğu, öncelikle kullanıcı verimliliğini, maliyetini ve kullanım kolaylığını sağlarken güvenlik göz ardı edilmiştir. Kötü niyetli kişiler, düşman devletler, suçlular veya terör örgütleri kolaylık sağlayan donanım ve yazılımlardaki güvenlik açıklarından istifade ederek ekonomimize zarar verebilir, devlet idaresini ve verilen hizmetleri sekteye uğratabilir.

İnternetin bilgisayar ve cep telefonlarının ötesinde diğer siber-fiziksel ya da “akıllı” sistemlere yayılması, bütün bu sistemleri uzaktan saldırıya açık hale getirmiştir. Enerji şebekeleri, hava trafik kontrol sistemleri, uydular, medikal teknolojiler, endüstriyel tesisler ve trafik ışıkları gibi günlük hayatımızı destekleyen sistemler ve teknolojiler internete bağlıdır ve bu nedenle potansiyel olarak saldırı ve müdahaleye karşı savunmasız durumdadır.

Yakın zamana kadar devletler kara, hava, uzay ve deniz alanlarını kontrol ederek ülkelerini koruyabilmiştir. Günümüzde siber alan devlet ve devlet dışı aktörlere, ülkelerin sınırlarını fiziki olarak geçmeden devletlerin siyasal, ekonomik ve güvenlik çıkarlarına karşı saldırı yapma olanağı sunmaktadır. Siber saldırılar, kritik altyapılara ciddi zararlar vermek, ticareti sakatlamak, ağlarımızı zayıflatmak ve vatandaşların her gün iletişim kurmak ve iş yapmak için kullandıkları araçlara ve cihazlara saldırmak için düşük maliyetli ve inkâr edilemez fırsatlar sunmaktadır.

Birçok ülke ulusal güvenlik strateji belgelerinde siber saldırıları öncelikli bir tehdit olarak görmekte ve bu tehditlere karşı savunma, caydırıcılık ve mukabil saldırı yeteneklerini geliştirmek için programlar yapmaktadırlar. Ancak meydana gelebilecek çatışmanın kuralları belirli değildir.

Tarihte her dönemde çatışma ve savaşın hukuksal ve etik kuralları olmuştur. Bir zamanlar onur ve haysiyet gibi yazılı olmayan etik kurallar varken daha sonra yazılı

kurallar ortaya çıkmıştır. Ancak siber çatışma ile ilgili kurallar belirgin değildir. Siber çatışma ve savaşa uygulanacak kuralların tespitinde konunun uzmanları ikiye bölünmüştür. Bir kısmı mevcut hukuk kurallarının yeni çatışma ortamına uyarlanabileceğini savunurken ve diğer kısmı siber alana özgü yeni kuralların belirlenmesini savunmaktadır.

Bu çalışma sonucunda devletlerin siber saldırılara vereceği karşılığın tespiti için mevcut hukuk kurallarının uyarlanmasının mı yoksa yeni kuralların konulmasının mı daha doğru olacağı hususunda bir değerlendirme yapılacaktır.

Can BOLAT

İSTANBUL 2020

İÇİNDEKİLER

	Sayfa
ÖZ.....	iii
ABSTRACT.....	v
ÖNSÖZ.....	vii
İÇİNDEKİLER.....	ix
KISALTMALAR.....	xv
GİRİŞ.....	1

BİRİNCİ BÖLÜM

SİBER ALAN VE SİBER SALDIRI

1.1.KURAMSAL ARKA PLAN.....	6
1.2.NORM HİPOTEZİ.....	8
1.3.NORM EVRİM TEORİSİ.....	10
1.3.1.Birinci Safha Normun Ortaya Çıkışı.....	12
1.3.2.İkinci Safha Norm Zincirinin Oluşması.....	13
1.3.3.Üçüncü Safha Normun İçselleştirilmesi.....	15
1.4 SİBER ALAN VE SİBER AKTÖRLER.....	15
1.4.1.Siber Alanın Tanımı.....	16
1.4.2.Siber Aktörler.....	18
1.4.2.1.Devlet Dışı Aktörler.....	18
1.4.2.2.Siber Alanda Devlet Aktörü.....	20
1.4.3.Devlet ve Siber Alan.....	22
1.4.3.1.Egemenlik.....	22

1.4.3.2.Devletin Yargı Yetkisi.....	23
1.4.3.3.Devletin Denetimi.....	24
1.4.3.4.Devletin Sorumluluđu.....	25
1.5.SİBER SALDIRI.....	25
1.5.1.Birleşmiş Milletler Kararına Göre Saldırı Tanımı.....	25
1.5.2.Siber Saldırının Tanımı.....	25
1.5.3.Siber Saldırının Sistemler Üzerinde Yarattığı Etkiler.....	26
1.5.4.Siber Saldırı Türleri.....	29
1.5.4.1.Hizmet Engelleme.....	29
1.5.4.2.Yetki Artırımı.....	29
1.5.4.3.Truva Atı.....	30
1.5.4.4.Botnetler.....	30
1.5.4.5.Mantık Bombası.....	31
1.5.4.6.Solucanlar.....	31
1.5.4.7.Gelişmiş Siber Tehditler.....	31
1.5.5.Siber Saldırıların Önemli Hedefleri.....	32
1.5.5.1.Sosyal Ağlar.....	32
1.5.5.2.Akıllı Şebekeler.....	33
1.5.5.3.Kapalı Devre Sistemler.....	33
1.5.5.4.Acil Yardım Sistemleri.....	34
1.5.5.5.Web Sayfaları.....	34
1.5.5.6 Kritik Altyapılar.....	35
1.5.6.Siber Saldırı Örnekleri.....	36
1.5.6.1.2003 ABD ve Kanada Elektrik Kesintisi.....	36

1.5.6.2.2007 Estonya Saldırısı.....	36
1.5.6.3.2008 Gürcistan Saldırısı.....	37
1.5.6.4.2009 İran Nükleer Tesislerine Yapılan Saldırıları.....	38

İKİNCİ BÖLÜM

SİBER SALDIRILAR VE ULUSLARARASI HUKUKTA KUVVET KULLANIMI

2.1.SİBER SAVAŞIN BELİRGİN ÖZELLİKLERİ.....	41
2.1.1 Siber Savaşın Muharebe Sahası.....	42
2.1.2.Siber Savaşın Tanımı.....	43
2.2.SİBER SAVAŞIN MEVCUT STATÜSÜ ve ULUSLARARASI NORMLAR.....	45
2.3.SİLAHLI ÇATIŞMA HUKUK ve SİBER ALAN.....	49
2.3.1.Kuvvet Kullanma Yasağı.....	49
2.3.2.Martens Hükmü.....	50
2.3.3.Kuvvet Kullanmanın Hukuka Uygun Olduğu Durumlar.....	50
2.3.3.1.Meşru Müdafaa Hakkı.....	50
2.3.3.2.BM Güvenlik Konseyinin Münhasıran Kuvvet Kullanması.....	53
2.3.4.Siber Saldırıları ve Kuvvet Kullanma Yasağı.....	53
2.3.5.Araç, Hedef ve Etki Odaklı Yaklaşım.....	54
2.3.6.Talinn Modeli.....	56
2.3.6.1.Siber Altyapının Kontrolü.....	56
2.3.6.2.Tehdit ve Kuvvet Kullanımı Yasağı.....	60
2.3.6.3. Kuvvet Kullanımının Tanımlanması.....	63
2.3.6.4. Silahlı Saldırıya Karşı Meşru Müdafaa.....	70

2.3.7. Wingfield Analizi.....	78
2.3.7.1.Estonya Siber Saldırısının İncelenmesi.....	83
2.3.7.2. İran Stuxnet Siber Saldırısının İncelenmesi.....	85

ÜÇÜNCÜ BÖLÜM

SİBER SALDIRILARIN BİR DEVLETE ATFEDİLMESİ

3.1. ATIF SORUNUNUN TANIMLANMASI.....	90
3.2. ATFETME İŞLEMİNİN SEVİYELERİ.....	93
3.3. ATFETMENİN TEKNİK KANITLARI.....	98
3.3.1. Gizliliği İhlal Göstergeleri.....	98
3.3.2. Hedefleme.....	99
3.3.3.Kullanılan Altyapı.....	101
3.3.4.Modülerlik.....	102
3.3.5.Zaman Planlaması ve Alışkanlıklar.....	102
3.3.6.Yazılımlarda Kullanılan Dil.....	103
3.3.7.Hatalar.....	104
3.3.8.Anonimlik ve Gizlilik.....	104
3.3.9.Yetki.....	106
3.3.10.Hazırlık.....	106
3.3.11.Gelişmiş Kalıcı Tehdit.....	107
3.3.12.Safhalı Planlama.....	107
3.3.13.Jeopolitik Bağlam.....	108
3.3.14.İçerden Gelen Tehdit.....	109
3.3.15.Hasar.....	109
3.3.16.Saldırının Gerekçesi.....	110

3.3.17.Gözden Geçirme.....	111
3.3.18.Önyargılar.....	112
3.3.19.Bireyden Organizasyona.....	112
3.4.ATFETMENİN SINIRLAMALARI.....	113
3.5.ATFIN KAMUOYUNA AÇIKLANMASI.....	114
3.6.ULUSLARARASI HUKUKA GÖRE DEVLETİN SORUMLULUKLARI.....	119
3.6.1.Devlet Dışı Aktörlerin Eylemlerinden Devletin Sorumluluğu.....	122
3.6.2.Devletin Siber Altyapısı Kullanılarak Başlatılan Siber Saldırılarda Sorumluluğu.....	128
3.6.3.Bir Devlet Üzerinden Yönlendirilen Siber Operasyonlar.....	130
3.6.4.Devletin Sorumluluğuyla İlgili Değişimler.....	131
DÖRDÜNCÜ BÖLÜM	
MEŞRU MÜDAFAA KAPSAMINDA SİBER SALDIRILARA VERİLECEK KARŞILIK	
4.1.MEŞRU MÜDAFAANIN TANIMI.....	133
4.2. MEŞRU MÜDAFAAYA STRATEJİK BAKIŞ.....	133
4.3.MEŞRU MÜDAFAANIN KOŞULLARI.....	137
4.3.1.Büyüklik ve Etki Kriteri.....	137
4.3.2.Siber Saldırının Kaynağı.....	141
4.3.3.Siber Saldırının Hedefi ve Amacı.....	143
4.3.4.Başka Bir Devletin Egemenliğinin İhlal Edilmemesi.....	144
4.3.5.Gerekliklik, Orantılık, Yakınlık ve İvedilik Kriterleri.....	145
4.4.GEREKLİLİK VE ORANTILILIK.....	145

4.4.1.Gereklilik.....	145
4.4.2.Orantılılık.....	146
4.4.2.1.Saldırıyı Atfetme Derecesi.....	149
4.4.2.2.Siber Saldırının Etkisi.....	150
4.4.2.3.Verilecek Karşılıkta Kullanılacak Araçlar.....	151
4.4.2.4.Verilecek Karşılık İçin Dikkate Alınması Gereken Politika Kuralları.....	153
4.4.2.5.Aşırı Tepki Riski.....	154
4.4.2.6.Verilecek Karşılık İçin Angajman Kurallarının Belirlenmesi.....	156
4.5.İVEDİLİK VE YAKINLIK.....	157
4.5.1.Yakınlık.....	158
4.5.2.İvedilik.....	160
4.6. Estonya Saldırısının Gereklilik, Orantılılık, Yakınlık ve İvedilik Kriterlerine Göre İncelenmesi.....	164
4.7. STUXNET Saldırısının Gereklilik, Orantılılık, Yakınlık ve İvedilik Kriterlerine Göre İncelenmesi	166
SONUÇ	168
BİBLİYOGRAFYA/KAYNAKÇA.....	175
ÖZGEÇMİŞ.....	188

KISALTMALAR LİSTESİ

AB	: AVRUPA BİRLİĞİ
ABD	: AMERİKA BİRLEŞİK DEVLETLERİ
APT	: ADVANCED PERSISTENT THREATS
AR-GE	: ARAŞTIRMA VE GELİŞTİRME
BM	: BİRLEŞMİŞ MİLLETLER
CCDCoE	: COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE
DDoS	: DISTRIBUTED DENIAL OF SERVICE
DNS	: DOMAIN NAME SYSTEM
GGE	: GROUP OF GOVERNMENTAL EXPERTS
ICANN	: INTERNATIONAL ESTABLISHMENT NAMES AND NUMBERS INSTITUTION
INTERNET	: INTERCONNECTED NETWORK
TCP/IP	: INTERNET PROTOCOL
NATO	: NORTH ATLANTIC TREATY ORGANIZATION
NCSD	: NATIONAL CYBER SECURITY DIVISION
NSA	: NATIONAL SECURITY AGENCY
PC	: PERSONAL COMPUTER
SCADA	: SUPERVISORY CONTROL AND DATA ACQUISITION
TÜBİTAK	: TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARAŞTIRMA KURUMU
USB	: UNIVERSAL SERIAL BUS
VB.	: VE BENZERİ

GİRİŞ

Siber savaş kavramı ve siber saldırıların gündemimize girmesi çok da uzak olmayan bir geçmişe sahiptir. Teknoloji ve bilişim sistemlerinin gelişmesi ile bu teknoloji ve sistemlere ucuz ve kolayca ulaşılabilmesi siber saldırıların sadece devletler değil bireyler tarafından da yapılabilmesine imkân vermektedir. Hizmet ve işlemlerin gittikçe artan şekilde internet üzerinden verilmeye başlanması ve internete ulaşımın yaygınlaşması sonucunda siber saldırılar küresel hale gelmiştir. Dolayısı ile devletlerin geleneksel egemenlik alanlarına “kara, deniz, hava ve uzay” ilave olarak siber egemenlik alanı ortaya çıkmıştır. Bu yeni egemenlik alanının en önemli özelliği diğerlerine kıyasla ulaşmanın daha kolay olmasıdır. Çünkü siber saldırı yöntemleriyle ilgili bilgi sahibi olan ve evinde internete bağlı bilgisayarının başında oturan herhangi bir kişinin siber saldırı yapma imkânı bulunmaktadır. Böyle bir ortamda devletlerin siber egemenlik alanlarındaki hak ve çıkarlarının nasıl korunacağı sorunu ortaya çıkmıştır.

Son yıllarda siber saldırı olarak nitelenebilecek birçok saldırı meydana gelmiştir. Bu saldırılardan en dikkat çeken; 2007 yılında Estonya’nın kritik altyapılarına yönelik siber saldırılardır. 2007 yılında Sovyet iktidarını temsil eden bir heykelin hükümet tarafından yerinin değiştirilmesinden sonra hükümet internet sitelerine ve banka sistemlerine siber saldırılar meydana gelmiştir¹. Saldırıları Rusya’nın yaptığı iddia edilmiş olsa da bu saldırıları Rusya’ya atfedebilecek herhangi bir kanıt bulunamamıştır.

Yine diğer saldırılardan farklı olarak dikkat çeken internete hiçbir bağı bulunmayan İran’ın uranyum zenginleştirmede kullandığı sistemlerine yapılan saldırıdır. 2010 yılında Stuxnet adlı bir virüs İran’ın uranyum zenginleştirme santrifüjlerini çalışmaz hale getirmiştir. Saldırının tam olarak kim tarafından gerçekleştirildiği bilinmese de

¹Stephen Herzog, “Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses”, *Journal of Strategic Security*, 2011, Cilt 4(2), s. 50-51

amacın İran'ın nükleer programını durdurmak veya yavaşlatmak olduğu bilinmektedir.²

Siber saldırılardan bir kısmı tespit edilebilirken bir kısmı da hiç tespit edilememektedir. Tespit edilemeyen siber saldırıların, devlet desteği alan devlet dışı bir aktör ya da bir devlet tarafından başka bir devlete karşı yapılması uluslararası hukuk açısından önemli ve hukuki olarak çözülmesi gereken bir problemidir.³ Ancak kara, deniz, hava ve uzay egemenlik alanlarına ilişkin devletlerin haklarını ne şekilde koruyabileceğini düzenleyen normlar geniş bir yaygınlık kazanmışken siber alanla ilgili normlar henüz yeni yeni ortaya çıkmaktadır. Bu yeni normlar oluşturulurken kara, deniz, hava ve uzay alanlarını düzenleyen normlardan istifade edilmektedir. Bu çalışmada siber saldırıların uluslararası teamül hukuku ve BM Anlaşması'na göre kuvvet kullanma olarak görülüp görülemeyeceği ve bu kapsamda bu saldırılara maruz kalan devletlerin meşru müdafaa kapsamında nasıl bir karşılık verebilecekleri incelenecektir.

Son dönemde dünyada meydana gelen “2007 Estonya'nın kritik altyapılarına yapılan saldırılar, 2010 Stuxnet virüsü ile İran'ın uranyum zenginleştirme programının sekteye uğratılması ve 2016 ABD Başkanlık Seçimlerine müdahale” gibi olaylar siber gücün (gelişmiş siber savaş yetenekleri) ülkeler arasında mücadele ve savaş aracı haline geldiğini göstermektedir. Son olaylar siber gücün, ciddi ekonomik kayıp, tahribat meydana getirme, yaralanma ve hatta ölüm gibi fiziksel hasarlara neden olma kapasitesi olduğunu göstermiştir. Siber saldırılarla kritik bilgiler elde edilebilir, her çeşit istihbarat, askeri komuta ve kontrol sistemleri devre dışı bırakılabilir, bilgisayar destekli silahlara ve sistemlere zarar verilebilir, bankalar ve borsalar gibi ekonomik açıdan kritik kurumlar çalışamaz hale getirilebilir, devletlerin milli güvenlikle ilgili web sitelerinden bilgiler sızdırılabilir ya da internet ağına bağlı sistemlere ciddi zararlar verilebilir.

²David A. Sanger, “Obama Order Step Up Wave of Cyber attacks Against Iran”, **The New York Times**, 1 June 2012, (Çevrimiçi) <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>, 25.11.2015

³ Muharrem Gürkaynak ve Adem Ali İren, “Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler”, **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, 2011, Cilt:16, Sayı:2, s.263-279.

Ülkelerin iletişim, sağlık, ekonomi ve ulusal hizmet altyapıları gittikçe artan bir şekilde ve öncelikli olarak ağ bağlantılı bilgi sistemlerine dayanmaktadır. Bu durum, toplumsal yaşamda kolaylık ve ekonomik yaşamda daha fazla refah ile bilgiye ulaşmadaki kolaylık ve hız nedeniyle verimli akademik çalışmaların ortaya çıkmasına neden olmuştur. Ancak, her şeyin bir maliyeti olduğu gibi bu imkânlarla sahip olmanın maliyeti de teknolojinin hızla benimsenmesi nedeniyle önemli ölçüde güvenlik açıkları olmuştur. Siber teknolojinin kamuya yayılmasının temel amacı, kamu ihtiyaçlarına uygun ve hızlı bir erişilebilirlik sağlamaktır. İnternet başlangıçta az sayıda güvenilir kullanıcının ihtiyaçlarına göre tasarlanmış, ağı, yönlendirme altyapısının önemli bir bölümünü etkileyen harici fiziksel saldırı veya kazaya karşı korunabilmesi için tedbirler düşünülmüş ancak içeriden gelecek saldırı olasılığıyla ilgili olarak hiçbir tedbir düşünülmemiştir.

Siber teknolojinin yayılması verimliliği ve etkinliği önemli ölçüde artırmakla birlikte, aynı zamanda, siber teknoloji savaşın sevk ve idaresinde devrim yaparak güç ve güvenlik anlayışının büyük ölçüde değiştiği hassas bir dünya yaratmıştır. Siber teknoloji ile ortaya çıkan sanal alan, vatandaşlar veya yetkililer, kamu ya da askeri endüstriler; özel veya resmi kuruluşlar tüm tarafları ayırım gözetmeksizin içermektedir.

İkinci Dünya Savaşı'ndan sonra Birleşmiş Milletler Anlaşması kapsamında oluşturulan dünya düzeni devletlerin kuvvet kullanmasını ve kuvvet kullanma tehdidini yasaklamıştır. Bu hüküm, Birleşmiş Milletler Antlaşması'nın 2. madde 4. fıkrasında: “Teşkilatın üyeleri, milletlerarası münasebetlerinde gerek bir başka devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı, gerekse Birleşmiş Milletlerin amaçları ile telif edilemeyecek herhangi bir surette, tehdide veya kuvvet kullanılmasına başvurmaktan kaçınırlar” şeklinde ifade edilmektedir.

Birleşmiş Milletler Anlaşması ile kurulan bu dünya düzenine karşı teknolojide meydana gelen gelişmeler nedeniyle yeni tehditler ortaya çıkmıştır. Bu yeni tehditlerin ortaya çıkmasının sebebi gelişen bilişim teknolojileriyle birlikte ülkelerin kara, deniz, hava ve uzay egemenlik alanlarına yeni bir sanal egemenlik alanının eklenmiş olmasıdır. Devletlerin siber alanda egemenliklerine karşı bu alana has özellikte tehditler ortaya çıkmıştır. Bu tehditlerin mevcut sözleşme ve teamüller kapsamı içinde

tanımlanması mümkün değildir. Tehdit tanımlanamadığından mevcut uluslararası düzeni korumak üzere oluşturulmuş uluslararası hukuk kuralları da bu tehditlere yaptırım uygulamakta yetersiz kalmaktadır.

Tespit edilen siber saldırıların bir devlete atfedilebilmesi de diğer önemli bir sorundur. 2016 ABD Başkanlık seçimlerini Rusya'nın siber saldırılarla manipüle ettiği yönündeki iddialar bulunmaktadır. Bu manipülasyonlar nedeniyle ABD, Rusya'ya diplomatik ve ekonomik yaptırımlar uygulamıştır. Bu manipülasyonların Rusya'ya ne şekilde atfedildiği uluslararası ilişkiler ve uluslararası hukuk açısından da geleceğe ışık tutacaktır.

Çalışmanın amacı aşağıdaki sorulara cevap vermek ve yeni problem sahalarını ortaya koymaktır. Siber saldırılar, BM Şartı 51.madde kapsamında bir saldırı olarak tanımlanabilir mi? Siber saldırıların saldırı olarak tanımlanabilmesi için kıstaslar neler olabilir? Siber saldırılar bir devlete nasıl atfedilecektir? Siber saldırıların saldırı kapsamına sokulması durumunda verilecek karşılığın kapsamı ne olacaktır? Bu kapsamda, araştırmanın hipotezi aşağıdaki şekilde oluşturulmuştur: "Siber saldırının belirli bir düzeye ulaşması ve düzenleyenin bir devlet olduğuna dair deliller yeterli düzeyde olursa, saldırıya uğrayan devletin (BM Antlaşması Madde 51'e göre) meşru müdafaa hakkı güçlenir/doğar." Hipotezin bağımsız değişkeni "konu hakkında yeterli delil", bağımlı değişkeni "meşru müdafaa hakkı"dır.

Yakın zamana kadar devletler kara, hava, uzay ve deniz alanlarını kontrol ederek ülkelerini koruyabilmiştir. Günümüzde siber alan devlet ve devlet dışı aktörlere, ülkelerin sınırlarını fiziki olarak geçmeden devletlerin siyasal, ekonomik ve güvenlik çıkarlarına karşı saldırı yürütme olanağı sunmaktadır. Siber saldırılar, kritik altyapılara ciddi zararlar vermek, ticareti sakatlamak, internet veya intranet(özel kapalı ağlar)ağlarımızı zayıflatmak ve vatandaşların her gün iletişim kurmak ve iş yapmak için kullandıkları sistemlere saldırmak için düşük maliyetli ve inkâr edilemez fırsatlar sunmaktadır.

Saldırganlar için bulunmaz bir fırsat iken; ülkesinin ve vatandaşlarının haklarını korumak için devletlerin elindeki mevcut normlar, saldırınlara karşı alınabilecek tedbir ve verilecek karşılık için yetersiz hatta işlevsiz kalmaktadır. Siber

alandaki kuvvet kullanımı ile ilgili kurallar üzerinde fikir birliği sağlanamaz ise; siber uluslararası ortama devletlerin birbirine güvensizliği ve her devletin sadece kendine güvenmesi (self help) sistemi hâkim olabilir ve bunun sonucu da klasik kuvvet kullanılması ihtimali ortaya çıkabilir.

Siber alanın, bilgisayar ve internet teknolojileri gibi çok teknik konuları kapsamaması ayrıca bu teknik hususların uluslararası hukuk açısından değerlendirilecek olması çalışmayı zorlaştırdığından teknik bilgilere ihtiyaç olduğu kadar değinilmiş ayrıntıya girilmemiştir. Bu çalışmada yerli ve yabancı literatürde siber saldırılar ve meşru müdafaa kapsamında yapılan çalışmalar, örnek olabilecek Uluslararası Adalet Divanı Kararları “belgesel tarama” tekniğinin literatür (alanyazın) taraması yapılarak basılı ve online ortamlardaki yayınlardan araştırmanın amacına, kaynağına ve gerçeğe uygun olarak faydalanılmıştır. İşlenen verilerle önce siber saldırının tanımı yapılmış, siber saldırı uluslararası hukukta kuvvet kullanımı kriterlerine göre sınanmış, siber saldırının bir devlete atfedilebilme kıstasları incelenmiş ve siber saldırılara meşru müdafaa kapsamında nasıl bir karşılık verileceği uluslararası hukuk normlarına uygun olarak ortaya konulmuştur.

Ayrıca Türkiye’de ve dünyada son dönemde yapılmış siber saldırılar ve bunlara karşı uygulanan yaptırımlar ile siber güvenliğin sağlanması için alınan tedbirler incelenmiştir. Son dönemde yapılmış siber saldırılarla ilgili hukuki süreç ve diğer devletlerin tepkileri gelecekte oluşabilecek normlar için işaret olarak değerlendirilmiştir.

Siber saldırının bir devlet tarafından yapıldığına ilişkin delillerin ne şekilde elde edilebileceği bu delillerin neler olabileceği ve buna mukabil siber saldırıya uğrayan devletin meşru müdafaa hakkının doğması durumunda nasıl bir karşılık vereceği neden sonuç ilişkisi kapsamında anlam ifade edilerek bir bütünlük içerecek şekilde yorumlanmıştır.

BİRİNCİ BÖLÜM

SİBER ALAN VE SİBER SALDIRI

1.1.KURAMSAL/KAVRAMSAL ÇERÇEVESİ

Tez konusu alan yeni gelişmekte olduğundan bu alanla ilgili normlar henüz oluşmamış veya oluşma aşamasındadır. Bu nedenle normatif teori bu çalışmanın kuramsal temelini oluşturması için en uygun teori olarak tespit edilmiştir. Normatif teori; bilimsel bir teori olmadığı için gözlem ve sınanamaya tabi tutulamaz. Normatif teori “ne olmalı, ne yapmalı” sorularını sorarak olması gereken düzenle ilgili kuralları tespit etmektedir. Bu çerçevede normatif uluslararası teori, olması gerekeni tespit için kurallar oluşturma işlevini ortaya koymaktadır.

Normatif kuram uluslararası sistem içinde devletlerin davranışları ile başka devletlere karşı yükümlülük, sorumluluk, hak ve ödevlerinin neler olduğuna ilişkin konular üzerinde çalışmaktadır. Uluslararası politikaya ait kurallar, değerler ve standartlar belirlemek ve uluslararası sistemin belirli bir düzen içinde devam etmesini sağlamak normatif teorinin temel hedefidir.

Britannica Ansiklopedisinde, normun tanımı şöyle yapılmıştır;¹ “Norm, bir faaliyet için gereken kural, standart veya kalıplardır. Sosyal normlar, davranış kurallarıdır. Normlar, bir davranışın yargılanmasına yarayan ve tasvip edilip edilmemesine dayanak noktası oluşturan davranış standartlarıdır.”

Normlara uygun olan davranış ahlakidir, aykırı davranışlar ise ahlak dışıdır. Bu anlamda, hukuk, gelenek, dini kurallar, ahlak gibi kavramlar normlarla ilişkili olarak kullanılmışlardır. Bu kavramlar birlikte düşünüldüğünde, “normların ortaya çıkması, toplumsal yaşamın düzene girme gereksinmesine bağlanabilir”.

Uluslararası normlar ise devletlerin davranışlarını düzenleyen standartlardır ve uluslar üstü alanda gereken düzenleme ihtiyacından kaynaklanmaktadır.

Uluslararası normların işlevleri; uluslararası ilişkiler aktörlerinin davranışlarını dayandırabileceği esasların belirlenmesi, buna bağlı olarak bu esasların düzenlenmesi

¹ **Encyclopaedia Britannica**, (çevrimiçi) <https://www.britannica.com/topic/norm-society>, 25.03.2019

ve gerektiğinde dönüştürülmesidir. Normatif uluslararası teori, uluslar üstü alandaki aktör davranışlarının ve mevcut sistemin normlara uygun olarak düzenlenmesini öngörür. Bir başka ifade ile olandan olması gerekene ulaşmayı amaçlayan bir yaklaşım olarak ifade edilebilir.

İnsan diğer canlılardan farklı olarak seçim yapabilmekte ve daha önemlisi seçim yaparken ahlaki bir takım değerleri dikkate almaktadır. İşte bu ahlaki değerler insanı diğer canlılardan farklı olarak olması gerekene ulaşması için motive etmektedir. Olması gerekenle mevcut arasındaki fark ahlaki olarak doğru olduğuna inanılana ulaşmak için yapılması gerekenleri ortaya çıkarır.

Uluslararası normlar, üç safhada oluşumlarını tamamlamaktadır. Birinci safhada normlar teamüller veya anlaşmalar yoluyla ortaya çıkmakta, ikinci safha normların kısıtlı da olsa devletlerarasında yaygınlık kazanması ve son safha da normların devletlerin çoğunluğu tarafından genel kabul görmesi safhasıdır. Bir normun ortaya çıkışından sonraki en kritik nokta, devletlerin çoğunluğunun normu benimsemesi sonucunda normun geniş yaygınlık kazanmaya başladığı “dönüm noktası”dır ve bu nokta ilk iki safha arasına tekabül etmektedir.

Normatif teorinin ana konusu bireylerin değer yargıları ile yine bireylerin aile, toplum, devlet ve uluslararası sistem gibi içinde yaşadıkları kurumlarla arasındaki bağlantıyı araştırmaktır. Eşitlik, hürriyet, demokrasi, adalet ve savaş gibi kavramlar ile bireylerin içinde yaşadığı kurumlar arasındaki ilişkinin nasıl kurulduğu da normatif teorinin incelediği temel konulardandır.²

Mevcut dünya düzeni egemen ve özerk devletlerden oluşmaktadır. Bireyden başlayıp, aile, toplum ve en örgütlü kurum olan devlete kadar her biri kendi varlığını haklı kılan ahlaki temellere dayandırmaya ihtiyaç duymaktadırlar. Bu ahlaki temeller uzun yıllar içinde oluşmuş ve çoğunluk tarafından kabul edilen evrensel kurallardan kaynaklanmaktadır.

² Katzenstein, Wendt, and Jepperson, **Norms, Identity, and Culture in National Security**, Columbia University Press, 1996, s.33– 75.

Siber alanla ilgili kural ve normların yerleşmesi için gayret ve çabalar devam etmektedir. Devlet liderleri siber güvenliğe dair yaptıkları her önemli açıklamada ortak davranış normlarına uyma çağrısında bulunmaktadırlar. Örneğin, Çin Cumhurbaşkanı Xi Jinping'in 2015 yılı Eylül ayında ABD'yi ziyaretinde, ABD Başkanı Obama “siber alanda uygun davranış şeklinin uluslararası kurallarını teşvik etmek için hep birlikte ve başka milletlerle çalışacağız.” demiştir.³

Uluslararası hukuk kuralları siber alanda uygulanırken, kuralların nasıl uygulanacağı tartışma konusu olmaktadır. Birçok rapor ya saldırı davranışını haklı çıkarmak ya da alanın yeniliklerini araştırmak için uluslararası hukuk kurallarına başvurmaktadır. 2013 yılında yayınlanan Tallinn El Kitabı anlaşmayı güçlendirmek için ümit vaat eden bir girişimdi, ancak devletler hatta araştırmacılar arasında fikir ayrılıklarının bulunması uluslararası bir anlaşma yapılmasına engel olmuştur.

Siber alan, interneti, uzay tabanlı interneti, yerel ve hücresel ağları, fiber-optik kabloları ve internete bağlı tüm bilgisayarları da içermektedir. Siber alanda, ekonomi yasaları, yargılama ve kontrol kuralları bulunan fiziksel bir altyapı katmanı vardır.

Siyasi söylemde siber alanın katmanlara ayrılması önem arz eder, çünkü devleti analiz dışında tutmak imkânsızdır. Devletlerin erişim ve teknoloji üzerindeki tekeli hala devam etmektedir. Uluslararası Tahsis Adları ve Numaraları Kurumu (ICANN) internet alanlarını yöneterek ve Birleşmiş Milletler Devlet Uzmanları Grubu (GGE) ise siber güvenlik raporlarını bir araya getirerek siber alanın kontrolünde önemli bir rol oynamaktadır.

Tez konusu olarak belirlenen çalışma konusu, teknoloji ve bilişim sistemlerinin gelişmesi ile ortaya çıkan siber alanı düzenleyen normlar yaygınlık kazanmadığından uluslararası sistemi tehdit edebilecek potansiyel çatışma alanıdır. Öncelikle mevcut normlar çerçevesinde yeni normların oluşmasına katkıda bulunacak tanımlamaların nasıl yapılabileceği incelenecektir.

³ The White House Office of the Press Secretary, **Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference**, 25.09.2015 (çevrimiçi) <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint>, 25.03.2019

1.2.NORM HİPOTEZİ

Normlar, davranış için bir reçete veya yasak niteliğinde olan doğru ve yanlış standartlarıdır. Normlar, “aktör beklentilerinin belirli bir alanda bir araya geldiği ilkeler, normlar, kurallar ve karar alma prosedürleri olan düzenlerin bir bileşeni olarak kabul edilir. ” ve böylece bazı oyuncu davranışlarını kısıtlar.⁴ Başka bir deyişle, bağlayıcı olmayan normlar, paylaşılan beklentiler veya uygunluk standartlarıdır ve çeşitli düzeylerde var olabilir ve farklı aktörler için de geçerli olabilir. En temel normlar, bireylerin davranışlarına uygulandıkları topluluk düzeyinde var olur. Örneğin, cinsel ilişkiye ilişkin toplum normlarının, sadece cinsel ilişkinin yalnızca evli çiftler arasında uygun olması beklentisi gibi, normların var olduğu toplumdaki bireyler üzerinde sınırlayıcı bir etkisi vardır. Bir topluluk normu evlilik öncesi cinsel ilişki yasağı tüm bireyler tarafından desteklenmeyebilir, ancak varlığı herkesin davranışını etkiler ve cesaret kırıcıdır veya norm tarafından teşvik edilen davranışlarda bulunma ile ilgili riskleri ve faydaları artırır. Bir topluluk, belirli bir dini veya etnik grup gibi bölgesel bir nüfusun küçük bir alt grubu olabilir veya tüm bölgesel nüfustan oluşabilir. Topluluk seviyesine ilave olarak, normlar, hükümetler de dâhil organizasyonları, ulusal düzeyle birlikte uluslararası düzeyde de devlet davranışlarını etkileyebilir. Ulusal düzeyde, normların yerel davranış üzerinde yapısal bir etkisi olabilir.⁵

Ulusal seviyenin ötesinde, bu bağlayıcı olmayan ortak beklentiler, bir dereceye kadar, uluslararası aktörlerin davranışlarını sınırlandırabilir ve düzenleyebilir ve bu anlamda, uluslararası sistem üzerinde bir bütün olarak yapısal bir etkiye sahip olabilir. Genellikle uluslararası normlar ulusal normlardan ortaya çıkmaktadır. Ronald Jepperson, Alexander Wendt ve Peter Katzenstein “sosyolojik kurumsallaşma” dedikleri şeyle uluslararası normların gelişimini incelemişleridir.⁶ Bu, incelemeye göre küresel bir siyasi kültürün parçası olan normlar, ulusal egemenlik, uluslararası hukuk ve diplomasi gibi konulardaki görüşlere şekil vererek ulusal güvenlik ortamımızı, etkilemektedir. Sürekli değişen normların bu dinamiği devletlerin

⁴ Brown, Gary, and Keira Poellet, "The Customary International Law of Cyberspace." **Strategic Studies Quarterly** 6, No. 3 , 2012, s. 126-145.

⁵ Mervyn Frost, **Ethics in International Relations: A Constitutive Theory**, (Cambridge: Cambridge University Press, 1996), s. 58.

⁶ Katzenstein, Wendt, and Jepperson, **a.g.e.**, s.33– 75.

karakterini ve davranışını etkilemektedir. Örneğin, nükleer silahlarla ilgili normların devlet davranışları üzerinde belirgin bir etkisi olmuştur. Nükleer çağ ilerledikçe, devletlerin nükleer silah edinme veya kullanma konusunda daha isteksiz olmasını sağlayan kısıtlayıcı bir norm gelişmiştir. Nobel Ödülü Thomas Schelling, nükleer silah kullanımına karşı normların bu hızla ortaya çıkmasının, ABD Dışişleri Bakanı John Foster Dulles'in nükleer silah kullanımının tabu olmaktan çıkarılması gerektiğinden bahsetmesinin çok etkili olduğunu belirtmiştir.⁷ Nükleer silahların kullanılmasını kısıtlayıcı norm o kadar güçlüydü ki Kore Savaşı'nda ve Vietnam'da ABD, Afganistan'da Sovyetler Birliği ve 1973 Savaşında İsrail nükleer silaha sahip olmasına rağmen nükleer silah kullanmaktan kaçınmıştır.

Hem realistler hem de inşacılar, soyut normatif faktörlerin uluslararası ilişkilerde rolünün savunuculuğunu yaparken, normların karşılaştırmalı açıklayıcı gücünü belirleme konusunda güçlük çekerken, nükleer silahlara ilişkin örnek normların bir etkisinin olduğunu göstermektedir. Bu nükleer norma benzeyen uluslararası normlar, biyolojik ve kimyasal silahlar ve stratejik bombalama gibi diğer konvansiyonel silah biçimlerinde de ortaya çıkmıştır.

Normları çeşitli seviyelerde (topluluk, ulusal ve uluslararası) uygulanacak şekilde kategorize etmenin yanı sıra, normlar genellikle iki geniş kategoriye ayrılabilir: kurucu ve düzenleyici normlar. Kurucu normlar yeni aktörler veya eylem kategorileri yaratır ve özel bir görev veya izin oluşturmazlar. Kurucu normların aksine, düzenleyici normlar davranışı düzenler ve sınırlar ve gerçekte bir miktar açıklayıcı nitelikleri vardır.⁸ Kurucu norma örnek olarak, kadın ve erkek arasında özel bir bağ kuran evlilik kurumudur. Düzenleyici bir norm örneği, nükleer silahların kullanılmasına karşı normdur. Kurucu normlar ayrıca düzenleyici normları da sağlayabilir. Örneğin, evlilik kurumu ortaya çıktıktan sonra belirli koşullar altında evlenme veya belirli koşullarda nişanlanma gibi düzenleyici normlar ortaya çıkmıştır.

⁷ Thomas Schelling, "The Nuclear Taboo," **MIT International Review**(Spring 2007), (çevrimiçi) <http://web.mit.edu/mitir/2007/spring/taboo.pdf>, 27.03.2019

⁸ Finnemore and Sikkink, "International Norm Dynamics," **International Organization**, Vol. 52, No. 4, (Autumn, 1998), s.891.

1.3.NORM EVRİM TEORİSİ

Uluslararası düzenleyici normların ortaya çıkışını ve gelişimini tartışan geniş kapsamlı ve disiplinler arası bir literatür bulunmaktadır. Normlar, davranışsal ve mikro ekonomik araştırmalara bağlı olarak, normların somut rolüne destek veren, artan sıklıkta uluslararası faaliyeti anlamak için bir mercekle olarak kullanılmıştır. Bu norm evrim teorisi, büyük ölçüde normların ortaya çıkması ve gelişmesine odaklanır ve devlet çıkarları ve maddi faktörler gibi diğer değişkenlere kıyasla göreceli etkileri çok fazla değildir. Ann Florini, uluslararası normların zaman içinde nasıl değiştiğini açıklamak için doğal seçime dayalı evrimsel bir analogi ortaya koymuştur.⁹

Darwin'in ortaya koyduğu doğal seleksiyon, biyolojik özelliklerin bir popülasyonda ortaya çıktığı veya yok olduğu aşamalı bir süreçtir. Normlar da büyüyebilir veya yok olabilir. Örneğin, stratejik bombalamaya karşı başlangıçta güçlü olan norm II. Dünya Savaşı sırasında devletlerin savaş sırasında karşılık vermek için artan çaresizliği, stratejik bombalamayı askeri açıdan daha etkili hale getiren gelişmiş ataletsel yön bulma (navigasyon) gibi temel teknolojik değişim nedeniyle aşınmıştır.¹⁰

Normlara evrimsel yaklaşım, normların ortaya çıkması teorisine ve belirli normların neden değiştiğini açıklamaya yardım edecek evrimsel bir yaklaşımdır. Genler kalıtım yoluyla taşınmakta; normlar ise bir devletten diğerine yatay üreme şeklinde veya bir devlet içinde dikey üreme şeklinde taşınmaktadır. Dikey norm üretmesi, tek bir devlette liderler aracılığıyla bir normun devamı anlamına gelir ve bu şekilde üretilen normlar nadiren değişir. Buna karşılık, yatay norm üretmesi, birden fazla devlette yayılmalıdır. Silah teknolojisini ve savaşları düzenleyen normlar göz önüne alındığında bu tür normların devletlerarası çatışmaları etkilemek için birden fazla devlete yayılması gerektiği için yatay norm üretmesidir.¹¹

Genel olarak, norm evrimi teorisi normların potansiyel yaşam döngüsünde üç ana aşamaya ayırır: (i) normların ortaya çıkışı, (ii) norm zincirinin oluşması ve (iii) normun

⁹ Ann Florini, "The Evolution of International Norms," **International Studies Quarterly** 40, No:3, Eylül 1996, s. 363– 389.

¹⁰ Jeffrey W. Legro, "Military Culture and Inadvertent Escalation in World War II", **International Security** 18, No. 4 (Spring 1994), s.108-142.

¹¹ Florini, a.g.e., 367-68

içselleştirilmesi.¹² Bu yaşam döngüsü aşamaları, norm evriminin tüm yelpazesini kapsamaktadır. Yeni bir normun ortaya çıkması, dünya genelinde neredeyse tamamen benimsenmesi ve kodlanması ile olmaktadır. Bununla birlikte, bir norm, her zaman üç safha boyunca hareket etmez ve herhangi bir aşamada nihai gelişimine ulaşabilir ve hatta gerileyebilir ve dağılabilir.

1.3.1.Birinci Safha Normun Ortaya Çıkışı

Genler gibi normlar da yarış içindedir, yani diğer normlarla rekabet içindedirler ve bunun sonucunda da normun yaygınlığı zamanla değişir. Normlar farklı çoğalma avantaj seviyelerine sahiptir ve farklı bir şekilde aktarılma olasılığı vardır. Normların ortaya çıkışı, başlangıçta yeni bir normun genellikle zayıf bir şekilde ortaya çıktığı aşamadır. Norm evrim teorisi biyolojik evrim teorisinden esinlenerek yeni bir norm ya da mevcut bir normun yerini almak için ortaya çıkan bir norm için gerekli olan bazı özel koşulları tanımlamaktadır. Örneğin, hafif makineli tüfekler, tüfekler ve otomatik silahlar gibi küçük silahların ve hafif silahların yasadışı olarak yayılmasını sınırlama amacı taşıyan norm henüz oluşmamıştır ve ortaya çıkabilmesi için aktif olarak desteklenmesi gerekmektedir. Bu aşamada normun başarısı için gerekli olan ilk şart, mevcut norm havuzunda normun bilinirlik kazanacak kadar belirgin olup olmadığıdır.¹³

Normların ortaya çıkması için, genellikle norm girişimcisi olarak adlandırılan ve öne çıkan belirli bir aktörün normu desteklemesi ve teşvik etmesi durumunda meydana gelmektedir. Norm girişimcileri, belirli bir normun ajanları ve savunucuları olarak ortaya çıkarlar ve örgütsel platformları mevcut normları değiştirmeye ve yeni normu teşvik etmek için bir mekanizma olarak kullanırlar. Bu bireysel norm girişimcileri genellikle fedakarlık, empati veya ideolojik bağlılık gibi faktörler tarafından motive edilirler ve temel olarak normlarını teşvik etmek için ikna etmeyi bir mekanizma olarak kullanmalarına rağmen tartışmalı normatif ortamda kendi normlarını savunmak için sivil itaatsizlik gibi bozucu davranışlarda bulunabilirler.¹⁴

¹² Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change”, **International Organization** 52 (4), s. 887–917.

¹³ Denise Garcia, **Small Arms and Security New Emerging International Norms**, Routledge; First Edition (November 1, 2006), s.374

¹⁴ Finnemore and Sikkink, **a.g.e.**, s.898– 917.

Norm girişimciler ya teşvik ettikleri yeni normlara dikkat çekmekte ya da konunun yeniden yorumlanması veya çerçevelenmesi yoluyla bunu yaratmaktadırlar.

Örnek olarak, antipersonel kara mayınlarına karşı ortaya çıkan normu oluşturma çabaları için İnsan Hakları Gözlemcisi, Uluslararası Engelliler, İnsan Hakları Doktorları, Mediko Enternasyonal, Mayınlar Danışma Grubu ve Vietnam Gazileri Amerikan Müessesesi gibi kuruluşların oynadığı kritik rol nedeniyle örgütsel platformların önemi ortaya çıkmıştır. Bu norm girişimcileri ve örgütsel platformlar sayesinde, normların ortaya çıkması büyük ölçüde, bazı devletlerin (norm liderleri olarak kabul edilir) normlara cevap vermesi ve benimsemesiyle oluşur.¹⁵ Normların öne çıkması ve girişimcilerin ve örgütsel platformların varlığına ek olarak, norm evrimi teorisi, çeşitli ilave faktörlerin yaşam döngüsünün ortaya çıkma aşamasında bir normun büyümesini ve gelişimini körükleyebileceğini veya engelleyebileceğini göstermektedir. Bunlar, örneğin ikna etme ve çerçeveleme gibi, bazı aktörler tarafından kullanılan özel mekanizmaları, belirli devletlerle veya bütün uluslararası toplumla ilişkili çevresel faktörleri kapsayan ve ortaya çıkan normla ilgili bazı faktörleri içermektedir. Norm liderleri genellikle iç politik nedenlerden ötürü normlara cevap veriyor ve bunları kabul ediyorlar. Örneğin, iç politik kaygılar, insan haklarıyla ilgili normların düzenlenmesinin arkasındaki itici faktördür.¹⁶ Devletlerin uluslararası statüleri konusunda güvensiz olmaları ve uluslararası meşruluk arayışları ortaya çıkan normları benimseme olasılığını daha fazla artırmaktadır. Sonunda, yeterli devlet yeni normu benimser ve bir dönülmez bir noktaya ulaşılır. Bu dönülmez noktanın kanıtı, bu kurumsallaşma dönülmez noktaya ulaşıncaya ve bir norm zinciri meydana gelinceye kadar tamamen oluşmasa da normun belirli uluslararası kurallar ve organizasyonlarda kurumsallaşmaya başlamasıyla görülebilir.

1.3.2. İkinci Safha Norm Zincirinin Oluşması

Bir evrilme noktasına ulaşıldığında, norm yaşam döngüsündeki ikinci aşama olan norm zinciri başlar. Bir normun uluslararası kabulü önemli ölçüde hızlandığında ve devletlerin normu savunan yerel bir koalisyonun varlığına bakılmaksızın,

¹⁵ Ann Florini, *a.g.e.*, s. 363– 389.

¹⁶ Andrew Moravcsik, “The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe”, *International Organization* 54(2), s.217-252.

uluslararası baskılara cevap olarak normu benimsediğinde bir norm zinciri meydana gelmektedir. Ancak bir evrilme noktasına ne zaman ulaşılacağını veya kesin olarak bu kritik eşiği aşmak için kaç tane devletin bir normu kabul etmesi gerekeceğini kesin bir şekilde belirtmenin bir yolu bulunmadığı konusunda araştırmacılar benzer kanaattedir.

Bununla birlikte, ampirik araştırmalar, uluslararası sistemdeki toplam devlet sayısının en az üçte biri normu benimsemeden genel olarak bir norm evrilme noktasına nadiren ulaşıldığını göstermektedir.¹⁷ Bazı devletler daha “kritik öneme” sahiptir veya normu etkileyen rolleri nedeniyle norm için kritik olarak kabul edilir (örneğin, antipersonel mayın normu için antipersonel kara mayını kullanan veya üreten ülkeler).Finnemore ve Sikkink, evrilme noktasına ulaşıp ve norm zinciri başlayınca uluslararası norm kabulünün çok daha hızlı bir şekilde olacağına işaret etmektedir. Artık norm kabulü büyük ölçüde yerel eylem ve baskının bir işlevi değildir; bunun yerine uluslararası sosyalleşme yoluyla yayılmaktadır. Bu aşamada, daha önce ortaya konan norm kavramının bir uzantısı şeklinde örnek olarak görülen devletler tarafından kabul edilirse normların yayılması ve içselleştirilmesi daha olasıdır. Bu norm zincirinin oluşumu sırasında, devletler bu uluslararası sosyalleşmeye çoğunlukla meşruluk, uyum ve saygınlık gibi çeşitli nedenlerle karşılık vermektedirler.¹⁸

Norm liderleri olan devletler, normların benimsenmesini teşvik etmek için ikili veya çok taraflı diplomatik övgü veya kınama (bazen yaptırımlar gibi maddi baskıları da içermek üzere) yöntemlerini kullanmaktadırlar. Ek olarak, hükümet dışı kuruluşlar ve devlet dışı destek ağları sosyal baskı uygulayabilmektedir. Artan uluslararası dayanışma ve hızlı iletişim kaynakları, norm sosyalleşmesi için artan fırsatlar yaratmıştır. Bazen bu sosyalleşme, belirli bir devletin veya devlet gruplarının çıkarlarını sağlamak için yapılır.

Örneğin, kimyasal silahları kısıtlayan normlar başlangıçta büyük güçlerin çıkarlarını tamamlamak için geliştirilmiştir. Bununla birlikte, zamanla bu devletlerin çıkarlarıyla ilgili hafıza kaybolmakta ve norm bağımsız bir güç olarak kalmaktadır. Bu sosyalleşme süreci boyunca, norm zinciri büyüdükçe ikna ve çerçeveleme önemli bir rol oynamaya devam etmektedir. Kitle imha silahları ile ilgili normlarla, uluslararası

¹⁷ Finnemore and Sikkink, **a.g.e.**, s.901

¹⁸ Finnemore and Sikkink, **A.e.**, s.901, 903,906

olarak belirli silahları konvansiyonel olmayan ve kitle imha silahları olarak sınıflandırmak, kullanımlarını kısıtlayan normların geliştirilmesine katkıda bulunmuştur. Ek olarak, bu norm zincirinin oluşumu aşamasında, bir şok veya büyük uluslararası bir olaya bağlı olarak en uygun zamanlama, bir normun evrilme noktasına itilmesine yardımcı olabilir veya içselleşmesini hızlandırabilir. Bir savaşta kaybeden tarafla veya çöküşe neden olan ekonomik krizle ilişkili normlar inandırıcılığını kaybedebilir ve alternatif normlar aranabilir.

1.3.3.Üçüncü Safha Normun İçselleştirilmesi

Norm yaşam döngüsündeki üçüncü ve son aşama normun içselleştirmesidir. Bu aşama, normu derin bir şekilde kodlama ve evrensel veya evrensele yakın bir bağlılık kazanma çabasıdır. Bu aşamada norm, o kadar derin ve geniş bir şekilde içselleştirilir ki sorgulamadan kabul edilen statüye ulaşır. Bilim adamları, bunun aslında normu ayırt etmeyi zorlaştırabileceğini, çünkü onu çevreleyen tüm itilaf ve tartışmaların çözülebileceğini belirtmişlerdir. Bununla birlikte, içselleştirmenin başarılması, her devlet tarafından normun yüzde yüz içselleştirildiği anlamına gelmez ve içselleştirme derecesi devletler ve bölgeler arasında değişebilir. Ayrıca içselleştirme zorunlu olarak, normun bağlayıcı bir kanun olduğu ve evrensel uluslararası anlaşmalara ya da mutabakatlara yakın olduğu anlamına gelmez ancak bu gerçekleşebilir. Daha önceki aşamalarda olduğu gibi, çeşitli iç ve dış faktörler bu aşamada bir norm hareketine katkıda bulunabilir. Örneğin, Andrew Moravcsik, insan haklarına ilişkin normların benimsenmesi ve ortaya çıkmasına bakar ve insan haklarıyla ilgili normların derinden içselleştirilmesinin hızlandırıcısı olarak iç politik kaygıları işaret etmektedir.¹⁹

Özellikle, insan hakları ile ilgili normlar, demokratik olmayan güçlerin daha sonra güç kazanabileceği ve gelecekteki bu potansiyel yerli aktörleri sınırlamak için normları kilitlemek isteğinden kaygılanan gelişmekte olan demokrasiler tarafından kabul edilmiştir. Bununla birlikte, genel olarak konuşursak, yerel faktörler bu aşamada önceki aşamalarda olduğundan daha az bir rol oynamaktadır. Dış faktörler, normun kimliklerin şekillendirilmesindeki rolünü içerebilir. Örneğin, nükleer norm, hala

¹⁹ Moravcsik, a.g.e., s.217-252

tamamen içselleşmemiş olsa da, medeni bir milleti neyin oluşturduğu fikri ile ilişkilendirilmiştir.²⁰

1.4.SİBER ALAN VE SİBER AKTÖRLER

Uluslararası hukuk ve iç hukuka göre bir devletin ülkesi kara, deniz ve hava bölümlerinden oluşmaktadır.²¹ Uzak çalışmalarının gelişmesiyle birlikte hava bölümü, hava ve uzak bölümü olarak ikiye bölünmüştür. Siber alan; diğer alanlardan pek çok açıdan farklı olmasına rağmen devletin ülkesinin beşinci bölümü olarak kabul edilmektedir. Bu alanın en önemli farkı tamamen insan yapımıdır. Suniliği, siber alanı ve onun siyasetle olan ilişkisini tanımlamakta soruna neden olmaktadır. Teknik düzeyde, siber alan, bir ağ, sosyal medya, iletişim kanalı ve bilgi deposu gibi yeni teknolojik gelişmeler için bir platformdur. ABD 2017 Ulusal Güvenlik Strateji Belgesinde; hava, kara, deniz ve uzak alanlarına siber alanı da dâhil etmiştir.²²

Başta ABD, Rusya, Çin olmak üzere Türkiye de dâhil birçok ülkenin siber komutanlıklar kurmaları, siber alanın askeri bir alan olarak yükselişini işaret etmektedir. Bu nedenle de, kara, deniz, hava ve uzak egemenlik alanlarına fiilen siber alanın eklendiğini kabul etmek gerekir. Bu durum, savaş gücü, saldırı, savunma, caydırıcılık gibi eski kavramların küçük bir değişiklikle siber alana uygulanabileceğine dair bir inançta yol açsa da bu mümkün değildir. Bunun yerine siber alan kendi terimleri ile anlaşılmalıdır.²³

Siber alan mimarisi açık bir ortam olarak tasarlandığından aktörler faaliyetlerini kolayca gizleme imkânına sahiptir. Bu nedenle siber alan içinde yapılan eylemlerin faillerini tespit etmek oldukça zor olmaktadır.

²⁰ Finnemore and Sikkink, **a.g.e.**, s.893

²¹ Hüseyin Pazarcı, **Uluslararası Hukuk**, Gözden Geçirilmiş 3.Bası, Turhan Kitabevi, Ankara 2014, s.143

²² **National Security Strategy of the United States of America 2017**, (Çevrimiçi) <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>, s.8, 09.09.2018

²³ Martin C. Libicki, **Cyber Deterrence and Cyber War**, The Rand Corporation, Santa Monica 2009, s.15

1.4.1.Siber Alan Tanımı:

ABD Savunma Bakanlığı Askeri Terimler Sözlüğünde Siber alanı “İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyiciler de dâhil olmak üzere, bilgi teknolojisi altyapıları ve yerleşik verilerin birbirine bağlı ağından oluşan bilgi ortamındaki küresel bir etki alanı” olarak tarif etmektedir.²⁴

Rusya siber alan yerine “bilgi alanı” terimini kullanmaktadır. “Bilgi alanı” terimi, dijital alanda ortaya çıkan ağ mimarisi ve süreçlerine odaklanan Amerikan teriminden daha geniş ve daha kapsamlıdır. Rusya bilgi alanını, “bilginin oluşumu, yaratılması, dönüştürülmesi, aktarılması, kullanılması ve saklanması ile bağlantılı olan ve bireysel ve toplumsal bilinç, bilgi altyapısı ve bilginin kendisi üzerinde bir etkiye sahip olan faaliyet alanı” olarak tanımlamaktadır.²⁵

Benzer şekilde, Çin bilgi alanını bütünsel olarak görmektedir. Çin'in tanımı şu şekildedir: ²⁶ “Bilgi alanının asıl işlevi, insanların veriyi edinip işlemesidir. İnsanlarla iletişim kurmak için yeni bir yer ve faaliyetler, tüm dünyadaki iletişim ağlarının, veri tabanlarının ve bilginin bütünleşmesidir. Üç boyutlu bir alan olan etkileşim farklı etnik ve ırksal özelliklerine sahip, birbirine bağlı bir “manzara” oluşturmaktadır. ”

Diğer bir tanım ise; siber alan sanal bilgisayar dünyasına ve daha özel olarak, çevrimiçi iletişimi kolaylaştırmak ve küresel bir bilgisayar ağı oluşturmak için kullanılan bir elektronik ortamdır. İletişim ve veri alışverişi etkinliklerine yardımcı olmak için TCP / IP protokolü (*Bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır*)kullanan dünya çapında birçok bilgisayar ağından oluşan büyük bir bilgisayar ağıdır. Siber Alanın temel özelliği, çok çeşitli katılımcılar için etkileşimli ve sanal bir ortamdır.²⁷

²⁴ US Department of Defense Dictionary of Military and Associated Terms, November 2010, (Çevrimiçi) http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2810-13%29.pdf, 06.09.2018

²⁵ Keir Giles and William Hagestad, **Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English**, (Çevrimiçi) https://ccdc.org/publications/2013proceedings/d3r1s1_giles.pdf, 06.09.2018

²⁶ Emilio Iasiello, “Are Cyber Weapons Effective Military Tools?”, **Military and Strategic Affairs** 7, No. 1, Mart 2015, s.27–28

²⁷ ÇÖLKESEN Rıfat, Bülent ÖRENCİK, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri**, Papatya Yayıncılık, Haziran, 1999, s.345-358

Türkiye 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde; siber uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam olarak tanımlanmıştır.²⁸

Farklılıklarına rağmen bütün tanımların ortak yanı insan yapımı olan siber alanın ağa bağlı niteliklerini ifade etmektir. Ancak Stuxnet saldırısı göstermiştir ki siber alanı sadece ağa bağlı niteliklerle tanımlamak yetersiz kalacaktır. Bu nedenle ağa bağlı olmayan ve bilgiyi işleyen sistemlerde siber alan tanımı içinde değerlendirilmelidir. Bilgilerin hızlı ve güvenilir bir şekilde taşınması için tasarlanan internet ağı, kullanıcıların bu ağı birbirlerine saldırmak için kullanacakları öngörülmemiştir. İnternet ağı ve bilgi teknolojileri konusunda daha fazla bilgi ve imkâna sahip olan aktörler, internetin güvenlik açıklarına karşı benzersiz araçlar ve istismar yöntemleri kullanarak saldırı ve eylemlerinde görünmezlik sağlamaktadırlar.

1.4.2. Siber Aktörler:

1.4.2.1.Devlet Dışı Aktörler:

Sınırsız ve hatta iç içe geçmiş ağlar, bilgisayar korsanları(hackerler), organize siber suçlular, bilgisayar eylemcileri (hacktivistler), siber teröristler ve aynı zamanda özel sektör, Sivil Toplum Kuruluşları vb. bir dizi devlet dışı aktörün ortaya çıkmasına neden olmuştur. Her ülkede farklı tanımları ve yasal çerçeveleri olduğu için bu aktörler arasında net bir ayırım yapmak çok olanaklı olmasa da genel kabul görmüş ayırıma göre bunlardan kısaca bahsedilecektir.

1.4.2.1.1.Bilgisayar Korsanı (Hacker):

Bilgisayar korsanı, teknik bir problemin üstesinden gelmek için bilgisayar, ağ iletişimi veya diğer becerileri kullanan bir kişidir. Bilgisayar korsanı terimi teknik beceriye sahip olan herkes için kullanılmakla birlikte genellikle suç işlemek için

²⁸ T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **2016-2019 Ulusal Siber Güvenlik Stratejisi**, (Çevrimiçi) <http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf>, 12.09.2018

sistemlere veya ağlara yetkisiz erişim elde etmek için yeteneklerini kullanan kişiler kastedilmektedir.²⁹

Genellikle bir bilgisayara veya ağa izinsiz giriş yapan kişileri ifade eder. Bilgisayar korsanı, sistemin orijinal amacından farklı bir hedefi gerçekleştirmek için sistem veya güvenlik özelliklerini değiştirebilir. Beyaz şapka korsanı, güvenliğini sınamak ve test etmek için korunan sistemlere ve ağlara giren bir bilgisayar güvenlik uzmanıdır. Beyaz şapka korsanları, kötü niyetli bilgisayar korsanlarının (siyah şapka korsanları olarak bilinir) bunları tespit edip kullanabilmeleri için güvenlik açıklarını kaldırarak becerilerini kullanırlar. Siyah şapka korsanı, bilgisayar güvenlik açıklarını bulmaya çalışan ve kişisel mali kazanç veya diğer kötü niyetli nedenlerden dolayı bunları kullanan bir kişidir. Bu, siyah şapka korsanlarının istismar edebileceği güvenlik kusurlarını bulmak için bilgisayar korsanlarının kullandığı güvenlik uzmanları olan beyaz şapka korsanlarından farklıdır.³⁰

Gri şapka korsanı, siyah şapka korsanlarına atfedilen kötü niyet olmaksızın etik standartları veya ilkeleri ihlal edebilecek kişidir. Gri şapka bilgisayar korsanları, güvenli sistemleri koruyanlar adına çalışan beyaz şapka bilgisayar korsanları ile sistemdeki güvenlik açıklarından yararlanmak için kötü niyetli davranan siyah şapka bilgisayar korsanları arasındaki orta yolu temsil etmektedir.

1.4.2.1.2. Organize Siber Suçlular

Siber suçlu, siber suçları işleyen, bilgisayarı bir araç ya da hedef olarak ya da her ikisini de kullanan kişidir. Siber suçlular bilgisayarları üç şekilde kullanırlar; bilgisayarı hedef olarak seçen suçlular, virüsleri yaymak, veri hırsızlığı, kimlik hırsızlığı, vb. kötü amaçlı etkinlikler gerçekleştirmek için diğer kişilerin bilgisayarlarına saldırırlar. Bilgisayarı silah olarak kullanan suçlular, isteğiniz olmadan size gönderilen reklam içerikli mailler, dolandırıcılık, yasa dışı kumar vb.

²⁹ Merriam-Webster Dictionary, (çevrimiçi) <https://www.merriam-webster.com/dictionary/hacker>, 31.07.2018

³⁰ Andress Jason , Winterfeld Steve, **Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners**, 2011, s.196

"geleneksel suç" işlemek için kullanırlar. Bilgisayarı aksesuar olarak kullanan suçlular; çalıntı veya yasa dışı verileri kaydetmek için bilgisayarı kullanırlar.³¹

Siber suç şebekesi tipik olarak iyi tanımlanmış rollere ve üzerinde anlaşmaya varılmış bir komuta zincirine sahip net bir organizasyon yapısına bağlı kalır. En üstte, her bir siber saldırıyı planlamaktan ve altında bulunan her bir kişinin rollerini anladığından ve komuta zincirinde yatay ve dikey olarak etkili bir şekilde iletişim kurabilen örgütsel bir lider bulunmaktadır.

1.4.2.1.3.Bilgisayar Eylemcileri (Hacktivists)

Bilgisayar Eylemcileri, bir sosyal veya politik mesajı iletmek için bir web sitesini veya bilgisayar ağını istismar etmektedirler. Bilgisayar eylemcileri, özel bilgileri çalma ya da başka bir zarara neden olma niyetinde olan bilgisayar korsanının aksine, politik ya da sosyal amaçları vurgulamak için benzer şekilde yıkıcı faaliyetlerde bulunurlar. Bilgisayar eylemcisi internet aracılığı ile sivil itaatsizlik eylemini hayata geçirme stratejisini uygular. Bilgisayar eylemleri arasında web sitesi bozma, hizmet reddi saldırıları (DDoS), yönlendirmeler, web sitesi parodileri, bilgi hırsızlığı, sanal sabotaj ve sanal oturumlar sayılabilir.³²

1.4.2.1.4.Siber Savaşçılar (Cyber Warriors)

Siber savaşçı, ister kişisel nedenlerden ister vatansever ya da dini inançtan olsun, siber savaş ile uğraşan bir kişidir. Siber savaş, bilgisayar ve bilgi sistemlerini savunmak ya da onlara saldırmak için kullanılabilir. Siber savaşçılar, rollerine bağlı olarak farklı biçimlerde olsalar da, ancak hepsi bilgi güvenliği ile bir şekilde ilgilenirler. Siber savaşçılar bilgi teknolojisini kullanarak savaşmayı sürdürürler. Bilgisayar ya da bilgi sistemlerine korsanlık ya da diğer stratejiler yoluyla saldırabilir ya da diğer korsanlara karşı bilgisayar ve bilgi sistemlerini savunabilirler.³³

³¹ Sarah Gordon, Richard Ford, "On the Definition and Classification of Cybercrime", **J. Computer Virology**, No:1, 2006, s.13;

³² Rukondo Solomon, "Electronic protests: Hacktivism as a form of protest in Uganda", **Computer Law & Security Review Volume 33**, 2017, s. 718-728

³³ Andress, Winterfeld, **a.g.e.**, s.207-220

1.4.2.1.5.Endüstri

Günümüzde Bilgi ve İletişim Teknolojileri sektörü, dünya ekonomisinin, politikasının ve sosyal hayatın birçok alanında stratejik olarak önemli bir rol oynamaktadır. Aslında, özel sektör küresel iletişim altyapısının çoğuna sahiptir, ancak hala devlete ait veya devlet kontrolünde ulusal internet servis sağlayıcıları bulunmaktadır. Bu altyapıya ilişkin tüm güvenlik ürünlerinin çoğunluğu, Bilgi ve İletişim Teknolojileri endüstrileri tarafından geliştirilmekte, üretilmekte ve sağlanmaktadır. Bu sektördeki önemli oyuncular; dünya çapında bilgisayar işletim sistemi sağlayıcısı olan Microsoft, ağ cihazlarının en önemli tedarikçisi Cisco ve kötü amaçlı yazılım koruma ürünleri ve diğerlerini sağlayan The Shadow Server Foundation (Gölge Sunucusu)'dur.

1.4.2.2.Siber Alanda Devlet Aktörleri

Devletler siber alanın önemli aktörleridir. Devlet adına hareket eden polis ve jandarma gibi kolluk kuvvetleri, istihbarat servisleri ve silahlı kuvvetler siber alanda faaliyet gösteren devlet aktörleridir.

1.4.2.2.1.Kolluk Kuvvetleri

Bir devletin öncelikli amaçlarından biri, hukukun üstünlüğünü sağlayarak iç güvenliği sağlamaktır. Günümüzde internet kullanımının geldiği seviye dikkate alındığında devletler için siber alanda hukukun üstünlüğünün sağlanması, iç güvenliğin sağlanmasında önemli hale gelmiştir. Birçok devlet, iletişimi kontrol altına almak için, ulusal pazarında faaliyet gösteren endüstri üzerinde özel yazılım veya düzenleyici kuvvet kullanır ve şifreli ve şifresiz verileri toplar. Bu tür özel yazılımların geliştirilmesi, kolluk kuvvetlerinde yaygın olarak bulunmayan bilgi ve becerileri gerektirmektedir. Kolluk güçleri siber alanda suç olarak belirlenmiş eylemleri tespit ederek failleri yakalayıp haklarında adli işlem başlatılmasını sağlarlar. Avrupa Siber Suçlar Sözleşmesi'ne göre siber suçlar; bilgisayar veri ve sistemlerinin mevcudiyeti, bütünlüğü ve gizliliğine karşı suçlar, bilgisayarla ilişkili suçlar, çocuk pornografisi gibi içerikle ilgili suçlar ve son olarak telif hakları ile ilgili suçlardır.³⁴

³⁴ **Convention of Cybercrime**, (çevrimiçi), <https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/8601684>, 09.09.2018

1.4.2.2.2.İstihbarat Servisleri

İstihbarat kuruluşlarının somut kabiliyetleri hakkında kamuoyunda çok sınırlı bilgi mevcuttur. Ancak ABD Ulusal Güvenlik ajanı Edward Snowden skandalı³⁵, iyi bir bütçe ve yeterli teknolojik güce sahip devletlerin ABD veya dışında elektronik ortamda depolanan her türlü veriye erişebileceklerini ve bu verilerin çoğunu nasıl çözdüklerini göstermektedir. Bir silahlı çatışma sırasında düşmana karşı gerçekleştirilen siber casusluk ve diğer bilgi toplama biçimleri, silahlı çatışma hukukunu ihlal etmemektedir. Siber casusluk, gizli olarak bilgi toplamak için siber yetenekleri kullanan bir eylemdir. Bazı siber casusluk eylemleri sadece bilgi toplama faaliyetinden daha fazlasını içerir ve bilgisayar sistemlerine zarar verebilir. Bu nedenle, asıl amacı siber casusluk olan eylemler bazen siber saldırıya yol açabilir, bu durumda siber saldırı kuralları uygulanır.³⁶

1.4.2.2.3.Silahlı Kuvvetler

Teknolojideki yaşanan olağanüstü gelişmeler neticesinde, bugünün silahlı kuvvetleri siber egemenlik alanını siber saldırılardan korumak için çeşitli zorluklarla karşı karşıyadır. Devletler askeri yeteneklerini siber alanda kullanabilmek için çalışmalar yapmaktadır. Bugünkü devlet davranışlarıyla konvansiyonel ve nükleer silahlanma yarışı sırasındaki devlet davranışlarını karşılaştıran bilim insanları siber alanda yeni silahlanma yarışının başlayacağına işaret etmektedir. Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü'nün 2013 sonuçlarına göre; 2011 yılında 30'dan fazla devlet askeri plan ve organizasyonlarında siber savaşa yer vermiştir. Bunlar arasında ABD, Çin ve Rusya'nın gelişmiş siber savaş yetenekleri bulunmaktadır. Birleşik Krallık 2016-2021 Ulusal Siber Güvenlik Stratejisinde “Saldırgan siber yeteneklerimize yatırım yapmaya devam edeceğiz, zira tespit etme, izleme ve misilleme yeteneği en iyi caydırıcılık imkânını sağlamaktadır.” Şeklindeki ifadeyle siber yeteneklerin geliştirmeye devam edileceği vurgulanmaktadır.³⁷

³⁵ Matthew Crosston and Frank Valli, “An Intelligence Civil War: “HUMINT” vs. “TECHINT””, Cyber, Intelligence, and Security, Volume1, January 2017, s.68-73

³⁶ Schmitt Micheal, **The Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge University Press, New York, 2013, s.36

³⁷ United Kingdom, **National Cyber Security Strategy 2016 to 2021**, (çevrimiçi) <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>, 09.09.2018

Son dönemde gelişmekte olan otonom silah sistemleri hakkındaki tartışmalar geleneksel silah sistemlerine odaklanmasına rağmen, otonomiye askeri ilgi sadece geleneksel sistemlerle sınırlı değildir. Otonomi siber operasyonlar için de önemlidir. Hem saldırı hem de savunma amaçlı siber operasyonlarda; çok yüksek karşılık verme hızı, öngörü kabiliyeti, karar desteği ve düşmanın zayıflıklarını tespit ve istismar etme kabiliyeti bulunan otonom sistemler cazip hale gelmektedir. Siber operasyonlarda artan otonomluk/özerklik için verilecek örnek “Azaltılmış veya hiç insan etkileşimi olmadan başarılı bir bilgisayar saldırısı oluşturma yeteneği” sunan (Automatic Exploit Generation) Otomatik İstismar Üretimi olarak bilinen tekniktir.³⁸

1.4.3. Devlet ve Siber Alan

1.4.3.1.Egemenlik

Bir devlet, siber altyapı ve kendi topraklarındaki faaliyetler üzerinde denetim yapabilir. Bu kural, hiçbir devletin siber alan üzerinde egemenlik iddia edememesine rağmen, devletlerin kendi topraklarında bulunan herhangi bir siber altyapı ve bu siber altyapı ile ilgili faaliyetler üzerinde egemen imtiyazlar kullanabileceğini vurgulamaktadır.³⁹

Devletin siber altyapı üzerinde egemenlik hakkını kullanabilmesinin iki sonucu bulunmaktadır. Birincisi siber altyapının devletin koyacağı kurallara ve denetime tabi olmasıdır. İkincisi devletin ülkesi üzerindeki egemenlik hakkı siber altyapının korunmasını sağlar. Bir devletin, başka bir devletin ülkesi sınırlarında bulunan siber altyapıya yönelik siber eylemi o devletin egemenlik hakkını ihlal eder. Ancak herhangi fiziksel bir hasara neden olmayan kötü amaçlı yazılımların (malware) yerleştirilmesinin, egemenliğin ihlali anlamına gelip gelmediğine dair Talin El Kitabını hazırlayan uzmanlar arasında bir fikir birliği yoktur. Bu tür bir siber operasyon hükümeti zorlamak amacıyla yapılmışsa, yasaklı bir “müdahale” veya yasaklanmış bir “kuvvet kullanımı” oluşturabilir.

Siber bağlamda, egemenlik ilkesi, diğerlerinin yanı sıra, insan hakları veya uluslararası telekomünikasyon hukuku gibi uygulanabilir uluslararası hukuka halel

³⁸ UNIDIR Resources, **Autonomous Weapon Systems and Cyber Operations**, 2017, s.4-15

³⁹ Schmitt, **a.g.e**, s.25

getirmeksizin, internete erişimi (kısmen veya tamamen) kısıtlama veya korumaya izin vermektedir.

Geleneksel olarak, egemenliğin devletler tarafından üstlenilen veya bir devlete atfedilebilecek eylemlerle ihlal edilebileceği görüşü bulunmaktadır. Ancak, bazı akademisyenler tarafından, devlet dışı aktörler tarafından yürütülen siber operasyonların, bir devletin egemenliğini ihlal edebileceğiyle ilgili henüz olgunlaşmamış bir görüş de bulunmaktadır.⁴⁰

1.4.3.2.Devletin Yargı Yetkisi

Bir devlet, uluslararası yükümlülüklerine halel getirmeksizin, ülkesinde siber faaliyetlerde bulunan kişiler ve siber altyapı üzerinde uluslararası hukuk kurallarına uygun olarak kendi yargı yetkisini kullanabilir.

Devlet ayrıca, kendi yetki alanında kayıtlı ancak internet servis sağlayıcıları gibi yurtdışında faaliyet gösteren özel kuruluşların faaliyetlerini düzenleyebilir. Devletin yargı yetkisi, kendi topraklarında bulunan siber altyapının işleyişini yöneten yasaları belirlemesine imkân verecektir.

Bazı durumlarda siber alanda yargı yetkisini belirlemek oldukça zor olmaktadır. Örneğin, bulut veya grid dağıtılmış sistemler birden çok devletin ulusal sınırlarını kapsayabilir. Örneğin, bir mobil bilgi işlem aygıtına (örneğin bir tablet veya akıllı telefon) sahip bir kişi, bir bulut tabanlı hizmet tarafından işlenmek üzere çeşitli veri tabanı sorguları veya güncellemeleri başlatabilir. Bu sorgulamalar ve güncellemeler gerçekleşirken, kullanıcı başka bir devletin ülkesine gidebilir. Bu işlem sırasında kişinin bulunduğu her devlet, söz konusu kişi ve cihazlar kullanıldığında kendi topraklarında bulunduğu için yargı yetkisine sahiptir.

İki çeşit ülkesel yargı yetkisi vardır. Sübjektif yargılama yetkisi kendi ülkesinde başlayan ancak başka bir ülkede tamamlanan olaya ilişkin yargı yetkisidir. Objektif yargı yetkisi ise eylem kendi toprakları dışında başlatılmış olsa bile, eylemden etkilenen devletin yargı yetkisidir. Örneğin 2007 yılında yurtdışından siber saldırılara

⁴⁰ Schmitt, a.g.e, s.26

maruz kalan Estonya'nın siber saldırıları yapan kişiler üzerinde objektif yargı yetkisi bulunmaktadır.⁴¹

1.4.3.3.Devletin Denetimi

Bir devlet, kendi topraklarında bulunan ya da münhasır hükümet denetimi altındaki siber altyapının, diğer devletleri düşmanca ve yasadışı bir şekilde etkileyecek fiiller için kullanılmasına bilerek izin vermemelidir. Uluslararası Adalet Divanı'nın Korfu Kanalı Yargılamasında belirttiği gibi, başka bir devletin egemenliğine saygı gösterme yükümlülüğü, "topraklarının diğer ülkelerin haklarına aykırı bir biçimde kullanılmasına bilerek izin vermemeyi" kapsamaktadır. Bu kural yasadışı olan ve başka bir devlet üzerinde zararlı etkileri olan siber eylemler de dâhil tüm eylemleri kapsamaktadır. Örneğin ülkesindeki siber altyapıyı başka bir ülkeye saldırı düzenleyen teröristlerin kullanmasına izin veren devlet bu kuralı ihlal etmiş olacaktır.

Bir devletin kendi topraklarındaki siber faaliyetlerin denetlenmesinde gerekli özeni göstermemesi ve bu nedenle söz konusu fiillerden habersiz olması durumunda bu kuralın ihlal edilip edilmediği belirsizdir. Eğer devlet bu kural uyarınca uygun adımlar atmazsa, mağdur-devlet orantılı tepkilere başvurarak uluslararası hukuk ihlaline cevap vermeye yetkili olabilir. Bunlar, uygun durumlarda, karşı önlemler veya kendini savunmada kuvvet kullanımını içerebilir.⁴²

1.4.3.4.Devletin Sorumluluğu

Devlet, kendisine atfedilebilecek ve uluslararası bir yükümlülüğü ihlal eden bir siber operasyon için uluslararası yasal sorumluluk taşımaktadır. Uluslararası hukukun gereği olarak devletler aşağıdaki durumlarda bir eylemin sorumluluğunu üstlenir: (i) Söz konusu eylem, uluslararası hukuka göre devlete atfedilebilir ve (ii) bu eylem devlete sorumluluk yükleyen uluslararası bir yasal yükümlülüğün (Uluslararası teamül veya anlaşma) ihlalini teşkil ediyorsa. İhlal, bir eylem veya ihmalden oluşabilir.

Siber alanda uluslararası bir haksız fiil, diğer şeylerin yanı sıra, Birleşmiş Milletler Sözleşmesi'nin ihlali veya devlete atfedilebilecek silahlı çatışma hukukunun ihlali anlamına gelebilir. Devletin bir organı tarafından siber alanda yürütülen siber

⁴¹ Schmitt, **a.g.e.**, s.27-29

⁴² Schmitt, **A.e.**, s.33-35

casusluk eylemi, uluslararası hukuk kurallarını ihlal etmedikçe uluslararası hukuka tabi değildir.

Uluslararası hukukun teamül kuralı uyarınca, devletlerin kendi topraklarındaki faaliyetlerle başka bir devlete önemli zarar vermeleri yasaktır. Bu tür bir zararın yokluğunda, hasar unsuru içermeyen başka bir kural ihlal edilmedikçe devletin hiçbir sorumluluğu bulunmaz. İstihbarat, silahlı kuvvetler, iç güvenlik, gümrük veya diğer devlet kurumları tarafından üstlenilen herhangi bir siber faaliyet, söz konusu devlete atfedilebilecek uluslararası bir yasal yükümlülüğü ihlal etmesi durumunda, uluslararası hukuka göre devlet sorumluluğu üstlenecektir.

Devlet organı olmasa da, “devlet otoritesini” uygulamak için iç hukuk tarafından özel olarak yetkilendirilen kişi veya kurumların eylemleri devlete atfedilebilir. Ancak bu kişi ve kurumlar devlet otoritesinin unsurlarını kullandığı durumlarda devletin sorumluluğu söz konusu olacaktır.

Bazı durumlarda, devlet dışı aktörlerin davranışı devlete atfedilebilir ve devletin uluslararası yasal sorumluluğunu doğurur. Devlet dışı aktörlerin davranışlarının devletin sorumluluğunu gerektirmesi için bu aktörler devletin kontrolünde veya devletin talimatlarıyla hareket ediyor olmalıdır. Örneğin devletler siber operasyonları yürütmek için özel bir şirket ile sözleşme yapabilir.

Uluslararası Adalet Divanı, askeri operasyonlar bağlamında, devletin bu aktörler üzerinde “etkili kontrol”ü varsa devlet dışı aktörlerin eylemlerinden sorumlu olduğunu kabul etmiştir. Sadece bu tür güçlerin finanse edilmesi ve donatılması yeterli değildir, askeri operasyonların planlanması ve denetlenmesine katılım gereklidir. Bu durum, bireysel olarak kendi inisiyatifleriyle siber operasyonlar yürüten yurttaşların durumundan farklıdır. Devletin sorumluluğunun gündeme gelmesi için devletin özel talimatlar vermesi veya belirli bir operasyonu yönetmesi veya kontrol etmesi gerekmektedir.⁴³

⁴³ International Court of Justice, **Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)**, (Çevrimiçi) <https://www.icj-cij.org/en/case/70>, 12.02.2019

Örneğin A devletinde bulunan bir grubun B devletinde bulunan bilgisayarların botnetini(*üçüncü taraflarca kontrol edilen ve kötü amaçlı yazılım veya spam iletmek veya saldırı başlatmak için kullanılan, güvenliği ihlal edilmiş bilgisayarlar grubudur*) ele geçirdiğini düşünelim. Grup, D devletinden alınan talimatlara dayanarak C devletindeki bilgisayar sistemlerini aşırı yüklemek için botneti kullandığında, eylemde D devletin sorumluluğu vardır.

Bununla birlikte, bir devletin devlet dışı aktörlere katılımı, devlet dışı aktörlerin eylemlerinin devlete atfedilemediği durumlarda bile, uluslararası hukukun ihlali anlamına gelebilir. Örneğin, A devleti, B devletine karşı kendi inisiyatifiyle hareket eden isyancı bir gruba bilgisayar korsanlığı için araç sağlarsa, bu grubun saldırılarını A devletine atfedebilmek için bu araçların varlığı yeterli değildir. Ancak, bu tür yardımlar uluslararası hukukun ihlali anlamına gelebilir.⁴⁴

1.5. SİBER SALDIRI

1.5.1. Birleşmiş Milletler Genel Kurulu'nun 3814 (XXIX) sayılı ve 1974 Tarihli Kararına Göre Saldırı Tanımı

Saldırı: *“Bir devletin diğer bir devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu tanımda belirtildiği üzere, Birleşmiş Milletler Antlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılmasıdır.”*

1.5.2. Siber Saldırının Tanımı:

Siber saldırı, ister taarruz ister savunma maksadıyla yapılsın, kişilerin yaralanmasına/ölmesine veya nesnelerin zarar görmesine/tahrip olmasına neden olması beklenen siber bir işlemdir.⁴⁵

Siber saldırı: bilgisayar sistemlerinin, teknolojiye bağımlı işletmelerin ve ağların kasıtlı bir şekilde istismar edilmesidir. Siber saldırılar, bilgisayar kodunu, mantığını veya verilerini değiştirmek için zararlı kodlar kullanır ve verilerin bozulmasına ve bilgi ve kimlik hırsızlığı gibi siber suçlara yol açabilecek yıkıcı sonuçlara yol açar.⁴⁶

⁴⁴ Schmitt, **a.g.e.**, s.35-39

⁴⁵ Schmitt, **A.e.**, s.91-95

⁴⁶ Andress, Winterfeld, **a.g.e.**, s.3-5

Lin'in tanımına göre siber saldırı; *“düşmanın bilgisayar sistemlerini ve ağlarını veya bu ağlarda bulunan ya da iletilen bilgi ve/veya programlarını bozmak, değiştirmek, yok etmek veya geriletmek amacıyla kısa veya uzun süreli olarak gerçekleştirilen kasıtlı hareket ve operasyonlardır.”*⁴⁷

Türkiye 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde; siber saldırı, *“Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler”* şeklinde tanımlanmıştır.⁴⁸

Siber saldırı, yetkili hükümet organlarının, yasal veya yasa dışı kuruluşların, teröristlerin, şirketler veya şahısların stratejik, operatif ve taktik amaçlarını gerçekleştirmek için siber ortamda uyguladıkları saldırı faaliyetleridir.⁴⁹

Bir devletin başka bir devletin bilgisayarlarına ve ağlarına zarar verme ve devre dışı bırakma veya yok etme eylemidir.⁵⁰

Yukarıdaki tanımlar incelendiğinde; siber saldırı, devlet veya devlet dışı siber aktörlerin muhasımın bilgi ve iletişim teknolojilerine dayalı sistemlerindeki zayıf noktaları istismar ederek ona zarar vermesidir.

Birleşmiş Milletler'in saldırı tanımıyla ile siber saldırı tanımı arasındaki en önemli fark kuvvet kullanma konusundadır. Üstelik tanımda bahsedilen kuvvet silahlı bir kuvvettir. Dolayısıyla Birleşmiş Milletler'in tanımladığı ve yasakladığı saldırı tanımına göre siber saldırı silahlı bir kuvvet kullanılma seviyesine ulaştığında ancak saldırı sayılacaktır. Ayrıca neyin silah olarak kabul edileceği sorusu gündeme gelecek bilgi sistemleri ve bu sistemlerde kullanılan virüs vb. yazılımlar veya programların silah olarak kabul edilebilip edilmeyeceği tartışılacaktır.

1.5.3.Siber Saldırıların Sistemler Üzerinde Yarattığı Etkiler

Saldırı sonucunda ölüm, yaralanma ve maddi zararlar meydana gelirken, siber saldırıların yarattığı etkiler istisnai olarak ölüm, yaralanma ve maddi zarara neden

⁴⁷ Herbert S. Lin, “Offensive Cyber Operations and the Use of Force”, **Journal of National Security Law & Policy**, Vol.4, No.63, 2010, s.63-86

⁴⁸ 2016-2019 Ulusal Siber Güvenlik Stratejisi

⁴⁹ Hasan Çiftçi, **Her Yönüyle Siber Savaş**, TÜBİTAK, Ankara, 2013, s.133.

⁵⁰ Oona A. Hathaway, et.al, “The Law of Cyber Attack”, **California Law Review**, Vol. 100, No.4,s.822-823

olmaktadır. Siber saldırıların sistemler üzerinde yarattığı etkiler aşağıdaki şekilde tasnif edilmektedir:⁵¹

- a. Verim kaybı (Degradation); sistem yavaşlar ve işlem hızı düşer.
- b. Kesilme (Interruption); saldırı bitinceye kadar hizmet aksar.
- c. Değiştirme (Modification); değiştirilen girdiler sistemlerin çalışmasının aksamasına neden olur.
- d. Aldatma (Fabrication); sahte hesap ve verilerle kişilerin, devlet ve özel kuruluşların bilgileri çalınmaktadır.
- e. Durdurma (Interception); sistem tamamen çalışamaz hale gelir.
- f. Yetkisiz kullanım (Unauthorized use); erişim imkanı kısıtlı ya da hiç olmayan kullanıcıların, erişime yetkisi olan başka kullanıcıların bilgi ve yetkilerini kullanarak sisteme erişim sağlamasıdır.

Siber saldırılar meydana gelen zararların hesaplanması oldukça zor olması nedeniyle saldırıların sistemlerde oluşturduğu kayıplar ancak tahmin edilebilmektedir.

1.5.4.Siber Saldırı Türleri

1.5.4.1.Hizmet Engelleme (Distributed Denial of Service-DDoS)

Hizmet Engelleme (DDoS) saldırısı, bir veya birden fazla saldırganın internet üzerinden verilen bir hizmetin yerine getirilmesini imkânsız kılmaya çalışmasıdır. Bu, neredeyse her şeye erişimi engelleyerek başarılabılır: sunucular, cihazlar, hizmetler, ağlar, uygulamalar ve hatta uygulamalar içindeki özel işlemler. Bu saldırıyla, hizmet sağlayan sunucu bilgisayara gerçekte var olmayan talepler göndererek bilgisayar meşgul edilmekte ve hizmet veremez hale getirilmektedir. Bu saldırılar, aşırı bilgi talebi ile sistemleri boğmaya çalışır. Bu, bir web sunucusuna çok fazla talep göndererek web sayfasının çökmesine neden olur. Örneğin bu tip bir saldırı e-devlet hizmeti veren herhangi bir sunucudan aşırı bilgi talep edilerek sunucunun kilitlenmesine neden olmaktadır.

Hizmet engelleme saldırıları, çevrimiçi aktivizmin aracı olarak ve hatta siber saldırı için yaygın olarak kullanıldığından çok sık rastlanan bir tehdit haline gelmiştir. Hizmet engelleme saldırıları, özellikle devletlerin kritik siber altyapılarını, komuta

⁵¹ Piret Pernik,” Improving Cyber Security: NATO and The EU”, **International Centre for Defence Studies**, Talinn, 2014, s.1.

kontrol sistemlerini, internet üzerinden hizmet veren bankacılık ve e-devlet gibi sistemleri, haberleşme sistemlerinin altyapılarını ve internet telefon rehberi diyebileceğimiz alan adı sistemlerini(DNS) hedef almaktadır.⁵²

1.5.4.2.Yetki artırımı (Privilege Escalation)

Yetki artırımı, siber saldırı için önemli bir adımdır. Yetki artırımı, amaçlanan yöneticilerden veya geliştiricilerden daha fazla erişim elde etmek için imtiyazları yükseltmek amacıyla sistem güvenlik açıklarından yararlanma pratiğidir. Başarılı yetki artırımı saldırıları, saldırganların hedef sistemler üzerindeki kontrol düzeylerini artırmalarını, böylece herhangi bir veriye erişme özgürlüğünü ya da operasyon özgürlüğünün sağlanması ve hedef sisteme sürekli erişimin sağlanması için gerekli herhangi bir konfigürasyon değişikliğinin yapılmasını sağlar. Bu saldırı tekniğinde saldırgan ya sistemin açık yanlarını kullanarak ya da sisteme girmeye yetkili bir kullanıcının verilerini çalarak sistemden içeri sızmaktadır. Saldırgan sistem yetkilendirme kodlarını çalarak sistemde istediği ayrıcalığa ulaşabilmektedir. Önce sisteme giriş yetkisini elde eden saldırgan daha sonra sistem içerisindeki uygulamalara zarar vermek için sistem kodlarını değiştirebilir veya gerçekte sisteme girme yetkisi olan kişilerin sisteme girmesini engelleyebilir. Daha ileri bir nokta ise saldırgan sistem yöneticisinin şifrelerine ulaşarak sistemi bozabilir. Bu saldırı içeriden bir kullanıcı tarafından da yapılabilir.⁵³

1.5.4.3.Truva Atı

Kendini faydalı ve zararsız göstererek gizlenebilen yazılımlar bu yolla sisteme girdikten sonra zamanı geldiğinde veya hedefe ulaştığında zararlı yanını devreye sokarak sisteme zarar vermektedirler. ‘Truva Atı’ adı verilen yazılımlar, taşınabilir harici bellekler, internet siteleri, gönderilen e-postalar ile sisteme girebilmekte hatta daha üretirken bu yazılımları sisteme yükleyerek zamanı geldiğinde kendiliğinden, uzaktan komutayla veya kullanıcının bilmeden yaptığı bir işlemle aktif hale

⁵² George V. Hulme, “**How Distributed Denial of Service Attacks are Evolving**”, (çevrimiçi) <https://www.csoonline.com/article/3222095/network-security/ddos-explained-how-denial-of-service-attacks-are-evolving.html>, 11.09.2018

⁵³ Michael C. Long II, **Attack and Defend: Linux Privilege Escalation Techniques of 2016**, s.6-16 (çevrimiçi) <https://www.sans.org/reading-room/whitepapers/linux/attack-defend-linux-privilege-escalation-techniques-2016-37562>, 11.09.2018

gelebilmektedir. Truva atına örnek vermek gerekirse bir sistemin güvenliğini sağlamak için yüklenen virüs programına eklenilen bir yazılımla o sistemdeki gizli bilgilere ulaşması, görünürde faydalı bir hizmet veren bir yazılımın geri planda sisteme zarar vermesidir.⁵⁴

1.5.4.4.Botnetler

Bir botnet, kötü amaçlarla kullanılmak amacıyla aralarında bağlantı yapılmış bir bilgisayar grubudur. Botnet'teki her bilgisayar bot olarak adlandırılır. Bu botlar, üçüncü taraflarca kontrol edilen ve kötü amaçlı yazılım veya spam iletmek veya saldırı başlatmak için kullanılan, güvenliği ihlal edilmiş bilgisayarlardan oluşan bir ağ oluşturur.⁵⁵

Botnetler, bir saldırı yapma amacıyla ele geçirilmiş ve gerektiğinde bu saldırı için kullanılabilecek birbiriyle irtibatlandırılmış bilgisayarlar grubudur. Bu bilgisayarlar grubu önceden yüklenmiş programlarla planlanmış görevleri yerine getirebilmektedir. Botnetler önceden ele geçirilip ihtiyaç duyulduğunda verilecek bir komutla da harekete geçirilebilir. Botnet olarak kullanılmak üzere ele geçirilen bilgisayara “zombi” bilgisayar adı verilmektedir.⁵⁶

Zombi olarak ele geçirilen bilgisayarların sahipleri bilgisayarlarının botnet olarak kullanılacağından veya kullanıldığından haberdar değildir. Bilgisayar korsanları ele geçirdikleri botnetler vasıtasıyla kurum veya kuruluşlardan maddi kazanç elde etmek için saldırı yapabildiği gibi bu imkanı başkalarına ücret karşılığında kiralayabilmektedirler. Çifçi, çalışmasında “*bir milyon üyesi olan bir köle bilgisayar ağının Fortune 500'deki tüm şirketleri, 10 milyon üyesi olan bir ağın ise büyük bir batılı ülkenin tüm iletişim altyapısını çökertebileceğini*” belirtmiştir.⁵⁷

1.5.4.5.Mantık Bombası (Logic Bomb)

Mantık bombası, herhangi bir programın içerisine, kasıtlı olarak yerleştirilen virüs programlarıdır. Önceden belirlenen şartların gerçekleşmesiyle harekete geçerek bulunduğu sisteme zarar vermektedir. Örneğin çalıştığı şirketten atılan bilgisayar

⁵⁴ Hasan Çiftçi, **a.g.e.**, s.153

⁵⁵ Andress, Winterfeld, **a.g.e.**, s.6

⁵⁶ Salih Bıçakçı, **21. Yüzyılda Siber Güvenlik**, Bilgi Üniversitesi Yayınları, İstanbul, 2013, s.40.

⁵⁷ Hasan Çiftçi, **A.e.** s.155

programcısının kasıtlı olarak sisteme yüklemiş olduğu bir kod parçası programcı ayrıldıktan sonra sistem dosyalarını silmeye başlayabilir.⁵⁸

1.5.4.6.Solucanlar

Truva atı ve mantık bombası gibi benzer yollarla sisteme giren solucanların truva atı ve mantık bombasından farkı çoğalması ve yayılmasıdır. Solucanlar girdiği sistemin bağlı olduğu ağ üzerinden bulduğu açıklıklardan istifade ederek başka sistemlere yayılabilen ve çoğalabilen programlardır.⁵⁹ Ayrıca solucanlar hizmet reddi saldırılarında kullanılabilme imkânına sahiptir.

1.5.4.7.Gelişmiş Siber Tehditler (Advanced Persistent Threats – APT)

Gelişmiş siber tehditleri diğerlerinden ayıran en önemli farklılıkları ısrarlı ve tekrarlayan şekilde saldırı yapması, karmaşık yöntemler kullanması, tespit edilmesi ve önlenmesinin oldukça zor olmasıdır.⁶⁰ Stuxnet saldırısında olduğu gibi bu saldırılar gelişmiş teknikler kullanmakta, birden fazla aşamada, disiplinli, başarısız olursa da tekrar geliştirerek ve uzun süre devam etmektedir. Bu saldırının ilk safhası belirlenmiş sisteme girilmesidir. Sisteme giriş yapıldıktan sonra sistem ve bağlı olduğu ağ keşfedilir ve açıklıklar belirlenerek saldırı gerçekleştirilir. Bu tür programların sisteme girdikten sonra adım adım ne yapacağı önceden plan ve programlanmıştır.⁶¹

Gelişmiş siber tehditleri diğer siber saldırılardan ayıran hususlar aşağıdadır.⁶²

- a. Önceden belirlenmiş hedefe saldırmak için programlanırlar.
- b. Hedef sisteme girdikten sonra öğrenme, sistem içinde yayılma ve gizli bilgileri elde etme kabiliyetine sahiptir.
- c. Stuxnet saldırısında olduğu gibi herhangi bir ağa bağlı olmayan sistemlere sızabilirler.

⁵⁸ Hasan Çiftçi, **a.g.e.** s.154

⁵⁹ Hasan Çiftçi, **A.e.** s.151

⁶⁰ Hasan Çiftçi, **A.e.** s.155

⁶¹ Neil Robinson et.al., **Data and Security Breaches and Cyber Security Strategies in The EU and Its International Counterparts**, European Union, 2013, s.30

⁶² Knapp Eric, Langill Thomas Joel, **Industrial Network Security**, Elsevier, Waltham, 2015, s.43-44.

d. Sistem içinde kendilerini gizleyebilecek yetenekleri vardır ve bu yetenekleri sayesinde uzun süre tespit edilmeden saldırılarını devam ettirebilirler.

1.5.5.Siber Saldırıların Önemli Hedefleri

1.5.5.1.Sosyal Ağlar

Sosyal ağlar son yıllarda hayatımıza giren en önemli fenomendir. Son on yılda sosyal ağ sitelerinin popülerliği, kullanılabilirliği ve erişilebilirliği nedeniyle insanlar arasındaki etkileşimler yavaş yavaş değişmiştir. Sosyal ağlar yaşamımızı rahatlatma, bilgi ve iletişim açısından geliştirmektedir. Konuşan ve paylaşan insanın günümüzde bu ihtiyacını karşıladığı en önemli ortam sosyal ağlardır. Sosyal ağlar yoğun çalışma ve eğitim hayatında koşturmayla geçen gün içinde insanın konuşma ve paylaşma ihtiyacı için yakaladığı fırsatları değerlendirme platformudur. Öte yandan, sosyal ağ kullanıcılarının bilgi güvenliği ve gizliliği, çoğu kullanıcının bilgisizliği nedeniyle istismar edilmektedir. Sosyal ağlar üzerinden gerçekleştirilen siber saldırı oranı oldukça yüksektir. Sosyal ağ kullanıcılarına daha iyi güvenlik sağlamak için bir çözüm bulmak önemli bir sorun haline gelmiştir. Araştırmacılar güvenlik sorunlarının çoğunlukla Facebook ve Twitter ile ilgili olduğuna atıfta bulunmaktadır.⁶³

1.5.5.2.Akıllı Şebekeler

E-devlet, bankacılık, ulaşım, su, doğalgaz, kanalizasyon, elektrik ve telekomünikasyon vb. kritik hizmetler internet üzerinde çalışan bilgisayar programları ile verilmektedir. Kritik hizmetleri internet üzerinden sağlayan devletlere zarar vermek isteyen başka devlet veya devlet dışı aktörler bu sistemlere siber saldırıda bulunmaktadırlar. Bu saldırılar sonucunda kritik hizmetlerin çok büyük ölçüde aksaması nedeniyle ülkenin ekonomisi alt üst olmakta ve ülkede kaos meydana gelmektedir. Bu sistemlerin yanında en önemlisi de bunları besleyen enerji şebekeleridir. ABD Dış İlişkiler Konseyi, ABD enerji şebekesinin siber saldırıya maruz kalacağıyla ilgili olarak üç senaryodan bahsetmektedir. Birinci senaryo; Amerikalıların günlük hayatlarında elektriğin önemi göz önüne alındığında, bir rakip, politik açıdan hassas bir zamanda ABD yönetimine yönelik kamu desteğini

⁶³ Azah Anir Norman et.al., **Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review**, **Future Technologies Conference 2017**, (çevrimiçi) https://umexpert.um.edu.my/file/publication/00007219_156865_68443.pdf, 12.09.2018

zayıflatmak için hizmetin aksatılmasında avantaj görebilecektir. İkinci senaryo; ABD'nin karşı çıkacağı diplomatik veya askeri bir girişimde bulunan bir devlet, ABD hükümetinin dikkatini dağıtmak, yanıtını aksatmak veya ertelemek için elektrik şebekesine karşı bir siber saldırı gerçekleştirebilir. Üçüncü senaryo; ekonomik yaptırımlar ve politik savaş gibi ABD eylemleri nedeniyle tehdit edildiğini düşünen bir devlet ABD'yi cezalandırmak için güç şebekesine siber saldırı yapabilir veya saldırı tehdidinde bulunabilir.⁶⁴ Görüldüğü gibi siber saldırılar devletlere karşı uluslararası politika aracı olarak kullanılabilir.

1.5.5.3.Kapalı Devre Sistemler

İnternete veya yerel bir ağa bağlı olmayan kapalı devre sistemlerin daha güvenli olduğu ve siber saldırılara maruz kalmayacağı yönünde yanlış bir algı bulunmaktadır. İran'ın tamamen kapalı bir sistem olarak tasarlanmış, internet ile hiçbir bağı bulunmayan uranyum zenginleştirme sistemlerine yapılan Stuxnet saldırısı bu algının yanlış olduğunu göstermiştir. Stuxnet, herhangi bir ağa bağlı olmayan yarı özerk uzak sistemlere sızmak ve bu sistemleri kontrol altına almak için tasarlanmış çok karmaşık bir bilgisayar programıdır. Program, siber alanda hedef alınabilecek hedeflere karşı yeni nesil "at ve unut" kötü amaçlı yazılımı temsil etmektedir. Stuxnet'in hedeflediği sistemler internete bağlı olmayan, erişim için ancak USB harici bellek gibi aygıtların kullanımını gerektiren sistemlerdir.⁶⁵

1.5.5.4.Acil Yardım Sistemleri

Acil durumlara yönelik alınacak tedbirlerin planlanması ve yönetilmesi bilgi sistemleri ile yönetilmektedir. Kaos çıkarmak isteyen saldırganların hedeflerinden birisi de acil durum yönetim sistemleri olmaktadır. Bu sistemlere yapılacak saldırılar örneğin polis imdat, orman yangını, ambulans hizmeti vb. hizmetlerin aksamasına neden olmakta acil durum yardım taleplerinin karşılanmasını sekteye uğratmaktadır.

⁶⁴ Robert K.Knake, "A Cyberattack on the U.S. Power Grid", **Contingency Planning Memorandum No. 31**, 2017, (çevrimiçi) <https://www.cfr.org/report/cyberattack-us-power-grid>, 12.09.2018

⁶⁵ James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", **Survival Global Politics and Strategy**, Volume 53, s.23-40

1.5.5.5.Web Sayfaları

Ülkemizde 2018 yılı ilk çeyrek verilerine bakıldığında, “12,3 milyonu sabit abone, 57,7 milyonu mobil abone olmak üzere toplam yaklaşık 70 milyon geniş bant internet abone sayısına ulaşılmıştır.”⁶⁶ İnternet kullanımı yaygınlaştıkça hem kamu hem de özel kurumlar hizmetlerinin birçoğunu internet üzerinden vermeye başlamıştır. İnternet üzerinden verilen hizmetler vatandaşlar üzerinde olumlu etki yaratmakla birlikte bu hizmetlerin güvenli ve kesintisiz olarak devam ettirilmesi çaba gerektirmektedir. Çünkü internet sitelerine yapılan saldırılar hem güven kaybına hem de hizmetin aksamasına neden olmaktadır. Bu saldırıların amaçları, bilgiye erişmek, web sitesine ve internet servis sağlayıcıya zarar vermek, web sitesini köleleştirerek bu siteyi ziyaret eden kullanıcıların bilgisayarlarına erişim sağlamak veya zarar vermek olabilir.⁶⁷

1.5.5.6.Siber Saldırının Hedefi Kritik Altyapılar

Kritik altyapılar: “işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara ve ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına, yol açabilecek bilişim sistemlerini barındıran altyapıları ifade eder.”⁶⁸

ABD’de 2001 yılında çıkan Vatanseverlik Yasası (Patriot Act of 2001)’nda kritik altyapılar “Yetersizliği veya tahribi, güvenliğe, milli ekonomik güvenliğe ve kamu sağlığına veya emniyetine zayıflatıcı bir etkisi olan fiziksel veya sanal sistem ve varlıklar” olarak tanımlanmıştır.⁶⁹

Bu tanımlardan yola çıkıldığında bilişim sistemlerini barındıran kamu hizmetleri, savunma teknolojileri, enerji üretim ve dağıtım sistemleri, telekomünikasyon alt yapıları, ulaşım, hava trafiği kontrol sistemleri, finans servisleri, sağlık servisleri, su üretim ve dağıtım şebekeleri kritik altyapılar olarak

⁶⁶ Bilgi Teknolojileri ve İletişim Kurumu, **2018 yılı 1. Çeyrek Pazar Verileri Raporu**, (çevrimiçi) <https://www.btk.gov.tr/uploads/pages/pazar-verileri/2018-1ceykraporu-kurumdisi.pdf>, 13.09.2018

⁶⁷ DWEN-REN Tsai et.al. “Optimum Tuning of Defense Settings for Common Attacks on the Web Applications”, **Security Technology**, 2009, 43rd Annual 2009 International Carnahan Conference, ss.89-94

⁶⁸ 2016-2019 Ulusal Siber Güvenlik Stratejisi

⁶⁹ Hasan Çiftçi, **a.g.e.** s.9

adlandırılmaktadır. Kritik alt yapıların internet üzerinden çalışan bilişim sistemlerine olan bağı arttıkça internet üzerinden gelecek her türlü tehdide karşı hassas olacaktır.

Bilişim sistemlerine bağımlı olarak çalışan kritik altyapılar saldırganlar tarafından ele geçirildiğinde ülkede meydana gelebilecek karışıklıkları ortaya koyan birçok siber savaş senaryosu bulunmaktadır. Örneğin trafik kontrol sistemini ele geçirerek şehirlerin trafiğinin altüst edilmesi, telekomünikasyon sistemin ele geçirilerek iletişimin kesilmesi, elektrik şebekesinin ele geçirilerek şehirlerin karanlığa mahkum edilmesi, doğalgaz ve petrol boru hatlarının çalışamaz hale getirilmesi, baraj kapaklarının açılarak afetlere sebep olunması, hava trafik kontrol sisteminin ele geçirilerek hava trafiğinin işlemez hale getirilmesi gibi birçok benzer tehlike film senaryosu olmaktan çıkmış çok muhtemel tehditler haline gelmiştir.

Ülkemizde kritik altyapı sektörleri, Siber Güvenlik Kurulu tarafından “Elektronik Haberleşme”, “Enerji”, “Su Yönetimi”, “Kritik Kamu Hizmetleri”, “Ulaştırma” ve “Bankacılık ve Finans” olarak altı başlık altında belirlenmiştir.⁷⁰

1.5.6. Siber Saldırı Örnekleri

1.5.6.1.2003 ABD ve Kanada Elektrik Kesintisi

Kanada ve ABD’nin birçok eyaletinde 14 Ağustos 2003 tarihinde yapılan siber saldırılar sonucunda elektrik kesintisi yaşanmıştır. Bu elektrik kesintisi yaklaşık bir hafta sürmüş ve 50 milyon insanı etkilemiştir. Elektrik kesintisinin ABD’ye maliyetinin 4 ila 10 milyar dolar, Kanada’ya olan maliyetinin ise 2,3 milyar dolar olduğu tahmin edilmektedir.⁷¹

Pek çok büyük şirketin faaliyeti elektrik kesintisi nedeniyle durmuştur. Elektrik kesintinin her iki ülkenin sanayisine verdiği zararlar aşağıda sıralanmıştır.

- a. Elektrik kesintisi nedeniyle su dağıtım şebekesi işlememiş ve birçok yere su verilememiştir.
- b. Petrol rafinerilerinde üretim durduğundan bazı eyaletlere akaryakıt verilememiştir.

⁷⁰ 2016-2019 Ulusal Siber Güvenlik Stratejisi

⁷¹ U.S.-Canada Power System Outage Task Force, **Final Report on the August 14, 2003 Blackout in the United States and Canada**, 2004

- c. Metro ve tren seferleri yapılamadığından ulaşım sekteye uğramıştır.
- d. Demir çelik fabrikalarında elektrikle çalışan soğutma sistemleri devre dışı kaldığından yangınlar meydana gelmiş ve üretimi durmuştur.
- e. Büyük otomobil şirketlerinin de bulunduğu fabrikanın faaliyetleri durmuş, kesinti süresince yaklaşık 100.000 çalışan işlerine gidememiştir.⁷²

1.5.6.2.Estonya 2007 Saldırısı

Estonya, 2007 yılı Nisan ayının sonlarından Mayıs ayının başına kadar saldırıya uğramıştır. Estonya Savunma Bakanı Jaak Aaviksoo'ya göre "saldırıların çoğu devlet sunucularına ve Estonya haber portallarına karşı yapılmış, özellikle Estonya'nın en büyük iki bankası ağır saldırıya uğramıştır. Devlet kurumlarını hedef alan Estonya dışından gelen siber trafik miktarı en yoğun anda normal oranından 400 kat daha yüksek olmuştur. Saldırıları çok iyi koordine edilmiş ve aynı zaman aralığında gerçekleştirilmiş ve muhtemelen daha önce bu amaç için kiralanmış bilgisayar gruplarını 'botnet' içermiştir.⁷³

Estonya saldırısı, altyapı boyutu ve saldırıların kapsamı göz önüne alındığında, dünya üzerindeki egemen bir devlete karşı en önemli koordine edilmiş siber saldırılardan birisi olarak bilinmektedir. Saldırganlar yenilmiş olmasına rağmen, internet bankacılığının kullanılamaması veya iletişim güçlükleri gibi Estonya halkını etkileyen bazı ani etkiler olmuştur. Banka işlemlerinin % 98'inin çevrimiçi yapıldığı ve vatandaşların çoğunluğunun vergi formlarını çevrimiçi doldurduğu bir ülkede, bu tür uzun süren olayların yaratacağı etki oldukça yıkıcı olabilmektedir. Siber saldırılar, doğrudan hedefi etkilemesinin yanı sıra, halk arasında yaygın karışıklık ve iletişim bozukluğuna neden olmuştur.⁷⁴

⁷² Electricity Consumers Resource Council (ELCON), **The Economic Impacts of the August 2003 Blackout, February 9, 2004**, (çevrimiçi) <http://www.elcon.org/Documents/Profiles%20and%20Publications/Economic%20Impacts%20of%20August%202003%20Blackout.pdf>, 30.04.2016

⁷³ Pauline C. Reich, v.d., "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents- and the Dilemma of Anonymity", **European Journal of Law and Technology**, Vol.1, Issue 2, 2010, s.12-13

⁷⁴ Pauline C. Reich, v.d., **A.e.**, s.12-13

1.5.6.3.2008 Yılında Gürcistan’a Yapılan Siber Saldırıları

Ağustos 2008’de Güney Osetya’da Rusya ve Gürcistan arasında başlayan sıcak çatışmaların Rusya tarafından eş zamanlı olarak siber alanda desteklenmesi siber güvenliğin öneminin algılanması açısından önem arz eden bir diğer olaydır. Gürcistan’ın 7 Ağustos 2008’de Güney Osetya’daki askeri harekâtını başlattığı aynı gün Gürcistan hükümet web sitelerine ve internet ağlarına karşı siber saldırılar gerçekleşmiştir. Öncelikle Gürcistan’ın devlet sitelerine ve medya kuruluşlarına erişim engellenmiştir. Siber alanını savunmaya çalışan Gürcistan Rusya’dan gelen trafiği engellemiş, bu kez Çin, Kanada, Türkiye ve Estonya üzerinden saldıran Ruslar önce Gürcü bankalarına ve onların üzerinden tüm dünya bankalarına saldırılar yöneltmiştir. Bunun üzerine bankalar Gürcistan ile ağ bağlantılarını kapatmışlardır.⁷⁵

US Cyber-Consequences Unit’in Ağustos 2009’da yayımlanan raporuna göre; siber saldırıların çoğu, askeri operasyonlara zaman olarak o kadar yakın ki, Rus askerleri ile sivil saldırganlar arasında yakın bir işbirliği olduğu muhakkaktır. Siber saldırıların keşif veya yer tespiti yapmadan, en uygun saldırı türlerinde yapılması, gerekli keşif ve saldırı komutlarının önceden yazıldığını göstermektedir. Salırganların eylemlerinin hızından atılan adımların hepsinin daha önceden hazırlanmış olduğu sonucuna varılmaktadır.⁷⁶

1.5.6.4.2009 Yılında İran’ın Nükleer Tesislerine Yapılan Siber Saldırıları

Saldırının 2009 yılında ABD tarafından İran’ın Natanz nükleer yakıt zenginleştirme tesislerine karşı düzenlendiğine inanılmaktadır. Bu saldırı, saldırıda kullanılan ‘Stuxnet’ virüsünün adıyla anılmaktadır.⁷⁷

İran devleti meydana gelen aksaklık ve hasarın siber bir saldırıdan kaynaklandığını ne saldırı sırasında ve ne de sonrasında farkına varabilmiş veya tespit edebilmiş değildir. Böyle bir saldırının yapıldığı ve kullanılan virüsün özellikleri ancak yaklaşık bir sene sonra tesadüfen tespit edilebilmiştir. Ukrayna bilişim şirketi

⁷⁵ Eneken Tikk et.al, **Cyber Attacks Against Georgia: Legal Lessons Identified**, Cooperative Cyber Defence Center of Excellence, November 2008, s.4-14

⁷⁶ Pauline C. Reich, **a.g.e.** s.13-14

⁷⁷ Şener Çelik, Stuxnet Saldırısı ve ABD’nin Siber Savaş Stratejisi, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 15, Sayı: 1, 2013, s.137-175 (Basım Yılı: 2014)

Virusblokada 2010 yılının Mayıs ayında Stuxnet virüs programını tespit etmiştir.⁷⁸ Virüs programının kaynağını bulmak için Kaspersky Anti Virüs Yazılım Şirketi ve Microsoft Şirketi ortak olarak araştırma başlatmış, bu araştırmaya daha sonra Symantec Bilişim Güvenlik Şirketi de dâhil olmuştur. Bulgulara göre; o zamana kadar bilinen zararlı yazılımlardan çok daha karmaşık bir virüs programıyla İran'ın nükleer yakıt zenginleştirme tesislerindeki bilgisayar sistemine karşı 22 Haziran 2009 tarihinde yerel saatle 16.30'da ve 07 Temmuz 2009 tarihinde yerel saatle 17.00'de iki ayrı saldırı meydana gelmiştir.⁷⁹

Hiçbir kişi, grup veya devlet Stuxnet solucanını oluşturduğunu ve kullandığını kabul etmese de birçok uzman, Stuxnet kadar karmaşık bir programın en az bir devlet yardımı olmadan yapılamayacağına inanmaktadır. Stuxnet bir silah olarak kullanılan ilk bilgisayar virüsüdür. Siber güvenlik uzmanlarının çoğu, Stuxnet'i ABD ve İsrail'in birlikte yaptığını ve kullandığını ve Stuxnet'in uluslararası çatışmaların büyük bir parçası haline gelecek siber savaşın kapısını açtığını düşünmektedir.⁸⁰

Yukarıda bahsedilen siber saldırı örneklerine bakıldığında; 2003 ABD ve Kanada Elektrik Kesintisi, bir devletin kritik altyapılarına yapılan saldırılarla büyük ekonomik zararların oluşmasından, Estonya 2007 Saldırısı, egemen bir devlete karşı yapılmış olmasından, 2008 Gürcistan saldırısı silahlı çatışmayı kolaylaştırdığından uluslararası silahlı çatışma hukukunun uygulanabileceği bir örnek olması açısından, Stuxnet ise siber savaşa neden olabilecek bir saldırı örneği olması nedeniyle özellik arz etmektedir.

Siber saldırılarda kullanılan vasıtaların kabiliyetleri kısıtlıdır, kolay ulaşılabilir ve satın alınabilirler. Örneğin bu vasıtaların en gelişmişleri Stuxnet gibi 'at unut' konseptiyle üretilmiş akıllı mühimmatlara benzetilmektedir. Ancak üst düzey güvenlik tedbirlerini aşabilen böyle bir virüsün üretilebilmesi için uzun sürelerle, büyük

⁷⁸ Sean Collins, Stephen McCombie, "Stuxnet: The Emergence Of a New Cyber Weapon And Its Implications" **Journal of Policing, Intelligence and Counter Terrorism**, Vol.7, No.1, 2012, s.84

⁷⁹ David Kushner, **The Real Story of Stuxnet**, **IEEE Spectrum**, 26 Feb 2013, (çevrimiçi) <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>, 30.04.2016

⁸⁰ Mohn, Elizabeth, "Stuxnet", **Salem Press Encyclopedia of Science**, 2015, (çevrimiçi) <http://eds.a.ebscohost.com/eds/detail/detail?vid=4&sid=84b9a4f9-291d-45a2-ac7e-e76289b32b9%40sessionmgr4007&bdata=Jmxhbm9dHlmc2l0ZT1lZHMtG1ZlZGQ%3d%3d#AN=87323878&db=ers>, 14.09.2018

arařtırma ve geliřtirme bütelerine ihtiya duyulmaktadır. Devletlerin son yıllardaki Ulusal Siber Gvenlik Stratejileri incelendiėinde, saldırgan siber yeteneklere ve aktif savunma tedbirlerine yatırım yapılmaya bařlandığı dikkat ekmektedir. Konvansiyonel ve nkleer silahlarda olduėu gibi geliřtirilecek saldırgan siber yeteneklerin savunma amalı kullanılacağı ifade edilmiř olsa da bu yeteneklerin saldırgan amalarla da kullanılabileceėi bu nedenle kritik siber altyapıların gvenliėinin saėlanması giderek daha fazla zorlařacağı deėerlendirilmektedir.



İKİNCİ BÖLÜM

SİBER SALDIRILAR VE ULUSLARARASI HUKUKTA KUVVET KULLANIMI

2.1.SİBER SAVAŞIN BELİRGİN ÖZELLİKLERİ:

“Siber savaş” terimi siber alanda siber araç ve yöntemlerle yapılan savaşı ifade eder. “Savaş”, silahlı çatışma durumunda askeri harekâtın yürütülmesine atıfta bulunurken, “siber alan”, internet, telekomünikasyon ağları dâhil olmak üzere, küresel olarak birbirine bağlı bir dijital bilgi ve iletişim altyapısı ağı olarak tanımlanmaktadır. Siber savaşın siber alanda yürütüldüğü gerçeği, siber alanın dışında kinetik veya diğer elektronik olmayan etkiler yaratmayacağı anlamına gelmez ve özellikle saldırgan tarafından bu şekilde tasarlanmış olabileceği göz ardı edilmez. Mesela, siber savaşın hedefleri arasında, hayatı ya da kullandığı nesnelerin işlevselliği bilgisayar sistemlerine dayanan, belirli güç istasyonları, ulaşım araçları ya da çeşitli tıbbi, askeri ya da profesyonel yaşam desteği ile bağlantılı kişiler yer alabilir.

Siber alanın kendi ortamında kuralları vardır. Mesela siber saldırılar, kuvvet kullanarak değil, düşmanın zayıf noktalarını istismar ederek yapılmaktadır. Sürekli etkilerin üretilmesi zordur. Ortam, kimin ve niçin saldırıya uğradığı, neyi gerçekleştirdikleri ve tekrar gerçekleştirip gerçekleştiremeyecekleri konusunda belirsizliklerle doludur. Bugün işe yarayan bir şey yarın yaramayabilir (aslında bugün işe yaradığı için). Bu nedenle, başka ortamda oluşmuş caydırıcılık ve savaş ilkelerinin siber alana uyarlanması aynı sonuçların alınacağı güvencesini sağlamayacaktır.¹

Bir ülkedeki enerji santralının başka bir ülke tarafından bombalanmasının bir saldırı ve savaş nedeni olacağı konusunda hiçbir tereddüt yoktur. Buna rağmen internete girip siber saldırı ile aynı elektrik santralını etkisiz hale getirmek saldırı ve savaş nedeni sayılır mı konusunda tereddüt edeceğimize şüphe yoktur. Eğer bir devlet ülkemizin elektrik şebekesini bombalarsa ve bomba atmak için ülkemize giren saldırganları gördüğümüzde bunun açık bir savaş sebebi ve meşru müdafaa hakkı doğuracağından hiç kuşku yoktur. Ancak aynı devlet elektrik şebekemizi bozmak için karmaşık bilgisayarlar kullanırsa bunun bir savaş sebebi ve meşru müdafaa hakkı

¹ Martin C. Libicki, Cyber Deterrence and Cyber War, The Rand Corporation, Santa Monica 2009, s.6-13

doğuracağını kesin olarak söyleyemesek de buna bir karşılık verme hakkımızın bulunduğunu söyleyebiliriz.

Mevcut uluslararası çatışma hukuku siber alana yorumlanırken ve uygulanırken, siber alanın belirli özelliklerine dikkat edilmelidir. En önemlisi siber alan, tamamen insan yapımı olan tek alandır. Siber alan dünya genelinde kamu ve özel paydaşlar tarafından oluşturulmakta, muhafaza edilmekte, sahiplenilmekte ve işletilmekte olup ve teknolojik yeniliklerle birlikte sürekli olarak değişmektedir. Siber alan, jeopolitik veya doğal sınırlara tabi değildir, bilgi ve elektronik yükler, herhangi bir başlangıç noktasından elektromanyetik spektrumla bağlanan bir varış noktasına anında ulaştırılabilir. Bu bilgi ve elektronik yükler hedeflerinde yeniden bir araya getirilmeden önce, önceden tahmin edilemeyen yollarla çoklu dijitalleştirilmiş parçalar halinde seyahat etmektedirler. Siber alana hükümetler, devlet dışı kuruluşlar, özel kuruluşlar ve bireyler kolayca erişebilirken örneğin IP sahtekârlığı ve botnet kullanımı, bir operasyonun kökenini gizlemeyi kolaylaştırmaktadır böylece siber faaliyetlerin güvenilir bir şekilde tanımlanması ve atfedilmesi özellikle zorlaşmaktadır.

2.1.1 Siber Savaşın Muharebe Sahası:

Siber savaşın uluslararası hukuk açısından statüsü belirlenirken “muharebe(çatışma) sahasının” belirlenmesi en önemli safhadır. Eğer muharebe sahasında bir saldırı gerçekleşirse silahlı çatışma hukuku uygulanır. Ancak, coğrafi olarak sınırlı bir muharebe sahasının dışından konvansiyonel bir saldırı meydana geldiğinde, çatışma hukukunun nasıl uygulanacağı belirsizdir. Siber harekât alanında muharebe sahası tanımlanırken yaşanan zorluk icra edilen siber operasyon sırasında birden fazla ülkeye yayılmış internet altyapısının anlık olarak kullanılıyor olmasıdır. Dolayısı ile siber çatışma sahasının nerede başlayıp nerede bittiğinin belirlenmesi mevcut paradigma ölçütleriyle oldukça sorunludur. Ancak çatışma alanını coğrafi olarak sınırlayan ne hukuk ne de teamül kuralı bulunmamaktadır.

Siber savaş, bir takım manevi ve ahlaki mülahazaların gündeme gelmesine sebep olacak şekilde savaşın çok uzak mesafelerden çatışmasına imkân vermektedir. ABD’de harekât merkezinde oturan, tehlikeden uzak, yorulduğunda kahve molası veren, ekrandaki görüntüleri soyut birer hedef olarak gören, bu yüzden birçok sivil

ölüme neden olan ve örneğin Afganistan’da bulunan İnsansız Hava Araçlarını kullanan operatörlerle ilgili olarak ortaya çıkan endişelerden farklı olmayacak şekilde siber saldırganlar da savaş alanından uzakta benzer koşullarda saldırılara iştirak etmektedir. Siber saldırganların savaşın dehşet dolu ortamından uzakta olması, saldırıların duygusal etkilerinden uzaklaşmalarına, gereksiz zarar ve ıstıraplar ile ikincil hasarın artması ihtimaline sebep olacaktır.

Bununla birlikte, bu tür manevi ve ahlaki düşünceler araştırma yapmaya gerekçe olsa da, Silahlı Çatışma Hukuku kuralları bu kapsamda ilave kısıtlamalar sunmamaktadır. Örneğin, uluslararası hukuk göğüs göğüse muharebe ile kıtalararası balistik füze ile yapılan saldırı arasında bir ayrım yapmaz. Bu nedenle siber alan da, muharebe sahasının sınırlarının belirsizliği veya siber saldırılara katılanların bulundukları yerlere bakılmaksızın herhangi bir başka muharebe sahası gibi dikkate alınabilir.

2.1.2.Siber Savaşın Tanımlanması:

Her şeyi kapsayan “siber savaş” terimi, saldırının birbirinden farklı etkilerinden dolayı siber alanda düşmanca eylemlerin tespiti için uygun bir tanımlama değildir. Bunun yerine siber saldırılar ve siber istismar arasında ayrım yapmanın daha yararlı olacağı değerlendirilmektedir.

Siber saldırılara bir tanımlama getirmiş tek uluslararası anlaşma, dolandırıcılık, çocuk pornografisi ve telif hakkı ihlali gibi siber suçlarla mücadelede işbirliğini artıran Avrupa Siber Suçlarla Mücadele Sözleşmesi'dir.² Sözleşme yaygın olarak kabul edilmediğinden, uluslararası hukuk açısından bağlayıcı değildir. Ancak Sözleşme, siber saldırıların kullanımıyla ilgili uluslararası kaygının var olduğunu ve bu saldırıları önlemek için devletin kendisine yüklenen görevleri kabul ettiğini göstermektedir. Sözleşmenin siber saldırılarla alakalı kısmı, veri ve sistemlere müdahaleyle ilgili olan hükümleridir. Sözleşme, imzacıların “haksız bir şekilde bilgisayar verilerinin silinmesi, bozulması, değiştirilmesi veya baskılanması” ile aynı şekilde “haksız yere

² **Convention of Cybercrime**, (çevrimiçi), <https://www.coe.int/en/web/conventions/fulllist/conventions/webContent/8601684>, 09.09.2018

bir bilgisayar sisteminin işleyişini ciddi bir şekilde engellemeyi” suç sayan yasaları kabul etmelerini şart koşturmaktadır.

Birinci bölümde ulaştığımız siber saldırı tanımı, devlet veya devlet dışı siber aktörlerin muhasımın bilgi ve iletişim teknolojilerine dayalı sistemlerindeki zayıf noktaları istismar ederek bu sistemlere zarar vermesidir. Siber saldırganlar çoğu zaman bilgisayar sistemi veya ağdan ziyade, bilgisayar sistemine veya ağa bağlı olarak hizmet veren varlıkları yok etmeyi amaçlamaktadır. Dolayısı ile siber savaş deyince; bilgisayar sistemlerini kullanarak muhasım devlet sistemlerine zarar vermek ve yok etmek için yapılan siber saldırıların bütünü anlaşılmalıdır.

Siber casusluk, bir rakibin bilgisayar sisteminden veya ağından gizli bilgileri almayı amaçlayan bir siber eylemdir. Modern bir casusluk biçimi olan siber casusluğun amacı, kullanıcının bilgisi olmadan bir bilgisayar ağından bilgi elde etmektir. Birinci bölümde belirttiğimiz gibi casusluk çoğu ülkenin iç hukukunda yasa dışıdır, ancak uluslararası çatışma hukukunda yasa dışı değildir.

Tarih boyunca, devletlerin ajanları rakip devletlere sızmak ve onlarla ilgili bilgi toplamak amacıyla casusluk yapmışlardır. Siber suçlular bilgisayar sistemlerini kullanarak yasadışı faaliyetlerini geliştirdiği gibi, devletler de benzer yöntemleri kullanmaktadır. Siber casusluk, “sistemin savunmasını değerlendirmek veya veri dosyalarının izinsiz olarak görüntülenmesi ve kopyalanması için hedef bilgisayarın yapılandırmasının yetkisiz olarak araştırılması” olarak tanımlanır ve devletler için düşük maliyetli ve düşük riskli bir araçtır.³

Siber casusluk, savaş seviyesine ulaşmaz çünkü siber casusluğun amacı veya sonucu bilgisayar sisteminin işleyişinin bozulması değil bilginin izlenmesidir. Ancak siber casusluğun bir siber saldırıya sebep olma olasılığı bulunmaktadır. Siber casusluk, geleneksel casusluğa benzer şekilde, birçok iç hukuk veya uluslararası sözleşmeyi ihlal etse de, uluslararası çatışma hukukunu ihlal etmemektedir.

Geleneksel olarak, savaş sınırlı kaynakları kontrol etmekle ilgilidir, ancak bir ağın gücü, kaynaklar tarafından değil, bilgi veya bilgiye erişim gücüne eşit olan

³ Jurriën Hamer, Rinie van Est & Lambèr Royakkers, **Cyberspace Without Conflict**, (çevrimiçi) <https://www.rathenau.nl/sites/default/files/2019-08/Cyberspace%20without%20conflict.pdf>, s.19-21, 30.08.2019

düğümünün sayısı tarafından belirlenir. Güvenliği artırılmış ağlar, sosyal ağlardaki ara bağlantılar, kritik altyapıyı çalıştıran sistemler veya veriler ne kadar fazla olursa buralardaki gizli bilgilere erişmek o kadar zorlaşacağından bu bilgilere ulaşmanın değeri de o kadar artacaktır.

Günümüzde kritik altyapıların bağlı olduğu ağlar, siber saldırılar için kilit hedeflerdir çünkü bu alt yapı ağları üzerinde komuta ve kontrol sistemleri işletilmekte, lojistik yönetilmekte, personel planlaması yapılmakta ve istihbarat yetenekleri kullanılmaktadır. Daha da önemlisi, komuta kontrol ve silah sistemleri de internete bağlı ya da bilgisayar sistemleriyle çalışmaktadır. Uçaklar sürekli hedef bilgisi gönderen yönlendiriciler haline gelmiştir. Hava savunma ve topçu, bilgisayar sistemleri tarafından yönlendirilmekte ve hedefleri tespit etmek için Küresel Konumlandırma Sistemi (GPS) güncellemelerine dayanmakta ve akıllı mühimmatlar uçuşlarını GPS sistemine göre ayarlayarak hedeflerini vurmaktadır.

2.2. SİBER SAVAŞIN MEVCUT STATÜSÜ VE ULUSLARARASI NORMLAR

Siber silahlar yeni ortaya çıkan teknoloji silahlarıdır ve kısa süredir var olduklarından çoğu siber operasyonu çevreleyen göreceli gizlilik söz konusudur, devlet uygulamalarına ilişkin kapsamlı bir kayıt yoktur. Jason Healey, siber çatışmanın tarihini üç aşamaya ayırmaktadır: 1980'lerde “farkına varma”, 1998'den 2003'e “kalkış” ve 2003'ten günümüze “askerileşme”. Healey'nin her bir evredeki temel farklılıklardan ikisi, ülkeler arasında yeteneklerin yaygınlaşmasının artması ve siber çatışmalara karşı geliştirilmiş ve resmi ve örgütsel yaklaşımlardır.⁴ Askerileşme aşamasına odaklanan James Lewis ve Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS), 2006'dan bu yana “önemli siber olayların” bir listesini tutmuş ve Temmuz 2013 itibarıyla, 153 düşmanca siber operasyonu tespit etmiştir. Lewis, bilgisayar istismarı ve siber saldırı operasyonları olarak bir ayırımı gitmemiş olmasına rağmen,

⁴ Jason Healey, **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**, Cyber Conflict Studies Association (June 1, 2013), s.18

olayların büyük çoğunluğu bilgisayar istismarı tarzı operasyonlar olduğu görünmektedir.⁵

Bugüne kadar düşmanca siber faaliyetlerin çoğu gerçek siber savaş değil, bunun yerine bilgisayar istismarı ve siber suçlar olmuştur. Bunun sebebi, siber çağın daha henüz başında olduğumuzdandır, toplumların siber alanlara bağımlılığı arttıkça dirençli hedef grupları ortaya çıkacak ve gelişmiş siber savaş ancak önümüzdeki dönemde mümkün hale gelecektir. Siber savaş düzenleyen kesin olarak belirlenmiş normlar olmadığından, devletler, uluslararası toplumun siber alanda kabul edilebilir davranışlar olarak bilinen davranışların sınırlarını test etmektedirler. Geçmişte yapılan siber saldırılar, siber savaşa mevcut silahlı çatışma hukukunun mu uygulanması gerektiği veya siber savaşla ilgili yeni uluslararası normların ortaya çıkmasının mı gerektiği hakkında bir fikir vermektedir. Siber saldırı sonucunda ölüm, yaralanma veya yaygın ve şiddetli fiziksel hasar henüz gerçekleşmemiştir. Ayrıca İran'ın nükleer tesisinde kullandığı santrifüjler ve Rus doğal gaz boru hatları gibi stratejik önem taşıyan tesislere yapılan siber saldırılar sonucunda ortaya çıkan fiziksel hasar yaygın veya şiddetli olmamıştır. Kitlel olarak yıkıcı siber saldırıların olmaması, siber yeteneklerin sınırlı olmasına bağlı olsa da, bu tür saldırıların olmaması da kısıtlayıcı bir normun ortaya çıkmasına neden olabilir.

Siber savaş düzenleyen çok az normatif kısıtlama olmasına rağmen siber savaş üzerine çekilen dikkat ve tartışmaların, siber savaş için çeşitli normlar üzerinde uzlaşmaya varmaya ve ortaya çıkan normları kodlamaya yardımcı olacağı düşünülmektedir. Norm evrimi teorisi, normların ortaya çıkmasının özellikle örgütsel platformlara sahip norm girişimcilerinin ve liderlerinin kilit aktör olarak varlığı halinde daha muhtemel olduğunu belirtmektedir. Şu anda BM ve NATO, siber savaş için ortaya çıkmakta olan normları teşvik etmek için kullanılan iki temel uluslararası organizasyondur. Birleşmiş Milletler'deki çalışma grupları, esas olarak Rusya önderliğinde, NATO'daki çalışma grupları ise ABD önderliğinde yürütülmektedir.

⁵ James Lewis, "Significant Cyber Events Since 2006," **Center for Strategic and International Studies**, July 11, 2013,(çevrimiçi) http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf, 21.03.2019

Birleşmiş Milletler’de siber savaş üzerine yapılan çalışmalar, BM Genel Kurulu Birinci Komitesi (Silahsızlanma ve Uluslararası Güvenlik Komitesi) yanı sıra, çeşitli yan kuruluş ve uzmanlık grupları özellikle Silahsızlanma Araştırma Enstitüsü ve Terörle Mücadele Uygulama Görev Grubu çalışma grubunda gerçekleşmektedir. Siber savaş üzerine ciddi olarak 1998 yılından itibaren odaklanılmaya başlanmıştır. 1998 yılında Rus temsilciler, BM Genel Kurulu Birinci Komite’sine silahların kontrolü anlaşmalarına benzer “*siber silahların kontrolü*” sürecinin tesisini başlatacak bir karar sunmuştur. Rus önerisi, siber saldırıların yasaklanmasından ziyade siber terörün ve saldırgan siber silahların yasaklanmasını içermektedir.⁶ Bu normların her ikisinde de önde gelen norm yapıcısı ve lideri olarak hareket eden Rusya’nın niyetinin ABD’nin siber üstünlüğünü bastırmak olduğu şeklinde yorumlanmaktadır. Teklif edilen antlaşmanın uygulanamaz olduğuna, pratik olmadığına, sivil özgürlükleri ve ifade özgürlüğünü ihlal ettiğine yönelik endişelerinden dolayı ABD, bu teklife itiraz etmiştir.⁷ Çoğunlukla Rusya’nın önderlik ettiği BM’deki çabalar, ABD, Almanya ve diğer ülkelerin kayda değer katılımıyla, tartışma için platform sağlamış ve siber faaliyetler için çeşitli normların ortaya çıkmasına imkân vermiştir. Siber savaşla ilgili olarak, üç kritik aday norm bulunmaktadır: siber silahların tamamen yasaklanması, siber silahların ilk kullanımının yasaklanması ve devlet dışı aktörlerin o ülkenin toprağı üzerinden siber saldırı yapmasına engel olma zorunluluğudur.

NATO, siber savaş için ortaya çıkmakta olan normları teşvik etmek için hükümetler arası bir ana yapı ve organizasyon platformu olarak da hizmet vermiştir. 2007’de Estonya’ya ve 2008’de Gürcistan’a yapılan büyük siber saldırıların ardından NATO, siber savaş tehdidine daha ciddi bir şekilde eğilmiştir. NATO, 2008’de Siber Savunma Mükemmeliyet Merkezi’ni kurmuş, araştırma, eğitim ve danışmanlık yoluyla NATO’nun siber savunmasını geliştirmeye odaklanmıştır. 2012 yılında, organizasyon, üye ülkelerin ulusal siber savunma politikalarını daha iyi geliştirmelerine yardımcı olmak için Ulusal Siber Güvenlik Çerçeve Kılavuzu’nu yayımlamıştır.⁸ 2010 yılının

⁶ Jeffrey Carr , **Inside Cyber Warfare: Mapping the Cyber Underworld**, O'Reilly Media; 2 edition (31 Dec. 2011), s.34

⁷ Tim Maurer, Cyber Norm Emergence at the United Nations, **Explorations in Cyber International Relations Discussion Paper Series**, Belfer Center for Science and International Affairs, 2011, s.17

⁸ Alexander Klimburg, **National Cyber Security Framework Manual**, NATO CCD COE Publications, December 2012, s.4

Kasım ayında NATO, siber savaşın ulusal ve Avrupa-Atlantik refahını, güvenliğini ve istikrarını tehdit eden bir eşiğe ulaşabileceğini kabul eden yeni bir stratejik kavramı kabul etmiştir. Genel olarak, Amerika Birleşik Devletleri öncülüğünde NATO, Rusya'nın BM'de önerdiği gibi daha kapsamlı ve yeni kısıtlamalar getirmekten ziyade, mevcut silahlı çatışma hukuku kurallarını siber saldırılara uygulamak isteyen bir bakış açısıyla siber savaşa yaklaşmıştır.⁹ NATO'nun bu çalışmadaki en önemli faaliyeti, Siber Savaş Uygulanacak Uluslararası Hukukla ilgili Tallinn El Kitabının geliştirilmesi olmuştur. Resmi NATO görüşünü yansıtmayan, yazarların kişisel görüşünü ("uluslararası bir uzmanlar grubu") yansıtan Tallinn Manual, Siber Savunma Mükemmeliyet Merkezi ve gözlemci olarak hareket eden NATO, Siber Komutanlık ve Uluslararası Kızılhaç Komitesi tarafından desteklenmiştir.

Tallinn El Kitabı* yalnızca NATO'ya bağlı katılımcıların ortak görüşünü değil, aynı zamanda ABD hükümetinin de temel duruşunu temsil etmektedir. ABD Dışişleri Bakanlığının Eylül 2012'de yapmış olduğu açıklamalar Tallinn El Kitabı'nda belirtilen ve bu bölümde açıklanacak görüşlerle tutarlıdır. İlave olarak, 2011 ABD "Uluslararası Siber Alan Strateji Belgesinde", devlet davranışını yönlendiren ve uzun süredir devam eden uluslararası normların (barış ve çatışma zamanlarında) siber savaş için de geçerli olduğunu belirtmiştir. Tallinn El Kitabı, ABD'nin uluslararası çatışma hukukunun siber savaş için yeterli ve uygulanabilir olduğu görüşünü ortaya çıkarmakta ve siber savaşın yeni ve farklı uluslararası normlar ve anlaşmalar gerektirdiği yönündeki Rusya'nın tutumunu reddetmektedir. BM ve NATO'ya ek olarak, bazı devletler bireysel olarak, siber savaş normlarını tartışmak için çok taraflı forumlar düzenleyerek norm girişimcisi ve norm lideri haline gelmiştir. Siber savaş için çeşitli aday uluslararası normlar ortaya çıkmaya başlarken, devletler de gittikçe daha fazla büyüyen siber tehditle boğuşmaya devam etmektedir.

⁹ Schmitt Micheal, **The Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge University Press, New York, 2017, s.16-24

*Tallinn El Kitabı: NATO Siber Savunma Mükemmeliyet Merkezi tarafından Uluslararası Bağımsız Uzmanlar Grubu'na mevcut uluslararası hukuk normlarının, siber savaş haline ne ölçüde uygulanacağına ilişkin hazırlamış oldukları dokümandır.

2.3.SİLAHLI ÇATIŞMA HUKUKU VE SİBER ALAN

2.3.1 Kuvvet Kullanma Yasağı:

Uluslararası hukukta, kuvvete başvurma hakkı (jus ad bellum) ile kuvvete başvurulduğunda uyulması gereken kurallar (jus in bello) arasında bir ayrım bulunmakta ve bu ayrıma bağlı olarak silahlı çatışma hukuku kuralları uygulanmaktadır.

Birleşmiş Milletler Anlaşmasının 2.maddesinin 4.fikrasına göre; “*Teşkilatın üyeleri, milletlerarası münasebetlerinde gerek bir başka devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı, gerekse Birleşmiş Milletlerin amaçları ile telif edilemeyecek herhangi bir surette, tehdide veya kuvvet kullanılmasına başvurmaktan kaçınırlar*”. Bu yasak “müdahale yasağı” (non-intervention) olarak tanımlanmıştır. Yasaklanmış olan kuvvet kullanmanın silahlı kuvvet kullanma olduğu yönünde hiç şüphe yoktur. Kullanılacak silahlı kuvvet devletin kendi silahlı kuvvetleri olabileceği gibi devlet tarafından desteklenen veya yardım edilen silahlı gruplar aracılığıyla dolaylı kuvvet kullanma da olabilir. Son dönemde devletler destekledikleri silahlı gruplar aracılığı ile vekâlet savaşları olarak adlandırılan dolaylı kuvvet kullanma yöntemini tercih etmektedirler. Uluslararası Adalet Divanı “*Nikaragua’da Askeri ve Yarı Askeri Faaliyetler Davası*” kararında ve Birleşmiş Milletler Genel Kurulu’nun 2625 sayılı Dostça İlişkiler Bildirisi’nde düzenli olmayan kuvvetler aracılığı ile başka bir devletin ülkesinde kuvvet kullanmanın Birleşmiş Milletler Anlaşmasının 2.maddesinin 4.fikrasına göre yasak kapsamında olduğu belirtilmiştir.¹⁰

Silahlı zararlar-karşılık eylemleri Birleşmiş Milletler Genel Kurulu’nun 2625 sayılı kararına göre Birleşmiş Milletler Anlaşmasının 2.maddesinin 4.fikrasına göre yasak kapsamında kabul edilmiştir. Ekonomik nitelikli zorlama yollarına başvurma kuvvet kullanma olarak değerlendirilmemektedir.

Birleşmiş Milletler Anlaşmasında kuvvet kullanmanın iki istisnası vardır. Birincisi Birleşmiş Milletler Anlaşmasının 51. maddesi çerçevesinde “*Meşru Müdafaa*”, ikincisi ise “*Birleşmiş Milletler Güvenlik Konseyi’nin bu yasağı ihlal eden*

¹⁰ Hüseyin Pazarcı, **Uluslararası Hukuk**, Gözden Geçirilmiş 3.Bası, Turhan Kitabevi, Ankara 2014, s.517-519

devletlere karşı, münhasıran kuvvet kullanma” yetkisidir. Birleşmiş Milletler Anlaşmasının 42. Maddesi ile takip eden maddeleri hukuka aykırı olarak kuvvet kullanan devletlere karşı Birleşmiş Milletler Güvenlik Konseyi’ne kuvvet kullanma yetkisi vermektedir.

2.3.2.Martens Hükümü:

Silahlı çatışma hukukunun siber saldırılara uygulanması problem teşkil etmektedir. Hague Sözleşmesi IV, 1949 Cenevre Sözleşmesi ve I. Ek Protokolde, silahlı çatışma hukukunun yetersiz kalması durumunda uluslararası hukukun ilkelerinin uygulanacağı belirtilmektedir. Hüküm şu şekildedir; “savaş yasaları tamamlanana kadar, Yüksek Akit Taraflar kendilerince kabul edilen sözleşmeler hükümlerinin kapsamadığı durumlarda toplulukların ve savaşların uygar uluslararası yerleşmiş uygulamalardan, insanlık yasalarından ve kamu vicdanının gereklerinden kaynaklanan uluslararası hukukun ilkelerinin etkisi altında bulunduklarını saptamaya uygun addetmektedir.” Uluslararası teamül hukuk kuralı olan Martens Hükümüne göre silahlı çatışma sırasında icra edilen siber saldırılar hukuk dışıdır.

2.3.3.Kuvvet Kullanmanın Hukuka Uygun Olduğu Durumlar

2.3.3.1.Meşru Müdafaa Hakkı:

Birleşmiş Milletler Anlaşmasının 2.maddesinin 4.fıkrası kuvvet kullanılmasını ve kuvvet kullanma tehdidinde bulunulmasını açıkça yasaklamasına rağmen meşru müdafaa hakkı bu yasağın kapsamı dışında tutulmuş ve devlete 51. madde çerçevesinde bireysel ve kolektif meşru müdafaa hakkı tanınmıştır. Birleşmiş Milletler Anlaşmasının 51. maddesi aynen şöyle kaleme alınmıştır:

“işbu Andlaşmanın hiçbir hükmü, Birleşmiş Milletler Üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi Milletlerarası barış ve güvenliğin muhafazası için lüzumlu tedbirleri alıncaya kadar, tabii olan münferit veya müşterek meşru müdafaa hakkına hanel getirmez. Bu meşru müdafaa hakkını kullanarak Üyelerin aldığı tedbirler derhal Güvenlik Konseyi’ne bildirilir ve Konseyin, işbu Andlaşmaya dayanarak milletlerarası barış ve güvenliğin muhafaza veya iadesi için

lüzumlu göreceği şekilde her an hareket etmek yetki ve ödevine hiçbir vesile tesir etmez.”

Birleşmiş Milletler Anlaşmasının 51.maddesine göre bir devletin meşru müdafaa hakkına başvurabilmesi için silahlı bir saldırıya hedef olması gerekmektedir. Bu durumda hangi eylemlerin saldırı olarak kabul edileceği sorusu akla gelmektedir. Birleşmiş Milletler Genel Kurulu’nun 3314 (XXIX) sayılı ve 1974 tarihli Kararı’nın 3. Maddesinde saldırının tanımı kabul edilmiştir.¹¹ Kabul edilen tanıma göre saldırı; *“bir başka devletin egemenliğine, ülke bütünlüğüne ya da siyasi bağımsızlığına karşı ya da BM Şartı’na aykırı herhangi bir biçimde silahlı kuvvet kullanma”* olarak tanımlanmıştır.

Bu karara göre; bir devletin topraklarının istilası, ilhakı, bombardıman edilmesi, bir devletin silahlı kuvvetiyle başka bir devletin silahlı kuvvetine saldırması, anlaşma gereği başka bir ülkede bulunan silahlı kuvvetlerin anlaşmaya aykırı olarak kullanılması, anlaşma sona ermesine rağmen ülkeyi terk etmemesi ve ülkesini üçüncü bir devlete saldırı için başka bir devletin kullanılmasına izin vermesi saldırı olarak tanımlanmıştır.

Bu tanımdan hareketle örneğin, konvansiyonel silahlarla yapılan saldırılar Birleşmiş Milletler Anlaşması 2.maddesinin 4.fıkrası kapsamına girmektedir. Doğrudan fiziksel bir tahribata veya insanları öldürmeye veya yaralamaya yönelmiş siber saldırılar da silahlı kuvvet kullanma kabul edilmekte bu yüzden yasak kapsamına girmektedir. Diğer taraftan Birleşmiş Milletler Anlaşma taslağının görüşülmesi sırasında gelişmekte olan ülkelerin ekonomik zorlamaları 2.maddenin 4.fıkrası kapsamına dâhil edilmesi çabalarına rağmen bu tür uygulamalar özellikle fıkra kapsamı dışında tutulmuştur. Bu nedenle Birleşmiş Milletler Anlaşması’nın 2.maddesinin 4.fıkrasının metnine veya metnin kabul edilmesi sırasındaki görüşmelere dayanan yorumlarda “ekonomik ve politik zorlama” kuvvet kullanma kapsamı dışında tutulmalıdır. Elektronik karıştırma ve engelleme gibi fiziksel hasara neden olmayan siber saldırılarla ekonomik ambargo gibi ekonomik ve politik zorlamalar aynı etkiye sahiptir. Bu nedenle fiziksel hasara neden olmayan siber saldırıların Birleşmiş

¹¹ **United Nations General Assembly Resolution 3314 (XXIX)**, (çevrimiçi) <http://hrlibrary.umn.edu/instreet/GAres3314.html>, 14.02.2019

Milletler Anlaşmasının 2. madde 4. fıkrası kapsamına girmesinin mümkün olmadığı sonucuna varılabilir.

Uluslararası silahlı çatışma hukuku 2007 yılında Estonya'ya karşı yapılan siber operasyonlara uygulanmamıştır, çünkü durum silahlı çatışma seviyesine erişmemiştir. 2008 yılında Rusya ve Gürcistan arasındaki uluslararası silahlı çatışma esnasında icra edilen siber saldırılara uluslararası silahlı çatışma hukuku uygulanmış ve Gürcistan açısından meşru müdafaa hakkı doğmuştur çünkü siber saldırılar silahlı çatışmayı kolaylaştırmıştır. Bu iki örnek değerlendirildiğinde; Uluslararası Silahlı Çatışma Hukuku'nun herhangi bir siber saldırıya uygulanabilmesi için bu saldırı ile Uluslararası Silahlı Çatışma Hukuku kurallarının uygulandığı uluslararası silahlı çatışma arasında nedensellik bağının bulunması gerekmektedir. Ayrıca Silahlı Çatışma Hukuku çatışmanın uluslararası veya uluslararası olmayan nitelik taşımasına bağlı olarak uygulanmaktadır.

Birleşmiş Milletler Uluslararası Adalet Divanı Nikaragua kararında, bir devletin başka bir devlete karşı savaştan gerillayı finanse etmesini kuvvet kullanma olarak görmemiştir.¹² Bu karardan yola çıkarak örneğin isyancılarla birlikte bir devlete karşı siber saldırı yapan bilgisayar korsanının (hacker) başka bir devlet tarafından finanse edilmesi kuvvet kullanma olmayacaktır.

Yine Birleşmiş Milletler Uluslararası Adalet Divanı Nikaragua kararında, bir devletin başka bir devlete karşı savaştan gerillaları silahlandırmasını ve eğitmesini kuvvet kullanma olarak nitelemiştir.¹³ Bu karara göre bir devletin kendi çıkarlarını gerçekleştirmek için başka bir devlete karşı siber saldırıda bulunmak için organize olmuş bir gruba kötü amaçlı yazılım “Malicious software”(virüsler, trojanlar, Truva atları vb.) ve eğitim vermesi kuvvet kullanma olarak nitelenebilecektir.

Bir devletin, kuvvet kullanma derecesine varacak şekilde siber saldırılar yapan bir gruba kendi sınırları içinde güvenli bir bölge(safe haven) sağlaması durumunda ne olacaktır sorusu akla gelecektir. Bu durumda uluslararası hukuk uzmanları, devlet dışı aktörlerin eylemlerini kuvvet kullanma olarak ilgili devlete atfetmek için tek başına

¹² International Court of Justice, **Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)**, (Çevrimiçi) <https://www.icj-cij.org/en/case/70>, 12.02.2019

¹³ International Court of Justice, **Nicaragua Judgement**

güvenli bir bölge sağlamanın yeterli olmadığı görüşündedirler. Ancak güvenli bir bölge sağlamaya ilave olarak örneğin devlet dışı aktöre önemli bir destek veya siber savunma sağlanırsa belli durumlarda kuvvet kullanma olacağı değerlendirilmektedir.

2.3.3.2. Birleşmiş Milletler Güvenlik Konseyi'nin Münhasıran Kuvvet Kullanması

Birleşmiş Milletler Anlaşmasının 42. maddesine göre “*Güvenlik Konseyi, 41. maddesinde öngörülen önlemlerin yetersiz kalacağı ya da kaldığı kanısına varırsa, uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için, hava, deniz ya da kara kuvvetleri aracılığıyla, gerekli saydığı her türlü girişimde bulunabilir. Bu girişimler gösterileri, ablukayı ve Birleşmiş Milletler üyelerinin hava, deniz ya da kara kuvvetlerince yapılacak başka operasyonları içerebilir.*” bu hükümdeki şartların oluşması durumunda Güvenlik Konseyi kuvvet kullanmaya karar verebilecektir. Güvenlik Konseyi'nin münhasıran kuvvet kullanması tez konusuyla doğrudan ilişkili olmadığından üzerinde durulmayacaktır.

2.3.4. Siber Saldırıları ve Kuvvet Kullanma Yasağı

Bir siber saldırının kuvvet kullanımına ilişkin yasağı ihlal edip etmediğini belirlemek, (i) uluslararası hukukta kuvvetin nasıl yorumlandığını ve (ii) siber saldırıların bu düzeye ulaşp ulaşmadığını tespit etmeyi gerektirmektedir. Birleşmiş Milletler Anlaşması, antlaşmaların yorumlanması için kurallar içeren 1969 tarihli Viyana Antlaşmalar Hukuku Sözleşmesi kapsamında incelenmelidir. Uluslararası hukuk uzmanları genellikle Birleşmiş Milletler Anlaşmasının geleneksel uluslararası hukuku yansıttığı konusunda hem fikirdirler.

1969 tarihli Viyana Antlaşmalar Hukuku Sözleşmesinin 31. maddesine göre “*Bir antlaşma, hükümlerine antlaşmanın bütünü içinde ve konu ve amacının ışığında verilecek alelade manaya uygun şekilde iyi niyetle yorumlanır.*”¹⁴ Kuvvetin tanımı kinetik saldırı dışında diğer zorlayıcı önlemleri de içermektedir. Diğer zorlayıcı önlemler: ekonomik araçlar, diplomatik araçlar, ideolojik veya propaganda araçlarıdır. Askeri, ekonomik, diplomatik ve ideolojik araçların her biri Birleşmiş Milletler

¹⁴ **Viyana Antlaşmalar Hukuku Sözleşmesi**, 1969, (çevrimiçi), <https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf>, 24.12.2018

Anlaşması dikkate alınarak yorumlanmalıdır. Birleşmiş Milletler Anlaşmasının konu ve amacı ışığında kuvvetin dar olarak yorumlanması gerekmektedir. Birleşmiş Milletlerin amacı uluslararası barış ve güvenliği sağlamanın yanı sıra “gelecek nesilleri savaş tehlikesinden korumaktır. Kuvvet kavramının tanımı 1945’te askeri araçlarla sınırlı olarak yapılmıştır. Birleşmiş Milletler Anlaşması taslağı da bu sonucu pekiştirmektedir. Birleşmiş Milletler Anlaşmasının hazırlık çalışmalarında, 2.madde 4.fıkrasının kapsamını diğer zorlayıcı araçlara, özellikle de ekonomik zorlamaya genişletmek için Brezilya’nın bir teklif sunduğunu ancak kabul edilmediğini göstermektedir.¹⁵ Ekonomik zorlama, Birleşmiş Milletler Anlaşmasının 2.madde 4.fıkrasının hazırlık çalışmasında kuvvet tanımından açıkça dışlanmıştır. Böylece ideolojik ve diplomatik araçlar da kuvvet tanımına dâhil edilmemiş bir devletin kuvvet kullanıp kullanmadığının tespitinin yalnızca askeri araçlara sınırlı olarak yapılacağı kararlaştırılmıştır.

Birleşmiş Milletler Anlaşmasının kuvvet tanımını dar olarak yorumlamış olduğunu tespit etmiş olmak incelemeyi sonuçlandırmayacaktır. Zira Uluslararası Adalet Divanı, kuvveti tanımlamak için Birleşmiş Milletler Anlaşmasının tek başına yeterli olmadığını, uluslararası teamül hukukuna göre tanımlamanın yapılmasının uygun olduğuna karar vermiştir.

2.3.5.Araç, Hedef ve Etki Odaklı Yaklaşım:

Siber saldırıların ne zaman saldırı olarak kabul edileceği ile ilgili üç görüş bulunmaktadır.¹⁶

2.3.5.1.Araç Odaklı Yaklaşım:

Siber saldırılarda kullanılan araçlar klasik askeri anlamda silah olarak kabul edilmediğinden Birleşmiş Milletler Anlaşmasının 51. maddesi kapsamındaki silahlı saldırı kapsamında değerlendirilemez. Askeri bir saldırı ile birlikte veya askeri saldırıyla koordineli olarak siber saldırı ya da siber saldırı aracılığıyla konvansiyonel silah kullanılıyorsa silahlı saldırı olarak kabul edilebilir. Siber saldırı ile yönlendirilen

¹⁵ **BM Şartı Hazırlık Görüşmeleri**, 1945, (çevrimiçi), <https://digitallibrary.un.org/record/1300969/files/UNIO-Volume-21-E.pdf>, 24.12.2018

¹⁶ Oona A. Hathaway, et.al, “The Law of Cyber Attack”, **California Law Review**, Vol. 100, No.4, s.845.

bir patlayıcının o ülkedeki önemli bir bilgisayarlı komuta veya yönetim merkezini hasara uğratması ve bu silahlı saldırının Birleşmiş Milletler Uluslararası Adalet Divanı'nın Nikaragua kararında ortaya koyduğu kritere uygun olması durumunda silahlı saldırı olarak nitelendirilebilmektedir. Birleşmiş Milletler Uluslararası Adalet Divanı Nikaragua kararında “yeterli ağırlık” kriterini ortaya atmıştır. Birleşmiş Milletler Uluslararası Adalet Divanı bu kriteri “*bir devletin başka bir devletin topraklarına silahlı çeteler göndermesi halinde, bu çetelerin silahlı saldırılarının düzenli orduların saldırıları ile aynı şiddet ve ölçekte olması şartıyla, Birleşmiş Milletler Anlaşmasının 51. maddesi çerçevesinde bir ‘silahlı saldırı’ olabileceğini kabul ederek, ‘silahlı saldırının’ tanımlanmasında bir ‘büyüklük ve etki’ testi ortaya koymuş; ‘yeterli ağırlık (sufficient gravity)’ koşulu getirmiştir*” şeklinde açıklamıştır.¹⁷

2.3.5.2. Hedef Odaklı Yaklaşım:

Siber saldırı ile örneğin ülkedeki enerji şebekesini kontrol eden veya hava ulaşımını kontrol eden kritik öneme sahip bir bilgisayar sisteminin hedef alınması saldırı olarak kabul edilmektedir. Böylece devletlere ulusal kritik alt yapıları koruma imkânı sağlanmaktadır. Bu yaklaşıma uygun olarak Matthew Hoisington şöyle bir öneri ortaya atmıştır; “Uluslararası toplum bir devletin aktif savunma ile koruyabileceği kritik ulusal altyapının listesini yayımlamalı, eğer listede tanımlanan kritik altyapı siber saldırıya maruz kalırsa saldırıya maruz kalan devlet meşru müdafaa ile karşılık verebilir.”¹⁸ Ancak bu yaklaşımın dezavantajı, kritik alt yapı sistemlerine yapılacak siber saldırılara karşı meşru müdafaa kapsamında kullanılacak fiziksel ve kinetik saldırıları meşrulaştırma, meşru müdafaa hakkı gerekçesiyle devletlerin aşırı kuvvet kullanmasına yol açma ve yıkıcı konvansiyonel silahlı çatışmalara sebep olma ihtimalidir.¹⁹

¹⁷ Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, **Research Publication 1 Information Series**, 1999, s.21-22

¹⁸ Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, **Boston College International and Comparative Law Review V.32**, s. 444-454

¹⁹ Matthew J. Sklerov, “Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent”, **Military Law Review, V.201, 2009**, s.56

2.3.5.3.Etki Odaklı Yaklaşım

Bu yaklaşım bu bölümün devamında ayrıntılı olarak bahsedilecek Talinn modeline de dayanak teşkil etmektedir. Bir siber saldırının, saldırı olarak kabul edilebilmesi için belirlenmiş olan kriter siber saldırının meydana getirdiği etkinin ağırlığına (gravity) bağlıdır. Bu yaklaşım uluslararası çevrelerde de en çok taraftar bulan yaklaşımdır. Siber saldırının etkisinin ağırlığının nasıl tespit edileceği hususunda değişik yaklaşımlar bulunmaktadır. Talinn modeli bunlardan biridir. 2009 yılında ABD ve Kanada’da meydana gelen bir haftalık elektrik kesintisine neden olan yazılım, 2007’de Estonya devlet kurumlarını hedef alan saldırı ve 2009’da İran nükleer tesislerini hedef alan virüs örneklerine baktığımızda bunlardan hangisinin meşru müdafaa amaçlı kuvvet kullanmak için yeterli ağırlık derecesine ulaşmış olduğunu belirlemek çok kolay bir işlem değildir.

2.3.6.Talinn Modeli:

Tallinn El Kitabı 2.0, mevcut uluslararası hukukun siber alan için nasıl uygulandığına dair en kapsamlı analizdir. On dokuz uluslararası hukuk uzmanı tarafından 2013 yılında yazılan “Siber Saldırlara Uygulanabilir Uluslararası Hukuk Üzerine Tallinn El Kitabı ” 2017 yılında güncellenmiş ve genişletilmiş ikinci baskısı “Siber Saldırlara Uygulanabilir Uluslararası Hukuk Üzerine Tallinn El Kitabı 2.0” Cambridge Üniversitesi Yayınları'nda (© Cambridge Üniversitesi Yayınları 2017) hem basılı hem de elektronik kopyalarda bulunmaktadır.²⁰ Tallinn El Kitabı 2.0'ın hazırlanması, NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi tarafından kolaylaştırılmış ve yürütülmüştür.

2.3.6.1.Siber Altyapının Kontrolü

Bir devlet, kendi toprağında veya münhasıran kendi kontrolü altında bulunan siber altyapının, diğer devletlere olumsuz ve yasadışı olarak etki edecek eylemlerde kullanılmasına bilerek izin vermemelidir.

²⁰ Michael N. Schmitt et.al, **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, Second Edition, Cambridge University Press 2017

Bu siber altyapı iki kategoride değerlendirilir: (i) kendi toprağında bulunan herhangi bir siber altyapı ve (ii) başka bir yerde bulunan, ancak söz konusu devletin münhasıran yasal veya fiili kontrolünde bulunan siber altyapı.

Egemen eşitlik ilkesi, tüm devletlerin diğer devletlerin ülkesi üzerindeki egemenliğine saygı duyma zorunluluğunu gerektirmektedir. Uluslararası Adalet Divanı, Nikaragua davasında, *“toprak bütünlüğüne saygının, bağımsız devletler arasında uluslararası ilişkilerin kurulmasının temeli olduğuna”* karar vermiştir.

Uluslararası Adalet Divanı'nın Korfu Kanalı kararında belirttiği gibi, başka bir devletin egemenliğine saygı gösterme yükümlülüğü, bir devletin *“ülkesini başka devletlerin haklarına aykırı davranışlarda kullanılmasına bilerek izin vermemeyi”* gerektirmektedir.²¹ Devletlerin egemenlik haklarını korumak için uluslararası hukuka uygun davranışlarda bulunması gerekmektedir. Bu zorunluluk sadece diğer devletlere zarar veren ve suç sayılan eylemler için değil, aynı zamanda örneğin hedef devletin ülkesi üzerindeki egemenliği nedeniyle koruması altında bulunan kişi ve nesnelere karşı ciddi zararlar meydana getiren veya ciddi zararlar meydana getirme potansiyeli olan faaliyetler için de geçerlidir.

Bu gereklilikler, zararlı siber davranışların doğası, özellikle zaman ve mekân sıkıştırması ve sıklıkla benzeri görülmemiş karakterleri nedeniyle karmaşık hale gelmiştir. Bir devletin başka bir devlete zarar gelmesini önlemesinin mümkün olmadığı durumlar olabilir. Örneğin, A Devletinin, topraklarından B Devlete karşı siber bir saldırı hazırlığı yapıldığını ve başlatılacağını bildiğini varsayalım. Ancak, A Devleti saldırının kesin zamanı ve hedefini bilmediğinden, *“ülkesini başka devletlerin haklarına aykırı davranışlarda kullanılmasına bilerek izin vermeme”* ilkesi kapsamında yapabileceği tek şey saldırıda kullanılacak ağı tecrit etmek olabilir. A Devleti, bunu yaptığında bu ağı kullanan kendi siber altyapı hizmetleri de işlemez hale gelecektir. Bu düzeltici önlemin gerekip gerekmediğini belirlemek için her iki devletin uğrayacağı potansiyel zararın niteliği, ölçeği ve kapsamı değerlendirilmelidir.

²¹ International Court of Justice, **Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)**, (çevrimiçi) <https://www.icj-cij.org/en/case/1>, 21.02.2019

Uygulama kapsamında, bu kural, yasadışı olan ve başka bir devlet üzerinde zararlı etkileri olan tüm eylemleri kapsamaktadır. Yasadışı terimi, etkilenen devletin yasal haklarına aykırı bir faaliyet anlamına gelmektedir. Diğer devletlerin haklarını etkileyen ve başka bir devletin toprakları üzerinde zararlı etkileri olan bir devletin topraklarından gelen tüm siber faaliyetleri kapsadığını vurgulamak için kasten, yasağın kuvvet kullanımı²² veya silahlı saldırı²³ gibi daha dar kavramlarla sınırlandırılmamasını tercih edilmiştir. Özellikle, söz konusu siber saldırıların nesnelere fiziksel hasar vermesi veya bireylerin yaralanmasıyla sonuçlanması şartı yoktur; sadece olumsuz bir etki yaratması yeterli görülmektedir.

Örneğin, başka bir devlete saldırı yapmak için siber altyapının bir terörist grup tarafından kullanılmasına izin veren bir devlet kuralı ihlal etmiş olacak veya başka bir devlet tarafından bu eylemin yapıldığına dair bir bildirimde bulunulmasına rağmen eylemi sonlandırmak için devletin makul ölçüde uygun önlem almada başarısız olması da kuralı ihlal edecektir.

Talin El Kitabı'nı hazırlayan uzmanlar, ilgili eylemlerin sadece geleceğe yönelik olduğu durumların bu kural kapsamında olup olmadığı konusunda fikir birliğine varamamıştır. Uzmanlardan bazıları, devletlerin onları engellemek için makul önlemler alması gerektiği konusunda fikir beyan etmiştir. Diğerleri, sadece siber bağlamda değil, olası tüm tehditlere karşı kapsamlı ve etkili savunma yapılmasının zorluğu nedeniyle önleme görevinin bulunmadığını ileri sürmüştür.²⁴

Bu kural ayrıca, bir hükümetin münhasır kontrolü altındaki siber altyapıdan başlatılan uluslararası hukuka aykırı davranışlar için de geçerlidir. Altyapının ilgili devletin topraklarının dışında olduğu durumlarda ise yine de bu devletin o altyapının üzerinde münhasır kontrolü bulunmaktadır. Örneğin, temel bir anlaşma uyarınca bir ülkedeki yabancı devletin kontrolüne tabi askeri bir tesis, açık denizlerdeki platformlar, uluslararası hava sahası veya diplomatik binalar.

Bu kural, devlet organları veya devlet kontrolü altındaki bireyler tarafından üstlenilebilen ilgili düzeltici siber operasyonlara(siber saldırıların etkilerini gidermek

²² Schmitt, **a.g.e.**, s.47

²³ Schmitt, **A.e.**, s.52

²⁴ Micheal N.Schmitt et.al, **Talinn Manual**, s.33

için yapılan) da uygulanır. Talin El Kitabı'nı hazırlayan uzmanlar, düzeltici eylemin özel bir kuruluş örneğın özel bir internet servis sağlayıcısı tarafından gerçekleştirilebilmesi halinde, devlet, bu kuruluşun faaliyetini sona erdirmek için gerekli tüm araçları kullanmakla yükümlüdür.

Devletin söz konusu eylemler hakkında gerçek bilgiye sahip olması durumunda ancak bu kural uygulanır. Örneğın istihbarat teşkilatı gibi devlet organı, kendi topraklarından kaynaklanan bir siber saldırıyı tespit ettiğinde veya devlet topraklarından siber bir saldırı yapılacağı konusunda güvenilir bir bilgi almışsa devletin gerçek bilgiye sahip olduğu kabul edilmektedir.

Bir devletin kendi topraklarındaki siber faaliyetleri kontrol etmede başarısız olması ve bu nedenle söz konusu eylemlerden habersiz olması durumunda bu kuralı ihlal edip etmediğı belirsizdir. Bilgi yeterli olsa bile, atfetme zorluğu, bir veya daha fazla hedefe koordine ve dağıtık bir saldırının parçası olarak ayrı olay setlerini ilişkilendirmenin zorlukları ve siber altyapının aldatmaya kolaylık sağlaması sebebiyle siber bağlamda gerekli kontrolün sınırı belirli değildir.

A devletinde bulunan bilgisayarları kullanarak B devleti siber altyapısı üzerinden yönlendirilmiş siber operasyonla C devetine zarar verilmesi durumunda üzerinden yönlendirme yapılan B Devetine(transit devlet) bu kuralın uygulanıp uygulanmayacağı konusunda fikir birliğine varılamamıştır. Talin El Kitabı'nı hazırlayan uzmanlar, siber operasyonda transit devletin suç işleyenden haberi olduğu ve buna son verme imkânına sahip olduğu ölçüde bu eyleme son vermesi gerektiğı yönünde fikir beyan etmiştir. Bununla birlikte, bu uzmanlar, siber yayınların yönlendirme sürecine dikkat çekmektedirler. Örneğın, bir iletinin bir ağın düğümünde engellenmesi durumunda, genellikle farklı bir iletim yoluna sıklıkla da farklı bir devlet üzerine yönlendirilmektedir. Böyle bir durumda, bu Talin El Kitabını hazırlayan uzmanlar transit devletin operasyonun sonucuna anlamlı bir etkisi olmayacağından harekete geçme zorunluluğının bulunmadığı konusunda fikir birliği içindedir. Diğer uzmanlar, kuralın yalnızca devletin kendi topraklarından veya münhasıran kontrolü

altındaki topraklardan operasyonun başlatıldığı durumlarda uygulanacağı konusunda fikir birliğine varmıştır.²⁵

Eğer bir devlet bu kural uyarınca gerekli adımları atmazsa, mağdur devlet, orantılı tepkilere başvurarak uluslararası hukukun ihlaline yanıt verme hakkına sahip olabilir. Bunlar, uygun olan hallerde karşı önlemleri²⁶ ya da meşru savunmada kuvvet kullanımını içerebilir.²⁷

2.3.6.2.Tehdit ve Kuvvet Kullanımı Yasağı

Birleşmiş Milletlerin amaçlarına aykırı olarak bir devletin bağımsızlığına veya toprak bütünlüğüne karşı bir tehdit veya kuvvet kullanımı oluşturan siber bir saldırı uluslararası hukuka aykırıdır.

Birleşmiş Milletler Anlaşmasının 2. Maddesi 4. fıkrası, “*Birleşmiş Milletlerin tüm üyelerinin, uluslararası ilişkilerinde herhangi bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı kuvvet kullanma veya kuvvet kullanma tehdidinden veya Birleşmiş Milletlerin Amaçlarına aykırı bir başka davranıştan uzak durmasını öngörür.*”. Bu yasak uluslararası teamül hukukunun bir normudur.

Bir devletin bağımsızlığına veya toprak bütünlüğüne karşı tehdit veya kuvvet kullanımının yasaklanmasına ek olarak, Birleşmiş Milletler Anlaşmasının hazırlık çalışmalarında 2. maddenin 4. fıkrasının tehdit veya kuvvet kullanımına atıfta bulunmasının “*Birleşmiş Milletler amaçlarıyla*” (Anlaşmanın 1. maddesinde ortaya konmuştur) uyumlu olarak herhangi bir tehdit veya kuvvet kullanımı için bir yasadışılık varsayımı yaratması amaçlanmıştır. Başka bir deyişle, bir devletin bağımsızlığına veya toprak bütünlüğüne karşı yönlendirilmeyen eylemler bile, Birleşmiş Milletlerin amaçlarına aykırılık halinde yasağı ihlal edebilir. Yukarıda da bahsedildiği gibi kuvvet kullanımının yasaklanmasına dair iki genel istisna vardır - Güvenlik Konseyi tarafından Birleşmiş Milletler Anlaşması Bölüm VII uyarınca yetkilendirilen kuvvet kullanımı ve yine Anlaşmanın 51. maddesi ile uluslararası teamül hukukuna göre meşru müdafaa hakkıdır.

²⁵ Micheal N.Schmitt et.al, **Talinn Manual**, s.33-35

²⁶ Schmitt, **a.g.e**, s.40

²⁷ Schmitt, **A.e**, s.53

Kuvvet kullanımı olarak nitelendirilen bir eylemin mutlaka bir devletin silahlı kuvvetleri tarafından yapılması gerekmez. Örneğin, silahlı kuvvetler tarafından gerçekleştirilirse “kuvvet kullanımı” olarak nitelendirilecek bir siber saldırının, bir devletin istihbarat teşkilatı veya davranışları devlete atfedilebilecek özel bir yüklenici tarafından üstlenilmesi durumunda da aynı şekilde “kuvvet kullanımı” olacağı açıktır.

Birleşmiş Milletler Anlaşması 2. madde 4. fıkrası yalnızca Birleşmiş Milletler üyeleri için geçerli olmakla birlikte, yasaklama aynı zamanda uluslararası teamül hukuku olması nedeniyle üye olmayan devletleri de kapsamaktadır. Ancak, Anlaşmanın 2. madde 4. fıkrası ve muadili olan uluslararası teamül hukuku bir devlete bağlı olmadıkça, bireyler, örgütlü gruplar ve terör örgütleri dâhil olmak üzere devlet dışı aktörlerin eylemleri için geçerli değildir. Böyle bir durumda, devlet dışı aktörün eylemi devletle ilişkilendirilebilirse ihlal etmiş sayılan devlet dışı aktör değil devlet olacaktır. Devlet dışı aktörlerin eylemleri uluslararası ve devletlerin iç hukuku uyarınca yasadışı olabilir, ancak kuvvet kullanımına ilişkin yasağın ihlali olarak kabul edilemez.

Bir siber saldırının kuvvet kullanma seviyesine yükselmemesi, uluslararası hukuka uygun olmasını sağlamayacaktır. Özellikle, siber saldırı müdahale yasağının ihlal edilmesine neden olabilir. Müdahale yasağı Birleşmiş Milletler Anlaşmasında açıkça belirtilmemiş olsa da, Birleşmiş Milletler Anlaşmasının 2. maddesi 1. fıkrasında belirtilen devletlerin egemen eşitliği ilkesiyle dolaylı olarak açıklanmıştır. En önemlisi Dostça İlişkiler Deklarasyonu²⁸ olan çok sayıda anlaşmada ve Birleşmiş Milletler kararlarında müdahale yasağından bahsedilmiştir. Uluslararası Adalet Divanına göre müdahale yasağı ilkesi “uluslararası teamül hukukunun önemli bir parçası” dır.

Müdahale yasağı ilkesinin kesin kapsamı ve içeriği, tartışmaya konu olmaya devam etmektedir. Nikaragua davasında, Uluslararası Adalet Divanı, müdahale yasağı ilkesinin, doğrudan veya dolaylı olarak tüm devletlere veya devlet gruplarına diğer devletlerin iç veya dış işlerine müdahale etmelerini yasakladığını kabul ve onaylamıştır. Bu nedenle, egemen bir devletin bu egemenliğine dayalı olarak üzerinde

²⁸ Declaration on Principles of International Law Friendly Relations and Co-Operation Among States in Accordance with The Charter of The United Nations, (çevrimiçi) <https://www.un.org/ruleoflaw/files/3dda1f104.pdf>, 27.12.2018

serbestçe tasarruf edebileceği meseleler ancak yasaklı müdahalenin kapsamına girmektedir. Devletlerin serbestçe tasarruf edebileceği konular, dış politika ile ekonomik, politik, sosyal ve kültürel sistemle ilgili seçimlerdir. Örneğin, Uluslararası Adalet Divanı, kuvvet kullanılmamasına rağmen isyancılara para temin etmenin “şüphesiz ki Nikaragua'nın iç işlerine müdahale eylemi ” olduğuna karar vermiştir.²⁹

Siber müdahalelerin tamamının, uluslararası hukukun müdahale yasağını otomatik olarak ihlal etmediği açıktır; “sadece karışma müdahale değildir”. Nikaragua davasında Uluslararası Adalet Divanı tarafından belirtildiği gibi, “zorlayıcı yöntemler kullanıldığında müdahale yanlıştır”.³⁰ Talin El Kitabı'nı hazırlayan uzmanlar, zorlayıcı bir unsur barındırmayan siber casusluk ve siber istismar operasyonlarının müdahale yasağı ilkesini ihlal etmeyeceği sonucuna varmıştır. Başka bir devletin sistemlerine sızmak, müdahale yasağı ilkesini ihlal etmemektedir. Talin El Kitabı'nı hazırlayan uzmanlara göre, izinsiz girişlerin koruyucu sanal engellerin ihlal edilmesini(örneğin, güvenlik duvarlarının ihlal edilmesi veya şifrelerin kırılması) gerektirdiği durumlarda bile müdahale yasağı prensibi ihlal edilmeyecektir.³¹

Bununla birlikte, geniş siber saldırı yelpazesi içerisinde diğer siber eylemler dikkate alındığında değerlendirme daha karmaşık hale gelmektedir. Bu durumlarda, müdahale yasağı ilkesinin ihlal edilip edilmediğine, her bir vakanın durumuna bağlı olarak özellikle bir zorlama unsurunun bulunup bulunmadığına göre karar verilmelidir. İlerleyen kısımlarda açıklanacak ölçütlere göre Stuxnet virüsüyle yapılan ve İran'ın nükleer tesislerindeki santrifüjlerine zarar veren siber saldırının kuvvet kullanma seviyesine ulaştığı değerlendirilmektedir.

Kuvvet kullanımı eşiğinin altında kalan siber saldırıların, müdahale yasağı ilkesinin ihlali olarak nitelendirilmesi daha zor olmaktadır. Rejim değişikliği sağlamaya yönelik eylemler genellikle açık bir müdahale yasağı ihlali olarak tanımlanmaktadır. Dolayısıyla, bu tür eylemler siber vasıtalarla gerçekleştirildiğinde veya kolaylaştırıldığında zorlayıcı “siyasi müdahale” müdahale yasağı ihlalini

²⁹ Pazarcı, **a.g.e.**, s.517-519

³⁰ International Court of Justice, **Nicaragua Judgement**

³¹ Micheal N.Schmitt et.al, **Talinn Manual**, s.45-47

oluşturmaktadır. Sözü edilen durumlar, seçim arifesinde siber vasıtalarla çevrimiçi haber hizmetleri belirli bir taraf lehine değiştirilerek, yanlış haber yayılarak veya bir tarafın çevrimiçi hizmetleri kapatılarak seçimin veya kamuoyunun manipüle edilmesidir. 2016 yılında ABD Başkanlık Seçimlerinde Rusya'nın bu yönde müdahaleleri olduğuna yönelik delillerin elde edildiği tartışılmaktadır. Her zaman olduğu gibi, belirleyici olan zorlama olup olmadığıdır. Dolayısıyla, her türlü siyasi veya ekonomik müdahale biçiminin müdahale yasağı ilkesini ihlal etmediği açıktır.

2.3.6.3. Kuvvet Kullanımının Tanımlanması

Bir siber saldırının büyüklüğü ve etkileri kuvvet kullanma seviyesine ulaşan eylemlerle kıyaslanabilir olduğunda bu siber saldırı kuvvet kullanımı oluşturmaktadır.

Birleşmiş Milletler Anlaşması, bir eylemin ne zaman kuvvet kullanma sayılacağını belirleyen herhangi bir kriter ortaya koymamıştır. Talin El Kitabı'nı hazırlayan uzmanlar, kuvvet kullanımı için uygun eşiğin ne olduğuna ilişkin tartışmada, Uluslararası Adalet Divanı'nın Nikaragua Kararını dikkate almıştır. Bu yargılamada, Uluslararası Adalet Divanı, eylemlerin 'silahlı saldırı' seviyesine ulaşp ulaşmadığını belirlerken 'büyüklük ve etkilerin' dikkate alınması gerektiğini belirtmiştir.³² Talin El Kitabını hazırlayan uzmanlar, büyüklük ve etkilere odaklanmanın, kuvvet kullanımı olarak nitelendiren eylemlerle kuvvet kullanımı olarak nitelendirilmeyen eylemleri birbirinden ayırırken yararlı bir yaklaşım olduğunu düşünmektedirler. Diğer bir deyişle, “büyüklük ve etkiler”, bir siber saldırının kuvvet kullanımı olarak nitelendirilip nitelendirilmediğinin belirlenmesinde analiz edilecek nicel ve nitel faktörleri ifade eden kısa bir terimdir.

Tehdit veya kuvvet kullanımı için kabul edilmiş hiçbir tanım veya kıstas bulunmamaktadır. Bununla birlikte, bazı zorlayıcı operasyon kategorileri kuvvet kullanımı değildir. 1945 yılında San Francisco'da yapılan Birleşmiş Milletler Anlaşma taslağının belirlendiği konferansta, devletler, ekonomik zorlamayı bir kuvvet kullanımı olarak dâhil etme önerisini reddetmiştir. Genel Kurul'un Dostça İlişkiler Deklarasyonu'na yol açan müzakereler sırasında mesele, çeyrek yüzyıl sonra tekrar ortaya çıkmıştır. Kuvvetin herhangi bir devletin toprak bütünlüğünü veya siyasi

³² Schmitt, **a.g.e.**, s.53-59

bağımsızlığını tehdit etme etkisine sahip siyasi veya ekonomik nitelikte olanlar dâhil tüm baskı biçimlerini içerip içermediği sorusuna olumsuz cevap verilmiştir. Buna göre, sadece ekonomik ya da politik baskı “kuvvet” olarak kabul edilmemiştir.³³ Bu zorlayıcı faaliyetlerin bulunduğu veya buna benzer siber işlemler kesinlikle yasaklanmış kuvvet kullanımı değildir.

Sadece ekonomik ya da politik baskı “kuvvet” olarak kabul edilmediğinden yalnızca bir devlete veya ekonomiye olan güveni zayıflatmayı amaçlayan yıkıcı olmayan siber psikolojik operasyonlar, kuvvet kullanımı olarak nitelendirilmez. İlave olarak, Uluslararası Adalet Divanı’nda görülen Nikaragua davasında, başka bir devlete karşı operasyonda bulunan gerillaların yalnızca finanse edilmesinin kuvvet kullanma eşiğine ulaşmadığına karar vermiştir. Örneğin, bir isyanın parçası olarak siber operasyonlar yürüten bir grup bilgisayar korsanına sadece fon sağlamak, kuvvet kullanımı olmayacaktır.

Kuvvet kullanımı, söz konusu devlet tarafından askeri veya diğer silahlı kuvvetlerin kullanımını gerektirmez. Uluslararası Adalet Divanı, Nikaragua’da, devlete karşı düşmanca davranışta bulunan gerilla kuvvetlerini silahlandırma ve eğitmeyi kuvvet kullanımı olarak nitelendirmiştir. Bu nitelendirmeden yola çıkarak, organize bir gruba kötü amaçlı bir yazılım sağlamanın ve bu yazılımı bir devlete karşı siber saldırıda kullanmak için gerekli eğitimi vermenin de kuvvet kullanımı olarak kabulü gerekir.

Bu sonuç, siber saldırıları gerçekleştirenlere güvenli bölge sağlamanın kuvvet kullanma(silahlı saldırı) anlamına gelip gelmediği sorusunu gündeme getirmektedir. Talin El Kitabını hazırlayan uzmanlar, devlet dışı aktörlere güvenli bölge sağlamanın, devlet dışı aktörlerin eylemlerini devlete atfetmek için yeterli olmadığı yönünde görüş bildirmişlerdir. Güvenli bölge sağlamanın yanında ayrıca devlet dışı gruba önemli bir destek vermek veya siber savunma sağlamak bu devlet açısından kuvvet kullanımı olarak kabul edilebilecektir.

Bir eylemin kuvvet kullanımı oluşturup oluşturmadığının belirlenmesinde, bir devletin meşru savunmada kullanabileceği gücün eşiği olarak “silahlı saldırı”

³³ Pazarcı, **a.g.e.**, s.509-517

kavramını göz önüne almak faydalı olacaktır.³⁴ Nikaragua Kararında, Uluslararası Adalet Divanı, kuvvet kullanımının en şiddetli biçimlerini daha az şiddetli biçimlerinden ayırmıştır. Talin El Kitabını hazırlayan uzmanlar, bu nedenle, büyüklük ve etkileri bakımından “silahlı saldırı” seviyesine ulaşan, devlet tarafından yönetilen veya devlete atfedilebilen, siber saldırıyı kuvvet kullanımı olarak nitelendirmektedir.

Uluslararası Adalet Divanının Nikaragua kararından sonra Amerika Birleşik Devletleri'nin kuvvet kullanımı ve silahlı saldırı kavramları arasındaki ayrımın önemsiz olduğu yönündeki görüşü, herhangi bir yasadışı kuvvet kullanımının silahlı olsun veya olmasın, meşru savunma hakkını tetikleyen silahlı bir saldırı olarak nitelendirilebileceğini savunmaktadır. Bu görüşe göre, hukuka aykırı bir kuvvet kullanımını silahlı saldırıdan ayıran hiçbir şiddet eşiği bulunmamaktadır. Bu durumda meşru müdafaa yapan devlet de gereklilik ve orantılılık ilkeleri kapsamında saldırı eylemi ile orantılı bir karşılık verebilecektir.

Özetlemek gerekirse, bazı siber eylemlerin inkâr edilemez bir şekilde kuvvet kullanımı olmadığı, kuvvet kullanımının bir devletin doğrudan silahlı kuvvet kullanımını içermesi gerekmediği ve tüm silahlı saldırıların kuvvet kullanımı olduğu söylenebilir. Bu, silahlı saldırı içermeyen hangi eylemlerin kuvvet kullanımı oluşturduğu yönündeki soruyu çözümsüz bırakmıştır. İnsanları yaralayan, öldüren veya nesnelere zarar veren veya tahrip eden davranışlar açıkça kuvvet kullanımıdır. Bunların dışındaki durumlar çok açık değildir. Talin El Kitabı'nı hazırlayan uzmanlar devletlerin bir siber saldırıyı kuvvet kullanımı olarak nitelendirebilmesi için nasıl bir yaklaşım izlemesi gerektiğiyle ilgili bir yönetime dikkat çekmişlerdir. Açıklanan yöntem, kesin bir tanımlayıcı eşik olmadığından, siber saldırıları planlayan veya hedef olan devletlerin, uluslararası toplumun saldırıların kuvvet kullanım yasağını ihlal edip etmediğine dair muhtemel değerlendirmesine oldukça duyarlı olması gerektiği temeline dayanmaktadır.³⁵

³⁴ Schmitt, **a.g.e.**, s.53-59

³⁵ Micheal N.Schmitt et.al, **Talinn Manual**, s.47-52

Yaklaşım, hem verilen zarar düzeyine ve hem de siber saldırının belirli niteliksel unsurlarına odaklanmaktadır. Genel olarak, yaklaşım, uluslararası toplumun kuvvet kullanma olarak tanımladığı kinetik veya kinetik olmayan diğer eylemlerle kıyaslayarak siber saldırıları tanımlamayı amaçlanmaktadır. Bu tür saldırılar, kuvvet kullanımı eşiğine ulaşmış olarak değerlendirildiği ölçüde, siber saldırılar da aynı ölçek ve etkide değerlendirilecektir. Yaklaşım, bir siber saldırı da dâhil olmak üzere herhangi bir saldırının kuvvet kullanımı olarak nitelendirilip tanımlanacağına karar verirken, devletlerin, diğerlerinin yanı sıra aşağıdaki faktörleri dikkate alacağı ve büyük ağırlık vereceğini öne sürmektedir. Bu faktörler sadece devletlerin kuvvet kullanımı değerlendirmesini etkileyen faktörlerdir ve resmi yasal kriterler değildir. Talinn belgesi siber saldırıları kuvvet kullanma olarak nitelendirebilmek için 8 kriter ortaya koymuştur.³⁶ Bu kriterler:

Yıkıcılık(severity): Bireylere veya mülklere fiziksel zarar vermenin doğuracağı sonuçlar, eylemi bir kuvvet kullanımı olarak nitelendirmektedir. Sadece rahatsızlık veren veya can sıkıcı olanlar hiçbir zaman kuvvet kullanımı olarak nitelendirilmezler. Sonuçlar kritik ulusal çıkarları ne kadar fazla etkiliyorsa, siber saldırının kuvvet kullanımı olarak tanımlanmasına o kadar katkıda bulunacaktır. Bu bağlamda, sonuçların kapsamı, süresi ve yoğunluğu şiddetin değerlendirilmesinde büyük etkisi olacaktır. Herhangi bir saldırı gibi siber saldırının, hasara, tahribata, yaralanmaya veya ölüme sebep olması durumunda siber saldırı yüksek ihtimalle kuvvet kullanımı olarak kabul edilecektir. Bu analizde şiddet en önemli faktördür.

Anılık(immediacy): Siber saldırıların sonuçları ne kadar çabuk ortaya çıkarsa, devletlerin barışçıl bir çözüm bulma ya da zararlı etkileri azaltma fırsatı o kadar azalmaktadır. Bu nedenle, devletler geciken ya da zamanla oluşan sonuçlardan daha çok anlık sonuçlara odaklanmaktadır. Etkilerinin ortaya çıkması haftalar ve aylar alan siber saldırılarla sonuçları hemen görülen siber saldırılar kıyaslandığında sonuçları hemen görülenlerin kuvvet kullanma olarak tanımlanma olasılığı daha yüksektir.

Nedensellik (directness): İlk eylem ile sonuçları arasındaki ilişki zayıfladıkça, devletlerin kuvvet kullanma yasağını ihlal eden aktörü sorumlu tutma ihtimali

³⁶ Schmitt, a.g.e, s.49-51

azalmaktadır. Anilik faktörü söz konusu sonuçların zamansal yönüne odaklanırken, nedensellik sebep sonuç ilişkisini incelemektedir. Örneğin, piyasa güçleri, piyasalara erişim ve benzerleri, ekonomik zorlamanın nihai sonuçlarını belirlemektedir. İlk eylem ve etkileri arasındaki nedensel bağlantı dolaylı olduğundan ekonomik yaptırımların etkilerinin ortaya çıkması haftalar hatta aylar alabilmektedir. Silahlı eylemlerde, aksine, sebep ve sonuç birbiriyle doğrudan ilişkilidir. Örneğin bir patlama doğrudan insanlara veya nesnelere zarar verir. Sebep ve sonucun birbiriyle açıkça bağlantılı olduğu siber saldırıların kuvvet kullanma olarak nitelendirilmesi daha muhtemeldir.

İstilacılık (invasiveness); İstilacılık, siber saldırıyla devletin çıkarlarına aykırı olarak devletin siber sistemlerine girme derecesini belirtir. Kural olarak, hedeflenen bir siber sistem ne kadar güvenli olursa, bu sisteme sızılması nedeniyle ortaya çıkan endişe de o kadar büyük olmaktadır. Örneğin, 7. Seviye Güvenlik Derecesi ile akredite edilmiş bir askeri sisteme girmek, akredite olmamış, açıkça erişilebilir sivil bir üniversitede veya küçük bir işletmede bulunan bir sistemin güvenlik açıklarından yararlanmaktan daha istilacıdır. Ayrıca, siber saldırının etkilerini belirli bir devlet ile sınırlandırma derecesi saldırının algılanan istila değerini arttırmaktadır.

Alan adı, siber alanda oldukça belirgin bir göstergedir ve bu nedenle bir işlemin istila düzeyinin değerlendirilmesinde önem taşımaktadır. Belirli bir devletin veya belirli bir devlet organının (örneğin gov.) alan adını özel olarak hedef alan siber saldırılar, bu nedenle, devlete özgü olmayan (örneğin com.) alan adı uzantılarına yönlendirilen saldırılar daha istilacı olarak kabul edilmektedir.

Bu faktör siber bağlamda dikkatlice uygulanmalıdır. Özellikle, bilgisayar ağının sömürülmesi, modern casusluğun yaygın bir aracıdır. Yüksek derecede istilacı olmasına rağmen, siber casusluk, casusluk konusundaki uluslararası yasada doğrudan yasaklanmadığından, kuvvet kullanımı seviyesine ulaşmayacaktır.³⁷

Dolayısıyla, tuş vuruşlarını izlemek için siber güvenlik mekanizmalarının devre dışı bırakılması gibi eylemlerin, istilacı olmalarına rağmen, kuvvet kullanımı olarak görülmesi pek olası değildir. Bu, siber casusluk yapmak için icra edilen eylemlerin

³⁷ Schmitt, a.g.e, s.158--161

kuvvet kullanımını oluşturmayaacağı anlamına gelmez. Örneğin, siber casusluk için bir platform görevi gören askeri bir hava aracının ulusal bir hava sahasına rıza olmadan nüfuz etmesi bazen kuvvet kullanımı olarak nitelendirilebilmektedir.

Ölçülebilirlik (measurability); Bu faktör, devletlerin, sonuçlar ortaya çıktığında eylemleri kuvvet kullanımı olarak nitelendirebilme imkânı sağlamaktadır. Geleneksel olarak, silahlı kuvvetler kuvvet kullanımı olarak nitelendirilen saldırılar gerçekleştirmekte ve saldırıların etkileri genellikle ölçülebilmektedir. Siber alanda, sonuçlar belirgin değildir. Bu nedenle, sonuçlar ne kadar ölçülebilir ve belirlenebilirse, söz konusu siber saldırının kuvvet kullanımı seviyesine ulaşmış olup olmadığına karar verirken devletin durumu değerlendirmesi o kadar kolay olacaktır. Buna göre, çok belirli terimlerle (örneğin, bozuk veri miktarı, çalışmayan sunucuların yüzdesi, gizli dosyaların sayısı) değerlendirilebilecek bir siber saldırının, ölçülmesi veya öznel sonuçlarla nitelendirilmesi zor olanlara kıyasla kuvvet kullanımı olarak nitelendirilmesi daha muhtemeldir.

Askeri Karakter(military character); Siber saldırı ile askeri operasyonlar arasındaki bağ, kuvvet kullanımı olarak nitelendirme olasılığını arttırmaktadır. Bu görüş, Birleşmiş Milletler Anlaşmasında geçen kuvvet kullanma yasağının özellikle askeri harekâtla ilgili olduğu gerçeğiyle desteklenmektedir. Anlaşmanın giriş kısmında, “silahlı kuvvetin kullanılmayacağını, ortak çıkarın korunacağını” öngörürken, madde 44, “kuvvet” terimini “silahlı” olarak nitelemeyen askeri kuvvet kullanımı anlamına gelecek şekilde kullanmıştır.³⁸ Ayrıca, kuvvet kullanımının geleneksel olarak askeri veya diğer silahlı kuvvetler tarafından kullanılan gücü ima ettiği anlaşılmaktadır.

Devletin Rolü(state involvement); Devletin siber bir saldırıya katılımının kapsamı, bir devletin bizzat kendisi tarafından yürütülen operasyonlardan (örneğin, silahlı kuvvetlerinin veya istihbarat teşkilatlarının faaliyetleri), katılımının önemsiz olduğu operasyonlara kadar bir süreç boyunca uzanmaktadır. Devlet ile siber saldırı arasındaki açık ve yakın bağın varlığı, diğer devletlerin siber saldırıyı, o devlet tarafından uygulanan kuvvet kullanımı olarak nitelendirmesi daha olası olmaktadır.

³⁸ Micheal N.Schmitt et.al, **Talinn Manual**, s.51

Muhtemel Meşruiyet (presumptive legitimacy); Uluslararası hukukun doğası genellikle yasaklayıcı bir yapıdadır. Yasaklanmayan bir eyleme izin verilmiştir. Bir antlaşma hükmü bulunmuyorsa veya kabul görmüş teamül hukuku yasağı yoksa eylem muhtemelen yasaldir. Bu yüzden siber saldırıların kuvvet kullanma olarak değerlendirilmesi bir istisna olarak kabul edilmektedir. Örneğin, uluslararası hukuk, propaganda, psikolojik operasyon, casusluk veya sadece ekonomik baskıyı yasaklamamaktadır. Bu nedenle, bu kategorilere ve diğer kategorilere giren eylemler muhtemelen yasaldir. Bu nedenle, siber saldırıların devletler tarafından kuvvet kullanımı olarak görülme olasılığı daha düşüktür.

Devletler değerlendirme yaparken, mevcut koşullara bağlı olarak, hâkim siyasi ortama, operasyonun gelecekteki askeri kuvvet kullanımına yönelik olup olmadığına, saldırganın kimliğine, saldırgan tarafından gerçekleştirilen siber saldırıların kaydına ve hedefin niteliğine (kritik altyapı gibi) bakmalıdır. Ayrıca bu faktörler ayrı ayrı değil birlikte bir bütün olarak değerlendirilmelidir. Örnek olarak, geçici hizmet reddi (DDos saldırısı) gibi rahatsızlıklara neden olan oldukça istilacı bir saldırının kuvvet kullanımı olarak sınıflandırılması çok muhtemel değildir. Buna karşılık, ekonomik zorlama varsayımsal olarak hukuka uygun olsa da bazı devletler ekonomiyi felce uğratan büyük siber saldırıları kuvvet kullanımı olarak kategorize edebilir.

Son olarak, silahlı saldırı tanımında kullanılan kuvvet kullanımı kavramının farklı normatif amaçlara hizmet eden standartlar olduğu anlaşılmalıdır. Bir devletin, Birleşmiş Milletler Anlaşmasının 2(4) maddesini ve ilgili uluslararası teamül hukuku yasağını ihlal edip etmediğini belirlemek için kuvvet kullanıp kullanmadığına bakılmaktadır. Örneğin devletin başka bir devlete karşı ayaklanan isyancılara silah sağlaması, mali yardım yapması, lojistik, eğitim ve bilgi desteği sağlaması Birleşmiş Milletler Antlaşması'nın kuvvet kullanma yasağı ve başka devletlerin iç işlerine karışmama ilkesine aykırıdır, fakat bu yardımlar "silahlı saldırı" olarak değil kuvvet kullanma olarak kabul edilebilirler. Bu nedenle bu eylemlerden herhangi biri nedeniyle menfaatleri zedelenen devletlerin, Birleşmiş Milletler Anlaşmasının devletlere bahsettiği meşru müdafaa kapsamında kuvvet kullanmaya hakları yoktur. Bu ayırım, kuvvet kullanılmış olmasının tek başına karşılık olarak kuvvet kullanılmasını haklı çıkarmayacağından oldukça kritiktir. Talin El Kitabını hazırlayan uzmanlara göre,

silahlı bir saldırı seviyesine ulaşmayan bir kuvvet kullanımıyla karşı karşıya kalan devletler yasal bir karşılık vermek istiyorsa siber karşı tedbirleri de kapsayan orantılı karşı tedbirlere başvurmak zorundadır.³⁹

2.3.6.4. Silahlı Saldırıya Karşı Meşru Müdafaa

Silahlı saldırı seviyesine ulaşan bir siber saldırıya uğrayan devlet, meşru müdafaa hakkını kullanabilir. Siber bir saldırının silahlı bir saldırı seviyesine ulaşıp ulaşmadığı, siber saldırının büyüklüğüne ve neden olduğu etkilere bağlıdır.

Birleşmiş Milletler Anlaşmasının 51. maddesine göre, “Birleşmiş Milletler’in bir üyesine karşı silahlı bir saldırı meydana gelirse Birleşmiş Milletler Güvenlik Konseyi uluslararası barış ve güvenliği sağlayacak tedbirleri alıncaya kadar, bu Anlaşmada yer alan hiçbir şey, mevcut bireysel veya kolektif meşru müdafaa hakkına zarar veremez.”⁴⁰

Silahlı bir saldırı sınır ötesi bir ögeye sahip olmalıdır. Bu kriter, bir devlet, başka bir devlete karşı silahlı saldırı olarak nitelendirilen bir siber saldırıya girdiğinde ya da devlet dışı aktörleri bunu yapmaları için yönlendirdiğinde karşılanmış olmaktadır. Daha zor olan durum, bir devlete karşı devlet dışı aktörler tarafından başka bir devlet adına yürütülmeyen siber saldırılardır. Devletin kendi toprağında yapılan, yönetilen ve yönlendirilen eylemlere karşı devletler kendi iç hukuklarına uygun olarak kuvvet kullanabilirler.

Meşru müdafada kuvvet kullanma hakkı, kinetik silahlı saldırıların ötesinde tamamen siber saldırılarla yapılanlara kadar uzanmaktadır. Talin El Kitabını hazırlayan uzmanlar, bazı siber saldırıların, Birleşmiş Milletler Sözleşmesi dâhilinde silahlı saldırı olarak sınıflandırılması için yeterince ciddi gerekçe barındırabileceği sonucuna varmıştır. Bu sonuç, saldırı aracı seçiminin bir saldırının silahlı saldırı olarak nitelendirilip nitelendirilmeyeceği hususunda önemsiz olduğuna ilişkin Uluslararası Adalet Divanı’nın Nükleer Silahların Yasallığıyla ilgili ısrarlı Tavsiye Görüşüyle

³⁹ Micheal N.Schmitt et.al, **Talinn Manual**, s.47-52

⁴⁰ **Birleşmiş Milletler Anlaşması**, (Çevrimiçi) <https://www.un.org/en/charte-united-nations/index.html>, 02.02.2019

uyumludur.⁴¹ Ayrıca, bu durum devlet uygulamalarıyla da uyumludur. Örneğin, kimyasal, biyolojik ve radyolojik saldırıların silahlı saldırı olarak nitelendirileceği ve meşru müdafaa hakkını doğuracağı evrensel olarak kabul edilmektedir. Kimyasal, biyolojik ve radyolojik saldırıların kinetik olmayan doğalarına rağmen silahlı saldırı olarak kabul edilmesinin sebebi bu saldırılar sonucunda meydana gelen ciddi yaralanma veya ölümlerin olmasıdır. Aynı akıl yürütme siber saldırılar için geçerli olacaktır.

Talin El Kitabını hazırlayan uzmanlar, silahlı terimiyle silahlı saldırı kavramının zorunlu olarak silah kullanılmasını gerektirip gerektirmediği konusunda görüş ayrılığına düşmüştür. Çoğunluk silah kullanmak gerekmediği ve onun yerine kullanılan araçlardan farklı olarak siber saldırının yarattığı etkilere bakılması gerektiği, bu etkilerin kinetik silahlı saldırıdan kaynaklanan sonuçlarla kıyaslanarak değerlendirilmesi gerektiği yönünde görüş belirtmişlerdir.⁴²

Talin El Kitabını hazırlayan uzmanlara göre, silahlı saldırı terimi kuvvet kullanımı terimi ile eşdeğer değildir. Silahlı bir saldırı, en azından Birleşmiş Milletler Anlaşmasının 2. Maddesi 4. fıkrası kapsamında bir kuvvet kullanımını öngörmektedir. Ancak, Uluslararası Adalet Divanı tarafından belirtildiği gibi, her kuvvet kullanımı silahlı saldırı seviyesine ulaşmamaktadır. Silahlı saldırı olarak nitelendirilecek bir eylem için gerekli olan, kuvvet kullanımı olarak nitelendirilen bir eylemin büyüklük ve etkilerini aşacak düzeyde olması gerekmektedir. Kuvvet kullanımı, ancak silahlı saldırı olarak nitelendirilme eşiğine ulaştığında, meşru müdafaa kapsamında devletin kuvvet kullanarak karşılık vermeye hakkı olacaktır.

Büyüklük ve etki nitelemeleri Nikaragua yargılamasında sarf edilmiştir. Bu yargılamada, Uluslararası Adalet Divanı büyüklük ve etkileri, silahlı saldırı niteliğindeki eylemleri olmayanlardan ayıran bir kriter olarak tanımlamıştır. Uluslararası Adalet Divanı bu kararında, kuvvet kullanımının en ağır biçimlerini (silahlı saldırıyı oluşturanlar) diğer daha hafif biçimlerinden ayırt etme gerekliliğine dikkat çekmiş, ancak bu konuda daha fazla yol gösterici olmamıştır.⁴³ Bu nedenle,

⁴¹ International Court of Justice, **Legality of the Threat or Use of Nuclear Weapons**, (Çevrimiçi) <https://www.icj-cij.org/en/case/93>, 29.01.2019

⁴² Schmitt, **a.g.e.**, s.118

⁴³ International Court of Justice, **Nicaragua Judgement**

büyükölük parametreleri ve etki kriterleri, kullanılan kuvvetin ağırlık göstergesi olmasına rağmen bazı durumlarda belirsiz kalmıştır. İnsanları yaralayan, öldüren veya mülke zarar veren veya imha eden herhangi bir kuvvet kullanımının büyükölük ve etki kriterlerini yerine getireceğı konusunda tartışma yoktur. Talin El Kitabını hazırlayan uzmanlar, siber istihbarat toplama ve siber hırsızlığın yanında zorunlu olmayan siber hizmetlerin kısa veya periyodik olarak kesilmesini içeren siber saldırıların, silahlı saldırılar olarak nitelendirilmeyeceğı görüşünü savunmaktadırlar.

Ancak siber saldırının neden olduğı ölüm, yaralanma, hasar, imha ya da acı derecesinin silahlı saldırı olarak nitelendirilemediğı durumda büyükölük ve etki kriterinin işlevsiz kalmaktadır. Uluslararası Adalet Divanı, Nikaragua Kararında,⁴⁴ bir silahlı saldırı ile basit bir sınır olayı arasında ayırım yapmıştır. Bu ayırım, çok sayıda yorumcu tarafından eleştirilmiştir. Bu bağlamda, Uluslararası Adalet Divanı, tek bir askeri platform veya tesise yapılan bir saldırının silahlı saldırı olarak nitelendirilebileceğini belirtmiştir.

Siber saldırıya maruz kalan devletin, bireysel olarak silahlı saldırı eşığının altında kalan toplu olarak değerlendirildiğinde silahlı bir saldırı oluşturabilecek bir dizi siber olaya karşılık meşru müdafaa hakkını kullanıp kullanamayacağı tartışmalıdır. Belirleyici faktör, aynı göndericinin, gerçekleştirdiğı birbiriyle ilişkili daha küçük ölçekli olayların birlikte alındığında gerekli ölçeğe sahip olup olmadığıdır. Talin El Kitabını hazırlayan uzmanlar, durumun böyle olduğuna dair ikna edici kanıtlar varsa, olayları bileşik silahlı saldırı olarak ele almak gerektiğini kabul etmiştir.

Yaralanma, ölüm, hasar veya imhayla sonuçlanmayan, ancak kapsamlı olumsuz etkileri olan eylemlerin nasıl değerlendirileceğı konusu çok tartışmalıdır ve henüz çözümlenmemiştir. Talin El Kitabını hazırlayan uzmanlardan bazıları, kişilere zarar vermenin veya mülke fiziksel olarak zarar vermenin, bir olayın silahlı saldırı olarak nitelendirilmesinde emsal teşkil eden bir koşul olduğu yönünde fikir beyan etmiştir. Bir kısmı ise önemli olan sonuçların zarar verici veya yıkıcı olup olmadığı değil, ortaya çıkan etkilerin derecesinin önemli olduğu görüşündedir. Bu görüş ayrılığını gösteren klasik senaryo, New York Borsasına karşı yönelen ve borsanın çökmesine neden olan

⁴⁴ International Court of Justice, **Nicaragua Judgement**

bir siber olaydır. Talin El Kitabını hazırlayan uzmanlar, böyle bir olayın nitelemesi üzerine görüş ayrılığına düşmüştür. Uzmanlardan bazıları, yalnızca finansal zararın silahlı saldırı olarak nitelendirecek zarar oluşturduğuna ikna olmamışlardır. Bazı uzmanlar ise, bu tür bir çöküşün vesile olacağı felaketin etkilerinin altını çizerek bu etkileri siber saldırıyı silahlı saldırı olarak nitelendirmek için yeterli görmüşlerdir. Aynı yaklaşımla, baktığımızda ikinci görüşte olanların desteklediği fikre göre bir devletin kritik altyapısının ana bileşenlerine (sistemlerine) yönelik yıkıcı olmasa da ciddi etkilere yol açan bir siber saldırı, silahlı saldırı olarak nitelendirilecektir.⁴⁵

Siber bağlamdaki diğer bir zorluk, bir eylemin silahlı saldırı olarak nitelendirilebilmesi için hangi etkilerin değerlendirileceğini belirlemektir. Uzmanlar, siber saldırının öngörülebilir tüm makul sonuçlarının bu şekilde nitelendirilebileceğini kabul etmiştir. Örneğin, bir su arıtma tesisini hedef alan bir siber saldırıyı ele aldığımızda, kirlenmiş suyun içilmesinden kaynaklanan hastalık ve ölümler öngörülebileceğinden bu etkiler hesaba katılmalıdır.

Talin El Kitabını hazırlayan uzmanlar, söz konusu etkilerin amaçlanmış olup olmadığına ilişkin olarak görüş ayrılığına düşmüştür. Örneğin, B Devletine karşı A Devleti tarafından yapılan siber casusluk eyleminin B Devletinin siber altyapısında beklenmedik bir şekilde önemli bir hasara sebep olduğunu düşünelim. Bazı Uzmanlar, saldırıyı silahlı saldırı olarak nitelendirmeye istekli olmamasına rağmen saldırının olumsuz etkilerini gidermek için önlemler alınabileceğini kabul etmişlerdir.⁴⁶ Uzmanların çoğunluğu, bir saldırıyı silahlı saldırı olarak nitelemede amacın önemsiz olduğunu sadece büyüklük ve etkisinin önemli olduğu yönünde fikir beyan etmişlerdir. Bununla birlikte, bunlara verilen herhangi bir karşılık, gereklilik ve orantılılık kriterlerine uymak zorunda olduğundan; gereklilik bu açıdan önemli bir engel oluşturmaktadır. Uzmanlar, verilen karşılığın hukuka uygunluğunun, B devletinin silahlı saldırının yapılıp yapılmadığı konusundaki değerlendirmesinin makul olup olmadığına göre belirleneceğine karar vermişlerdir.

A Devletinin B Devletine karşı siber silahlı saldırısı, C Devletinde taşkın etkilere neden olabilir. Bu etkiler, silahlı saldırı için büyüklük ve etki kriterlerini karşılıyorsa,

⁴⁵ Micheal N.Schmitt et.al, **Talinn Manual**, s.47-52

⁴⁶ Schmitt, **a.g.e**, s.40

uzmanların çoğunluğu, C Devletinin gereklilik ve orantılılık kriterlerini yerine getirdiği sürece, meşru müdafaa için kuvvet kullanımına başvurma hakkı bulunduğu sonucuna varmıştır. Nitekim, B Devletine karşı siber saldırılar silahlı saldırı olarak nitelendirilmese bile, taşkın etkilerin C devletine karşı silahlı saldırıya neden olmasını engellemeyecektir.⁴⁷

Uluslararası toplum tarafından, 2012'den beri, hiçbir uluslararası siber olayın silahlı bir saldırı eşiğine ulaştığı kesin ve aleni olarak nitelendirilmemiştir. Özellikle, yaygın olarak siber savaş olarak adlandırılan Estonya'ya yönelik 2007 siber operasyonları, Estonya veya uluslararası toplum tarafından silahlı bir saldırı olarak açıkça nitelendirilmemiştir. Talin El Kitabını hazırlayan uzmanlar, bu değerlendirme temelinde büyüklük ve etki eşiğine ulaşılmadığına karar vermiştir. 2009 Stuxnet operasyonlarının İran santrifüjlerine verdiği hasarın ışığında, uzmanların bazıları, operasyonların silahlı saldırı eşiğine ulaştığını düşünmektedir.

Bir eylemin silahlı saldırı olarak nitelendirilip nitelendirilmeyeceğini belirlerken saldırının menşei meselesini de düşünmek gerekmektedir. Devlet organlarının yürüttüğü bir eylemin bu şekilde nitelendirilebileceği tartışılmazdır. Nikaragua Kararında Uluslararası Adalet Divanına göre; bir silahlı saldırı, yalnızca uluslararası bir sınır boyunca düzenli kuvvetler tarafından yapılan eylemler değil, aynı zamanda bir devlet tarafından gönderilen veya o devlet yararına başka bir devlete karşı düzenli birlikler tarafından icra edilen silahlı bir saldırı seviyesine ulaşan eylem gerçekleştiren veya büyük oranda o eyleme katılmış olan silahlı kollar, gruplar, düzensiz birlikler veya paralı askerler tarafından yapılan eylemler de anlaşılmalıdır. Bu karar ışığında devlet dışı aktörlerin eylemleri bir devlete atfedilebildiğinde de silahlı saldırı olarak nitelendirilecektir.

Örneğin, A Devletinin yönetimindeki bir grup özel şahıs veya tek bir birey, B Devletine yönelik siber saldırıları üstlenirse ve bu eylemlerin sonucu gerekli büyüklük ve etkilere ulaşırsa, A Devleti silahlı bir saldırı gerçekleştirmiş olacaktır.

Bir devlet yönetimi altında olmayan devlet dışı aktörlerin eylemlerinin bir silahlı saldırı teşkil edip edemeyeceği konusu tartışmalıdır. Geleneksel olarak, 51. madde ve

⁴⁷ Micheal N.Schmitt et.al, **Talinn Manual**, s.53-59

uluslararası teamül hukukuna göre meşru müdafaa hakkı yalnızca bir devlet tarafından başka bir devlete yapılan silahlı saldırılara uygulanabilir niteliktedir. Devlet dışı aktörler tarafından uygulanan şiddet eylemlerinin iç hukukta adli yaptırımını bulunmaktadır. Ancak, uluslararası topluluk El Kaide'nin ABD'ye yaptığı 11 Eylül saldırılarını meşru müdafaa hakkını doğuran silahlı saldırı olarak nitelendirmiştir.⁴⁸ Böyle bir devlet uygulaması devletlerin, devlet dışı aktörler tarafından yürütülen saldırılara karşı meşru müdafaa hakkını kullanma istekliliğine işaret etmektedir. Dahası, Birleşmiş Milletler Anlaşmasının 2 (4) maddesi devletlerin eylemlerini ele alırken, 51. madde silahlı saldırılara karşı böyle bir sınırlama içermez (metin, yalnızca devletlerin kendini savunma hakkına sahip olduğunu açıkça belirtmektedir.). Ancak Uluslararası Adalet Divanı, bu yaklaşımı benimsemiş gibi görünmüyor.

Talin El Kitabını hazırlayan uzmanların çoğunluğu, devlet dışı aktörlerin (terörist veya asi gruplar vb.) bir devlete silahlı saldırı yapması durumunda devletin bu aktörlere karşı meşru müdafaa hakkının doğacağını savunmaktadırlar. Devlet dışı siber aktörlerin siber saldırıları silahlı saldırı seviyesine ulaşırsa, devlet dışı siber aktörlere karşı meşru müdafaa hakkı doğacaktır. Örnek olarak, uzmanların çoğunluğu, B Devleti'nde bulunan kritik altyapıya karşı, A Devleti'nde bulunan bir grup terörist tarafından yürütülen yıkıcı bir siber saldırıyı B devletine karşı siber teröristlerin silahlı saldırısı olarak ele almaktadır. Uzmanların bir kısmı ise bu önermeyi kabul etmemiştir.⁴⁹

Talin El Kitabını hazırlayan uzmanlar, hukuken ve herhangi bir coğrafi sınırlama olmadan silahlı saldırı düzenleyebilecek bir grubun sahip olması gereken örgütlenme derecesi gibi konularda uluslararası hukuk kurallarının belirsiz olduğu sonucuna varmışlardır. Ek olarak, bir devlete bağlı olmayan devlet dışı bir grubun silahlı saldırı düzenleyebileceğini düşünen uzmanlar, bireysel olarak bir kişinin büyüklük ve etki eşliğini karşılayan bir saldırıyı yapıp yapamayacağı konusunda farklı görüşler ortaya koymuşlardır.

⁴⁸ United Nations Security Council, **Resolution 1368(2001)**, (çevrimiçi) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement>, 25.02.2019

⁴⁹ Micheal N.Schmitt et.al, **Talinn Manual**, s.45-47

Söz konusu hedef, devletin topraklarının dışında bulunan mülk veya vatandaşlardan oluşuyorsa, siber saldırının uluslararası hukuka göre silahlı saldırı olarak nitelendirilip nitelendirilemeyeceği ise belirsizdir. Ticari olmayan devlet tesislerine veya ekipmanlarına ve hükümet personeline yönelik saldırılar, yukarıda belirtilen kriterler yerine getirildiği sürece kesinlikle silahlı saldırılar olarak nitelendirilmektedir. Örneğin, A Devleti tarafından B Devletinin Devlet Başkanı yurtdışındayken öldürmek için yapılan bir siber saldırı, bir silahlı saldırı olarak nitelendirilecektir. Siber saldırıların silahlı saldırı olup olmadığının tespiti, bunlarla sınırlı olmamak üzere, şu faktörlere bağlıdır: saldırının neden olduğu hasarın kapsamı; söz konusu mülkün devlet veya özel nitelikte olup olmadığı; hedeflenen kişilerin durumu; ve saldırıların politik olarak motive edilip edilmediği, yani mülkiyete veya bireylere karşı milliyetleri nedeniyle gerçekleştirilip gerçekleştirilmediği. Böyle durumlar için kesin kurallar yoktur. B Devletinin yurtdışındaki devlet kuruluşlarından birinin yönetim kurulu başkanını öldürmek için A Devleti tarafından yürütülen bir siber saldırının silahlı saldırı olup olmadığı konusunda uzmanlar görüş ayrılığına düşmüştür.

Meşru müdafaa hakkının kullanılması, gereklilik, orantılılık, yakınlık ve anilik şartlarına tabidir⁵⁰. Tabii ki, meşru müdafaa, silahlı bir saldırının gerçekleşmek üzere olması veya gerçekleşmesinin yanı sıra saldırganın kimliğine dair makul bir tespitin varlığına bağlıdır. Bu tespit eylem sonrasında değil, önceden yapılmalıdır.

Meşru müdafaa önlemleri, menşei devlet toprağı, mağdur devlet toprağı, açık denizler, uluslararası hava sahası veya dış uzaydan (ilgili uzay hukukuna tabi) icra edilebilir ve bu alanların içindeki veya üzerindeki varlıklara yöneltilebilir.

Savunmaya yönelik siber operasyonlar, saldırının atfedilemeyeceği bir devletten veya devlette bulunan varlıklardan başlatıldığında, egemenlik ilkesi dikkatli değerlendirilmelidir. Egemenliğini ihlal etmeden, bu devletin rızasıyla yabancı topraklarda meşru müdafaa önlemlerinin alınabileceği tartışmasız kabul edilmektedir. Bu nedenle, başka bir devletin toprağındaki savunma eylemi ile ilgili kritik mesele, rıza dışı eylemlerin nasıl karakterize edileceğidir. Talin El Kitabını hazırlayan uzmanlar, bu konuda fikir ayrılığına düşmüştür. Çoğunluk, bu durumda siber bir silahlı

⁵⁰ Schmitt, **a.g.e.**, s.59-60

saldırıya karşı kendini savunmaya, saldırının menşei devletin yapamadığı (örneğin, uzmanlık veya teknolojiden yoksun olduğu için) veya silahlı siber saldırıyı bastırmak için etkili eylemler yapmak istememesi durumunda izin verilebileceği sonucuna varmıştır. Talin El Kitabını hazırlayan uzmanlar özellikle, devletlerin kendi topraklarının uluslararası hukuka aykırı davranışlarda kullanılmamasını sağlama görevinin olduğunu vurgulamıştır.⁵¹ Grubun azınlığı ise, silahlı saldırının atfedilemeyeceği bir devletin topraklarında meşru müdafaa için kuvvet kullanmaya, uygun olsa da zorunluluğa dayanan diğer karşılıklara izin verilemeyeceği yönünde tutum almıştır. Bu, devletin rızasının bulunmadığı veya Birleşmiş Milletler Güvenlik Konseyi tarafından yetkilendirilmediği varsayımına göre yapılmış bir değerlendirmedir.⁵²

Sınır ötesi saldırı uğrayan mağdur devletin savunma eylemlerinin yasal olduğunu kabul eden Talin El Kitabını hazırlayan uzmanlar, mağdur devletin önce eylemin yapıldığı devletin silahlı saldırıyı içeren faaliyetlere son vermesini talep etmesi gerektiğini vurgulamıştır. Mağdur devlet, aynı zamanda saldırının kaynaklandığı devlete de durumu ele alma fırsatı vermelidir. Bu gereklilikler, savunma eylemlerinin gerçekleştirileceği devletin egemenliğine saygı duyma konusundaki uluslararası hukuk zorunluluğundan kaynaklanmaktadır. Ayrıca, saldırının kaynaklandığı devletin durumu ele alma isteksizliği veya yetersizliği konusunda hatalı bir sonuca karşı usuli bir güvencedir. Saldırının kaynaklandığı devlete talebi iletme veya durumu çözmesi için zamanın olmadığı istisnai durumlar olabilir. Silahlı bir saldırı olarak kabul edilen siber saldırıyı püskürtmek veya sonuçlarını en aza indirmek için derhal harekete geçmek gerekliyse, hedef devlet meşru müdafaa için derhal harekete geçebilir. Bu nedenle, bu gereksinimler her olayın kendisine özgüdür.⁵³

Bu sınıflandırma yoluyla, siber savaş eyleminin sonuçları ortak özellikler açısından ölçülerek bu sonuçların, karakteristik olarak silahlı kuvvet kullanmanın sonuçlarına mı daha yakın, yoksa kuvvet kullanma sınırının dışında tutulmasının mı daha iyi olduğu tetkik edilmelidir. Talinn metodu, mevcut silahlı çatışma hukuku ve teamül

⁵¹ Schmitt, A.e, s.32

⁵² Schmitt, a.g.e, s.65

⁵³ Micheal N.Schmitt et.al, **Talinn Manual**, s.53-59

hukukundan kaynaklı yapının dengesini deęiřtirmeden teknolojik geliřmelerden kaynaklı yeni kuvvet kullanma imkânlarının ortaya ıkmasıyla meydana gelen boşlukların doldurulması için kuvvet kavramının genişletilmesine imkân vermektedir.

Talinn metodu uygulanarak, bir siber saldırının daha esnek ve sonuç tabanlı kuvvet anlayışı kapsamına girip girmediğine karar verilir. Eylemin doğasından kaynaklanan öngörülebilir sonuçlar silahlı bir saldırıya benzeyip benzemediğine karar vermek için değerlendirilir. Eğer sonuçlar silahlı bir saldırıya benziyorsa, meşru müdafaa kapsamında karşı kuvvet kullanma yasağının genişlemesini haklı çıkaracaktır. Eğer sonuçlar silahlı bir saldırıya benzemiyorsa, uluslararası hukuka göre haksız bir fiil olup olmadığına, kuvveti yasaklayanlardan başka emredici hükümlere başvurarak karar verilmelidir. Siber saldırının silahlı bir saldırı olduğunun tespiti durumunda meşru müdafaa kapsamında verilecek karşılıklar tezin dördüncü bölümünde incelenmiştir.

2.3.7. Wingfield Analizi

Michael Schmitt liderliğinde uluslararası uzmanlar tarafından hazırlanan Talinn El Kitabı siber saldırıları kuvvet kullanma olarak nitelendirebilmek için kriterler ortaya koymuştur. Profesör Thomas Wingfield sonuçların niteliksel ölçümlerini nicelleştirme yoluyla Talinn Kitabının analitik tekniğini genişletmiştir.⁵⁴

Wingfield, Talinn Analizinin bir siber saldırıya karşı verilecek yasal bir karşılığı etkileyen faktörlerin daha akademik olarak titiz bir değerlendirmesi için kullanılabileceğini savunmaktadır.

Michael Schmitt, *“düşmanca bir hareketin doğası, sonuçlarından daha az belirleyici hale geldikçe, devletlerin yasal zorlayıcı davranış biçimlerinin ve bunlara uygun tepkilerin, buna göre evrimleşme ihtimalinin yüksek olduğunu”* belirtmiştir.⁵⁵ Michael Schmitt, Birleşmiş Milletler Anlaşması çerçevesinin neden her bir zorlama türünü olduğu gibi nitelendirmeyi seçtiğini incelemiştir:

⁵⁴ T. C. Wingfield, J. B. Michael, and D. Wijesekera (2003), **"Optimizing Lawful Responses to Cyber Intrusions,"** (çevrimiçi) http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf, 10.04.2019

⁵⁵ Michael N. Schmitt, "Bellum Americanum: The U.S. View of Twenty-first Century War and Its Possible Implications for the Law of Armed Conflict," **Michigan Journal of International Law** 19 (1998), s.1051

Mevcut normatif tasarımda, bir eylemin yapısı genellikle sonuçlarından daha önemlidir. Örneğin, yıkıcı bir ekonomik ambargo, muazzam ızdıraba neden olsa bile, kuvvet kullanarak yapılacak meşru bir müdafaayı haklı çıkaracak kuvvet kullanımı veya silahlı saldırı değildir. Öte yandan, sınır boyunca nispeten küçük, silahlı bir saldırı hem kuvvet kullanımı hem de silahlı saldırıdır. Bu aykırı sonuç yasaların eylemleri, gerçekten önemli olan sonuçların kestirme yolu olarak kullanımından kaynaklanmaktadır. Davranışlar daha kolay ifade edilmekte (belirli bir miktar ve nitelikte zarara neden olmak yerine kuvvet kullanmak) ve maruz kalınan zarara bağlı olarak etki temelli bir standarda göre daha kolay anlaşılmaktadır. Bu kestirme yollar bilgi işlem çağında iyi işlemeyecektir, çünkü potansiyel olarak sonuçları felaket olsa da siber saldırılar fiziksel olarak algılanamayabilir.

Talinn El Kitabının belirlediği yedi faktörlü niceliksel bir ölçeğin eyleme uygulanarak eylemin yasak mı yoksa izin verilmiş bir eylem mi olduğunun tespitini önermiştir. Talinn El Kitabı, Birleşmiş Milletler Anlaşmasının niteliksel paradigmasını nicel bileşenlere dönüştürmüş, araştırmacılar ve uygulayıcıların analiz organize etmeleri için yararlı bir çerçeve sağlamıştır. Talinn El Kitabının yedi faktörün her birinin önemini veya ayırt ediciliğini belirttiği kısa açıklaması, Profesör Thomas Wingfield tarafından faktörün gerekliliklerini yerine getirebilecek bazı ek sorularla ayrıntılarıyla açıklamıştır. Bu yedi faktör için elde edilen sonuçların, bir operasyonun uluslararası hukuk uyarınca kuvvet kullanımı olduğuna dair niteliksel statüsünü ortaya çıkarmak için genel bir puan ortalaması alınmaktadır.

Yıkıcılık (severity): Schmitt'e göre, “Silahlı saldırılar, diğer zorlama biçimlerinden çok daha fazla fiziksel yaralanma veya eşyanın tahrip edilmesini tehdit etmektedir. Fiziksel olarak iyi durumda bulunmak insan ihtiyaçlar hiyerarşisinin en temel ihtiyacını teşkil etmektedir.”⁵⁶ Wingfield’e göre saldırıların sonuçları şöyle sınıflandırılabilir:

-İnsanların ölmesi ve ağır maddi zarar,

-İnsanların yaralanması, orta maddi hasar,

⁵⁶ Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *Columbia Journal of Transnational Law* 37 (1999), s.914–915.

-Ölen veya yaralanan ve tespit edilmiş maddi bir hasarın olmaması.

Başka bir deyişle, şunu sormak gerekir: Kaç insan öldürüldü? Saldırı yapılan alanın büyüklüğü nedir (kapsam)? Bu alanda ne kadar hasar meydana gelmiştir.(yoğunluk)?

Anilik (immediacy); Schmitt, “Silahlı zorlamanın ya da tehdidin olumsuz sonuçları genellikle büyük bir anilikte ortaya çıkarken, diğer zorlama biçimlerinin sonuçları daha yavaş gelişmektedir. Bu nedenle, silahlı zorlamanın ya da tehdidin olumsuz sonuçları hedef devlete veya uluslararası topluluğa barışçıl bir uzlaşma imkânı bulma fırsatını engellenmektedir. ”⁵⁷ Wingfield’e göre anilik şu şekilde değerlendirilebilir:

- Saniyeler-dakikalar,
- Saatler-günler,
- Haftalar-aylar.

Başka bir deyişle, eylemin süresi neydi? Etkileri ne kadar sürede hissedildi? Etkilerin azalması ne kadar sürmüştür?

Nedensellik (directness); Schmitt’in üçüncü kriteri nedenselliklidir: “Silahlı zorlamanın sonuçları, suç teşkil eden eyleme diğer zorlama biçimlerine kıyasla daha doğrudan bağlıdır. Bu nedenle, kuvvet yasağı daha kesin bir şekilde olumsuz sonuçları engellemektedir. ”⁵⁸ Wingfield’e göre sonuçlar aşağıdaki gibi değişebilir:

- Sonucun tek nedeni olan eylem,
- Sonucun bir sebebi olarak ve belirsiz bir derecede tanımlanabilen eylem,
- Sonuçla tanımlanabilir bağlantısı olmayan eylem.

Soruyu sormanın başka bir yolu şudur: Eylem, paralel veya rakip eylemlerden ayırt edilebilir miydi? Eylem, sonuçların en yakın sebebi miydi?

İstilacılık (invasiveness); Silahlı zorlamada, hasara neden olan eylem genellikle hedef devlet sınırını geçer, ekonomik savaşta ise genellikle eylem hedef devlet

⁵⁷ Schmitt, **a.g.e.**, s.914-915

⁵⁸ Schmitt, **A.e.**, s.914-915

sınırlarının ötesinde gerçekleşmektedir. Wingfield'e göre operasyonlar şöyle sınıflandırılabilir:

- Sınır fiziksel olarak geçilmiş, eylemin yeri belirli,
- Sınır elektronik olarak geçilmiş; eylem dağınık bir alanda gerçekleşmiş,
- Sınır geçilmemiş; eylemin hedef ülkede tanımlanabilir bir yeri yok.

Eylem, fiziksel olarak hedef ülkenin sınırlarını aşmayı da içeriyor mu? Eylemin yeri hedef ülke içinde mi?

Ölçülebilirlik (measurability); Silahlı zorlamanın sonuçlarının tespit edilmesi genellikle kolay olmakla birlikte (örneğin, belirli bir tahribat seviyesi), diğer zorlama biçimlerinin fiili olumsuz sonuçlarını ölçmek daha zordur. Bu gerçek, toplumun kınamasının uygunluğunu ve içerdiği şiddet derecesini silahlı kuvvet kullanılması durumunda daha az şüpheli kılmaktadır. Ölçülebilirliği değerlendirmek, Wingfield'e göre⁵⁹ operasyonları şu kategorilerden birine sokmak anlamına gelir:

- Etkiler derhal yüksek oranda kesinlik ile geleneksel yöntemlerle (bomba hasarı değerlendirmesi gibi) belirlenebilir,
- Etkiler makul bir kesinlik ile kabaca büyüklük sırası ile tahmin edilebilir,
- Etkiler diğer eylemlerin etkilerinden ayrılamaz; genel kesinliği düşüktür.

Bu nedenle, eylemin etkilerinin nasıl ölçülebildiğini, eylemin etkilerinin paralel veya rekabet eden eylemlerin sonuçlarından farklı olup olmadığını ve kesinliğin seviyesinin ne olduğunu sorulabilir.

Muhtemel Meşruiyet (presumptive legitimacy): İster ulusal ister uluslararası hukuk çerçevesinde olsun, çoğu durumda meşru müdafaa gibi istisnalar dışında şiddet uygulamak gayri meşru kabul edilmektedir. Kavramsal yaklaşım yasaklayıcıdır. Buna karşılık, çoğu diğer zorlama biçimi ulusal ve uluslararası alanda varsayımsal olarak hukuka uygundur, aksine bir yasak yoktur. Kavramsal yaklaşım izin vericidir. Dolayısıyla, silahlı zorlamanın sonuçları tahmin edilemez şekilde kabul edilirken, diğer zorlayıcı eylemlerin sonuçları (çok genel bir kural olarak) değildir. Dolayısıyla,

⁵⁹ T. C. Wingfield, J. B. Michael, and D. Wijesekera (2003), **a.g.e.**

silahlı zorlamanın sonuçları varsayımsal olarak yasak kapsamındayken, diğer zorlayıcı eylemlerin sonuçları (çok genel bir kural olarak) değildir.

Wingfield'e göre muhtemel meşruiyet şu şekilde değerlendirilebilir:

- Kinetik saldırı şeklinde gerçekleştirilen eylem,
- Siber alanda gerçekleştirilen ancak fiziksel alanda sonucu ortaya çıkan eylem,
- Siber alanda gerçekleştirilen eylem ve fiziksel dünyada görünmeyen etkiler.

Bu nedenle, muhtemel meşruiyet, bu tür bir eylemin uluslararası toplum içinde geleneksel olarak kabul görmüş olup olmamasına ve uluslararası hukukta meşru olduğu varsayılan araçların niteliksel olarak diğerlerine benzer olup olmamasına bağlıdır.

Sorumluluk (state involvement): Silahlı baskı devletlerin münhasır yetkisidir, yalnızca sınır ötesinde kuvvet kullanabilirler ve çoğu durumda yalnızca anlamlı bir etkiye sahip olma yetenekleri vardır. Buna karşılık, sivil toplum kuruluşları çoğu zaman diğer zorlama biçimlerine (propaganda, boykot vb.) dâhil olma yeteneğine sahiptirler. Özetle, silahlı baskının sonuçları devlete yüklenmeye diğer baskı biçimlerinde olduğundan daha müsaittir.⁶⁰ Wingfield'e göre devletin sorumluluğu;

- Eylem sorumluluğu, icracı devleti tarafından kabul edilir; iştirak derecesi büyük,
- Hedef devlet hükümeti, icracı devletin sorumluluğunun farkındadır; kamu rolü onaylanmamış; iştirak derecesi düşük,
- Eylem icracı devlete atfedilemez; iştirak derecesi düşük.

Eylem doğrudan veya dolaylı olarak icracı devlete atfedilebilir mi? Ancak, eylemde bulunan devletin hakkı için, eylem gerçekleşmiş midir?

Siber operasyonu, Birleşmiş Milletler Anlaşmasının 2 (4). maddesi uyarınca yasaklanmış bir kuvvet kullanımı olarak nitelemek için bir kuvvet kullanımı niteliğinin yeterince tanımlanmış olması gerekmektedir.

⁶⁰ Schmitt, **a.g.e.**, s.914-915

2.3.7.1.Estonya Siber Saldırısının Wingfield Analizi Kapsamında İncelenmesi

Winfield kriterlerine göre, Estonya'ya Nisan-Mayıs 2007'de yapılan siber saldırılar kuvvet kullanımı seviyesine yükselip yükselmediği incelenecektir.

Yıkıcılık (severity): Estonya'daki siber saldırıların yaygın ve devam eden doğasına, çok fazla maddi olmayan varlık kaybedilmesine rağmen, hiç kimse ölmemiş, yaralanmamış ya da herhangi bir maddi hasar olmamıştır. Maddi ve maddi olmayan kayıpları karşılaştırmak için kayıpların ekonomik değeri hesaplandığında, saldırının yıkıcılık ölçeğine göre **orta derecede maddi hasar** olduğu gözükmektedir.

Anilik (immediacy): Tam olarak 08 Mayıs 09 Mayıs bağlayan gece yarısından itibaren başlayan saldırının gelişme hızı, saldırıların başlangıcında yüksek düzeyde anilik içerdiğini göstermektedir. Siber saldırıların başlatılması ve hedeflerine ulaşması arasında sadece dakikalar, belki de sadece saniyeler geçtiği görülmektedir. Ayrıca, Estonya'nın tepkilerine karşılık olarak en az üç kez saldırılar yoğunlaştırılmış ve azaltılmış, saldırıya karar verilmesi ile hedefler üzerinde etkilerinin ortaya çıkması arasında çok kısa bir gecikme olmuştur. O zaman, anilik ölçeğine göre saldırı **yüksek anilik derecesinde** gözükmektedir.

Nedensellik (directness): Saldırıların nedenselliğini tespit etmek zordur. Bu tür hizmet reddi saldırılarında, birçok yerden birkaç yüz bin ila birkaç milyon arasında değişen bireysel olarak bakıldığında zararsız erişim talepleri ile sistemi işlemez hale getirmek için bir araya gelmektedir. Bu tür saldırıları yapmak için yaygın olarak dağıtılmış botnetler bir kişi tarafından kontrol edilirse, o zaman aktörün saldırıya başlamasının tek sebep olarak nitelendirilmesi uygun olacaktır. Hedeflenen bankalara, gazetelere, devlet dairelerine veya kamu hizmetlerine verilen zarar, bu sebebin doğrudan etkisidir. Nispeten az sayıda aktör nispeten az sayıda büyük, kurumsal sistemi etkilediğinden, **saldırının nedenselliği belirsiz bir derecede tanımlanabilen eylem** olarak kabul edilmektedir.

İstilacılık (invasiveness):İstilacılık, bu vakada düşük seviyede olan sınırın fiziksel olarak geçilmesi veya bu vakada yüksek olan belirli bir devletin topraklarındaki saldırıların dikkate alınması olarak nitelendirilebilir. Estonya'nın sınırını ihlal eden bir

kuvvet tespit edilmemiş olsa da, web sitelerini tahrip eden, büyük bankaları kapatılmasına neden olan ve ulusal acil telefon sisteminin çalışmasını birkaç saat engelleyen saldırıların hedefi münhasıran Estonya olmuştur. Sonuç olarak **Estonya sınırı elektronik olarak geçilmiş; eylem dağınık bir alanda gerçekleşmiştir.**

Ölçülebilirlik (measurability); Saldırıların ölçülebilirliğini değerlendirmek zordur. Birkaç büyük, açıkça tanımlanabilir hedef olmasına ve bu hedeflerin birçoğu ölçülebilir bir gelir kaybına uğramasına rağmen, ticari sistemlerin bütünlüğüne ve kamu hizmetlerinin güvenilirliğine ilişkin güven kaybını ölçmek mümkün olmamıştır. Terör saldırılarında olduğu gibi, saldırgan için asıl hedef, saldırıdan ziyade daha geniş bir nüfusun korku duymasıdır. Estonya hükümeti tarafından saldırılara meydan okuyan karşılıklar ve Kuzey Atlantik Antlaşması Örgütü (NATO)ve Avrupa Birliği(AB) tarafından verilen hızlı destek, saldırıların ardından Estonya'yı eskisinden daha güçlü, teknik, siyasi ve moral konuma çıkarmıştır. Siber saldırıların meydana getirdiği hasarı ölçmenin zorluğu, neyin ölçüleceğine karar vermekten ziyade hasarın derecesini belirleme meselesidir. Sonuç olarak saldırıların **ölçülebilirliği düşüktür.**

Muhtemel Meşruiyet (presumptive legitimacy):Estonya saldırılarının **muhtemel meşruiyeti düşüktür.** Hedefler, Rusya'nın muazzam gücünü Estonya'ya hatırlatmaya yönelik bir bakış açısıyla seçilmiş olsa da, saldırılar sadece bir devlet tarafından yapılabilecek büyüklükte veya karmaşıklıkta değildir. Araştırmacılar saldırılarda kullanılan, herhangi bir hükümet, şirket, organize suç örgütü, siyasi grup ve hatta onları çalıştırmak için yeterli araca sahip bireyler tarafından kiralanmaya müsait botnetler tespit etmiştir. Bu saldırı araçlarının geniş ölçüde kullanılabilirliği ve bu araçların ortak yapısı, siber alanda gerçekleştirilen eylem ve fiziksel dünyada görünmeyen etkiler nedeniyle düşük muhtemel meşruiyet değerlendirmesiyle sonuçlanır.

Sorumluluk (state involvement): Son olarak, **sorumluluk unsuru düşüktür.** Rus hükümeti saldırılara katılmış ve hatta yönlendirmiş olabilir, ancak saldırılardan Rusya'nın sorumlu olduğu iddia edilemez. Böyle bir iddia, askeri ve askeri olmayan eylemlerin temel belirleyicisidir. Rus hükümeti ya saldırıya iştirak etmemiş ya da saldırıdaki rolünü gizlemeyi seçmiştir. Her iki durumda da, bir devlet sorumluluğunun olduğuna ilişkin doğrudan veya ısrarlı iddia olmamıştır.

Genel tabloya baktığımızda, yüksek aralıktaki bir faktör (anilik), orta aralıktaki üç faktör (yıkıcılık, nedensellik ve istilacılık) ve düşük aralıktaki üç faktör (ölçülebilirlik, muhtemel meşruiyet ve sorumluluk) ortaya çıkmıştır. Bu tablo saldırıların uluslararası hukukta kuvvet kullanımı olarak nitelendirilemeyeceğini göstermektedir.

Bu saldırılar uluslararası barış ve güvenliği potansiyel olarak tehdit etmekte ve BM Anlaşmasını ihlal etmektedir. Siber saldırılar kuvvet kullanma seviyesine yükselmese de, onlara izin verildiği anlamına gelmez; sadece verilecek karşılığın askeri güçten başka bir araç olmasını gerektirmektedir. Bunlar meşru müdafaa yöntemleri değil verilebilecek diğer karşılıklardır. Bu karşılıkların bir dava, bir tutuklama, diplomatik bir taarruz veya gizli bir operasyon şeklinde olması mağdur devletin seçimi olacaktır.

Siber saldırıların yeni olması hedefleri, araçları savaş hukukuna göre ne tür bir davranışın yasal olduğu konusunda büyük bir kafa karışıklığına yol açmıştır. Etkileri dereceli olarak farklılaşan ancak türü değişmeyen silahlar geliştikçe, kinetik eylemlere uygulanmak üzere savaş hukukunu geliştirmek için yüzyıllar sürmüştür. Bazı siber saldırılar hala bu paradigmaya uymaktadır. Örneğin bir radyo vericisinin özel bilgisayar operasyon ekibi tarafından imha edilmesi, hiçbir yeni fikri zorluğa neden olmayacaktır. Bununla birlikte, başka bir ülkenin devlet ana bilgisayarına bir truva atını yerleştiren ve ardından tetikleyen devlet dışı bir dizi yeni konuyu gündeme getirecektir.

2.3.7.2. İran'ın Nükleer Reaktörlerine Stuxnet Siber Saldırısının Wingfield Analizi Kapsamında İncelenmesi

2009 yılında İran'ın Natanz nükleer yakıt zenginleştirme tesislerine yapılan ve kullanılan virüsün adıyla 'Stuxnet saldırısı' anılan bu saldırının ABD tarafından yapıldığına ilişkin yaygın bir kanaat vardır. ABD, bu saldırıyla ilgili olarak saldırıyla bir ilgisinin olduğuna veya olmadığına ilişkin resmi bir açıklama yapmamıştır.

Yıkıcılık (severity): İran'ın nükleer reaktörlerine yapılan siber saldırılarda insan veya mal kaybına yönelik fiziksel bir etki gözlemlenmemiştir. Ancak saldırı sonrasında nükleer tesisin soğutma sisteminde ortaya çıkabilecek bir arıza nükleer bir serpintiye neden olabilirdi. Ancak bu konuda bir açıklama yapılmamıştır. Uranyum zenginleştirme tesisi kapasitesi %15 dolayında düştüğüne ilişkin yapılan açıklamalar

da dikkate alındığında saldırının yıkıcılık ölçeğine göre **ağır maddi hasar** olduğu gözükmemektedir.

Anilik (immediacy); 22 Haziran 2009'da yerel saatle 16.30 ve 07 Temmuz 2009 tarihinde yerel saatle 17.00'de başlayan saldırının gelişme hızı, saldırıların orta düzeyde anilik içerdiğini göstermektedir. Siber saldırıların başlatılması ve hedeflerine ulaşması arasında günler, saatler geçtiği görülmektedir. Anilik ölçeğine göre saldırı **orta anilik derecesinde** gözükmemektedir.

Nedensellik (directness); Stuxnet'in virüsünün hedefi nükleer tesisin kontrolü için kullanılan SCADA (Siemens supervisory control and data acquisition) sistemlerini ele geçirip sonrasında fiziksel olarak kontrol sistemlerinin çalışmasını değiştirmektedir. Saldırının hedefi ile nükleer reaktörlere verilen zararlar buna sebep olan stuxnet virüs saldırısı arasında doğrudan bir bağ vardır. Bu nedenle **sonucun tek nedeni olan eylem nedeniyle saldırının nedenselliği yüksek** olarak kabul edilmektedir.

İstilacılık (invasiveness); İstilacılık, bu vakada düşük seviyede olan sınırın fiziksel olarak geçilmesi veya bu vakada yüksek olan belirli bir devletin topraklarındaki saldırıların dikkate alınması olarak nitelendirilebilir. İran sınırını ihlal eden bir kuvvet tespit edilmemiş olsa da, nükleer tesislerdeki bilgisayar ağına karşı düzenlenen virüs saldırısının hedefi münhasıran İran olmuştur. Sonuç olarak İran sınırı elektronik olarak geçilmiş; eylem belirli bir alanda gerçekleştiğinden **saldırının istilacılık niteliği orta seviyeden yüksek seviyeye yaklaşan olarak tespit edilmiştir.**

Ölçülebilirlik (measurability); Saldırıların ölçülebilirliğini değerlendirmek zordur. Hedef İran'ın Natanz nükleer yakıt zenginleştirme tesisleridir ve tesisin kapasitesinin %15 dolayında düştüğü açıklanmıştır. Ayrıca resmi bir açıklama bulunmasa da saldırının İran'ın nükleer çalışmalarını birkaç yıl geriye götürdüğü, saldırıdan kaynaklı kazaların saldırıdan aylarca sonra da devam ettiği söylenmektedir. Uluslararası Atom Enerjisi Kurumu'nun verilerinde İran'ın uranyum zenginleştirme faaliyetlerinde dikkate değer bir düşüşün gözlemlenmesi, tesislerde birtakım zararların meydana geldiğini göstermektedir. Sonuç olarak; saldırının etkileri makul bir kesinlik ile kabaca büyüklük sırası ile tahmin edilebilir olduğundan saldırıların **ölçülebilirliği orta derecededir.**

Muhtemel Meşruiyet(presumptive legitimacy): Gazeteci David Sanger, makalesinde “*Stuxnet’in Obama’nın emriyle NSA’nın Maryland’deki merkezinde geliştirildiğini ve İsrail’de kurulan bir model nükleer tesiste denendiğini*” iddia etmektedir. Sanger, “*Bush döneminde oluşturulan ve “Olympic Games” (Olimpiyat Oyunları) adı verilen bu virüsü Obama’nın geliştirmeye ivme kazandırıp, İsrail ile birlikte geliştirdiğini ve adının “Stuxnet” olarak değiştirildiğini*” ifade ediyor.⁶¹ Stuxnet virüsü, saldıracağı hedef veya hedefleri hakkında önceden belirli bilgilere sahip olan, çoklu sistem zafiyetlerinden faydalanabilen, çok gelişmiş, çalınmış güvenlik sertifikaları sayesinde sistemlere nüfuz edebilen ve bu sayede sistemleri çökertebilen özel bir virüs olarak tanımlanmaktadır. Siber alanda gerçekleştirilen ancak fiziksel alanda sonucu ortaya çıkan eylemin **muhtemel meşruiyeti orta derecededir.**

Sorumluluk (state involvement): ABD resmi makamları veya yetkilileri, Stuxnet’le bir ilgileri olduğu veya olmadığına ilişkin bir açıklama yapmamıştır. Ancak bu virüsün yazılması ve saldırı amacıyla kullanılmasında ABD’nin bir rolü olduğuna ilişkin iddiaları hiçbir zaman yalanlamamıştır. Savunma Bakan Yardımcısı William Lynn, gazeteci Melissa Lee’nin “ABD Stuxnet’in geliştirilmesinde herhangi bir şekilde yer aldı mı?” sorusunu son derece politik bir cevapla geçiştirmiştir. Ancak bilişim dünyasının ileri gelen uzmanları, Stuxnet’in teknik özellikleri göz önüne alındığında, virüsün ABD tarafından geliştirildiği ve Stuxnet saldırısının da yine ABD tarafından düzenlendiğine kesin olarak bakmaktadırlar. Eylemin sorumluluğu, icracı devlet tarafından kabul edilmemiş olsa da reddedilmemiş olduğundan; iştirak derecesi büyük olduğundan **sorumluluk unsuru yüksektir.**

Genel tabloya baktığımızda, yüksek aralıktaki dört faktör (yıkıcılık, nedensellik, istilacılık ve sorumluluk), orta aralıktaki üç faktör (anilik, ölçülebilirlik ve muhtemel meşruiyet) ortaya çıkmıştır. Bu tablo saldırıların uluslararası hukukta kuvvet kullanımı olarak nitelendirilebileceğini göstermektedir. Ancak uluslararası topluluk tarafından böyle nitelendirme yapıldığına ilişkin bir açıklama yapılmamıştır.

⁶¹ David A. Sanger, “Obama Order Step Up Wave of Cyber attacks Against Iran”, **The New York Times**, 01 June 2012, (Çevrimiçi) <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>, 23.03.2019

Bitkiler ve hayvanların tehlikeye karşı reaksiyonu “karşılıklı evrimsel silahlanma yarışı teorisi” kapsamında değerlendirildiğinde, bir türe ait genetik kompozisyonda bir değişiklik olduğunda karşılık olarak diğerinde de değişiklik meydana gelmektedir. Sürekli değişim ve gelişmeyi temsil eden Heliconius kelebeği ile tutkulu asma arasındaki karşılıklı evrim bir örnek olarak verilebilir. Tutkulu asma kendini korumak için zehir geliştirirken Heliconius Kelebeği ise zehri özümseme yeteneğini geliştirip bu zehir kendi düşmanlarına karşı bir silah olarak kullanmıştır. Benzer şekilde Heliconius asmayı yiyerek beslenirken asmanın üremesini ve hayatta kalmasını sağlamıştır.⁶²

Bu benzetmeden yola çıktığımızda devletlerin de çıkar ve menfaatlerini gerçekleştirmek için belirli şartlara bağlı olarak kullandıkları geleneksel kuvvet kullanma yöntemlerinin benzer şekilde sürekli değişim ve gelişim içinde olduğunu söyleyebiliriz. Devletlerarasındaki çıkar ve menfaat mücadelesinin daha adil ve hakkaniyetle devamı için Birleşmiş Milletler Anlaşmasıyla oluşturulan hukuki düzenin de çıkar ve menfaatleri elde etme yöntemlerinde meydana gelen bu değişime ayak uydurması beklenmektedir.

İnsan var olduğundan bugüne barutun icadından nükleer silahların kullanımına kadar meydana gelen gelişmeler kara, deniz, hava ve uzay alanlarıyla ilgili olmuştur. Ancak siber alan bu alanlardan çok farklı, insan yapımı ve suni bir alandır. Siber alanın özellikleri bu alanlara özgü kriterlerle açıklanamayacak kadar karmaşıktır. Ayrıca bu alanda kullanılan araçlar diğer alanlardan çok farklıdır. Bu alanlara ilişkin olarak yüzyıllar içinde değişip gelişerek ortaya çıkan hukuk kurallarının bu yeni alana uygulanmasının daha başlangıçta ayrıntılara girmeden pek mümkün olmadığı aşikârdır.

Bütün bunların yanında bu yeni siber alanlarla ilgili normlar da henüz tam olarak ortaya çıkmamıştır. Siber alanla ilgili normlar yaygınlaşıp içselleştirilinceye kadar bu ortamda yapılabilecek en iyi şeyin Talinn Belgesi ve Wingfield Analizi gibi yöntemlerden istifade ederek mevcut Silahlı Çatışma Hukuku kurallarını siber alana

⁶² Ruthmery Pillco Huarcaya, Passionflowers and Butterflies: A love-hate relationship, **Osa Conservation**, (çevrimiçi) <http://osaconservation.org/2017/10/passifloras-butterflies-a-love-hate-relationship/>, 09.04.2019

uygulamak olduđu deęerlendirilmektedir. Norm teorisine gre uluslararası bir normun varlıęı herkesin davranışını etkiler ve cesaret kırıcıdır veya norm tarafından teşvik edilen davranışlarda bulunmayı artırır. Ancak şimdiye kadar meydana gelen siber saldırılarla ilgili olarak Silahlı Çatışma Hukuku uygulamaları bir tespitten teye geçmemiş, mağdur devletleri korumada başarısız olduđu gibi güçlü devletleri cesaretlendirerek daha ok devletin ulusal gvenlik strateji belgesinde saldırgan yntemleri tercih ettięi grlmektedir. Bu nedenle Silahlı Çatışma Hukuku kurallarının mevcut siber saldırılara tatbik edilmesi sonularının lkeleri saldırgan davranışlardan caydırıcılıęının yeterli olmadığı dřnlmektedir. Bugnk devlet davranışları siber alanda yeni silahlanma yarışının bařladıęına veya bařlayacaęına işaret etmektedir.

Bu sonular, nmzdeki yıllarda daha ayrıntılı analizler iin yalnızca ıkış noktalarıdır. Bu yeni siber silahlar ve bu silahları kullanma taktikleri geliřtike, yeni organizasyonlar tasarlanıp yaratıldıka ve gittike daha profesyonel bilgi operatrleri eęitildike, hukuki konularda saęlanacak netlik gelecekteki askeri komutanlar ve siyasi karar vericiler iin en byk alışma alanını ve en fazla sayıda seeneęi sunacaktır.

ÜÇÜNCÜ BÖLÜM

SİBER SALDIRININ ATFEDİLMESİ

3.1.ATIF SORUNUNUN TANIMLANMASI

Atfetme, kim yaptı sorusunu cevabını bulmaktır. Uluslararası hukuk açısından iyi bir atıfta bulunma, uluslararası ve yerel olan her türlü zorlama ve caydırma biçiminin temelini oluşturmaktadır. Atfı hatalı yapmak, bir devletin güvenilirliğini, etkinliğini ve nihayetinde özgürlüğünü ve güvenliğini zayıflatmaktadır.

Bazen atfetme kararsızlığa ve büyük olaylara sebep olmaktadır. Ağustos 2013'te Suriye'nin başkenti Şam'ın Ghouta bölgesinde kimyasal silah kullanımı; 2014 yılında Malezya Hava Yollarına ait yolcu uçağının Ukrayna üzerindeyken düşürülmesi; 2014 Gazze'de savaş başlatan üç İsrailli gencin kaçırılması olaylarının ortak yanı faillerin kim olduğunun tam olarak tespit edilememiş olmasıdır. Atfetme sorunu, son yıllarda ortaya çıkmış bir problem değildir. Atfetme ile ilgili kararsızlık savaşlara da neden olmaktadır. Avusturya tahtının veliahdı Ferdinand ve eşinin, bir Sırp milliyetçisi tarafından 1914 yılında Saraybosna'da öldürülmesi sonucunda Avusturya, bu olayı gerekçe göstererek Sırbistan'a savaş ilan ederek I. Dünya Savaşını başlatmıştır.¹

Uluslararası olaylar sistematik bir atıf tartışması yapmak için fazlaca karmaşık olduğundan konunun daha iyi anlaşılması için iç hukuktan örnek vermek faydalı olacaktır. İşlenen bir suç ancak ilgili kolluk birimlerine gelen ihbar veya şikâyetle ortaya çıkabilir. Sonra soruşturma başlar. Kolluk görevlileri suç mahallini emniyete alır ve tanıkların ifadesine başvurur. Adli tıp uzmanları, örneğin, kurbanın vücudunda bulunan bir mermiyi, olay yerinde bulunan ve üzerinde parmak izi var olan silahla eşleştirmek gibi belirli delilleri bulmaya ve analiz etmeye çalışır. Elde edilen kanıtlardan ve olaya ilişkin tanıklardan şüpheli kişi tespit edilir. Ancak hala bu kişinin suçu işlediği kesin değildir. Kim yaptı sorusuna verilecek yanıtın tespiti ve atıf sorununun çözümü açılacak dava ve bu dava sonunda verilecek kararlar son bulacaktır.

¹John Graham Royde-Smith, Dennis E. Showalter, World War I, **Encyclopediia Britanica**, (çevrimiçi) <https://www.britannica.com/event/World-War-I>, 27.04.2019

Görüldüğü gibi iç hukuk örneğinde sistemli ve düzenli bir yaklaşımla atıf sorunu çözümlenmektedir.

Yukarıdaki örnekten de anlaşılacağı üzere atfetme, her zaman tek bir kişinin baş edemeyeceği kadar büyük ve karmaşıktır; atfetme, uzmanlıkların ve alt uzmanlıkların olduğu bir işbölümünü gerektirmektedir. Atfetme, kademeli olarak farklı seviyelerde, teknik kanıtların toplanmasını, soruşturma başlatılmasını, analiz yapılmasını ve ardından yasal işlemlerin başlatılarak davanın açılmasını gerektirmektedir.

Uluslararası olaylarda atıf yukarıda da bahsettiğimiz gibi fazla karmaşıktır. Siber saldırıların atfedilmesi ise diğer uluslararası olaylardan daha karmaşık ve daha az bilinen bir süreçtir. Siber alanda, atfetmenin nasıl yapılacağına ilişkin tartışmalar son derecede yavaş bir şekilde gelişmektedir.² Halen, siber saldırıların atfedilmesi ile ilgili tartışmalara üç genel varsayım hâkimdir.

İlk varsayım, siber alanda atıfta bulunmanın temelde internetin teknik mimarisi ve yapısından kaynaklanan ve yeni gelişen bir alan olması nedeniyle güçlüklerle karşılaşıldığına ilişkindir.³ Bu varsayıma göre bu sorun ancak internetin teknik olarak yeniden tasarlanması ile tam olarak çözülebilir. İkinci varsayım, atfedilmeye ilişkin ikili bir bakış açısını ortaya koymaktadır. Bu varsayıma göre atfetme bizi ya suçluya götürecek ya da sadece sahte bir internet adresi, gizlenmiş dosyalar veya çıkmaz bir yol ile sona erecektir. Üçüncü varsayıma göre, atfetme için kullanılacak kanıtları analiz etmek, zenginleştirmek ve sunmak zor değildir asıl zorluk bu kanıtları bulmaktır.⁴ Bu üç varsayım oldukça yaygındır, sezgiseldir ve yanlış da değildir ama sınırlı ve yetersizdir. Atfetme son on yılda önemli ölçüde gelişmiştir. Siber olayların gerçek niteliği şimdiye kadar literatürde kabul edilenden çok daha incelikli, daha yaygın ve daha politiktir.⁵

² Susan Brenner, At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, **The Journal of Criminal Law & Criminology**, 97/2 (2007), s.379–475.

³ W. Earl Boebert, 'A Survey of Challenges in Attribution', in Committee on Deterring Cyberattacks (ed.), **Proceedings of a Workshop on Deterring Cyberattacks** (Washington DC: National Academies Press 2011), s.51–2

⁴ Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, **Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains**, Bethesda, MD: Lockheed Martin Corporation 2010

⁵ Amir Lupovici, 'The "Attribution Problem" and the Social Construction of "Violence"', **International Studies Perspectives** 2014, s.1–21.

Atıf üzerindeki tartışmayı mevcut tartışmaların ötesine taşıyan çalışmalar üç soruyu gündeme getirmektedir.

Birinci soru: eğer atfetme ilk ve en başta teknik bir sorun değilse, o zaman nedir? İkinci soru: eğer atfetme ikili ilişki meselesi değil, bir derece meselesi ise, o zaman normal atfetme nedir ve yüksek kaliteli atfetme ile düşük kaliteli atfetmenin farkı nedir? Üçüncü soru: eğer kanıt önemsiz ve şüpheli ise nasıl sıralanmalı ve analiz edilmelidir? Bir bütün olarak atfetme nasıl yönetilmeli ve üçüncü şahıslarla paylaşılmalıdır?

Siber suçlular, casuslar ve sabotajcılar izlerini gizleyebilmekte, çevrim içinde gizli olarak kalabilmekte ve atfetme probleminin arkasına saklanabilmektedirler. Ancak son zamanlarda atfetme daha doğru ve başarılı olarak yapılabilmektedir. Saldırganlar, artık gizlilik örtüsünün altında ciddi zarar ve hasara neden olabileceklerini ve hiçbir şey olmamış gibi kurtulamayacaklarının farkına varmışlardır. Atfetme sorunu tam olarak çözülmesi bile, doğru yönetilerek suçlulara erişilebilecektir.

İnternetin devletlerden güç aldığı ve zayıf devlet dışı aktörler, özel kuruluşlar ve suçluların bu güce teknolojinin sağladığı imkânlarla eriştiğine ilişkin yaygın bir kabul bulunmaktadır.⁶ Atfetmede ise sadece devletler, en karmaşık işlemleri yüksek bir kesinlik düzeyi ile atfetmek için yeterince kaynağa sahip bulunmaktadır.

İnternette en savunmasız ülkelerin en sanayileşmiş ve internete bağlı olanlar olduğu, daha az gelişmiş ve dolayısıyla daha az internete bağlı ülkelerin savunma açısından bir avantaja sahip olduğu yönünde bir kabul bulunmaktadır. Atfetmede, ise bu mantık ters işlediği için en sanayileşmiş ve internete bağlı ülkelerin atfetme kabiliyetleri daha yüksektir. Bir devletin teknik üstünlüğü, elindeki yetenek ve beceri havuzu ne kadar büyükse, devletin kendi örtülü operasyonlarını gizleme, başkalarını ortaya çıkarma ve buna cevap verme yeteneği o kadar yüksek olacaktır.⁷

İnternetin saldırı baskın bir ortam olduğuna ilişkin yaygın bir görüş vardır. Bu görüşe göre saldırırganlar, savunma yapanlara karşı yapısal bir avantaja sahiptir ve bu avantaj internetin teknik mimarisine dayanmaktadır. Savunmada olanların her zaman

⁶ Joseph S. Nye, **Cyber Power**, Belfer Center for Science and International Affairs, 2010, s.6-18

⁷ Joseph S. Nye, **A.e.**,s.6-18

doğru hareket etmesi gerekirken saldırganın sadece bir kez doğru hareket etmesi yeterlidir. Atfetmede ise saldırganın yalnızca bir kez hata yapması yeterlidir, savunma yapan yapacağı incelemeyle saldırganın yaptığı hatadan yola çıkarak ipuçlarını ortaya çıkarabilir ve saldırganı tespit edebilir.

3.2 ATFETME İŞLEMİNİN SEVİYELERİ

Bir suçlunun bir suçla eşleştirilmesi, çeşitli düzeylerde belirsizliği en aza indirgeyerek yapılmaktadır. Teknik düzeyde, atfetme hem bilim hem de bir sanattır. Doğru atfetme için tek bir reçete, tek bir yöntem veya akış şeması veya kontrol listesi yoktur. Doğru ipuçlarını bulmayı, bir dizi ayrıntılı soruya disiplinli bir şekilde odaklanmayı ve aynı zamanda teknik olarak deneyimli operatörleri ve onların güçlü sezgilerini gerektirmektedir. Atfetme, ancak düzensiz ölçümlerden ve karmaşık veriler arasından doğru tespiti yapabilme becerisidir. Sonuç olarak, aynı zamanda takım halinde çalışmayı gerektiren başarılı bir atfetme bir kişinin yapabileceğinden daha fazla beceri ve kaynağı gerektirmektedir. Sonuçları en iyi şekilde kullanmak, dikkatli bir yönetim ve örgütlü bir süreci gerektirmektedir.

Atfetme işlemi taktik, operatif ve stratejik seviyedeki analiz ve değerlendirmeleri içermektedir. Taktik düzeydeki atfetme teknik atfetmeye karşılık gelmekte, teknik olarak elde edilecek ipucu ve verilerden hareket ederek atıf işlemi gerçekleştirilmektedir. Operatif düzeydeki atfetmede ise teknik verilere ilave olarak çeşitli farklı kaynaklardan gelen teknik olmayan analizler ve jeopolitik bilgilerle bu teknik veriler sentezlenerek saldırının yüksek seviye mimarisi ve saldırganın profili tespit edilmektedir. Operatif düzeyde meydana gelen saldırıyı açıklamak için geliştirilen hipotezlere dayanılmaktadır. Stratejik seviyedeki atfetmede operatif seviyedeki atfetmeye politik riskler de dâhil edilerek saldırının gerekçesi ve önemi ortaya konularak saldırıyı kimin yaptığı bulunmaktadır. Politik riskler, en önemlisi meydana gelen hasar olan bir dizi faktör tarafından belirlenmektedir. Bu hasar finansal, fiziksel veya itibari olabilir.⁸

⁸ Thomas Rid & Ben Buchanan, Attributing Cyber Attacks, **Journal of Strategic Studies**, 2015, Vol. 38,s.7

Üç aşamada gerçekleşen atfetmenin ilk aşaması kaynak ayırma ve süreci yönetmek; ikinci aşaması elde edilen delilleri değerlendirmek ve karar vermek ve son aşama ise ulaşılan sonucu üçüncü taraflara ve kamuoyuna kısmen iletmektir.⁹

Atfin başarısı, doğru soruların sorulmasıyla ilişkilidir. Taktik, operatif ve stratejik seviyelerin her birinde bu seviyelerin özelliklerine has soru kümeleri bulunmaktadır. Bir alt seviyeden gelen soruların cevapları bir üst seviyenin başlangıç noktasını oluşturmaktadır. Bir takımın tüm sürece bakışı ne kadar iyiye, yapılan atfin başarısı da o kadar iyi olacaktır. Bu süreç dinamiktir, doğrusal değildir ve her bir durum diğerinden farklıdır, bu nedenle esnek olmayan bir akış modeli ya da doğrusal bir kontrol listesi yaklaşımı uygun değildir. Süreç, taktik ve teknik değerlendirmelerden başlayarak, yavaş yavaş stratejik düşünceye doğru ilerleyerek katman katman devam etmektedir. Teknik katman genellikle bir soruşturmanın başlangıç noktasıdır. Süreç hem genişliğine hem de derinliğine uzanmaktadır. Bu süreçte analistlerin bilgisayar kodu, ağ etkinliği, dil ve daha pek çok konuyla ilgili soruları cevaplamak için verimli, takım odaklı bir şekilde çalışması gerekmektedir.

Atfetme işleminin stratejik, operatif ve taktik seviyelerinin her biri ayrı bir analitik zorluğu temsil etmekte, belirli girdi verilerine ve özel uzmanlığa dayanır ve başarılı bir atıfta bulunmanın ayrı bir yönünü aydınlatmaktadır. Her seviyedeki analizin diğer seviyedeki analizler hakkındaki bilgiye ve tadil edilmeye ihtiyacı vardır. Atfetme sürecinin tipik olarak bir başlangıcı ve bir sonu olmasına rağmen, döngünün yeni ayrıntılarla karşı karşıya kaldığı ve yeni ayrıntıların sırayla yeni hipotezlere yol açtığına, belirli bir ardışık veya kronolojik sıra izlemesi gerekmemektedir.

Bununla birlikte, katmanlar birbirleriyle ilişkili olsalar da ayrı ayrı analiz edilecekleri farklı görevleri temsil etmektedirler. Bazen bir olayın ilk bilenleri, teknik seviyenin üstünde olabilir bu nedenle atfetme işlemi operatif veya stratejik düzeyde başlayabilir. Teknik olmayan bilgi kaynakları ya da daha geniş jeopolitik bağlamın yönlendirmesiyle, bazen sezgiyle bile, kötü niyetli faaliyet, teknik göstergeler tespit edilmeden önce ya da hatta teknik incelemeye başlamadan önce belirlenebilir. Atıf için

⁹ Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, a.g.e., s.8

her iki yöntem de uygulanabilir, bazen stratejik ve operatif düzeyde yapılan değerlendirmeden sonra teknik analizler yapılabilir veya bazen bunun tersi yapılabilir.

Siber tehditler yüksek düzeyde karmaşıklığa ulaşmıştır. Bu nedenle atfetme geniş beceriler gerekmektedir. Hem bu tehditlerin üstesinden gelmek hem de atfetme analizi yoluyla tehdidin mimarisini ortaya çıkarmak, tam bir iş bölümü gerektirmektedir. Örneğin, bir virüsten koruma araştırma ekibi, kötü amaçlı bir yazılımın mekanizmasını tersine çevirerek tehdidin mimarisini bulmaya çalışırken, kontrol mühendisleri bir endüstriyel tesise karşı yapılmış siber saldırıda kullanılan hedefe özel bir yükün tasarımını incelemeye odaklanabilirler. Siber güvenlik şirketleri İran'ın nükleer tesislerine yapılan siber saldırıda kullanılan stuxnet virüsünün mimarisini ortaya çıkarmak için virüsün yayılma mekanizmasını, komuta kontrol kurulumunu ve endüstriyel kontrol sistemini hedefleyen yükünü analiz etmişlerdir.¹⁰ Askeri doktrinlerde olduğu gibi, taktiksel faaliyetler hayati öneme haiz operatif düşüncelerin altında kalmaktadır. Farklı seviyeler için yapılan analiz, çok farklı beceriler gerektirmektedir. Bu uzmanlık, askeri operasyonlarda kesin olarak belirlenmiş bir ilkedir. Hiçbir komutan, terörle mücadelede etkin olarak kullanılan komando birliklerine teröristlerin finansmanını veya patlayıcı cihazların tedarik zincirini inceleme görevi kesinlikle vermez. Savaş uçaklarının pilotları kendi hedeflerini seçmezler. Füze mühendisleri nükleer strateji yapmazlar. Siber saldırılar ele alındığında, bu tür temel beklentiler henüz atıf çalışmaları yapan küçük uzman topluluğu için tam olarak oluşmamıştır.

Dünyada her gün birçok siber olay meydana gelmekte ve bu olayların çoğu ile ilgili hiçbir soruşturma yapılmamaktadır. Bu nedenle atfetme işlemi, gerçekleşen siber saldırıların tamamı için değil genellikle hasarla sonuçlanan saldırılara yönelik olarak yapılmaktadır. Meydana gelen siber saldırıyla ilgili soruşturmanın başlatılması ortaya çıkan hasarla doğrudan ilgilidir. Meydana gelen hasarın maliyeti de siber olayı atfetmek için kullanılan kaynak miktarını belirlemektedir. Bilgisayar ağına izinsiz giriş herhangi bir belirgin hasara neden olmadıysa, bir şirket ya da bir devlet kurumu onu görmezden gelmeye, kısmen araştırmaya ya da genel olarak savunmasını

¹⁰ Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), s.365–404.

iyileştirmeye meyillidir. Görünüşte önemsiz görünen ihlalin kökenine yönelik pahalı bir soruşturma başlatmayı hiçbir yönetici göze almayacaktır. Hasarın eksik veya yanlış algılanması da atıf sürecinin hiç başlatılmamasına sebep olmaktadır.

Taktik seviyede amaç, olayın öncelikle teknik yönlerinin ne olduğunun anlaşılmasıdır. Operatif hedef, saldırının yüksek seviye mimarisini ve saldırganın profilini ne olduğunu anlamaktır. Stratejik amaç, saldırıdan kimin sorumlu olduğunu anlamak, saldırının gerekçesini, önemini, kim ve niçin sorularına verilen uygun cevabı değerlendirmektir. İletişim de çok önemlidir, adli bir soruşturmanın sonucunun açıklanması, atıf sürecinin önemli bir parçasıdır ve değerlendirmede düşük öncelik verilmemelidir. Nitekim saldırıdan kimin sorumlu olduğunun kamuya açıklanması da önemli etkilere sahip olabilir, suçlular operasyonu iptal edebilir, taktiklerini değiştirebilir veya iddialara açıkça tepki verebilir, böylece saldırıya uğrayan mağdur alacağı tedbirler bu tepkilere göre şekillendirebilecektir.¹¹

Siber saldırıların atfında detay çok önemlidir. Ancak detaylar aynı zamanda çok uğraştırıcı olabilmektedir. Bilgi teknik katmandan, operatif ve stratejik katmanlara geçerken, mutlaka sentezlenmeli her seviyeye uygun bir değerlendirme yapılmalıdır. Ancak o zaman elde edilen veriler anlaşılabilir ve faydalı olacaktır. Teknik analizler siber saldırılar hakkında çok miktarda ayrıntı sağlayabilir. Bu ayrıntılar, sıklıkla kullanılan yöntemleri, kullanılan virüsün yük taşıma mekanizmasını, komuta ve kontrol altyapısını, hedeflenen verileri, tersine mühendislik analizini ve saldırıya uğramış ağlardan elde edilen ham verileri içermektedir. Toplanan teknik detayların bazılarının, hatta çoğunun, olayla alakası sınırlı düzeyde olmaktadır. Olayla ilgili bazı taktiksel detayların, tıpkı siyasi bağlamın ayrıntılarının adli araştırmacıyı fazla ilgilendirmediği gibi operatif ve stratejik seviyelerde hiçbir önemi olmayabilir. Uygun bir sentez yapılmadığında, birçok teknik materyalin bulunması, operatif veya stratejik olarak cevaplanması gereken soruların daha kesin bir şekilde cevaplanabileceği anlamına gelmeyecektir. Veriler, teknik seviyeden operatif ve stratejik seviyeye akarken, cevaplanması gereken sorular genel sorulara, analizler teknik seviyeden

¹¹ Jon R. Lindsay, **a.g.e.**, s.365–380

stratejik seviyeye doğru kaydıkça atfetmeyle ilgili açıklamalar da daha genel ifadelere dönüşmektedir.

Bilgisayarlara izinsiz giriş mekanizması adli bulgulara dayanarak tespit edilebilir. Ancak bu izinsiz girişin sebebinin ne olduğunun tespiti bu konuda bir hipotez geliştirmeyi ve bu hipotezi testlerden geçirmeyi gerektiren bir süreçtir. Operatif seviyedeki hipotezler, adli değerlendirmeleri içerebilir, ancak bu hipotezler mevcut teknik ve teknik olmayan kanıtlarla tam olarak desteklenemeyebilir. Stratejik düzeydeki sonuçlar, adli bulgulardan iyice arındırılmış olduğundan önemli miktarda faraziye ve yargı içerebilir. Stratejik düzeyde, liderler ve üst düzey analistler, operatif soruların cevaplarını toplamak ve anlamlı sonuçlar çıkarmakla görevlendirilmelidir. Liderlerin ve üst düzey analistlerin ön analizleri eleştirmeleri, ayrıntıların araştırılmasını ve alternatif açıklamalar talep etmeleri, stratejik analiz açısından vazgeçilmez bir unsurdur.

Atfetme sürecindeki en zor unsurlardan biri, istihbarat eksikliğidir. Verimli istihbarat kaynaklarının sayısı arttıkça, atfetmenin kalitesi de artacaktır. Üstelik istihbarat eksikliğinin önemi, atıf işleminin seviyelerine bağlı olarak artmaktadır. Bilgisayar sistemlerine izinsiz girişlerden kaynaklanan sayısal adli kanıtlar, çoğunlukla çok sınırlıdır. Operatif ve özellikle stratejik bir seviyede, diğer istihbarat kaynakları örneğin ele geçirilen telefon görüşmeleri veya operasyon yöneten veya organize eden kişilerin e-postaları büyük resmi ortaya çıkarabilir. Yüksek yetenekli istihbarat teşkilatlarına sahip devletlerin, yüksek nitelikli özel şirketlerden bile daha fazla atfetme sürecine hâkim olmalarının en önemli sebeplerinden biri tüm istihbaratının kaynaklarının kullanılması ve daha az istihbarat eksikliğinin bulunmasıdır.¹²

1998 yılında yapılan saldırılarda saldırganlar ABD Savunma Bakanlığını, Enerji Bakanlığını, Ulusal Havacılık ve Uzay Dairesini, Ulusal Okyanus ve Atmosfer İdaresini, birçok savunma şirketini ve üniversiteleri hedef almıştır. Saldırganlar pilotların kask tasarımlarından atmosferik verilere kadar değişen bilgileri ele geçirmiştir. ABD Federal Araştırma Bürosu (FBI) araştırmacıları başlangıçta çok

¹² Thomas Rid & Ben Buchanan, **a.g.e.**, s.8

başarısız olmuşlardır.1999 yılının başlarında, ABD Savunma Bakanlığı soruşturmayı desteklemeye başlamıştır. Savunma Bakanlığına bağlı Bilgisayar Ağı Savunma Ortak Görev Gücü işe, kolluk güçleri tarafından elde edilen dijital adli verileri incelemekle başlamış, ancak daha sonra sinyal istihbaratı, insan istihbaratı hatta son zamanlarda iletişim sistemlerinin kurulup kurulmadığını görmek için şüpheli binaların havadan eski görüntülerini bile incelemeye dâhil etmiştir. Sonuç olarak ABD kritik siber altyapısına izinsiz girişlerin dijital adli bulgularının ötesine geçen istihbarat kaynakları, ihlallerinin Rus hükümetine makul bir kesinlikle atfedilmesini sağlamıştır.¹³Yapılan soruşturma ve analizler tüm kaynak istihbaratının ne kadar önemli olduğunu ve istihbarat eksikliği giderildikçe atfetmenin daha fazla kesinlik kazandığını ortaya çıkarmıştır.

3.3.ATFETMENİN TEKNİK KANITLARI

Birçok durumda teknik kanıtlar atıf sürecinin temelini oluşturmaktadır. Bu kanıtların açığa çıkması her zaman mümkün değildir, ancak hayatidir. Soruşturmaya, gizliliğin ihlal edildiğine ilişkin göstergelerden başlanması muhtemeldir. Gizliliğin ihlal edildiğine ilişkin göstergeler, genellikle ağa sızma veya kötü amaçlı faaliyetlerin teknik bulgularıdır. Bu göstergeler tipik olarak geniş tabanlı otomatik tarama veya olağandışı bilgisayar davranış raporları ile ortaya çıkarılmaktadır. Çok sayıda bilgisayarda derinlemesine ve düzenli adli analiz yapmak ağ yöneticileri için genellikle aşırı maliyetlidir. Ağa sızma veya kötü amaçlı faaliyetler, takip eden araştırmaların kapsamını daraltmaya yardımcı olmak için yararlı bir buluşsal yöntem olarak kullanılmaktadır.

3.3.1.Gizliliği İhlal Göstergeleri

Etkili bir çalışma, gizliliği ihlal göstergelerini üç ana kategoriye ayırmıştır: atomik, hesaplanmış ve davranışsal.¹⁴

Atomik göstergeler, adli değerlerini kaybetmeden bileşenlerine ayıramayan ayrı veri parçalarıdır. Atomik göstergeler, kendi başlarına, kötü niyetli aktiviteyi belirlemektedir. Bilinenler internet adresleri, e-posta adresleri, alan adları ve küçük

¹³ Thomas Rid & Ben Buchanan, **a.g.e**, s.12

¹⁴ Thomas Rid & Ben Buchanan, **a.g.e**, s.15

metin parçalarıdır. Hesaplanan göstergeler benzer şekilde ayrı veri parçalarıdır, ancak bazı hesaplama öğelerini içerirler. Örnek olarak, bir şifre veya program gibi girdi verilerinden türetilmiş benzersiz bir imza olan bir değer özet (hash) verilebilir. Bir veri girişi değişmediği sürece her zaman aynı değerdir. Ağ bilgisayarlarında çalışan programların özet değerleri, zararlı olduğu bilinen programların özet değerleriyle eşleşebilir. Davranış göstergeleri, hem kötü niyetli faaliyeti ortaya çıkaran eylemlerin hem de diğer göstergelerin birleşimidir ve bazı durumlarda geçmişte benzer davranışlarda bulunan belirli bir rakibi işaret etmektedir. Davranışsal bir gösterge, düşük seviyeli çalışanlara karşı ağda bir basamak kazanmak için e-posta yoluyla belirli tarzdaki sosyal mühendislik girişimleri ve müteakiben ağdaki kötü amaçlı yazılımlar sunan bilgisayarlara yetkisiz bağlantıları ile tekrarlanabilir. Bilgisayar ağı savunması konusunda dikkatli olan organizasyonlar, üç tür gizliliği ihlal göstergesini toplamakta ve bu ihlallerin olup olmadığını tespit için rutin olarak ağlarını ve bilgisayarlarını taramaktadırlar. Bir gizlilik ihlalinin kanıtı bulunduktan sonra, daha teknik sorular gündeme gelecektir. Soruların sıraları gösterge, rakip ve tehdide göre değişecektir.

3.3.2.Hedefleme

Neredeyse tüm saldırganların bilgisayar sistemlerine giriş zorluğunun üstesinden gelmesi gerekmektedir. Her bir saldırganın yetkisiz bir sistemde kod çalıştırma yeteneği edinmesi gerekmektedir. Bu tür bir kod, bir sistemin güvenlik açığından yararlanmakta ve saldırgana daha fazla erişim veya işlevsellik imkânı sağlamaktadır. Bu kodu sisteme sokmanın en bilinen yolu teknik güvenlik açıklarından değil, seçilmiş hedefli avlama, sosyal mühendislik mesajları göndererek kullanıcıyı harekete geçmesi için kandırmak gibi yöntemlerle insan zayıflığından yararlanmaktadır. Alt seviyede çalışanlardan oluşan küçük gruplara gönderilen bir e-posta ile ihlal gerçekleştirilmektedir.¹⁵ Adı ilgi çekici bir e-posta, çalışanlardan birinin onu önemsiz posta klasöründen alıp açmasına yetecek kadar ikna edici olabilmektedir. Saldırganların sisteme erişmesine izin veren kötü amaçlı bir kullanım içeren ofis dosyası olabilir. Ağa ilk girişi sağlayıp tutunduktan sonra ağ üzerinden daha değerli bilgisayarlara sızılmaktadır. Yüksek profilli hedeflere karşı yapılan saldırılarda bile bu

¹⁵ Thomas Rid & Ben Buchanan, **a.g.e**, s.16

tür olaylar oldukça yaygındır ve araştırmacılar atıfta bulunma ipuçlarını görmek için bu olayları incelemektedir. Örneğin e-postanın kökeni gibi, ancak dil hataları ve hedeflemede karmaşıklık gibi sosyal veriler incelenmektedir. Başka bir giriş yöntemi, uzaktan erişim yazılımıyla virüs bulaşan taşınabilir belleklere dayanmaktadır. Bu taşınabilir bellekler, saldırgan veya saldırıyla ilişkili bir ajan veya hedef çalışanı tarafından bilmeden bilgisayara takılabilir. Bunlardan başka tamamen teknik giriş yöntemleri de bulunmaktadır.

Sulama deliği saldırısı denen yaygın bir yöntem vardır. Bu yaklaşım, hedef tarafından ziyaret edilmesi muhtemel bir web sitesinin ele geçirilmiş olmasını gerektirir, böylece hedeflenen kişi siteyi ziyaret ettiğinde, bilgisayarına web tarayıcısındaki bir güvenlik açığı yoluyla girilir.¹⁶Bazı giriş teknikleri, mevcut internet ağ altyapısını kontrol ederek meşru ağ isteklerini başka bir siteye yönlendirmeye ve manipüle etmeye dayanmaktadır.

Hedefleme, ihlal türünü veya ihlalcinin tipini aydınlatılabilir. Kredi kartı bilgileri ve kolayca para kazanılan diğer hedefler organize suçlulara işaret etmektedir. Ürün tasarımları, ekonomik casusluk yapan ülkelerde bir dizi rakip firmaya işaret edebilir. Siyasi ve askeri stratejiyle ilgili detaylar istihbarat teşkilatlarına işaret edebilir. Teknik boyut, operasyon katmanındaki çalışma varsayımlarını ortaya çıkaracak hedeflemeye ilişkin belirli bulgular sağlayabilir. Örneğin, saldırganın ihlal ettiği bir ağdaki bilgisayarlar arasındaki hareketlere bakarak, araştırmacılar saldırganların neyin peşinde olduklarına dair fikir sahibi olabilirler. Eğer saldırganlar belirli bir şeyi göz önünde bulundurmuş veya değeri olabilecek bir şey arıyorlarsa, araştırmacılar saldırgan tarafından kullanılan belirli komutları yeniden yapılandırarak, virüslü makinelerin hafızasından görebileceklerdir. Bazen kod aynı zamanda arama terimlerini de içermektedir. 2014'te ortaya çıkarılan 'Ouroboros' olarak bilinen bir operasyonun, "NATO" ve "AB Enerji Diyalogu" arama terimlerini içerdiği tespit edilmiştir.¹⁷

¹⁶ Nicole Perlroth, 'Hackers Lurking in Vents and Soda Machines', **New York Times**, 8 Nisan 2014, A1.

¹⁷ The Epic Turla Operation, **Kaspersky Lab**, 7 Ağustos 2014.

Hedefleme analizi saldırganın organizasyon yapısını aydınlatmaya yardımcı olabilir. Saldırganın kullandığı kaynaklar, saldırganın hedefe ne kadar değer verdiğinin bir göstergesi olabilir. Bir saldırı, ihtiyaç duyduğundan çok daha fazla kaynak kullanıyorsa, örneğin düşük seviyeli casusluk için karmaşık bir set, bu operasyonun hedeflemesinde etkinliği değerlendiren bir grubun parçası olma ihtimalinin daha düşük olduğunun bir işareti olabilir. Fazladan hedefleme benzer bir gösterge olabilir: teşebbüs başarılı olduktan sonra bile bazı saldırganlar aynı hedef için aynı metodu birden fazla kere kullanmaya devam edebilirler. Böyle fazladan sarf edilen bir çaba, saldırganın, muhtemelen karmaşık bir görev düzeni ile büyük bir organizasyonu temsil ettiğinin bir göstergesi olabilir. Çok sayıda hedefe yönelik bu saldırılar, saldırganlar arasında hedefe nüfuz edenler ve hedefi istismar edenler olarak bir işbölümü olduğunun göstergesi olabilir.

3.3.3.Kullanılan Altyapı

Siber saldırı yapmak için altyapı gereklidir. Hedeflenen bilgisayarın anlamsız bilgilerle meşgul edilmesine dayanan bir hizmet engelleme saldırısı söz konusu olduğunda, aslında altyapı saldırıyı gerçekleştirmektedir. Diğer kötü niyetli eylemlerde, altyapı genellikle bir sıçrama noktası olarak veya tehlikeye maruz kalan bilgisayarların komuta ve kontrolü için kullanılmaktadır. Saldırganlar verimliliği artırmak ve lojistik maliyetleri en aza indirmek için, dijital altyapıyı çoğunlukla bir ihlalden diğerine yeniden kullanmaktadırlar. Bu nedenle, atıf sürecinde farklı saldırılar arasında ve potansiyel olarak farklı gruplar arasında bağlantılar kurmak değerli bir ipucu olabilmektedir. ABD’de beş Çinli saldırganı yönelik iddianamede, savcılar, özellikle operatörler tarafından kullanılan alan adı sunucularını, atıf işlemlerinin bir parçası olarak gördüklerini belirtmişlerdir.¹⁸ Bir saldırgan, çeşitli şekillerde altyapı sahibi olabilir: Örneğin bir bilgisayar, meşru mal sahibinin haberi olmadan bir “bot” olarak ele geçirilebilir; bir sunucu yasal olarak bir servis sağlayıcıdan kiralanabilir ve daha sonra kötü amaçlar için kullanılabilir veya altyapı saldırgan tarafından sahiplenilebilir ve fiziksel olarak idame edilebilir. Bir saldırganın altyapıyla arasındaki bağlantı türü, takip eden soruları belirlemektedir. Örneğin, sanal bilgisayarlar ve

¹⁸ Thomas Rid & Ben Buchanan, **a.g.e**, s.17

sunucular gibi kiralanmış altyapı, servis sağlayıcılar aracılığıyla daha fazla kayıta erişim sağlayabilmektedir. Bir saldırganın sahip olduğu ve idame ettiği altyapı, bizi saldırganın fiziksel konumu hakkında ipuçlarına götürebilmektedir. Her durumda, bir saldırganın altyapısının izlenmesi, yeni analiz yollarını ortaya çıkarabilir ve gelecekteki saldırıların engellenmesine yardımcı olabilir. Bu nedenle, bazı kurnaz saldırganlar kendi altyapılarını daha iyi gizlemeye çalışmak için adımlar atmaktadır.¹⁹

3.3.4.Modülerlik

Modülerlik, bilgisayarda kullanılan kodun en belirgin özelliklerinden biridir. Saldırganlar genellikle tekerleği yeniden icat etmekten kaçınırlar ve işlemlerinde rasyonel davranarak temel işlemleri gerçekleştirmek için mevcut yazılımlardan istifade ederler. Saldırının bir parçası olarak, bu yazılım saldırganlar tarafından doğrudan hedef ağlara yüklenmektedir. Yazılım saldırganların kimlikleri hakkında fikir verebilecek imza ve özellikler taşımaktadır. Bu yazılımları sağlayan tedarikçilerin tespit edilmesinden sonra programı satın alan saldırganların bilgilerine ulaşma imkânı olabilmektedir. Modüllerde kullanılan bazı kodlar saldırganlar tarafından izinsiz girişlerde o kadar yaygın kullanılır ki, saldırganı tanımlamak için çok yararlı bir gösterge olabilmektedir. Stuxnet yazılımında kullanılan kod gibi diğer kodlar da saldırganları tanımlamak için çok yararlı olacak kadar belirli bir yeri işaret edebilmektedir. Stuxnet araştırmasında; temel modüllerde kullanılan kötü amaçlı iki yazılım ve kodun yaygın olarak kullanılmaması nedeniyle araştırmacılar Stuxnet virüsünü kimin yazdığına ilişkin daha kesin bir sonuca varmışlardır.

3.3.5.Zaman Planlaması ve Alışkanlıklar

Saldırıların durumunu hayatın olağan akışına göre incelemek, soruşturmaların önemli bir parçasıdır. Tüm organizasyonlar, verimliliği en üst düzeye çıkarmak maksadıyla zaman planlaması ve alışkanlıklara güvenmektedir. Bilgisayar korsanları da benzer bir plan ve alışkanlıklara sahiptir. Bu nedenle zamanlama ve diğer eylem şablonları saldırganların konumları ve kimlikleri hakkında ipuçları verebilmektedir. Örneğin, Amerika Birleşik Devletleri'nde, Çin Ordusuna mensup beş saldırgana karşı düzenlenen iddianamede, saldırganların belirlenmiş bir çalışma programını takip ettiği

¹⁹ Ned Moran, Joshua Homan and Mike Scott, Operation Poisoned Hurricane, **FireEye**, 6 Aug. 2014

ifade edilmiştir. İddianamede; saldırganların, öğle yemeği, gece ve hafta sonlarında faaliyetleri kaldıklarını, sadece mesai saatlerinde verilen talimatlara göre hareket ettikleri iddia edilmektedir.²⁰ İddianamede, bu davranış şablonunun saldırganların bulunduğu Şangay'daki mesai saatleriyle eşleştiği tespiti yapılmıştır. Başka bir örnekte ise, saldırıların yapıldığı saatlerin Rusya'daki mesai saatleriyle uyduğuna ilişkin iddialar bulunmaktadır. Bu tür şablonların taklit edilmesi çok kolay olduğundan bu şablonlar ancak araştırmacıların varsayımlarını desteklemek amacıyla kullanılabilir.

3.3.6.Yazılımda Kullanılan Dil

Kötü amaçlı yazılımdaki kullanılan dil göstergeleri de atfetme için ipuçları sağlayabilmektedir. Saldırgan tarafından kullanılan değişken, klasör ve dosya adları için seçilen kelimeler ile genel yapılandırma ayarlarını gösteren bilgisayar bulguları atfetme için birer ipucu olarak ortaya çıkmaktadır. Her ikisi de karmaşık sahte saldırılarda taklit edilebilmektedir. Yine de dil analizi, atıf sürecinin bir parçası olmaya devam etmektedir. Bu konuda birçok örnek bulunmaktadır ancak bilgisayar güvenlik firması Kaspersky tarafından keşfedilen “Careto” adlı kötü amaçlı casusluk yazılımı bazı farklılıklar arz etmektedir. Casusluk yazılımının komuta ve kontrolünü sağlayan sunucuların çoğunluğunun, Malezya, Avusturya, Çek Cumhuriyeti, Singapur ve ABD gibi İspanyolca konuşmayan ülkelerde bulunduğu tespit edilmiş ancak dil bulguları farklı bir sonuç ortaya çıkarmıştır.²¹ Yapılan analiz sonucunda bulunan ilk gösterge, muhtemelen oltalama (spear-phishing) saldırısı için kullanılan İspanyol gazetesi olduğu iddia edilen alt dizinlerdi. İkinci bir gösterge, kodu ortaya çıkaran veri biçimlerinin, İspanyolca dil ayarlarına sahip makinelerde geliştirildiğinin ortaya çıkmasıdır. Üçüncü gösterge ise, ana dili İspanyolca olmayan birinin çok nadir olarak bilebileceği argo sözcüklerin kullanılmış olmasıdır.

²⁰ United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Criminal Nr 14-118, Erie, PA: US District Court Western District of Pennsylvania, 1 May 2014, 12-13, Exhibit F

²¹ Thomas Rid & Ben Buchanan, a.g.e, s.19

3.3.7.Hatalar

Hatalar çoğu zaman açığa çıkmaktadır. Hatalar, saldırganın gizli tutmak istediği, bir kişinin veya dosyanın adı, gerçek bir İnternet Protokolü(IP) adresi, eski bir e-posta adresi veya kod içindeki kendini açığa vuran bir yorum gibi bilgileri doğrudan ortaya çıkarabilmektedir. Örneğin, yasadışı uyuşturucu satışlarını kolaylaştırdığı bilinen Silk Road adlı web sitesinin operatörü, aynı kullanıcı adını, yasadışı girişiminin satış için ve daha önce teknik yardım talebi gönderisinde kullanmıştır. Bu gönderi araştırmacılar için bariz bir ipucu olabilecek gerçek ad ve e-posta adresini kapsamaktaydı.²² Hatalar, doğrudan bilgiyi açığa vurmasalar bile, değerli ipuçları olabilmektedir. Örneğin, yaygın olarak kullanılan komutlardaki yazım yanlışları, saldırganın tecrübesi ve kimliği hakkında genel bir ipucu sağlamaktadır. Ampirik olarak, daha deneyimli operatörler ve standart uygulamalarla daha bürokratik bir yapıya sahip olan kuruluşların bireysel operatörlere nazaran hata yapma olasılığı daha düşüktür.

3.3.8. Anonimlik ve Gizlilik

Bugün internetle ilgili var olan en önemli çelişki, anonimlik, saldırganın izini bulabilmek ve atıf meselesidir. Bazı kişiler için, anonimlik kötü bir şeyken bazıları için çok iyi bir şeydir. Anonimlik, kolluk kuvvetleri için kötü bir şeydir çünkü siber ortamdaki suçluları tespit etmeye çalışırken işlerini zorlaştırmaktadır ve aynı şey saldırı kaynaklarının izini bulmaya çalışan bilgi güvenliği uzmanları için de geçerlidir. Aksine, internette gezinirken, korsanlara, kolluk kuvvetlerine, ulusal güvenlik görevlilerine ve grup üyeleri ile güven içinde iletişim kuran askeri yetkililere karşı gizlilik sağlamak isteyenler için iyi bir şeydir. Her durumda, anonimlikten vazgeçmek internetin her bir kullanıcısının kendisine bağlıdır, çünkü dünyanın herhangi bir yerinde internet kullanmayı yasaklayan bir kanun yoktur. Eğer anonimliği kaldırırsak o zaman kimin kime saldırdığını, kimin önemsiz posta, virüs, kötü niyetli yazılım gönderdiğini görebiliriz ve belki Estonya, Gürcistan ile Güney Kore'ye hizmet engelleme saldırısını yapan aktörlere kesin olarak atıf yapabiliriz.

²² Nate Anderson, and Cyrus Farivar, 'How the feds took down the Dread Pirate Roberts', **Ars Technica**, 3 Oct. 2013.

Dahası, internette kimliği belirsiz kullanıcılarımız yoksa suçluların kim olduğunu tespit etmek ve dolayısı ile bunları cezalandırmak için atfetmek kolay olacaktır. Böylece, şiddetsiz bir siber alana sahip olabiliriz, bununla birlikte, mevcut internet mimarisi daima anonimliğe imkân sağlamaktadır.

Teknik olarak, anonimliği kaldırmak mevcut internet teknik mimarisi ve yapısı değiştirilmeden mümkün değildir. Siber suçluları ve teröristleri belirleyebilen uluslararası örgütleri ve kuruluşları güçlendirmek daha önemli bir ilk adım olabilir. Bununla birlikte, her ülke bu hedefi desteklemek için kendi güvenliğini sağlamlaştıracak bu ilk adımı atmalıdır. İnternetteki anonimliği engelleme konusunda teknik yeteneğe sahip olduğumuzu varsaysak bile demokratik ülkelerde anonimliği önlemek için siyasi irade olduğu şüphelidir. Muhtemelen sivil özgürlük yanlıları ve gizlilik hakları gruplarından büyük itirazlar gelecektir. Dolayısıyla, sivil özgürlüklere saygı duyulurken internette gizliliğin ortadan kaldırılması ihtiyacını dengeleyen bir politika üretmek bugün için çok kolay değildir.²³

Gizlilik açığa çıkarılabilir. Herhangi bir saldırıda, açık ipuçları olabilecek şekilde hız ve gizlilik arasında bir tercih bulunmaktadır. Tespit edilmekten ve daha sonra yapılabilecek soruşturmadan kaçınmak için tasarlanmış hukuka aykırı adımlar kusurlu ve zaman alıcıdır. Bir saldırganın hukuka aykırı faaliyetleri, onun niyetini, misilleme korkusunu ve saldırının karmaşıklığını ortaya çıkarabilir. Bazı hukuka aykırı davranışlar yaygındır, oldukça kolaydır ve doğrudan görevin başarısı ile bağlantılıdır. Örneğin; saldırganlar, ağdan alınan değerli dosyaları arayan otomatik savunma sistemlerini engellemek için çaldığı verileri şifreleyebilir. Olay incelemesini zorlaştırmak için kayıt dosyalarındaki zaman damgalarını değiştirmek için araçlar kullanmak gibi diğer hukuka aykırı davranışlar daha zor ve daha az yaygındır. Dikkat ölçmek oldukça zordur. Ancak saldırganların izlerini kapatma girişimlerini izlemek oldukça faydalı olabilir.

²³ Thomas Rid & Ben Buchanan, **a.g.e**, s.18

3.3.9.Yetki

Bazı devletler yürütme organlarını, silahlı kuvvetlerini ve istihbarat teşkilatlarını yasal gözetim altında tutmaktadır. Bu, bilgi toplama ve özellikle siber saldırı eylemlerinin genellikle bir makam tarafından onaylanması gerektiği anlamına gelmektedir. Bu kısıtlamaların işaretleri bazen teknik analizler yoluyla görülebilir ve atfetmeye yardımcı olarak kullanılabilir. Eski terörle mücadele ve siber güvenlik yetkilisi Richard Clarke, ikincil zararı en aza indirmek için kullandığı hedef doğrulama prosedürleri nedeniyle, Stuxnet virüsünün Washingtonlu hukukçular tarafından yazıldığını ya da yönetildiğini düşündüğünü belirtmiştir.²⁴

3.3.10. Hazırlık

Bilgisayar ağının istismar edilmesi için önceden hazırlık yapılması gerekmektedir. Belirli bir ağa saldırmak için gereken yetenekleri analiz etmek, atfetme sürecinde faydalı bir ipucu olabilir. İran'ın çok sıkı korunan nükleer zenginleştirme tesislerine yapılan Stuxnet saldırısı, emek yoğun bir saldırıdır. Stuxnet yazılımının faydalı yükü, santrifüj motorlarının dönüş hızlarını kontrol etmek için kullanılan frekans dönüştürücü sürücülerle ilgili bilgiler, santrifüjlerin ayrıntılı teknik parametreleri veya bu santrifüjlere giriş frekansı gibi hedefe özel bilgiler gerektirmekteydi.²⁵

Stuxnet eşi benzeri görülmemiş sayıda sıfır gün kullanmış ve endüstriyel makineleri kontrol etmek için kullanılan programlanabilir bir mantık denetleyicisi için ilk uzaktan komuta sağlayan yazılımı sergilemiştir.²⁶ Bu özellikler, olası faillerin sayısını büyük ölçüde sınırlamıştır. Diğer hazırlıklar hedef keşif ve yük taşıma test yeteneklerini içermektedir. Yine Stuxnet saldırısı kinetik bir etki elde etmek için karmaşık bir hedefleme sistemi programlamıştır. Bu durum daha gelişmiş testlerin uygulanmasını gerektirmiştir.²⁷ Bu test ortamını oluşturabilmek için pahalı ve elde edilmesi zor olan İran Nükleer tesislerinde kullanılan santrifüjleri kullanmak gerekliydi. Bırakın sadece oluşturma ve sahaya yerleştirmesini, hiçbir devlet dışı aktörün ve hatta birçok devletin

²⁴ Ron Rosenbaum, 'Cassandra Syndrome', **Smithsonian Magazine** 43/1, (April 2012), s.12

²⁵ Ivanka Barzashka, 'Are Cyber-Weapons Effective?', **RUSI Journal**, 158/2 (April/May 2013), s.48–56.

²⁶ Kim Zetter, 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', **Wired Magazine**, 11 July 2011.

²⁷ William Broad et al., 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', **New York Times**, 15 Jan. 2011.

Stuxnet'i test etme yeteneğine sahip olmasının mümkün olmadığı düşünüldüğünde saldırıyı kimin yaptığına ilişkin ihtimaller azalmaktadır.

3.3.11. Gelişmiş Kalıcı Tehdit

Saldırılar kapsamına göre değişmektedir. Saldırılar tek bir hedefe karşı tecrit edilmiş olaylar şeklinde olabileceği gibi uzun bir süre boyunca ve geniş bir coğrafi alana yayılmış değişik hedeflere karşı büyük bir operasyonun parçası olabilmektedir. Bu çok aşamalı operasyonları yürütenlere genellikle gelişmiş kalıcı tehdit denmektedir. Bu gruplar genellikle bir operasyondan diğerine taktiklerini, altyapılarını ve genel hedeflerini muhafaza ederler, bu nedenle gelişmiş kalıcı tehdit kavramı, atıf sürecinde önemli bir buluştur. Dikkate değer bir örnek, Çinli bilgisayar korsanlarından oluşan ve sosyal mühendislik taktiklerini ve altyapının özensiz olarak yeniden kullanımıyla tanınan APT1 veya Yorum Ekibi olarak bilinen bir gruptur.²⁸ Gelişmiş kalıcı tehdit olarak değerlendirilen saldırgan gruplar çok kullanılmayan nadir güvenlik açıklarını kullanmakta ve savunma, bilgi teknolojisi gibi kar amacı gütmeyen sektörleri hedef almaktadır. Bir dizi kümelenmiş olayın gelişmiş kalıcı tehdit olup olmadığı kullanılan yöntemlerden anlaşılmaktadır. Bu ayrımı yapmak için kullanılan yöntemler güvenlik şirketlerine göre değişmektedir. Böylece bir şirket veya istihbarat teşkilatı bir saldırının diğer bir grup analistin gücünden daha küçük veya daha büyük olduğu sonucuna varabilmektedir.

3.3.12. Safhalı Planlama

Bazı saldırılar birden fazla safhadan oluşmaktadır. Farklı safhalar, operasyon tasarımı etkileyebilecek veya engelleyebilecek kabiliyetleri hedef alabilmektedir. Bir başka deyişle bir saldırı, daha büyük ve daha karmaşık bir saldırıya imkân sağlayan sadece bir safha olabilir. Böylesine büyük bir saldırının unsurları, parçaları bir araya getirmeyi zorlaştıracak şekilde önemli ölçüde farklılık gösterebilmektedir. Kapsamlı safhalı saldırıya verilebilecek iyi bir örnek DigiNotar saldırısıdır. Takma adı “Comodohacker” olan İranlı bir korsan, Hollanda hükümetine bağlı, web sunucularını doğrulayan sertifika yetkilisi olan DigiNotar'ın web sitesine izinsiz olarak girmiştir. Sertifika yetkilisiyle uzlaştıktan sonra, Google ve diğer siteler gibi davranan önemli

²⁸ APT1, Alexandria, VA: Mandiant, 18 Feb. 2013.

sayıda sahte sertifika yayınlamıştır. Bu sertifikalar korsana, 300.000 kadar masum İranlıya ait şifreli e-posta trafiğini durdurma imkânı sağlamıştır.²⁹

Bazı operasyonlar önceden planlanmış safhalara uygun olmayan şekilde gelişebilir. Bu gelişme değişen siyasi ve teknik gerçeklerin ve hedeflerin ipuçlarını sağlayabilir. Stuxnet bu konuda da dikkat çekici bir örnek teşkil etmektedir. Stuxnet'in analizine katkıda bulunan kontrol sistemi uzmanı olan Ralph Langner, santrifüjleri bozan kötü amaçlı yazılımın farklı biçimleri olduğuna dikkat çekmiştir.³⁰ Bu farklı biçimler farklı metotlar kullanarak ve değişik zamanlarda harekete geçirilmişlerdir. Saldırının Temmuz 2010'da keşfedilmesinden sonra, geriye dönük yapılan analizler sonucunda Stuxnet virüsünün ilk sürümlerinin Kasım 2005'in başlarında görüldüğünü ortaya koymuştur. En eski sürüm farklı bir yayılma mekanizmasına sahipti, herhangi bir Microsoft sıfır günü içermiyordu ve sonraki sürümlerde devre dışı bırakılmış gibi görünen Siemens 417 programlanabilir mantık denetleyicilere karşı çalışan bir yük taşıyordu.³¹ Taktiklerdeki bu tür değişiklikler, değişen öncelikleri ve koşulları göstermektedir.

3.3.13.Jeopolitik Bağlam

Operatif seviyede atıf yapabilmek için meydana gelen saldırının jeopolitik bağlamı değerlendirilmelidir. Saldırının jeopolitik bağlamını yorumlamak, aktörler ve organizasyonları hakkında bölgesel, tarihi ve politik bilgiler gerektirmektedir. Yani saldırının arkasında olabilecek devlet veya devletler tespit edilirken bölgesel, tarihi ve politik bilgiler dikkate alınmalıdır. Özellikle açıklanamayan ve yüksek hedefli saldırılar için jeopolitik bağlam şüpheli sayısını önemli ölçüde sınırlayabilmektedir. Ancak teknik analistler bu analizi yapmak için yeterli bilgi ve donanımına sahip değildir.

Örneğin, 2007'de Estonya'daki hizmet engelleme saldırıları ve Ağustos 2008'deki Rusya-Gürcistan Savaşı sırasında siber saldırılar jeopolitik bağlamda değerlendirilmiş olsaydı her iki ülkenin de dağılan Sovyetler Birliğine mensup olduğu, Sovyetler Birliğinin halefi olan Rusya'nın bu devletler üzerinde hâkimiyetini devam

²⁹ Thomas Rid, *Cyber War will Not Take Place*, Oxford/New York: OUP 2013, s. 9.

³⁰ Ralph Langner, 'Stuxnet's Secret Twin', *Foreign Policy*, 19 Nov. 2013.

³¹ Geoff McDonald, Liam O' Murchu, Stephen Doherty and Eric Chien, Stuxnet 0.5: The Missing Link, Version 1.0, *Symantec*, 26 Feb. 2013.

ettirmek istediği ve bu ülkelerdeki çıkarları nedeniyle bu saldırıların Rusya tarafından yapılmış olduğu sonucuna kolayca ulaşılabilir. ³²

3.3.14.İçerden Gelen Tehdit

Çalışanlar aynı zamanda bir organizasyonun hem en büyük gücünü ve hem de en büyük riskini temsil etmektedir. 2013 yılında gerçekleşen Verizon adlı bir incelemede, organizasyonun içinden gelen tehditleri ve kötüye kullanımı organizasyonlar için en önemli risklerden biri olarak tanımlamıştır. İncelemede ayrıcalıklı erişimi olan bireylerin katıldığı 11.000'den fazla doğrulanmış olay tespiti yapılmıştır. ³³ Şimdiye kadar en fazla zarara neden olan Suudi Petrol Şirketi Aramco saldırısının içeriden bilgi almadan yapılmasının mümkün olmadığı değerlendirilmektedir. ³⁴ Endüstriyel kontrol sistemlerine bilinen az sayıdaki yapılmış başarılı saldırıların en yaygın sebebi kuruluşun içinden gelen tehditlerdir. Kamuoyuna daha önce hiç yansımamış olsa bile, içerdekilerin maruz bıraktığı bir dizi kontrol sistemi olayının yaşanmış olması yüksek ihtimal olarak görülmektedir. İçeridekilerin yardım etme ihtimali, bilginin elde edilmesi zorlaştıkça daha yüksek bir olasılık olarak değerlendirilmeli ancak asla başlangıçtan itibaren değerlendirme dışında tutulmamalıdır.

3.3.15.Hasar

Siber saldırılar birbirine eşit değildir. Hasar, bir saldırının en önemli ayırt edici özelliklerinden biridir. Fiziksel şiddeti içeren saldırıların aksine, siber saldırılarda meydana gelen hasarı tespit etmek ve ölçmek son derece zordur. Hasar dörde ayrılmaktadır. Birincisi hasar doğrudan ve ani olarak ortaya çıkabilir, örneğin, sunucuların çalışma sürelerinin azalması dosyaların kullanılma sürelerinin azalmasına, verilerin bütünlüğünün azalmasına ve hatta saldırganlar tarafından donanımın iş göremez hale getirilmesine neden olabilir. Bu tür ani hasarı yüksek olan saldırıya örnek, Suudi Petrol Şirketi Aramco'ya yapılan ve bir seferde 30.000 iş istasyonunun işlemez hale gelmesine neden olan saldırıdır. İkincisi, hasar doğrudan ve gecikmeli olarak ortaya çıkabilir. Stuxnet virüsü, İran nükleer santrifüjlerinin bileşenlerini

³² Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, 'Cyclones in Cyberspace', **Security Dialogue** 43/1 (2012), s.24.

³³ '2014 Data Breach Investigations Report', **Verizon**, 22 April 2014, s.23.

³⁴ Jim Finkle, "Exclusive: Insiders suspected in Saudi cyber attack", **Reuters**, 7 Sept. 2012.

bozarak hasar meydana getirmiştir. Stuxnet virüsü aylarca mekanik arızalara ve sistemlerin çökmesine neden olmuştur. Üçüncü olarak, örneğin itibar kaybı veya gizlilik ihlali gibi hasarlar dolaylı ve ani olabilmektedir. Bir firmanın müşteri bilgilerinin çalınması hem itibar hem de gizliliğin ihlaline neden olabilecektir. Son olarak, hasar dolaylı ve gecikmeli olarak ortaya çıkabilir. Örneğin, rakip cep telefonu şirketi çaldığı tasarımı kullandığında cep telefonu şirketi fikri mülkiyet kaybı nedeniyle pazardaki rekabette kayba uğrayacaktır. Hasar ne kadar dolaylı ve gecikmeliyse, bunu ölçmek o kadar zorlaşmaktadır.

Hasarın şekli, özellikle operatif düzeyde uygun bir izahı yapılabilirse saldırganın niyetini, ortaya çıkarabilir. Sabotaj, genel bir kural olarak, açık veya gizli olarak doğrudan hasarı en üst düzeye çıkarmaya çalışırken bilgi toplama, tespit edilmekten kaçınmak ve gelecekte daha fazla bilgi toplayabilmek için mağdura yönelik doğrudan hasardan kaçınmaya çalışır. Elbette, hasar görmüş hedefin türü de her saldırganın farklı bir önceliği olduğundan saldırganın niyeti hakkında ipucu vermektedir.

Siber saldırılar sonucunda meydana gelen hasar, amaçlanan ve gerçekleşen olmak üzere iki farklı şekilde ortaya çıkabilir. İlk ihtimal, hasarın amaçlanmış olması ancak bir sebeple gerçekleşmemesidir. 2012 yılında Suudi Petrol Şirketi Aramco'ya yapılan büyük saldırı başladığında, yöneticiler, saldırganların Aramco'nun petrol üretimini yöneten kontrol sistemlerini sabote etmek niyetinde olduklarından ancak başarısız olduklarından şüphelenmişlerdir.³⁵ Buna mukabil diğer senaryo ise, amaçlanmamış bir zararın gerçekleşmiş olmasıdır. Bilgisayar sistemlerinin karmaşık yapısı ve saldırganların internet ağının yapısını tam olarak bilmemesi nedeniyle bu özelliklerin keşfini yaparken yanlışlıkla hasara neden olabilirler. Dolayısıyla analistler, hasar değerlendirmesi yaparken bunları dikkate almak durumundadırlar. Küçük bir elektrik kesintisine neden olan bir siber saldırı, bir uyarı, başarısız bir stratejik ağ ihlali girişimi ya da keşif yaparken yanlışlıkla meydana gelmiş olabilir.

3.3.16.Saldırının Gerekçesi

Bir saldırının gerekçesini anlamak zor ama çok önemlidir. Bir rakibin motivasyonunu ve davranışını bilmek, gelecekte karşılaşılabilecek saldırıları atlatmayı

³⁵ Jim Finkle, "Exclusive: Insiders suspected in Saudi cyber attack", **Reuters**, 7 Sept. 2012.

kolaylaştıracaktır. Tanımından da anlaşılacağı üzere böyle bir stratejik analiz teknik bir analiz değildir. Örneğin, bu analiz jeopolitik kapsamda operatif seviyede sağlam bilgi ve analizlere dayanmaktadır. Bu değerlendirmeye karşı, ister ticari, ister askeri ya da ekonomik olsun amacın analiz edilmesi diğer devletlerin önceliklerini anlamayı da gerektirir. Bütün bunlar, bir siber saldırının ne yapmak için tasarlandığını anlaşılması için dikkate alınması gereken hususlar olarak karşımıza çıkmaktadır. Ayrıca, bu tasarının anlaşılması rakibin gelecekteki eylemine dair bir ipucu sağlayabilir. Bir saldırı teşebbüsü başarısız olduğunda, saldırının neden başarısız olduğunu ve rakibin gelecekte bu hatayı düzeltmek için neler yapabileceğini anlamak, saldırının etkilerini azaltmak ve karşılık vermek için yardımcı olacaktır. Siber saldırıların ortaya çıkışı fiziki saldırılara kıyasla çok yeni olduğundan daha önce karşılaşılmamış olaylarla karşılaşma ihtimali oldukça yüksektir. Meydana gelen yeni olayları analiz etmek ve gelecek için neler ifade ettiklerini ortaya çıkarmak kolay değildir, bu analiz için kullanılan yöntemler bir kereye mahsus kullanılıp bir daha hiç kullanılmayacağı gibi yeni bir trend etkileyecek kalıcı bir yöntem de olabilecektir. Bazen, Stuxnet'teki programlanabilir uzaktan bilgi sistemlerine zarar vermeye imkân sağlayan zararlı yazılımlar gibi endüstriyel komuta sistemlerinin kontrolünü sağlayan yeni yöntemler ortaya çıkabilmektedir. Olaylar dizisinin anlamlı bir örnek oluşturup oluşturmadığını belirlemek, hem atıf süreci hem de verilecek karşılık hakkında bilgi verebilmektedir.³⁶

3.3.17. Gözden Geçirme

Atfetme sürecinin sonucunu araştırmak çok önemlidir. Mevcut kanıtlar ve ilk sonuçlar mutlaka teste tabi tutulmalıdır. Bilgisayar güvenlik uzmanları, günlük dosyalar ve kod satırları biçimindeki somut kanıtlara ulaşabilecek imkâna sahiplerdir. Operatif seviyedeki analistler diğer kaynakların yanı sıra bu kanıtlardan yararlanmaktadırlar. Stratejik düzeyde, politika yapıcılar ve üst düzey analistler, alt seviyeler tarafından üretilen hipotezleri inceleyerek bir bütün olarak sürece büyük faydalar sağlayabilmektedir. Stres testi, analizin zayıf varsayımlarını, hayal gücü ve kolektif düşünce eksikliğini ortaya çıkarabilmektedir. Ek detayları veya alternatif

³⁶ Thomas Rid & Ben Buchanan, **a.g.e**, s.20

açıklamaları araştırmak süreç hakkında ayrıntılı bilgi gerektirebilir. Bu analiz ve model, böyle bir araştırmayı kolaylaştırmak için tasarlanmıştır. Risk yüksekse, tüm süreci tekrar gözden geçirmesi için veya orijinal takımın çalışmalarını tekrar kontrol etmek için özel bir ekip görevlendirilebilir.

3.3.18.Önyargılar

Peşin hükümler, önyargılar, tarafgirlik, psikolojik ve politik önyargılar atfı etkilemektedir. Bu dinamiğin bir iç ve bir dış yönü bulunmaktadır. Her seviyedeki analist ve yönetici bulguları beklenen şekilde ortaya koyma ve kanıtları belirli bir şekilde yorumlama eğilimindedir ayrıca kurumsal dinamikler de iç raporlar iletilirken bu sorunu artırabilmektedir. Politik öngörüler önyargıyı azaltır, idari iş yükü istihbarat başarısızlıklarının önde gelen çalışmalarından biri olarak, yansımayı engellemektedir.³⁷ Bir örnek vermek gerekirse, Suudi petrol şirketi Aramco'ya yönelik 2012 yılındaki saldırıyı Şii eylemcilerinden oluşan bir grubun yapmış olduğunu farz edelim. Sünni çoğunluktaki bir ülkede Şii azınlığa karşı bulunan önyargı, mevcut kanıtlar Şii kökenli Suudi vatandaşlarının Tahran'la bağını tam olarak desteklemese de Suudi araştırmacıları, grubun İran tarafından görevlendirildiğini kabul etmeye teşvik edebilir. Önyargı ne kadar büyük olursa, hata riski de o kadar büyük olacaktır.

3.3.19.Bireyden Organizasyona

Ağ ihlallerini atfederken bireyler önem kazanmaktadır. Eğer izinsiz girişi organizasyon içindeki bir kişiye bağlayan kanıtlar elde edilebilirse, o takdirde atfetme daha güçlü olacaktır. Bu konu, önceki bilgilerimizle değerlendirilen pek çok uluslararası olayla, özellikle askeri olaylarla açıkça çelişmektedir. Örneğin Suriye'deki bir kimyasal tesise yapılan hava taarruzu coğrafi bağlam, uçak tipi veya uçuş yolları ile tek tek pilotların kim olduğuna bakılmaksızın bir devlete atfedilebilmektedir. Silahlı kuvvetleri tanımlarken onu oluşturan bireyleri ve birimleri tanımlamaya gerek yoktur, ancak siber operasyonlarda bu durum tamamen farklıdır.

Atfetmenin nihai amacı, bireyleri değil, bir kuruluşu veya hükümeti tanımlamaktır. Ancak, işaretler, üniformalar, coğrafya ve bireysel operatörler, siber saldırılar ve

³⁷ Richard K. Betts, 'Analysis, War and Decision: Why Intelligence Failures Are Inevitable', **World Politics**, 31/1 (Oct. 1978), s. 61.

organizasyonlar arasındaki bağlantının kurulabilmesi için güçlü birer delil olmaktadır. En yararlı örneklerden biri CrowdStrike adlı güvenlik şirketinin 09 Haziran 2014'te yayımladığı Putter Panda adlı raporudur. Şirketin İngiltere merkezli araştırmacılarından biri olan Nathaniel Hartley, koordineli olarak yapılan saldırılarda 'cpyy' tanıtıcısını kullanan kötü niyetli bir saldırganı tespit etmiştir. Bir sonraki adım 'cpyy' tanıtıcısını gerçek bir kişiye bağlamaktır. Hartley, tanıtıcıyı Chen Ping'e bağlamak için kayıt verilerini kullanmıştır. Son adım Chen ya da "cpyy"nin hangi kuruluşa bağlı olduğunu bulmaktır. Hartley, paylaşım siteleri ve fotoğraf albümlerinin dâhil olduğu çeşitli kaynaklardan daha fazla tanımlayıcı bilgi elde etmiştir. "Ofis" klasöründeki resimler, askeri şapkalar, binalar, teçhizat ve hatta Chen'in portreleri dâhil olmak üzere resimlerdeki çeşitli ayrıntılarla Chen'in Şangay'daki bir binayla irtibatını tespit etmiştir. Hartley bu fotoğrafların yardımıyla Şangay Zhabei Bölgesi'nin merkezindeki bir yerin koordinatlarına ulaşmıştır. Adres, Halkın Kurtuluş Ordusu Karargâhında 3. Daire, 12. Büro, 1486 Biriminin merkezini temsil etmekteydi.³⁸ Birden fazla kaynağı birleştiren Hartley'in kanıtları oldukça ikna edicidir.

Buna benzer raporların tümü, bireyler ve kuruluşlar arasında çevrimiçi oldukları kişiler aracılığıyla bağlantılar oluşturur. Kendi başına, böyle bir kişisel bağlantı, yüksek kaliteli atıf için yeterli olmayabilir. Yine de bir kuruluşun güvenilir bir şekilde tanımlanması, önce kişisel seviyede bir inceleme daha sonra teşkilat veya ünite seviyesine incelemeyi gerektirebilir. Kişisel bağlantı diğer kaynaklardan gelen göstergelerle uyuyor ise, kanıtlar durumu önemli ölçüde güçlendirebilir.

3.4.ATFETMENİN SINIRLAMALARI

Birinci sınırlama bilgi ve delillendirmeye ilgilidir. Atfetmenin kalitesi, mevcut bilgi ve delillerin niteliği ile doğrudan ilgilidir. Üst düzey adli becerilerin yanı sıra karmaşık saldırılardaki örgütsel deneyimler, hızla büyüyen bir uluslararası siber güvenlik piyasasında bile yetersiz kalmaktadır. Atfetme için ne kadar az bilgi ve delil elde edilmişse, atfetmenin kalitesi de o kadar düşük olacaktır.

Atfetme için ikinci ciddi sınırlama zamandır. Atfetmenin kalitesi elde mevcut zamanla doğrudan ilgilidir. İyi icra edilen bir saldırıyı dar bir zaman diliminde analiz

³⁸ Nathaniel Hartley, Hat-tribution to PLA Unit 61486, **CrowdStrike**, 09 June 2014

etmek, en profesyonel ve en iyi donanımlı ekipler, firmalar ve ajanslar için bile önemli bir zorluk olacaktır. Ciddi durumlarda, üst düzey kararların baskı altında alınması gerektiğinde, politik gelişmelerin hızı atfetme sürecinin hızını aşabilir. Atfetme için ne kadar az zaman kalırsa, atfetme kalitesi o kadar düşük olacaktır.

Üçüncü önemli bir sınırlama, rakibin davranışıyla ilgilidir. Atfetme kalitesi, rakibin karmaşıklığının bir işlevidir. İncelenen vakalarda yayımlanan en ikna edici kanıt, ya bazı operatörlerin hata yapmasının sonucu ya da belirgin yöntemler kullanmanın adli yansımalarını göz önünde bulundurmamış olmalarıdır. Karmaşık bir yapıya sahip saldırganlar geride bıraktıkları adli izleri en aza indirmek ve gizlemek için daha fazla güvenlik tedbiri almaktadır. Bu nedenle çoklu kaynaklardan elde edilen kanıtları ortaya çıkarmak ve dolayısıyla atfetmek zorlaşacaktır. Bunun olumlu yanı ise saldırganların hata yapma ihtimalinin yüksek olmasıdır. Mükemmel siber saldırı, mükemmel bir suç kadar zordur. Bununla birlikte, saldırganın gelişmişliği ne kadar yüksek olursa, atfetme o kadar uzun sürecek ve o kadar zor olacaktır.

3.5.ATFIN KAMUOYUNA AÇIKLANMASI

Atfetmeyi açıklamak, atfetme işleminin bir parçasıdır. Karmaşık durumlarda, atf sürecinin sadece küçük bir kısmı tecrübeli uzmanlar ve politikacılar tarafından görülebilmekte daha az bir kısmı da kamuoyuna açıklanmaktadır. Kamuya açıklanan kısmın hazırlanması ve yönetilmesi, bir kurumun faaliyetlerinin siyasi liderler, teknik uzmanlar ve halk tarafından nasıl algılandığını belirleyecektir. Birçok yönden, sürecin açıklanması diğerleri için süreci tanımlanmasını sağlamaktadır. İstihbaratın açıklanması, kaynaklara ve yöntemlere zarar verebilir. Açıklama kararları zordur ve yetkililer genellikle dikkat ve gizlilik açısından hata yapmaktadırlar. Böyle yapmak için birçok neden bulunmaktadır. Yine de, gizlilik kültürü olanlar için sezgisel olarak, daha fazla açıklığın üç kritik faydası bulunmaktadır. Bunlar; daha fazla inandırıcılık, geliştirilmiş atfetme ve gelişmiş savunma anlamına gelmektedir.

İlk olarak, daha fazla ayrıntı yayınlamak hem mesajın hem de mesajlaşma programının güvenilirliğini artıracaktır. ABD'den verilen iki örnek öğretici bir farklılık sunmaktadır. 11 Ekim 2012'de ABD Savunma Bakanlığı'nın en yüksek profilli siber saldırılardan birine maruz kaldığını açıklamıştır. Bu saldırıdan sonra

Pentagon yetkilisi Leon Panetta, yaptığı konuşmada şunları söylemiştir.” Son iki yılda, Pentagon atıf sorununu çözmek için adli inceleme için önemli yatırımlar yaptı ve şimdi bu yatırımların getirilerini görmekteyiz. Potansiyel saldırganlar, ABD’nin onların yerini tespit etme ve ABD’ye veya çıkarlarına zarar veren eylemlere karşı sorumlu tutma kapasitesine sahip olduğunu bilmelidir.”³⁹

Mayıs 2014’te, ABD Adalet Bakanlığı oldukça sıra dışı bir adım atmış ve yabancı bir istihbarat teşkilatı olan Halkın Kurtuluş Ordusu(Çin) 61398 Birimi’nin beş üyesini bilgisayar dolandırıcılığı ve istismarı iddiası, bir bilgisayarı hasara uğratmak, nitelikli kimlik hırsızlığı ve ekonomik casuslukla suçlamıştır. Belge, son derece alışılmadık bir şekilde, ayrıntılı olarak Pensilvanya’daki altı mağdur örgütten, çalınmış verilerin niteliği ve değerinden aynı zamanda hassas bilgilerin açıklanmasının zamanlamasından bahsetmiştir. Ancak iddianame, atıfta bulunmak için çok miktarda kanıt ortaya koymamıştır. İddianame; mağdurları araştırmak için giriş noktası kullanmak, şifre çalmak için e-posta göndermek, kötü amaçlı yazılımları depolamak ve dağıtmak, kötü amaçlı yazılımları yönetmek ve çalınmış verileri aktarma gibi iddiaları içermektedir.⁴⁰ Hükümetin bu tür internet adreslerini, e-postaları, kötü amaçlı yazılım örneklerini ve çalınan belgeleri üretebileceği ima edilmekte, ancak iddianamede bunlara ilişkin çok az adli delil ortaya konabilmiştir. Bu bağlamda ABD Adalet Bakanlığı belgesi, bilgisayar güvenlik firması Mandiant’ın 15 ay önce yayınlanan aynı konudaki raporundan daha az ayrıntı içerdiği belirtilmiştir. Bununla birlikte, bu ayrıntıların açıklanması hükümetin davasına ve onun atfetme konusundaki güvenilirliğine destek sağlamıştır.

Kamuoyuna açıklamayı destekleyen ikinci bir neden, daha fazla ayrıntı yayınlamak, atıfta bulunmayı geliştirmektedir. Bir saldırının detayları kamuya duyurulduğunda, atfetme niteliğinin yükselmesi muhtemeldir. Belki de en etkileyici örnek Stuxnet kodunun çok katmanlı ve son derece yenilikçi kolektif analizidir. Çeşitli şirketler ve araştırma kurumları kötü amaçlı yazılımı analiz etmiş ve operasyonun farklı yönlerine

³⁹ Leon Panetta, ‘Remarks on Cybersecurity to the Business Executives for National Security’, (çevrimiçi) <https://www.lawfareblog.com/secdef-panetta-speech-cybersecurity>, 15.06.2019

⁴⁰ United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Criminal Nr 14-118, Erie, **a.g.e.**

odaklanan bir dizi ayrıntılı rapor hazırlamıştır.⁴¹ Diğer bir örnek ise, güvenlik şirketleri arasındaki rekabete dayanan Çin casusluk savaşları hakkında daha detaylı raporlardır. Sonuç olarak, atfetme pazarı önemli ölçüde büyümektedir. Halka açık olan en faydalı ve en ayrıntılı atıf raporları, hükümetler tarafından değil, şirketler tarafından yayımlanmaktadır. İstihbarat teşkilatları onlarca yıldır hatta yüzlerce yıldır atfetme pratikleri yapmaktadır. Yine de bunu, göreceli ulusal izolasyonda, gelişmeyi teşvik eden açık rekabet yerine gizlilikle yapmışlardır. Bu dinamiğin bir sonucu özellikle dikkat çekicidir. Atfetme süreci, sorumluları kamuoyuna açıklamakla sona ermeyecek sadece yeni bir aşamaya geçecektir. Bu yeni aşama, sırayla, yeni kanıtlar ve analizler üretebilir ve bu nedenle hem değerlendirme hem de destek kampanyalarını uyumlu hale getirmeyi gerektirmektedir.

Açıklığın üçüncü faydası belki de en önemlisidir. Daha fazla detayın kamuoyuna açıklanması, daha iyi kolektif savunma imkânı sağlayacaktır. Bulguların açıklanması sadece bireysel güvenliği değil, aynı zamanda kolektif güvenliğin de gelişmesine katkıda bulunacaktır. Örneğin, izinsiz girmek için kullanılan internet altyapısının ayrıntılı olarak tartışılması, diğer ağların yöneticilerinin özellikle buna karşı korunmalarını sağlayabilecektir. Kötü amaçlı programlar için yeni imzalar oluşturmak, diğer yöneticiler tarafından indirilip otomatik izinsiz giriş tespit sistemlerine yüklenebildiğinden benzer şekilde faydalı olabilir. Belirli yararlar olmasa bile, saldırganlar tarafından kullanılan yeni teknikler hakkında ayrıntılı teknik tartışma, diğer durumlara karşı da araştırmacılara bilgi sağlayacaktır. Bu göstergeleri ve daha iyi savunmayı bir ücret karşılığında sağlamak, siber güvenlik şirketlerinin iş modelidir. Hükümetlerin bu dinamığa karşı nasıl davranması gerektiği açık ve önemli bir sorudur.

Belirli suçluların beklenmeyen açıklamalara nasıl tepki verdiğini incelemek daha fazla atfetme raporunun ortaya çıkmasıyla mümkün olacaktır. Örneğin, Kaspersky Lab Siber Güvenlik Şirketi, 10 Şubat 2014 tarihinde, siber saldırılar hakkındaki İspanyolca raporu yayınladıktan bir saat sonra operasyon kaldırılmıştır.⁴² Flame raporu Mayıs

⁴¹ Kim Zetter, **Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon**, Broadway Books; Reprint edition (September 1, 2015), s.121

⁴² Unveiling "Careto"- The Masked APT, Version 1.0, **Kaspersky Lab**, 06 Feb. 2014.

2012'de yayınlandığında, saldırganların operasyonu bitirmesi iki hafta sürmüştür.⁴³ Bir operasyonun sonlandırılma şekli, örneğin sonlandırma işleminin profesyonelce yapılıp yapılmaması, yüksek düzeyde operasyon güvenliğinin muhafaza edilmesi veya muhtemelen operasyonun durdurulması kararının verilmesinin büyük bir bürokratik prosedürü gerektirmesi nedeniyle yavaşça yapılması, atfetme için ilave ipuçlarını sağlayabilir. Uсталık gerektiren bir saldırı olan Duqu ortaya çıktığında, operatörler silinmiş ancak kurtarılabilir dosyaları parçalamayı unutmuşlar, bu nedenle operasyonla ilgili ayrıntılar ortaya çıkmıştır.⁴⁴ Kaspersky'nin açıkladığı saldırıların bir kısmı ilk açıklamadan sonra, bazıları daha hızlı, bazıları iz bırakmadan ortadan kaybolmuştur. Bu iki örnek dikkat çekicidir, çünkü Kaspersky'nin raporları şüpheli bir suçluyu, hatta şüpheli bir ülkeyi tanımlamamasına rağmen saldırganlar yine de geri çekilmiştir. Flame saldırılarını yönetenler, Kaspersky'nin raporunun kamuya açıklanmasından iki hafta önce muhtemelen erken ikazla 14 Mayıs 2012 tarihinde oldukça ayrıntılı bir komuta ve kontrol altyapısını sökmeye başlamıştır. Güvenlik şirketi Mandiant, 18 Şubat 2013'te rapor yayımladığında, ortaya çıkan saldırıyı büyük oranda açıkladığından saldırı ilk önce 41 gün durmuş, ardından yaklaşık 160 gün normalin altında kalmıştır. 2013 Mart ayında Kaspersky Lab şirketinin web siteleri, Çin'den kaynaklanan uzun süredir devam eden hizmet engelleme saldırılarına maruz kalmıştır.⁴⁵ Çin'den yapılan saldırılar, teknik olarak daha az gelişmiş olmalarına rağmen operasyonla ilgili hassas detaylar açığa çıkarılarak bir atıf yapılmasından sonra bile, ısrarcı şekilde saldırılarını devam etmişlerdir.⁴⁶

Nihayetinde, kamuya yapılan açıklamada, atfetmenin mutlak olmadığı belirli derecelerde ihtimaller içerdiği vurgulanmalıdır. Bu nedenle güvenlik firmaları ve hükümetler dikkatli ve olasılık içeren tahmine dayalı ifadeler kullanmaktadır. İstihbaratta, bilgi toplarken bilinmeyenlerin yeri bilinenlerden yola çıkarak tahmin etme yoluyla doldurulmaktadır. Buradaki tahmin gerçek ve değerlendirmenin bir karışımından oluşmaktadır. Bu gerçek ve değerlendirme karışımı özellikle siber güvenlik bağlamıyla yakından ilgilidir. Tahminler hassas bir şekilde ifade edilir ve bu

⁴³ Alexander Gostev, The Flame: Questions and Answers, **Kaspersky Lab**, 28 May 2012

⁴⁴ Vitaly Kamuk, “**The Mystery of Duqu: Part Six**,” (çevrimiçi), <https://securelist.com/the-mystery-of-duqu-part-six-the-command-and-control-servers-36/31863/>, 15.06.2019

⁴⁵ Threat Report: Beyond the Breach, Reston, VA: **Mandiant**, 18 Feb. 2014, s.18.

⁴⁶ Dean Cheng, **Cyber Dragon**, Preager, Santa Barbara, California, 2017, s.18-28

nedenle eleştiriye açıktır. Bilgi sınırlamaları ve tahminlerinin niteliği hakkında bir belge ne kadar objektif olursa genel analiz de o kadar güvenilir olur.

Atfetme bir sanattır, basit ya da karmaşık yalnızca teknik rutin analiz, atfetmeyi biçimlendiremez, hesaplayamaz, ölçemez ya da tamamen otomatik hale getiremez. Yüksek kaliteli atfetme, becerilere, araçlara ve organizasyonel kültüre bağlıdır. İyi çalışan ekipler, yetenekli bireyler, zor kazanılmış deneyimler ve genellikle bir şeylerin yanlış olduğunu ifade eden başlangıçta ifade edilmesi zor bir duygudur.

Atfetme basitçe çözülebilen veya çözülemeyen bir problem değil, çok yönlü ve çok katmanlı bir süreçtir. Bu süreç dikkatli bir yönetim, eğitim ve liderlik gerektirir. Atfetme politik risklere bağlıdır. Bir olayın sonuçları ne kadar şiddetli ve zarar ne kadar yüksek olursa, hükümet failleri tespit etmek için o kadar fazla kaynak ayıracaktır. Belirli bir suç işlendiğinde ilk yapılacak iş yasal, diplomatik veya askeri olsun önce suçlunun tespitini gerektirir. Devletler atfin nasıl yapılacağına ve atfetmenin eylem için yeterince iyi olup olmadığına karar vermektedir.

Yazılım ve programlama büyük ölçüde gelişmiş; ama internet bu hıza uyum sağlayamamıştır. İnternet ağının temel mimarisi çok yavaş değişmektedir. Dolayısıyla atfetme de yavaş yavaş değişmekte ancak çelişkili bir evrim geçirmekte, diğer yandan ise kolaylaşmaktadır. Daha iyi saldırı tespit sistemleri, gerçek zamanlı olarak saldırılar tanımlayabilmekte ve daha fazla veriyi daha hızlı kullanabilmektedir. Daha uyumlu ağlar, saldırgan eylemin maliyetini artırabilir, böylece yüksek profilli saldırıları daha iyi tanımlanabilir. Daha fazla siber suç, dost olmayan devletlerarasında bile yasaların uygulanması için işbirliğinin geliştirilmesini sağlayabilir ve böylece devletlerarası casusluğunun gizlenmesini zorlaştırır ve politik olarak daha maliyetli hale getirir.

Ancak atfetme aynı zamanda diğer yönden gittikçe zorlaşmaktadır. Saldırganlar kamuya açıklanan hatalardan ders almaktadır. Güçlü kriptolomanın artan kullanımı, adli sorunlara neden olmakta ve toplu depolama olanaklarını sınırlamaktadır. Anlamlı sonuçların olmaması, ilgisiz fiili ve ihmal edilebilir sonuçların ortaya çıkması nedeniyle devletler ve devlet dışı aktörlerin yakalanma korkusu ortadan kalkabilir. Bu durum, demokratik olmayan devletlerin kamuoyuna hesap vermek durumunda olan demokratik devletlerden daha az yakalanma endişesi duyacağı anlamına gelebilir. Bu

yüzden tartışma başlangıçtaki noktaya geri dönmektedir. Atıf süreci, hem teknolojik hem politik bir sorundur, zamana, kaynaklara, politik sermayeye yatırım yaparak ve rakiplerini geride bırakmaya çalışarak devletler tarafından yapılmaktadır.

En önemli atıf çalışmalarının bir kısmı birçok ülkede gizlenmiş ve sınıflandırılmıştır. Gelecekte, devlet kurumları veya güvenlik şirketleri ilave araçlar geliştirebilir veya atfın yeni açılarını ortaya koyabilecek araçları kamuoyu ile paylaşabilir. Bazı sinyal istihbarat yetenekleri teorik olarak çok az hata yapan veya hiç yapmayan çok karmaşık saldırganlar için bile mevcut atfetme sürecinin açıklığını artırabilir.

3.6.ULUSLARARASI HUKUKA GÖRE DEVLETİN SORUMLULUKLARI

Meşru müdafaa kapsamında karşılık vermeden önce saldırıyı devlete sorumluluk atfetmek için birçok husus dikkate alınmalıdır. Siber saldırının kolluk kuvvetleri tarafından ele alınması gereken adli bir vakıa olarak mı veya ulusal güvenlik meselesi olarak görülmesi gerektiği önemli bir sorundur. Bu tespit ile birlikte, daha önceki bölümde tartışıldığı gibi siber saldırılarda kullanılan kuvvet seviyesinin, silahlı saldırı seviyesine yükselip yükselmediği de dikkate alınmalıdır. Diğer bir husus, saldırının menşei olan devletin suça iştirak edip etmediğidir. Meşru müdafaa eylemi devam eden bir saldırıya derhal müdahale şeklinde değilse devlet kendi sınırının ötesine geçerek karşı saldırıya başlamadan önce o devlete sorumluluğu atfetmiş olmalıdır. Siber saldırı alanında devletin sorumluluğunu saptamak, özellikle devletlerin yetki alanlarında faaliyet gösteren devlet dışı aktörleri de dikkate alarak devletlerin diğer devletlere olan yükümlülüklerini anlamayı gerektirmektedir. Birleşmiş Milletler Genel Kurulu'nun 2001 yılında hazırladığı devletlerin sorumluluğuna ilişkin taslak kararının 1. maddesine göre devletin yanlış yaptığı her uluslararası eylem, devletin uluslararası sorumluluğunu gerektirmektedir. Bu kural, devlet uygulamasının yanı sıra teamül hukuku tarafından da desteklenmektedir.⁴⁷

Devlet, kendisine atfedilebilen ve uluslararası bir yükümlülüğün ihlalini teşkil eden bir siber operasyon için uluslararası yasal sorumluluğa sahiptir. Devletin sorumluluğu

⁴⁷ United Nations General Assembly, **56/83. Responsibility of States for Internationally Wrongful Acts**, (çevrimiçi) <https://undocs.org/en/A/RES/56/83>, 24.06.2019

uluslararası teamül hukukuna dayanmaktadır. Bununla birlikte, silahlı çatışma hukukunun ihlal edilmesi halinde devletin sorumluluğuna dair bir takım özel kurallar bulunmaktadır. Özellikle, IV. Lahey Sözleşmesinin 3. Maddesi ve I. Ek Protokolün 91. maddesi, silahlı çatışma hukukunun belirli kurallarının ihlali durumunda tazminat ödenmesini sağlamaktadır.⁴⁸

Yapılan eylemin uluslararası hukuk uyarınca devlete atfedilebilir olması ve uluslararası bir yasal zorunluluğun devlet tarafından ihlal edilmesi durumunda, yapılan bu eylemden devletin sorumlu olması uluslararası bir hukuk prensibidir. Bu ihlal bir eylem veya ihmalden kaynaklanabilir.

Siber alanda, uluslararası hukuka aykırı bir eylem, Birleşmiş Milletler Anlaşmasının (örneğin, siber araçlarla kuvvet kullanımı) ihlal edilmesi veya devlete atfedilebilen silahlı çatışma hukukunun (örneğin, sivil hedeflere yönelik siber saldırı) ihlal edilmesinden oluşabilir. Çatışma içermeyen barış zamanı kurallarının ihlali (örneğin, deniz yasalarının veya müdahale etmeme ilkesinin ihlali) de uluslararası hukuka aykırı bir eylemi oluşturur. Örnek olarak, bir devletin savaş gemisinin, zararsız geçiş sırasında kıyı devletinin çıkarlarına aykırı siber operasyonları yürütmesi yasaktır.⁴⁹

Devletin hukuken sorumluluğu, yalnızca uluslararası hukuku ihlal eden bir fiil ya da eylemden kaçınmayı kapsar. Başka bir deyişle, devlet organları tarafından işlenmiş veya devlete atfedilebilecek bir davranış, uluslararası hukuka aykırı olması durumunda, yalnızca uluslararası olarak hatalı bir eylem olarak kabul edilebilir. İzin verilmiş ya da uluslararası hukukta düzenlenmemiş eylemlerde devletlerin hukuken sorumluluğu yoktur. Örneğin, uluslararası hukuk kendiliğinden casusluğu ele almamaktadır. Bu nedenle, siber alanda bir devlet organı tarafından yürütülen siber casusluk eylemine ilişkin devletin sorumluluğu, casusluk faaliyetleri uluslararası hukuku ihlal etmediği sürece uluslararası hukuk meselesi olarak görülmemektedir.

Uluslararası sorumluluk hukukunda devletin sorumluluğu uyarınca meydana gelen zararın nedeni, bir siber operasyonun uluslararası çapta hukuka aykırı bir eylem olarak

⁴⁸ Jean-Marie Henckaerts and Louise Doswald-Beck, **Customary International Humanitarian Law**, Cambridge University Press, 2009, s.530-551

⁴⁹ United Nations Convention on the Law of the Sea, **Article 19. Meaning of innocent passage**, s. 27

nitelendirilmesinin bir ön şartı değildir. Ancak, söz konusu kural, zararı temel bir unsur olarak içerebilir. Bu gibi durumlarda, zarar devletin ek sorumluluğunun zorunlu koşulu olarak kabul edilmektedir. Örneğin, uluslararası teamül hukuk kuralı uyarınca, devletlerin kendi topraklarındaki faaliyetlerle başka bir devlete ciddi zarar vermeleri yasaktır. Böyle bir hasarın bulunmaması durumunda, hasar unsuru içermeyen başka bir kural ihlal edilmedikçe o devlete sorumluluk yüklenmeyecektir.⁵⁰

Bir eylemin uluslararası hukuka aykırı olmasının yanı sıra, aynı zamanda bir devlete atfedilmesi gerekir. Daha önce de bahsi geçtiği gibi bir devletin organlarının tüm eylemleri veya ihmalleri otomatik ve zorunlu olarak bu devlete atfedilir. Uluslararası sorumluluk hukukunda bir devletin organları kavramı oldukça geniştir. Devletin iç mevzuatında bu statüye sahip olan her kişi veya kurum, devlet hiyerarşisindeki işlevine veya konumuna bakılmaksızın devletin bir organı olacaktır.⁵¹ İstihbarat, askeri, iç güvenlik, gümrük veya diğer devlet kurumlarının üstlendiği siber faaliyetler, söz konusu devlet için geçerli uluslararası bir yasal zorunluluğu ihlal ettiği takdirde, uluslararası hukuka göre devletin sorumluluğunu gerektirmektedir.

Söz konusu organın talimatlara uyup uymadığı ya da talimatların ötesine geçmiş olması önemli değildir. Devletin bir organı tarafından işlendiğinde ve organın görünüşte resmi bir kapasitede hareket etmesi şartıyla, sözde yetki aşımı bir eylem bile olsa, uluslararası yükümlülükleri ihlal etmesi halinde devletin uluslararası yasal sorumluluğunu doğuracaktır.

Uluslararası sorumluluk hukuku açısından, devletin organları olmasa da, kendi devlet yasalarını devlet otoritesini kullanma konusunda özel olarak yetkilendirilmiş kişiler veya kuruluşlar, devlet organları olarak kabul edilmektedir. Böyle kişiler ve kuruluşların eylemleri de devlete atfedilmektedir. Örneğin, hükümet tarafından başka bir devlete yönelik siber saldırı yapma yetkisi verilmiş bir özel şirket veya siber istihbarat toplanma yetkisine sahip özel bir kuruluşun eylemleri o devlete atfedilecektir. Devlet sorumluluğu sadece söz konusu kurum devlet otoritesinin unsurlarını kullandığı zaman ortaya çıkmaktadır. Örneğin, devlet özel sektör siber

⁵⁰ Hüseyin Pazarcı, **Uluslararası Hukuk**, Gözden Geçirilmiş 3.Bası, Turhan Kitabevi, Ankara 2014, s.642-645

⁵¹ Pazarcı, **A.e.**, s.642-645

olaylara müdahale ekiplerine devlet ağlarının siber savunmasını yürütme yetkisi vermiş olabilir. Bu ekiplerin faaliyetleri otomatik olarak devletin sorumluluğunda olacaktır. Ancak, bu ekipler özel şirketler için bilgi güvenliği hizmetleri gerçekleştirirken devletin sorumluluğuna gitmek söz konusu olamayacaktır.

3.6.1.Devlet Dışı Aktörlerin Eylemlerinden Devletin Sorumluluğu

Bazı durumlarda, devlet dışı aktörlerin davranışları bir devlete atfedilebilir ve devletin uluslararası yasal sorumluluğunu doğurabilir. Uluslararası teamül hukukunu yeniden düzenleyen Birleşmiş Milletler Genel Kurulu'nun devletlerin sorumluluğuna ilişkin taslak kararının 8. maddesi, "Uluslararası hukuka göre bir şahsın veya bir grubun davranışı, şahıs veya şahıs grubunun fiili olarak devletin talimatına veya talimat veya kontrolüne uygun hareket etmesi durumunda, davranış devletin eylemi olarak kabul edilir".⁵² Bu norm özellikle siber bağlamla ilgilidir. Örneğin, devletler siber saldırı yapmak için özel bir şirketle anlaşabilirler. Benzer şekilde, devletler vatandaşlarını gönüllü olarak diğer devletlere veya yurtdışındaki hedeflere karşı siber saldırılarda bulunmaya çağırabilir.

Uluslararası Adalet Divanı, askeri operasyonlar bağlamında, bir devletin, bu tür aktörler üzerinde fiili kontrolü olduğunda, devlet dışı aktörlerin eylemlerinden de sorumlu olduğunu kabul etmiştir.⁵³ Örneğin, belirli siber saldırıların planlanması sırasında bir devletin siber uzmanlık sağlaması, bu katılımın ne kadar derine gittiğine bağlı olarak, bu tür devlet dışı aktörler tarafından işlenen uluslararası hukuka aykırı eylemler için devletin sorumluluğunu doğurabilir. Bazen devlet dışı bir aktörün devlete atfedilebilir davranışı için gerekli olan kontrol derecesi belirsiz olabilir. Eski Yugoslavya Uluslararası Ceza Mahkemesi, bireysel cezai sorumluluğu tespit etmek ve silahlı çatışmanın niteliğini belirlemek için devletin devlet dışı aktörler üzerindeki genel kontrolünü yeterli görmüştür.⁵⁴ Bununla birlikte, Uluslararası Adalet Divanı soykırım kararında, böyle bir değerlendirmeyi devletin sorumluluğunu tespit etmek amacıyla yapılan değerlendirmeden ayırmıştır. Ayrıca, devletin sorumluluğunu

⁵² United Nations General Assembly, **56/83. Responsibility of States for Internationally Wrongful Acts**, (çevrimiçi) <https://undocs.org/en/A/RES/56/83>, 24.06.2019

⁵³ Pazarcı, **a.g.e.**, s.515

⁵⁴ International Criminal Tribunal for the Former Yugoslavia, **Tadic Case, Case No. IT-94-1-T**, 07 May 1997, (çevrimiçi) <http://www.icty.org/en/press/tadic-case-verdict>, 08.07.2019

belirlemek için genel kontrol kabul edilse bile, eylemi yapanların finanse edilmesi, donatılması, askeri operasyonların planlanması ve denetlenmesinin ötesine geçen bir kontrolün olması gerekecektir. Ayrıca, genel kontrol, bireyler veya örgütlenmemiş gruplar için geçerli olmayacaktır.

Birleşmiş Milletler Genel Kurulu'nun devletlerin sorumluluğuna ilişkin taslak kararının 4. maddesine göre herhangi bir devlet organının davranışı, uluslararası hukuk uyarınca bu devletin bir eylemi olarak kabul edilmektedir. Bir devlet organı, devletin organizasyonunu oluşturan ve onun adına hareket eden tüm bireysel veya kolektif varlıklar olarak kabul edilmektedir. Bu kabul, uluslararası teamül hukukundan kaynaklanmaktadır. Bu kurala göre devletin mensupları görevlerinin dışına çıkarak hareket etmiş olsa bile, bu görevlilerin yaptığı eylemlerden devletin tamamen sorumlu olduğu kabul edilmektedir.⁵⁵Bu kural aynı zamanda bir devlet organı olmayan ancak yine de devlet otoritesinin öğelerini kullanan bir kişi veya kurum için de geçerlidir. Bu kural devletin otoritesini kullanan resmi veya özel kuruluşları kapsamaktadır. Örneğin, Türkiye Cumhuriyeti Devleti özel bir savunma şirketine iş verse ve aktif savunma önlemlerini alması için yetkilendirse, özel savunma şirketinin eylemi Türkiye Cumhuriyeti Devleti'ne atfedilecektir. Birleşmiş Milletler Genel Kurulu'nun devletlerin sorumluluğuna ilişkin taslak kararının yorumuna göre devletin bir eylemi uluslararası sorumluluk açısından kabul edilmesi gerekiyorsa, kuruluşun eylemi kuruluşun dâhil olabileceği diğer özel veya ticari faaliyetlerle ilgili olmamalı, devlet faaliyetleriyle ilgili olmalıdır.

11 Eylül 2001'de ABD'ye yapılan saldırılara Birleşmiş Milletler nezdinde verilen uluslararası tepki, uluslararası teamül hukukunun bu ilkesinin onaylanmasıdır. 11 Eylül 2001 saldırılarından sonra, Birleşmiş Milletler Güvenlik Konseyi 1368 sayılı kararla Birleşmiş Milletler Anlaşmasının 51'inci maddesi uyarınca ABD'nin meşru müdafaa kapsamında saldırılara karşılık verme hakkının bulunduğunu onaylamıştır. Daha sonraki haftalarda, 11 Eylül 2001 saldırılarını devlet dışı aktörlerin gerçekleştirdiği açıkça belli olduğunda, ABD meşru müdafaa hakkını kullanacağını

⁵⁵ Pazarcı, **a.g.e.**,s.641-645

açıkladığında, Birleşmiş Milletler Güvenlik Konseyi de dâhil olmak üzere neredeyse bütün devletlerden destek almıştır.

Hangi gerekçelerle devlet dışı aktörlerin eylemleri için bir devlete sorumluluk yükleyebiliriz? Eğer devlet, devlet dışı aktörleri yönetir veya kontrol ederse, devlet dışı aktörlerin kendi yargı alanı içinde olup olmadıklarına bakılmaksızın, devleti sorumlu tutmak için bazı gerekçeler bulunmaktadır. Bununla birlikte, devleti onaylamadan hareket eden münferit bilgisayar eylemcileri için durum daha karmaşıktır. Birleşmiş Milletler Uluslararası Adalet Divanı'nın Korfu Kanalı kararına göre, bir devlet kendi ülkesinin başka bir devletin haklarını ihlal eden eylemler için kullanılmasına bilerek izin vermemelidir.⁵⁶ Bu karar esas alınarak yapılan değerlendirme sonucunda bir devlet kendi sınırları içindeki devlet dışı aktörlerin başka bir devlete saldırmasına da bilerek izin vermemelidir. Devletin sorumluluğuna ilişkin hükümler kişi veya bir grubun söz konusu devletin talimatlarını yerine getirmesi, onayı veya kontrolü altında hareket etmesi durumunda devlete sorumluluk yüklemektedir.

Devlet sorumluluğu hakkındaki hükümler Nikaragua Davası kararını desteklemektedir. Nikaragua davasında, Uluslararası Adalet Divanı önüne getirilen mesele, kontra gerillalarının Nikaragua hükümetine karşı isyan etmelerinden ABD'nin sorumlu olup olmadığıydı. Mahkeme, kontra gerillaları üzerinde harekât sırasında fiili denetime sahip olması durumunda ABD'nin uluslararası sorumluluğunun doğacağını kabul etmektedir.⁵⁷ Böyle bir bulgu, devlet kontrolünün kendi topraklarının ötesine uzandığını göstermektedir. Bu nedenle, eğer bir devlet başka bir bölgede faaliyet gösteren devlet dışı aktörler üzerinde fiili kontrolü varsa, bu aktörlerin eylemlerinden sorumlu tutulabilir.

Uluslararası Güvenliğin Güçlendirilmesi Deklarasyonu, her devletin başka bir devlette meydana gelen sivil çatışma veya terör eylemlerini organize etmekten, kışkırtmaktan veya katılmaktan kaçınmak zorunda olduğunu beyan eder.⁵⁸ Bu standart

⁵⁶ International Court of Justice, **Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)**, (çevrimiçi) <https://www.icj-cij.org/en/case/1>, 21.02.2019

⁵⁷ Pazarcı, **a.g.e.**, s.644

⁵⁸ UN General Assembly, **Implementation of the Declaration on the Strengthening of International Security**, 18 December 1973, (çevrimiçi), <https://www.refworld.org/docid/3b00f1c754.html>, 08.07.2019

uyarınca, eğer bir devlet vekâleten bilgisayar eylemcilerini organize etmiş, yardım etmiş ve kontrol etmişse, bilgisayar eylemcilerinin eylemlerinin sorumluluğu, devlet tarafından kontrol edilen operasyona ilişkin olarak, devlete yüklenebilecektir.

Diğer taraftan, Eski Yugoslavya Uluslararası Ceza Mahkemesi, Tadic davasında daha düşük bir kontrol derecesini kabul etmiştir.⁵⁹ Tadić'i yargılayan mahkeme, grubu bir dereceye kadar devletin organlarıyla eşit olarak tutmuştur. Bu standart sadece askeri veya paramiliter bir güç gibi organize ve hiyerarşik yapıya sahip bir grubun üyelerine uygulanmıştır. Böyle bir paramiliter gruba örnek, resmi olmasa da, genellikle Rusya'nın siyasi ve askeri seçkinleriyle ilişkilendirilen Rus ticaret şebekesidir. Rus ticaret şebekesinin, Rusya'nın reddettiği Estonya ve Gürcistan'a yönelik siber saldırılarıyla yakından ilgisi bulunduğu ilişkin şüpheler bulunmaktadır.⁶⁰ Tadić mahkemesinin kontrol derecesine göre, Rus ticaret şebekesi ve Rus devleti arasındaki ilişki devlet sorumluluğunu uygulamak için yeterli olmalıdır.

Birleşmiş Milletler Genel Kurulu'nun devletlerin sorumluluğuna ilişkin taslak kararının 11. maddesi, "önceki maddelere göre bir devlete atfedilemeyen eylemlerin, devletin söz konusu eylemin kendi eylemi olduğunu kabul etmesi ve onaylaması halinde, uluslararası hukuka göre devletin eylemi olarak kabul edileceğini beyan eder." hükmünü içermektedir. Amerika Birleşik Devletleri'nin Tahran'daki büyükelçilik ve konsolosluk personeli davası uygulamada bu ilkenin kanıtıdır. ABD Büyükelçiliği ve personelinin militanlar tarafından ele geçirilmesi, İran devleti tarafından tasvip edilmiştir. Birleşmiş Milletler Uluslararası Adalet Divanı, militanların eylemlerini onaylayan İran'ın devlet sorumluluğu olduğuna karar vermiştir.⁶¹

Bu çerçevede, eğer bireysel veya örgütlenmemiş bilgisayar eylemci grupları bir devletin elektrik santralini tahrip etmek için siber saldırı düzenliyorsa ve saldırganların bulunduğu devlet bu eylemi kesin olarak onaylıyorsa, saldırı bu ev sahibi ülkeye atfedilecektir. Bir eylemin devlete atfedilmesi için en zor durum, bir devlet tarafından

⁵⁹International Criminal Tribunal for the Former Yugoslavia, **a.g.e.**

⁶⁰ Catherine Lotrionte, "State Sovereignty And Self-Defense In Cyberspace: A Normative Framework For Balancing Legal Rights", **Emory International Law Review**, Vol.26,(çevrimiçi) http://law.emory.edu/eilr/_documents/volumes/26/2/symposium/lotrionte.pdf, 09.07.2019

⁶¹ International Court of Justice, **United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) Case**, 24 May 1980, (çevrimiçi) <https://www.icj-cij.org/en/case/64>, 08.07.2019

aktif bir şekilde cesaretlendirilmeden bireysel olarak hareket eden bilgisayar eylemcisinin eylemlerinden devletin sorumlu olup olmadığıdır. Bu durumda, uluslararası hukuk devletlerin makul önleyici tedbirler almalarını gerektirmektedir. Bir devletin görevinin, bireysel bilgisayar eylemcisini engellemek için nereye kadar uzandığı belli değildir. Örneğin, bir devlet teknolojisini bir şekilde çevrimiçi gizliliği ortadan kaldırmak için kullanmalı mıdır? Böyle bir gereksinim, bireylerin özgürlük ve mahremiyeti konusunda ciddi sorular ortaya çıkarmaktadır. Ancak bu mesele, silahlı çatışma hukukundan ziyade, iç hukukun kapsamına giren bir konudur. Diğer devletlerin öngörülebilir siber saldırılara karşı korunmasını sağlamak için uluslararası hukuk devletin makul önlemler alması gerektiğini belirtmektedir. Bu kural uyarınca, saldırıları başlatan siber saldırganları tespit eden bir devlet, saldırıları durdurarak, saldırganları adalete teslim ederek veya daha fazla saldırı yapılmasını önleyerek görevini yerine getirmek için makul adımlar atmalıdır. Eğer ilgili devlet işbirliği yapmazsa, hedef alınan devlet Birleşmiş Milletler Sözleşmesinin 51. maddesine göre meşru müdafaa hakkını kullanarak o devlete karşılık verebilir. Eğer bir devlet devlet dışı bir aktörün saldırı gerçekleştirmesine eylemiyle veya ihmal yoluyla bilerek izin verirse, devlet uluslararası olarak sorumlu tutulacaktır. Ancak eğer devlet diğer devletleri korumak için yeterli tedbirleri almasına rağmen kendi topraklarından siber saldırı gerçekleşirse, devlet sorumlu olmayacaktır.

Bu durumlar, vatandaşların kendi inisiyatifleriyle gerçekleştirdikleri siber operasyonlardan ayırt edilmelidir. Birleşmiş Milletler Genel Kurulu'nun devletlerin sorumluluğuna ilişkin taslak kararının 8. maddesinin uygulaması sıkı talimatlara bağlanmış olması nedeniyle uyulması zorunludur. Devletin sorumluluğuna gidilebilmesi için bir saldırıyla ilgili özel talimatlar vermiş olmalı veya saldırıyı yönetmeli ya da kontrol etmelidir. Devlet dışı aktörlerin eylemlerini sadece teşvik etmek veya devlet dışı aktörün eylemine destek ifade etmek 8. maddeye göre devletin sorumluluğunu gerektirmez.

Söz konusu eylemin gerçekleştiği yer ya da eyleme katılan aktörlerin bulunduğu yer, devlete ilave sorumluluk yüklenilmesini etkilemeyecektir. Örneğin, B devletinde bulunan bilgisayarları botnet olarak ele geçiren A devletindeki bir grup, C devletinde konuşlu bilgisayar sistemlerini, D devletinden aldığı talimatlara uyarak aşırı yüklemek

için botneti kullanmaktadır. Bu eylem, sorumluluk hukuku uyarınca D devletine atfedilebilir. Grubun topraklarında bulunması nedeniyle A devletinin ve grubun ele geçirdiği botların topraklarında bulunması nedeniyle B devletinin sorumluluğuna gidilemeyecektir.⁶²

Bu kural yalnızca devlete sorumluluk atfetmek için geçerlidir. Bununla birlikte, bir devletin devlet dışı aktörlerle eyleme iştiraki, devlet dışı aktörlerin eylemlerinin devlete atfedilemeyeceği durumlarda bile uluslararası hukuku ihlal edebilir. Örneğin, eğer A devleti kendi inisiyatifiyle, B devletine karşı isyancı bir gruba siber saldırı araçları sağlarsa bu grup A devletinin kontrolü altında hareket etmiyorsa, sadece bu araçların sağlanması grubun saldırılarını A devletine atfetmek için yetersiz olacaktır. Bununla birlikte, bu tür bir yardımın kendisi uluslararası hukuka aykırılık teşkil edebilir.

Birleşmiş Milletler Genel Kurulu'nun devletlerin sorumluluğuna ilişkin taslak kararının 8. maddesinin koşulları başlangıçta karşılanmasa bile, eylemler geriye dönük olarak devlete atfedilebilir. Devletlerin sorumluluğuna ilişkin taslak kararının 11. maddesi uyarınca, “önceki maddelere göre bir devlete atfedilemeyen eylem, devlet söz konusu eylemin kendi eylemi olduğunu kabul ve benimsediği ölçüde, yine de uluslararası hukuka göre bu devletin bir eylemi olarak kabul edilir.” Örneğin, devlet dışı aktörler tarafından bir devlete karşı yürütülen bilgisayar ağı ile ilgili eylemleri ele alalım. Eğer başka bir devlet bu devlet dışı aktörlere destek verirse ve siber yeteneklerini bu aktörleri siber operasyonlara karşı korumak için kullanırsa, devlet bu operasyonlardan ve grubun ilgili sonraki eylemlerinden sorumlu olacaktır. Bu hüküm dar bir şekilde yorumlanmaktadır. Bu destek “onay” ve “kabul” koşullarının birlikte gerçekleşmesinin yanında, ayrıca basit bir tasdik veya zımni kabulden daha fazlasını gerektirmektedir.

⁶² Micheal N. Schmitt et.al, **Talinn Manual on The International Law Applicable to Cyber Warfare**, Cambridge University Press, 2017, s.38

3.6.2.Devletin Siber Altyapısı Kullanılarak Başlatılan Siber Saldırılarda Sorumluluğu

Bir siber operasyonun devletin siber altyapısından kaynaklanmış veya başlatılmış olması, operasyonun o devlete atfedilmesi için yeterli kanıt değildir, ancak söz konusu devletin operasyonla ilişkili olduğuna dair bir göstergedir.

Bu kural yalnızca devlet siber altyapısı kullanılarak yapılan veya başlatılan operasyonlarla ilgilidir. Bu kural başka bir devletten başlatılan ancak devlet üzerinden yönlendirilen işlemleri kapsamamaktadır. Ayrıca devletin topraklarında bulunsa bile, devlete ait olmayan siber altyapıdan kaynaklanan veya başlatılan operasyonlar için bu kural geçerli değildir. Bu kural, siber olayları devlete atfedebilecek sonuçları önceden tespit etmiş değildir.⁶³

Resmi karakteri dikkate alındığında, söz konusu siber altyapının devlete ait olması veya özel kişilerin mülkiyetinde ancak devlet tarafından kiralanmış olmasının bir önemi yoktur. Kullanım ticari değilse, ilgili ekipmanın devletin hangi amaçlarına hizmet ettiği önemli değildir. Devletin tüm birimleri bu terim kapsamına girmektedir. Buna göre, siber altyapı askeri, polisiye, gümrük veya diğer amaçlarla kullanılabilir.

İngiltere ile Arnavutluk arasındaki 1949 Korfu Kanalı Davasında, Birleşmiş Milletler Uluslararası Adalet Divanı bir devletin sınırları dâhilindeki eylemlerin sorumluluğunu atfetmek için kritik eşiğin ne olması gerektiği konusunu incelemiştir. Birleşmiş Milletler Uluslararası Adalet Divanı, ülke egemenliği uluslararası ilişkilerin temel dayanağı olduğu gibi, aynı zamanda uluslararası teamül hukuku uyarınca, her bir devletin diğer devletlerin haklarına aykırı hareketler için topraklarının kullanılmasına bilerek izin vermemesi zorunluluğu bulunduğuna karar vermiştir. Bununla birlikte, bu karar, devletlerin sorumluluk derecesinin ayrıntılarını dikkate almamaktadır. Bir devletin kritik altyapısını yok etmek için siber saldırı kullanan tek bir asker veya vatansever bir bilgisayar korsanından uluslararası olarak bir devlet sorumlu tutulmalı mı? Bir devlet görevlisinin başka bir devlete fiziksel bir saldırı

⁶³ Micheal N. Schmitt et.al, **Talinn Manual**, s.39-40

yapması durumunda, düşmanca davranışın devlete atfedilebileceği konusunda hiç şüphe yoktur.

Bir siber saldırının izlenmesi zorlu teknik güçlükler içerse de, hedeflenen devlet siber saldırıyı kaynak devletin siber birimine veya devletin yetki ya da kontrolünde hareket eden birime kadar başarılı bir şekilde izlerse, kaynak devlet sorumlu tutulmalıdır. Devlet dışı aktörler bir saldırı gerçekleştirdiğinde, hem siber alan hem de geleneksel savaş kapsamında devlet sorumluluğunun belirlenmesi çok daha zor bir sorundur. Birleşmiş Milletler Anlaşmasının 51. maddesi, bir devletin devlet dışı bir aktöre kuvvetle karşılık verip veremeyeceği konusunda bir hüküm içermemektedir.

Siber saldırıların gizli ve kontrol edilemez niteliklerinden dolayı Birleşmiş Milletler Uluslararası Adalet Divanı, Korfu Kanalı Davası kararı özellikle önemlidir.⁶⁴ Önceki bölümlerde vurgulandığı gibi, birçok devlet askeri veya istihbarat kuruluşlarında siber birimler oluşturmuşlardır. Birçok devlet siber saldırı yeteneklerinin bazı unsurlarını özel sektöre devretmiştir. Bir devlet, kendi adına bir saldırı başlatmak için başka bir devleti kullanmayı düşünebilir.

Devlet dışı aktörler, genellikle de bilgisayar eylemcileri, hedeflenen devletler için karmaşık bir sorundur. Bilgisayar eylemcileri genellikle siber saldırılara katılmak için yeterli beceriye sahip olan milliyetçi veya ideolojik duygularla motive edilmiş vatandaşlardır. Siber alanın doğası, bilgisayar eylemcilerinin, herhangi bir yerden, istedikleri zaman, devletin direktifi olmadan başka bir devlete saldırı başlatmasına izin vermektedir. Bilgisayar eylemcilerinin dünyanın hemen her yerinden siber saldırı yapabilme kabiliyeti onların üçüncü bir devletin topraklarında faaliyet göstermelerine imkân vermektedir. Üçüncü taraf devletin topraklarında bulunan bilgisayar eylemcisine karşı yapılan herhangi bir eylem, bu devletin egemenliğinin ihlal edilmesine sebep olacaktır. Birleşmiş Milletler Anlaşması, açıkça, uluslararası çatışmaların bu yönünü ele almamış, bilgisayar eylemcilerinin istismar edebileceği yasal bir boşluk bırakmıştır. Yine de teamül hukuku ve uygulama, devletlerin devlet dışı aktörlere güçle karşılık verebileceklerini ve yaptıklarını göstermektedir.

⁶⁴ International Court of Justice, **Corfu Channel** (United Kingdom of Great Britain and Northern Ireland v. Albania), (çevrimiçi) <https://www.icj-cij.org/en/case/1>, 21.02.2019

Bir siber operasyonun devletin siber altyapısından başlatılmış olması, tek başına bu devletin bu operasyona dâhil olduğuna dair bir gösterge olabilir mi? Siber saldırıların ortaya çıkmasından önce, devlet varlıklarının, özellikle askeri teçhizatın kullanılması durumunda bu eylem sorgulanmadan devlete atfedilirdi çünkü devlet organları dışındaki kişiler veya hükümet işlevlerini yerine getirmeye yetkili şahıslar veya gruplar tarafından bu teçhizatın kullanılma ihtimali düşüktü. Bu geleneksel yaklaşım siber bağlamda kullanılamaz. Çünkü devletin siber altyapısı, siber operasyonları yürütmek için bu altyapıyı kullanan devlet dışı aktörlerin kontrolü altına izinsiz olarak girmiş olabilir.

Her durum kendi içinde ele alınmalıdır. Örneğin, siber operasyonları başlatmak amacıyla devlet dışı bir grup tarafından devletin siber altyapısının kontrolünü ele geçirilmesi, devletin o operasyonla bağlantılı olmadığına ilişkin bir gösterge olabilir. Benzer şekilde, devlet bilgisayarlarının devlet dışı aktörler tarafından siber operasyon yürütmek için kullanılabileceğini veya kullanıldığının anlaşılması çok zor değildir. Aslında, aldatma, başka bir kişi veya örgütmüş gibi rol yapmak için tasarlanmış, yaygın olarak kullanılan bir siber tekniktir. Estonya (2007) ve Gürcistan (2008) saldırılarında bu teknik yaygın olarak kullanılmıştır.

Kural bir devletin kendi toprakları ile sınırlı değildir. Açık denizlerdeki gemilerden, uluslararası hava sahasındaki uçaklardan ve uydulardan başlatılan siber operasyonlar bulunmaktadır.

3.6.3. Bir Devlet Üzerinden Yönlendirilen Siber Operasyonlar

Bir siber operasyonun bir devlette bulunan siber altyapı aracılığıyla yönlendirilmiş olması, bu işlemi o devlete atfetmek için yeterli kanıt değildir.

Bir devlette bulunan siber altyapıdan başlatılan siber operasyonları, diğer devlette bulunan devlet veya devlet dışı siber altyapı aracılığıyla yönlendirildiğinde, diğer devletin siber operasyonla ilişkili olduğu varsayılmaz. Bunun nedeni, bir devlette yer alan siber altyapı üzerinden verilerin doğrudan geçişinin(transit devlet), o devletin siber operasyona dâhil olduğunu göstermeyeceğine ilişkin siber alanın özellikleri yüzündendir.

Bir devletin, siber altyapısının diğer devletlerin haklarına aykırı eylemlerde kullanılmasına bilerek izin vermemesi gerekir. Ancak, bu kuralın siber operasyonların yönlendirildiği devletlere uygulanıp uygulanmayacağı konusunda uzmanlar arasında fikir birliği yoktur. Ancak transit devletin, transit geçişi önlemek için makul önlemler alma sorumluluğu bulunmaktadır. İlgili eylemin bir devlete atfedilebileceği başka kriterler olabilir. Örneğin, bu durum, uluslararası silahlı çatışma sırasında tarafsız devletlerin hak ve yükümlülüklerine hâlel getirmez.

Saldırı yapanın bir devlet mi yoksa ferdi bir saldırı mı olduğunu tanımlamak çok önemlidir. Gelişmiş siber tehdit; ısrarlı ve etkili bir şekilde belirlenmiş bir hedefe tekrarlayan şekilde saldırılar yapabilen, çok karmaşık yöntemleri kullanan, tespit edilmesi ve önlem alınması oldukça zor olan gelişmiş saldırı programlardır. Gelişmiş siber tehditler, çok aşamalı, çok disiplinli, gelişmiş teknikler kullanan ve uzun süre devam eden saldırılardır. Gelişmiş siber tehditler, tezin birinci bölümünde açıklanan özellikleri ve bu saldırı için gerekli imkân ve kabiliyetlerin ancak bir devletin elinde olabileceğinden hareketle devlet veya devlet destekli siber saldırganlarda işaret etmektedir. Bu kriter saldırganın bir devlet mi yoksa bireysel mi olduğunu ayırt etmek için önemli bir kriter olabilir.⁶⁵

Bundan sonraki sıradaki tespit ise saldırganların hangi devlet adına bu saldırıyı yaptıkları olacaktır. Saldırganların kullandıkları teknikler ve daha önceki yaptıkları saldırılar saldırganların hangi devlet adına bu saldırıyı yaptıklarının tespitinde kullanılabilecek bir ölçüt olabilir. Sonuç olarak yapılan saldırılarda kullanılan tekniklerden yola çıkarak saldırıyı gerçekleştiren bilgisayar korsan grubuna oradan da devlete saldırı atfedilebilir.

3.6.4. Devletin Sorumluluğuyla İlgili Değişimler

Bilim insanları 11 Eylül saldırılarından bu yana, silahlı çatışma hukuku doktrininde devletin sorumluluğu konusunda değişiklik olduğunu savunmaktadırlar. Devletin sorumluluğu, saldırıların faillerini bilerek topraklarında barındırmayı kapsamamaktadır. 11 Eylül'den bu yana, devletin sorumluluk anlayışıyla ilgili

⁶⁵ Eric Cole, **Advanced Persistent Threat**, (Çevrimiçi), <http://index-of.es/Varios/Syngress.Advanced.Persistent.Threat.Nov.2012.ISBN.1597499498.pdf>, s.19-21, 25.02.2019

tartışmalar devam etmektedir.11 Eylül 2001'den sonra ABD'nin El Kaide'ye karşı yürüttüğü savaşa verilen büyük uluslararası destek devlet sorumluluğuna ilişkin değişikliğin kanıtı olarak görülmektedir. Bu değişiklik, Birleşmiş Milletler Güvenlik Konseyi'nin 1368 ve 1373 sayılı kararları ile ABD'nin eylemlerini onaylamasıyla somutlaşmıştır. Birleşmiş Milletler Güvenlik Konseyi 1368 sayılı kararında, 11 Eylül saldırılarının faillerine yardım eden, destek veren veya topraklarında barındıranların hesap vereceğini açıkça belirtmiştir. Devlet sorumluluğuna ilişkin bu görüş oldukça tartışmalıdır. Bu görüş Birleşmiş Milletler Uluslararası Adalet Divanı'nın Nikaragua kararı ve Eski Yugoslavya Uluslararası Ceza Mahkemesi'nin Tadić davasında ortaya konulan standartlardan kayda değer bir farklılık öngörmektedir.

Silahlı çatışma hukuku doktrindeki devletin sorumluluğuna ilişkin değişime itiraz eden Talin El Kitabı Uzmanları, Birleşmiş Milletler Güvenlik Konseyi kararlarının istisnai koşullara istisnai bir cevap olduğunu iddia etmektedirler.⁶⁶ Bununla birlikte, 11 Eylül saldırılarının faillerini barındırmanın, saldırganların eylemlerini onaylamaya benzer olduğu gerekçesiyle açıklanabilir, bu durum devletin kendi topraklarından kaynaklanan saldırıları önleme görevini bilerek ihlal ettiği anlamına gelmektedir. Bu değişiklik, siber alanda, devlete yüksek bir sorumluluk getirmektedir. Siber saldırılar hemen hemen her yerden gerçekleştirilebilir, saldırganların saldırıyı başlattığında ülkesi toprağında bulunan her devletin uluslararası olarak sorumlu tutulabilmesi anlamına gelmektedir.

⁶⁶ Micheal N. Schmitt et.al, **Talinn Manual**, s.35-39

DÖRDÜNCÜ BÖLÜM

MEŞRU MÜDAFAA KAPSAMINDA SİBER SALDIRILARA VERİLECEK KARŞILIK

4.1.MEŞRU MÜDAFAANIN TANIMI

Meşru müdafaa, bir kişinin, yasanın öngördüğü şartlar altında yakın bir tehlikeye karşı kendi koruması için normal olarak yasayla izin verilmeyen araçlara başvurmasını ifade etmektedir.¹ Bazı uluslararası kararlarda, kendini savunma yerine meşru müdafaa ifadesi bulunmaktadır. Çünkü koşulları oluştuğunda kendini savunma meşru hale gelmektedir. Uluslararası hukuk kurallarının öngördüğü koşullar altında meşru müdafaa, saldırıya uğrayan devlete meşru bir hak sağlamaktadır. Birleşmiş Milletler Anlaşması, meşru müdafaayı doğal bir hak olarak kabul etmektedir.

Devletler söz konusu olduğunda, meşru müdafaanın amacı, devletin kendi varlığını ve vatandaşlarının hayatlarını ve mallarını korumaktır. Her halükarda, meşru müdafaa hak sahibi devletin savunmasıyla sınırlı kalmalıdır. Uluslararası ilişkilerde devletlerin, hayati çıkarlarını zorla savunabileceklerine belirli kurallar çerçevesinde izin verilmiş olmasına rağmen bunun için bir ölçüt getirilmemiştir. Ancak devletin güvenliğine, vatandaşlarının hayatlarına veya mallarına karşı ani ve karşı konulmaz bir tehlikenin varlığı meşru müdafaanın olmazsa olmazıdır.

4.2. MEŞRU MÜDAFAAYA STRATEJİK BAKIŞ

Son yıllarda, siber alanla ve siber alanın kullanımıyla ilgili konular, realizm tarafından devletin güvenliği ve ulusal çıkarların korunması gibi yüksek politika olarak adlandırılan en yüksek politika alanına girmiştir. Önceden, siber alan düşük politika, arka plan koşulları ve süreçler meselesi olarak düşünülmekteydi. Günümüzde siber güvenlik, yerel ve uluslararası çıkar çatışmasının ve giderek artan bir şekilde devlet gücünün planlanması için bir odak noktası haline gelmiştir.²

Siber alanı devlet bakışı ile değerlendirdiğimizde, bugünün güncel siber sorularının daha çok politika ile ilgili olduğu görülmektedir. Kara, deniz, hava ve uzay gibi diğer

¹ Bin Cheng, **General Principles of Law**, Cambridge University Press, 2006, s.92

² Jelle van Haaster, **Assessing Cyber Power**, **8th International Conference on Cyber Conflict**, (Çevrimiçi)<https://ccdcoe.org/uploads/2018/10/Art-01-Assessing-Cyber-Power.pdf>, s 7-21, 29.08.2019

alanların yanında siber alan öncelikle politik olarak ele alınmalıdır. Siber politikayı kısaca tanımlamak gerekirse siber güvenliğin sağlanması için izlenen yol ve yöntemler olarak ifade edebiliriz. Politika söz konusu olduğunda, güç ve güç kullanımı ile ilgili meseleler daima ön plana gelmektedir. Örneğin, savaşta kullanılan kara, deniz ve hava gücü gibi siber güç de politik bir amaç elde etmek veya gücü arttırmak için bir araçtır. Siber alanın kullanımının her alandaki artışıyla birlikte politik amaçlara ulaşmak ve jeostratejik bir avantaj elde etmek için stratejik kullanımı da artmıştır.

Siber alanın ortaya çıkması ve siber alana gittikçe artan bağımlılığımız siyasetin yürütülmesi için yeni bir alan oluşturmuş, hatta yeni bir politika şekli ortaya çıkarmıştır. Siber alan farklı araçlarıyla tüm siyasal alanlara nüfuz etmeye devam etmektedir. Bu nedenle, siber alanla ilgili konuların politikalara dâhil edilmesi zamanı gelmiştir. Nasıl ki deniz politikası, politik süreçler ile deniz alanındaki etkileşimlere ilişkin iki sürecin birleşiminden oluşuyorsa, siber politika da politik süreçler ile siber alanı kullanan dijital(sayısal) etkileşimlere ilişkin iki sürecin birleşimini ifade etmektedir. Siber ve fiziksel alanlarda politika, temel değerlerin niteliği üzerindeki tartışmaları çözüme ulaştırmak için müzakere ve pazarlık etmeyi içermektedir. Bu yüzden, devletlerin siber saldırılara orantılı tepkileri arasında siber politikalar önemli bir yer tutacaktır.

Siber alan güvenliği, günümüzün güvenliğinin, savaşın ve siyasetinin ayrılmaz bir parçası haline gelmiştir. Bu nedenle, siber saldırılara ve siber alandaki diğer faaliyetlere daha geniş politik, stratejik ve jeopolitik kapsamlarda bakılması gerekir. Örneğin, Ukrayna'daki son çatışma ve Kırım'ın Rusya tarafından ilhak edilmesi bir anlaşmazlığın genel politik gidişatını şekillendirmek için siber saldırıların etkin olarak kullanıldığı bir örnek olarak ortaya çıkmış ve çatışmanın fiziki alanlarının yanında siber alan da savaşın ayrılmaz bir parçası olduğunu ortaya koymuştur.³

ABD Savunma Bakanlığı, 1999 yılında, ABD hükümetinin siber alandaki eylemlerini desteklemek için siber savaşın yürütülmesiyle ilgili olabilecek uluslararası anlaşma ve uluslararası hukuku inceleyen bir belge hazırlamıştır. Hazırlanan belge, ilk

³ James J. Wirtz, . "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy ", **NATO Cooperative Cyber Defence Centre of Excellence Publications**, Tallinn 2015, s.29-32

olarak uluslararası toplumun konuyla ilgili çok hızlı bir şekilde normlar üretmesi ihtimalinin bulunmadığını ve mevcut uluslararası hukuk ilkelerinin siber savaşa uygulanabilirliğini belirlemek için geçmiş savaşların çeşitli unsurlarını ve koşullarını analiz etmenin uygun olacağını önermektedir. ⁴

Birleşmiş Milletler Anlaşmasının 51. maddesinin kapsamı, uluslararası hukuk açısından öğretide tartışma yaratmaktadır. Maddenin metnini, bir kısım uzmanlar dar bir kısım uzmanlar da geniş yorumlamaktadır. Madde metnini dar yorumlayan uzmanlar, bir devletin silahlı bir saldırıya uğrayıncaya kadar kendini savunma eyleminde bulunamayacağını ileri sürmektedir. ⁵ Bu görüşe göre, bir devlet silahlı saldırı beklentisiyle hareket ederek önleyici meşru müdafaada bulunamayacaktır. Bununla birlikte, başta ABD olmak üzere bazı devletler kısıtlayıcı görüşe karşı konum alarak ve belirli durumlarda silahlı bir saldırıdan önce kuvvet kullanmanın yasal olabileceği yönündeki görüşü desteklemektedirler. ABD 2003 yılında Irak'a yaptığı müdahaleyi önleyici meşru müdafaaya dayandırmıştır.

Madde metnini geniş yorumlayan hukuk uzmanları, çok yakın ve gerçek bir tehlikenin varlığı karşısında eğer başka herhangi bir yol yoksa Birleşmiş Milletler Anlaşmasının 51. maddesinin, önleyici meşru müdafaaya izin verdiğini iddia etmektedir. ⁶ Savaş ilan edilmesine ilişkin koşul ve nedenleri kapsayan haklı savaş (Jus ad bellum) paradigması altında, silahlı saldırıya uğrayan devletin bu saldırıya verdiği karşılığı meşru müdafa olarak nitelendirmek için üç şartı yerine getirmesi gerekmektedir. Bunlar; gereklilik, orantılılık ve aniliktir.

Silahlı bir saldırıya uğrayan devlet gereklilik ilkesini yerine getirmek için saldırıyı belirli bir kaynağa atfetmeli, saldırının arkasındaki amacı tanımlamalı ve devletin karşılık olarak güç kullanması gerektiği sonucuna varmalıdır. Orantılılık ilkesi karşılık vermek için kullanılan güç ile saldırıda kullanılan gücün orantılı olmasını ifade etmektedir. Anilik ilkesi, çok fazla zaman geçtikten sonra gerçekleşen bir karşılığı

⁴ Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, **Boston College International and Comparative Law Review** V.32, s.439-454

⁵ Ian Brownlie, **International Law And The Use Of Force Between States**, Oxford Scholarship Online: March 2012, s.275-278

⁶ Hüseyin Pazarcı, **Uluslararası Hukuk**, Gözden Geçirilmiş 3.Bası, Turhan Kitabevi, Ankara 2014, s. 513

yasaklamaktadır. Bununla birlikte, genel bir kriter olarak anilik ile ilgili olarak, silahlı bir saldırının hemen ardından, savunma eyleminin gerçekleştirilmesi gerekli olduğu sonucu çıkarılmamalıdır.

Siber saldırı bağlamında özellikle saldırının atfedilmesi ve saldırının amacının tanımlanması çok önemlidir. Uluslararası hukukun meşru müdafaa ile ilgili kuralları yapılan saldırı bir devlete veya onun bir ajanına atfedilemediği sürece, saldırıya uğrayan devletin uluslararası sınırları boyunca aktif savunma eylemleri yapmasını müsaade etmez. Siber alanın siber saldırıyı uzaktan komuta etme ve saldırganın kimliğinin kolayca gizleyebilme imkânları göz önüne alındığında, siber saldırıların faillerini tanımlamak için bir önceki bölümde ayrıntılı olarak açıklandığı gibi özel bir çalışma yapmak gerekmektedir. Atfetme, bir devletin masum bir insanı veya yeri hedeflemesine engel olacaktır. Ayrıca, saldırıya uğrayan devletin saldırıyı başka bir devlete veya devlet dışı aktöre atfetmesi gerekir çünkü karşılık vermeye imkân sağlayan hukuk kuralları, saldırganın bir devlet veya devlet dışı bir aktör olmasına bağlı olarak değişiklik içermektedir.

Birleşmiş Milletler Anlaşması'nın 2. Maddesinin 4. Fıkrasında ifade bulan güç kullanma yasağı, bireyler için değil sadece devletler için geçerlidir. Bu nedenle devletlerin, uluslararası hukuk kuralları uyarınca, birbirlerine karşı tehdit ve güç kullanmaları yasaklanmışken bireylerin tehdit ve güç kullanmaları ise yerel ceza kanunlarınca engellenmiştir. Güç kullanarak karşılık verebilmek için saldırıya uğrayan devletin önce saldırganın niyetinin düşmanca olduğunu ortaya koyması gereklidir. Konvansiyonel savaşın yürütüldüğü kara, deniz, hava ve uzay alanlarından farklı olarak siber alanın yapısı saldırıya uğrayan devleti önleyici meşru müdafaaada bulunma fırsatından mahrum etmektedir. Bu zafiyetin giderilmesi için bir takım tedbirlerin alınmasının gerekli olduğu ortadadır. Bu konudaki dikkat çekici bir öneriye göre önce tüm devletler hayati çıkarları için kritik öneme sahip bilgisayar sistemlerini Birleşmiş Milletler nezdinde beyan etmelidir. Sonra bu bilgisayar sistemlerine nüfuz ederek düşmanca niyet sergileyen herhangi bir devlete karşı angajman kuralları belirlenmelidir. Bu tedbirler alındıktan sonra saldırı beklentisi olan devletin, önleyici meşru müdafaa

kapsamında belirlenen angajman kurallarına uygun olarak saldırgan devlete karşı güç kullanması meşru hale gelecektir.⁷

4.3.MEŞRU MÜDAFAA KOŞULLARI

Son yıllarda yapılan analizler, devletlerin siber saldırılara verilen karşılıkların büyük ölçüde değiştiğini göstermektedir. Bir şeyler yapılması için önemli bir politik baskı olmasına rağmen, geçmiş deneyimler siber saldırılara verilen karşılıkların çoğunun geçici olduğunu göstermektedir. Silahlı saldırı seviyesine ulaşan siber bir saldırının hedefi olan devlet, uluslararası hukuk kurallarına göre meşru müdafaa hakkını kullanabilir. Birleşmiş Milletler Anlaşmasının 51. maddesi açıkça silahlı bir saldırıya uğrayan devlete meşru müdafaa hakkı tanımaktadır. Ancak buradaki en büyük zorluk bir siber saldırının silahlı bir saldırı olup olmadığına nasıl karar verileceğiyle ilgilidir. Birleşmiş Milletler Uluslararası Adalet Divanı kararlarına göre bu karar genellikle yapılan siber saldırının büyüklüğüne ve saldırı sonucunda ortaya çıkan etkilere bağlıdır.

Ayrıca meşru müdafaa hakkının doğabilmesi için saldırıya uğrayan devletin sınırlarının ihlal edilmiş olması gereklidir. Bir devlet başka devlete veya devlet dışı aktöre karşı silahlı saldırı olarak nitelendirilen bir siber saldırıya girdiğinde, saldırı sınır ötesine geçtiğinde bu kriter karşılanmış olacaktır. Ancak devlet dışı aktörler tarafından bir devlete karşı herhangi bir devlet adına yapılmayan siber saldırıda durum karmaşık bir hal almaktadır. Ancak bu durumun konumuzla doğrudan ilgisi olmadığından burada incelenmeyecektir. Bir devlet kendi iç hukukuna uygun olarak kendi ülkesinde düzenlenen, yürütülen ve yönlendirilen siber saldırılar ile ilgili olarak insan hakları ihlali oluşturmayacak şekilde güç kullanarak bu saldırıları durdurabilir.

4.3.1.Büyüklük ve Etki Kriteri

Birleşmiş Milletler Uluslararası Adalet Divanı'nın Nükleer Silahların kullanımı ile ilgili tavsiye kararında, bir saldırının silahlı saldırı olarak nitelendirilip nitelendirilemeyeceği hususunda saldırı araçlarının seçiminin önemsiz olduğunu

⁷ Walter Gary Sharp, Cyberspace and the Use of Force, **Ageis Research Corp**, 01.02.1999, s.130-139

ısrarla vurgulamıştır.⁸ Örneğin, kimyasal, biyolojik ve radyolojik saldırıların büyüklük ve etkilerinin silahlı bir saldırıyı oluşturduğu ve meşru müdafaa hakkını doğurduğu bütün dünyada kabul edilmektedir. Kinetik olmayan yapısına rağmen kimyasal, biyolojik ve radyolojik saldırılar için yapılan kabulün, aynı akıl yürütmeye siber saldırılar için de geçerli olacağı değerlendirilebilir. Çünkü saldırı sonrasında ortaya çıkan sonuçlar ciddi ıstırap ya da ölüm içerebilir. Bu durumda meşru müdafaa güç kullanma hakkı, sadece kinetik silahlı saldırıları değil siber saldırıları da kapsamalıdır. Öğretide bazı siber saldırıların Birleşmiş Milletler Anlaşması kapsamında silahlı saldırı olarak değerlendirilebilecek ciddi sonuçlara yol açabileceği kabul edilmektedir.

Birleşmiş Milletler Anlaşmasının 51. maddesi meşru müdafaa hakkının doğması için silahlı bir saldırıdan bahsetmekle birlikte mutlaka silah kullanılmasının gerekip gerekmediği konusu öğretide tartışmalıdır. Çoğunluk silah kullanılmasının gerekmediğini, bir siber saldırıda kritik faktörün, bu etkilere ulaşmak için kullanılan araçlardan çok ortaya çıkan etkinin silahlı bir saldırı eyleminden kaynaklanacak sonuçlarla kıyaslanması gerektiği konusunda fikir birliğindedir.

Önceki bölümde de ifade edildiği gibi silahlı saldırı terimi ile kuvvet kullanımı terimi eşdeğer değildir. Silahlı bir saldırı, Birleşmiş Milletler Anlaşmasının 2. maddesi 4. fıkrası anlamında kuvvet kullanımını öngörmektedir. Birleşmiş Milletler Uluslararası Adalet Divanı'nın da belirttiği gibi, her güç kullanımı silahlı saldırı değildir. Silahlı saldırı olarak nitelendirilecek bir eylem için gerekli olan büyüklük ve etkinin, eylemin kuvvet kullanımı olarak nitelemenin ötesinde büyüklük ve etkiye sahip olması gerekmektedir. Bir devlet, kendisine karşı kullanılan kuvvetin silahlı saldırı seviyesine ulaşması durumunda, meşru müdafaa kapsamında kuvvet kullanma hakkını kazanacaktır.

Silahlı saldırı olarak nitelendirilecek bir eylem için gerekli olan büyüklük ve etki ibaresi Birleşmiş Milletler Uluslararası Adalet Divanı'nın Nikaragua davası kararında zikredilmiştir. Bu durumda, Mahkeme büyüklük ve etkiyi, silahlı saldırı niteliğindeki eylemleri diğer eylemlerden ayıran kriterler olarak tanımlamıştır. Mahkeme, güç

⁸ International Court of Justice, **Nuclear Weapons Advisory Opinion**, 08.07.1996, para.39, (çevrimiçi)<https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf>, 18.07.2019

kullanımının silahlı saldırı oluşturanlar ve silahlı saldırı oluşturmayanlar olarak ayırt etmek gerekliliğine dikkat çekmiş, ancak bu konuda daha ayrıntılı bir yorum getirmemiştir.⁹ Bu nedenle, büyüklük parametreleri ve etki kriterleri, tam olarak anlaşılamamıştır. Örneğin insanların ölümüne veya yaralanmasına neden olan ya da insanların mülküne zarar veren bir güç kullanımının, büyüklük ve etki şartını yerine getirmiş olacağı konusunda hiçbir şüphe yoktur. Ancak siber casusluk ve siber hırsızlık ile elzem olmayan siber hizmetlerin kısa veya periyodik olarak kesilmesine neden olan siber saldırılar, silahlı saldırı olarak nitelendirilemeyecektir.

İnsanların ölümüne veya yaralanmasına, mülklerin hasar veya yok olmasına neden olan siber saldırıların silahlı saldırı olarak nitelendirilmesi noktasında, Birleşmiş Milletler Anlaşmasının 51. Maddesi çok açık değildir. Birleşmiş Milletler Uluslararası Adalet Divanı'nın Nikaragua davası kararında silahlı bir saldırı ile basit bir sınır olayı arasında ayırım yapmıştır.¹⁰ ABD, 1987 yılında İran'a ait iki adet petrol platformunu bombalayarak imha etmesini meşru müdafaa hakkına dayandırmıştır. İran sorunu Birleşmiş Milletler Uluslararası Adalet Divanı önüne taşımıştır. Bu davada taraflar arasındaki uyuşmazlık ABD'nin silahlı çatışma hukuku kapsamında kullandığı gücün orantılı ve gerekli olup olmadığıdır. ABD, İran'ın ABD bayraklı bir petrol tankerine düzenlemiş olduğu saldırının meşru müdafaa hakkı doğurduğunu savunmuştur. İran ise ABD'nin petrol platformlarına yaptığı saldırıların orantılılık ve gereklilik kriterini karşılamadığını iddia etmiştir. Birleşmiş Milletler Uluslararası Adalet Divanı gerçekleşen silahlı saldırının büyüklük ve etki bakımından ciddi bir seviyeye ulaşması gerektiğine karar vermiş, tek bir askeri platform veya tesisten yapılan saldırının silahlı saldırı olarak nitelendirilebileceğini belirtmiştir.¹¹

Bir devletin, birer birer ele alındığında silahlı saldırı eşiğinin altında kalan bir dizi siber saldırıya karşılık olarak meşru müdafaa hakkını kullanıp kullanamayacağı da cevap bulunması gereken en önemli sorulardan birisidir. Başka bir deyişle, bu saldırıların toplamı silahlı bir saldırı oluşturabilir mi? Belirleyici faktör, aynı kaynağın birbiriyle ilişkili ve birlikte ele alınması zorunlu olan silahlı saldırı eşiğinin altında

⁹ International Court of Justice, **Nicaragua Judgment**, para. 191

¹⁰ **A.e.**, para.195

¹¹ International Court of Justice, **Oil Platforms Judgment** 12.12.1996, paras.57,61, (çevrimiçi) <https://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf>, 23.07.2019

kalan saldırılar gerçekleştirip gerçekleştirmediğidir. Durumun böyle olduğuna dair ikna edici kanıtlar varsa, öğretide silahlı saldırı eşiğinin altında kalan siber saldırıların birleşik silahlı saldırı olarak ele almanın mümkün olabileceği yönünde görüşler bulunmaktadır.

İnsanların yaralanması veya ölümü ile mülklerinin hasarı veya yok olmasına neden olmayan ancak kapsamlı olumsuz etkileri bulunan eylemlerin silahlı saldırı sayılıp sayılmayacağı konusunda öğretide bir fikir birliği yoktur. Talin El Kitabını hazırlayan uzmanların bir kısmı, bir saldırı silahlı saldırı olarak nitelendirilecekse mutlaka kişilere veya mülke zarar verilmiş olmasının gerekli olduğu yönünde fikir beyan etmektedir. Bazı uzmanlar ise, sonuçların mahiyetinin önemli olmadığını, ortaya çıkan etkilerin derecesinin daha önemli olduğu görüşündedir.¹²

Örneğin yapılan siber saldırılar sonucunda Borsa İstanbul'un çöktüğünü varsayalım, bu saldırılar sonucunda sadece finansal bir zarar ortaya çıkacaktır. Bu nedenle uluslararası silahlı çatışma hukuku ve Birleşmiş Milletler Uluslararası Adalet Divanı kararları ışığında bu saldırıların silahlı saldırı olarak nitelendirilmesi pek mümkün değildir. Ancak günümüzde devletler için refah ve ekonomiye verilen önemin artmış olması sebebiyle böyle bir çöküşün devlet nezdinde etkisi silahlı bir saldırıdan bile fazla olacaktır. Aynı yaklaşımla, bir devletin kritik altyapısına yönelik yıkıcı olmasa da ciddi etkilere yol açan bir siber saldırının etkileri silahlı bir saldırıdan fazla olabilecektir.

Siber bağlamdaki diğer tartışılmalı konu ise, bir eylemin silahlı saldırı olarak nitelendirilip nitelendirilmeyeceğinin tespitinde hangi etkilerin dikkate alınacağını belirlemektir. Bir şehrin su arıtma tesisini hedef alan siber saldırı örneğinde kirli suyun içilmesinden kaynaklanan hastalık ve ölümler nasıl değerlendirilmelidir?

Örneğin, X devleti Y devletine karşı siber casusluk yaparken beklenmedik bir şekilde Y devletinin siber altyapısında ciddi zararlar meydana geldiğinde saldırıları silahlı saldırı olarak nitelendirmek mümkün olmasa da saldırıların olumsuz etkilerini

¹² Micheal N.Schmitt et.al, **Talinn Manual**, s.55-59

önlemek için önlemler alınabileceği kabul edilmektedir. Bununla birlikte, verilen herhangi bir karşılık gereklilik ve orantılılık kriterlerine uymak zorundadır.

Örneğin X devletinin Y devletine karşı siber silahlı saldırısı, Z devletinde olumsuz etkilere neden olur ve bu etkiler, silahlı saldırı olarak nitelendirebilmek için büyüklük ve etki kriterlerini karşılarsa, Z devleti gereklilik ve orantılılık kriterlerine uyduğu sürece, meşru müdafaa için güç kullanabileceği konusunda bir şüphe yoktur.

Bugüne kadar yapılan uluslararası siber saldırılardan birinin silahlı saldırı eşiğine ulaştığına yönelik uluslararası toplum tarafından bir açıklama ve tespit yapılmamıştır. Siber savaş olarak adlandırılan Estonya'ya yönelik 2007 siber saldırıları, Estonya veya uluslararası toplum tarafından silahlı bir saldırı olarak açıkça nitelendirilmemiştir. Saldırının büyüklük ve etkisinin silahlı saldırı eşiğini aşmadığı yönünde yaygın bir görüş bulunmaktadır. 2010 yılında İran'ın uranyum zenginleştirme tesisine Stuxnet virüsü ile yapılan siber saldırılar sonucunda santrifüjlere verilen fiziksel zarar ışığında, siber saldırıların silahlı saldırı eşiğine ulaştığı yönünde güvenlik uzmanları arasında yaygın bir kanaat bulunmaktadır.

4.3.2.Siber Saldırının Kaynağı

Siber bir saldırının silahlı saldırı olarak nitelendirilip nitelendirilemeyeceğinin belirlenmesinde siber saldırı kaynağının mutlaka dikkate alınması gerekmektedir. Silahlı saldırı eşiğine ulaşan siber bir saldırıyı devlet organları yürütüyorsa bu saldırının silahlı bir saldırı olarak nitelendirilebileceğine hiç şüphe yoktur. Bir devlete atfedilebilen devlet dışı aktörlerin silahlı saldırı eşiğine ulaşan siber saldırılarının da silahlı saldırı olarak nitelenebileceği tartışılmazdır. Birleşmiş Milletler Uluslararası Adalet Divanı Nikaragua kararına göre; silahlı saldırı, yalnızca uluslararası bir sınır boyunca düzenli kuvvetler tarafından yapılacak eylemleri değil, aynı zamanda başka bir devlete karşı bir devlet adına silahlı kuvvet eylemleri yürüten silahlı gruplar, düzensiz birlikler ve paralı askerlerin silahlı saldırı seviyesine ulaşan eylemleri de bu kapsamda anlaşılması gerekmektedir.¹³

¹³ International Court of Justice, **Nicaragua Judgement**, para.195

Birleşmiş Milletler Uluslararası Adalet Divanı'nın yukarıdaki kararı dikkate alındığında örneğin, X devleti yönetimindeki bir grup özel şahıs, Y devletine yönelik siber saldırıları üstlenirse ve bu eylemlerin sonuçları yeterli büyüklük ve etki kriterlerini karşılar, X devleti silahlı bir saldırı gerçekleştirmiş olacaktır. Aynı sonuç, bir devlet yönetimindeki tek bir birey tarafından yürütülen siber saldırılar için de geçerli olacaktır.

Bir devlete atfedilemeyen devlet dışı aktörlerin eylemlerinin, bir silahlı saldırı teşkil edip etmeyeceği, silahlı bir saldırı teşkil etse bile devletin nasıl bir karşılık verebileceği konusu tartışmalıdır. Birleşmiş Milletler Anlaşması'nın 51. maddesi ve uluslararası teamül hukukuna göre meşru müdafaa hakkı, geleneksel olarak yalnızca bir devletin diğerine karşı yürüttüğü silahlı saldırılara karşı uygulanabilir niteliktedir. Devlet dışı aktörler tarafından uygulanan şiddet eylemleri, ilgili devletin kendi iç hukuku kapsamında kolluk kuvvetleri yetkisi içinde kalmaktadır. Bununla birlikte, uluslararası toplum, El Kaide'nin ABD'ye karşı 11 Eylül 2001 saldırısını ABD'ye meşru müdafaa hakkı doğuran silahlı bir saldırı olarak nitelendirmiştir. Birleşmiş Milletler Güvenlik Konseyi 1368 ve 1373 sayılı kararlarında meşru müdafaa hakkına atıfta bulunmuştur. ABD, Birleşmiş Milletler Güvenlik Konseyi'nin bu kararlarında atıf yaptığı meşru müdafaa hakkına dayanarak Afganistan'a müdahalede bulunmuştur. Bu müdahale, devlet dışı aktörler tarafından yürütülen saldırılara karşı meşru müdafaa hakkının kullanılabilmesine örnek teşkil etmektedir. Birleşmiş Milletler Anlaşması'nın 2. maddesinin 4. fıkrası devletlerin kuvvet kullanmasını ve kuvvet kullanma tehdidini yasaklamakta iken, devletlere meşru müdafaa hakkı veren 51. madde devlet dışı aktörler tarafından gerçekleştirilen silahlı saldırıya karşı herhangi bir sınırlama içermemektedir.¹⁴

Yukarıda anlatılan örnek ve açıklamalardan hareketle terörist veya asi gruplar gibi devlet dışı aktörler tarafından yapılan silahlı saldırılar karşısında devletin meşru müdafaa hakkı bulunduğunu savunan uzmanlar bulunmaktadır. Bu uzmanlar, bilgi teknolojisi şirketleri veya internet servis sağlayıcıları tarafından gerçekleştirilen siber saldırılar silahlı saldırı eşiğine ulaşırsa, saldırıya uğrayan devletin meşru müdafaa

¹⁴ Thomas M. Franck, Terrorism and the Right of Self-Defense, **The American Journal of International Law** Vol. 95, No. 4 (Oct., 2001), s. 839-843

hakkına sahip olacağını savunmaktadırlar. Örnek olarak, bu durumda Y devletinde bulunan kritik altyapıya karşı X devletinde bulunan bir grup terörist tarafından yürütülen yıkıcı bir siber saldırıyı Y devletine karşı yapılmış silahlı bir saldırı olarak değerlendirilebilecektir. Ancak bir kişinin büyüklük ve etki eşiğini aşan bir saldırı yapıp yapamayacağı konusu tartışmalıdır.

4.3.3.Siber saldırının Hedefi ve Amacı

Büyüklük ve etki kriterlerini karşılayan bir eylemin silahlı saldırı olarak nitelendirilip nitelendirilemeyeceğine o eylemin hedefi ve amacına bakılarak karar verilebilir. Sınır ötesine yapılmış, büyüklük ve etki kriterlerini karşılayan eylemin amacı saldırıya uğrayan devletin toprakları içindeki malları veya şahısları kapsıyorsa, eylem bu devlete karşı silahlı bir saldırı olarak nitelenebilecektir. Söz konusu hedef, saldırıya uğrayan devletin toprakları dışında kalan mülk veya vatandaşlardan oluşuyorsa, uluslararası hukuka göre siber saldırının silahlı saldırı olarak nitelendirilip nitelendirilemeyeceği belirli değildir. Bir devletin tesislerine veya malzeme ve devletin vatandaşlara yönelik saldırılar, yukarıda belirtilen kriterler yerine getirildiği sürece kesinlikle silahlı saldırı niteliğindedir. Örneğin, X devleti tarafından Y devletinin devlet başkanını yurtdışındayken öldürmek için yapılan bir siber saldırı, silahlı bir saldırı olarak kabul edilecek seviyeye ulaşmaktadır.

Diğer saldırıların silahlı saldırı olup olmadığının belirlenmesi, bunlarla sınırlı olmamak üzere, saldırının neden olduğu hasarın kapsamı; söz konusu mülkün devlet veya özel nitelikte olup olmadığı; hedeflenen bireylerin durumu ve operasyonların politik olarak motive edilip edilmediği, yani mülkiyete veya bireylere karşı milliyetleri nedeniyle yürütülüp yürütülmediği gibi faktörlere bağlıdır. Bu gibi durumlarda kesin bir kural yoktur. Y devletinin yurtdışındaki devlet kuruluşlarından birinin yönetim kurulu başkanını öldürmek için X devleti tarafından yürütülen bir siber saldırıyı ele aldığımızda; saldırının silahlı saldırı olup olmadığı konusunda bir yargıya varmak mümkün değildir.

4.3.4. Başka Bir Devletin Egemenliğinin İhlal Edilmemesi

Meşru müdafaa nedeniyle verilecek karşılık, saldırının gerçekleştiği devletin ülkesi, saldırıya uğrayan devletin toprakları, açık deniz, uluslararası hava sahası veya uzaydan yürütülebilir ve yönetilebilir, bununla ilgili hiçbir kısıtlama bulunmamaktadır.

Siber saldırılar, saldırının atfedilemeyeceği bir devletten başlatıldığında veya o devlette konuşlu bir tesis, araç vb. kullanıldığında meşru müdafaa kapsamında verilecek karşılık saldırının atfedilemediği devletin egemenliğini ihlal etmemelidir. Ancak başka bir devletin topraklarında devletin rızası ile egemenliğini ihlal etmeden meşru müdafaa önlemlerinin alınabileceği tartışılmazdır. Meşru müdafaa kapsamında verilecek karşılığın başka bir devletin topraklarını rızası dışında kullanılması durumunda rıza dışı eylemlerin niteliği önem kazanmaktadır. Bu konudaki baskın görüş ilgili devletin uzmanlık veya teknolojik yoksunluk nedeniyle yapamadığı veya siber silahlı saldırının ilgili unsurlarını bastırmak için etkili adımlar atmak istemediği durumlarda siber bir silahlı saldırıya karşı meşru müdafaaya müsaade edilebileceği yönündedir. Uluslararası hukuka göre devletlerin kendi topraklarını hukuka aykırı davranışlarda kullanılmasını engelleme görevi bulunmaktadır.

Meşru müdafaa kapsamında verilecek karşılık için başka bir devletin topraklarının kullanılmasının yasal olduğunu kabul eden görüş, saldırıya uğrayan devletin ilk önce saldırının yapıldığı devlete silahlı saldırıya son vermesini talep etmesi gerektiğini savunmaktadır. Saldırıya uğrayan devlet, aynı zamanda saldırının yapıldığı devlete durumu ele alma fırsatı vermelidir. Bu gereklilikler, meşru müdafaa eylemlerinin gerçekleştirileceği devletin egemenliğine saygı duyma konusundaki uluslararası hukuk zorunluluğundan kaynaklanmaktadır. Ayrıca, saldırının yapıldığı devletin durumu ele alma isteksizliği veya yetersizliği konusunda hatalı veya erken bir sonuca karşı usule ilişkin bir güvencedir. Saldırıya uğrayan devletin, saldırının yapıldığı devletten saldırıya son vermesini talep etmesi veya durumu çözmesi için yeterli zaman yoksa o takdirde saldırının yapıldığı devlete bir bildirim yapılmayabilir. Siber saldırıyı püskürtmek veya sonuçlarını en aza indirmek için derhal harekete geçmek gerekirse, saldırıya uğrayan devlet saldırının yapıldığı devlete haber vermeden meşru müdafaa hakkını kullanabilir.

4.3.5.Gereklilik, Orantılılık, Yakınlık ve İvedilik Kriterleri

Yapılan saldırının Birleşmiş Milletler Anlaşmasının 51. Maddesinde tanımlanan silahlı bir saldırı kriterlerini karşıladığı yönünde kanaat oluşması durumunda saldırıya uğrayan devletin meşru müdafaa hakkı doğmaktadır. Ancak meşru müdafaa hakkının kullanılması, gereklilik, orantılılık, yakınlık ve ivedilik şartlarına tabidir.¹⁵ Tabii ki, meşru müdafaa silahlı bir saldırının gerçekleşmek üzere veya gerçekleşmiş olmasının yanı sıra saldırganın kimliğine dair makul bir kararın varlığına tabidir. Bu karar, meşru müdafaa hakkından doğan karşı eylem sonrası değil, önceden verilmelidir. Bu kriterlerin daha iyi anlaşılabilmesi için müteakip başlıklarda daha ayrıntılı olarak incelenmiştir.

4.4.GEREKLİLİK VE ORANTILILIK

Meşru müdafaa için yapılan eylemler gereklilik ve orantılılık kriterlerini karşılamalıdır. Birleşmiş Milletler Uluslararası Adalet Divanı, hem Nikaragua kararında hem de Petrol Platformları kararında bu kriterleri esas almıştır.¹⁶ Bu kararlar hiç şüphesiz uluslararası teamül hukukunu yansıtmaktadır. Kuvvete başvurma meşru olduğu durumlarda dikkate alınacak gereklilik ve orantılılık kavramları, askeri gereklilik kavramından ve savaş sırasında kuvvet kullanımındaki orantılılık kuralından farklıdır.

4.4.1.Gereklilik

Gereklilik, silahlı bir güç kullanımına varan siber saldırıları da kapsayan yaklaşmakta olan bir saldırıyı başarılı bir şekilde defetmek veya devam etmekte olan bir saldırıyı başarılı bir şekilde boşa çıkarmak için güç kullanımını gerektirmektedir. Güç kullanımına başvurmadan önce zorlayıcı olmayan diğer tedbirlerin alınmasıyla ilgili bir kısıtlama yoktur. Ancak alınacak tedbirler yalnızca tedbirleri alan tarafın temel güvenlik çıkarlarını koruma eğiliminde olmamalı, aynı zamanda temel güvenlik çıkarlarını koruma amacı için gerekli de olmalıdır.¹⁷

¹⁵ Pazarcı, **a.g.e.**, s.512-517

¹⁶ International Court of Justice, **Nicaragua Judgment**, paras 176,194, **Oil Platforms Judgment**, paras. 43, 73-74, 76.

¹⁷ **A.e**, para.282

Hatta gereklilik kriteri, ancak zorlayıcı olmayan önlemlerin saldırıyı engellemek için yetersiz kalması durumunda güç kullanmayı gerektirmektedir. Güç kullanımını gerektiren zorlayıcı eylemler diplomasi, ekonomik veya hukuki yaptırım gibi zorlayıcı olmayan önlemlerle birlikte de kullanılabilir. Siber alanda yapılan saldırılar doğası gereği genellikle silahlı güç kullanımına varmayan saldırılar olacaktır. Bu nedenle siber alanda genellikle verilecek karşılıkta uygulanacak gereklilik kriteri, güç kullanımı seviyesine yükselmeyen alternatif eylem yöntemlerini kullanmayı gerektirecektir. Ancak silahlı saldırı seviyesine ulaşan siber bir saldırıyı engellemek için güvenlik duvarları gibi pasif siber savunma tedbirleri güvenilir ve tamamen yeterli ise, bu takdirde de güç kullanımı seviyesine ulaşan siber veya kinetik diğer karşılıkların verilmesi gereklilik kriterine uygun olmayacaktır. Bununla birlikte, kuvvet kullanımına varmayan tedbirlerin, silahlı bir saldırıyı defetmesi ve müteakip saldırıları önlemesi mümkün değilse, meşru müdafaa hakkı kuvvet kullanma seviyesine varan siber ve kinetik eylemlere imkân vermektedir.

Gereklilik kriteri saldırıya uğrayan devlet penceresinden bakılarak değerlendirilir. Örneğin, X devletinin, Y devletinin kritik siber altyapısına karşı siber saldırılar gerçekleştirdiği, büyük bir hasara ve can kaybına neden olduğu bir durumda Y devleti X devletine karşı önce zorlayıcı olmayan tedbirlere başvurarak saldırıyı defetmeye çalışmalı eğer bu tedbirler başarılı olmazsa o takdirde ancak güç kullanımına başvurmalıdır. Y devleti güç kullanmayı gerektiren bir tedbire başvurduktan sonra X devletinin saldırılarını ve etkilerini bertaraf edinceye kadar devam etmesi gereklilik kriterine uygun olacaktır.

4.4.2.Orantılılık

Orantılılık, siber güç kullanımı da dâhil olmak üzere, kuvvet kullanmak gerekli olduğunda ne kadar kuvvete müsaade edilebilir olduğu sorununu ele almaktadır.¹⁸ Bu kriter, meşru müdafaa hakkına neden olan durumu sona erdirmek için gereken müdahalenin ölçeğini, kapsamını, süresini ve yoğunluğunu sınırlamaktadır. Yeterli bir savunma yapmak için gereken kuvvet seviyesi saldırının niteliğiyle ilgili olduğundan,

¹⁸ International Court of Justice, **Nicaragua Judgement**, para.282

kullanılan kuvvet miktarını kısıtlamaz; saldırıyı uzaklaştırmak veya saldırganı yenmek için daha fazla güç gerekli olabilir veya daha az güç yeterli olabilir. Ayrıca meşru savunmada kullanılan kuvvetin, silahlı saldırı yapan ile aynı nitelikte olması şartı aranmayacaktır. Bu nedenle, kinetik bir silahlı saldırıya siber güç kullanarak karşılık verilebilir veya bunun tersi de olabilir.

Yemen hükümetiyle çatışan ve İran'ın desteklediği iddia edilen Husi isyancıları Eylül 2019'da Suudi Arabistan petrol tesislerine yönelik saldırıları üstlenmesine rağmen saldırıların arkasında İran'ın olduğuna yönelik şüpheler bulunmaktadır. ABD Başkanı Trump gazetecilere yaptığı açıklamalarda saldırının arkasında İran'ın olup olmadığı konusunda kısa sürede net bir sonuca varacaklarını ve bundan sonra ne yapacaklarına karar vereceklerini söylemiştir. Suudi petrol tesislerine yönelik saldırıya karşılık olarak ABD'nin İran'a askeri bir saldırıda bulunmasının orantılı olup olmayacağına yönelik soruya ilişkin Trump, *"Orantılı olacağını düşünüyorum. Bu soruya yanıtım evet"* şeklinde cevap vermiştir.¹⁹

Silahlı saldırı seviyesine ulaşan siber saldırıyı yapan, siber saldırılara karşı göreceli olarak dayanıklı ise bu durumda meşru müdafaa yapan meşru müdafaanın amacıyla orantılı ise kinetik bir karşılık verebilir.

ABD hükümeti Ekim 2016'da, Rus hükümetinin ABD başkanlık seçimlerini siber yöntemler kullanarak etkilemek ve manipüle etmek için saldırılar yaptığını açıklamıştır. ABD eski başkanı Barack Obama, devletlerin askeri konular gibi bilinen protokolleri olmayan ve neyin kabul edilebilir neyin olmadığı konusunda elde yeterli tecrübe olmayan siber alan için *"keşfedilmemiş sular"* benzetmesini yapmıştır.²⁰ ABD eski Dışişleri Bakanı Hillary Clinton, *"ABD siber saldırılara aynı diğer saldırılar gibi muamele edeceğini"* açıkça belirtmiştir.²¹

¹⁹ Matthew Hoye, "Trump on Iran: 'We'll know for certain over the next very short period of time'", CNN, (Çevrimiçi) <https://edition.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/index.html>, 18.09.2019

²⁰ White House, **Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting**, June 8, 2013, (çevrimiçi) <https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china/>., 23.07.2019

²¹ Andrew Blake, "Hillary Clinton: U.S. Will Treat Cyberattacks 'Just Like any Other Attack,'" **Washington Times**, October 7, 2016, (çevrimiçi) <http://www.washingtontimes.com>, 24.07.2019

ABD Başkan Obama, ABD'nin orantılı bir tepki vermeyi değerlendirdiğini ve bir dizi karşılığın masada olduğunu doğrulamış ve verilecek karşılığın en büyük etkiyi sağlayacak zaman ve şartlarda olacağını belirtmiştir.²² Bu açıklamadan sonra ABD seçimlerini etkilemeye yönelik siber saldırı yaptığı iddia edilen Rusya'ya karşı meşru müdafaa kapsamında verilecek orantılı bir karşılığın neler olacağı merak konusu olmuştur. ABD yaptığı açıklamada, dokuz Rus şirketine ve şahıslara yaptırım uygulayacağını, misilleme olarak otuz beş Rus diplomatını kovacağını, ayrıca kamuoyuna açıklanmayacak bir zamanda ve yerde başka karşılıklar vermeye devam edeceğini söylemiştir.²³

ABD seçimlerine müdahale ve siber saldırıya orantılı bir karşılığın dikkate alınması birkaç soruyu gündeme getirmektedir: Siber düşmanlıklara karşı siyasi bir karşılık çerçevesi oluşturmak neden önemlidir? Bir siber saldırıya orantılı bir karşılığa karar verirken nelere dikkat edilmeli? ABD seçimlerine müdahale, gittikçe artan bir şekilde dijitalleşen bir dünyada siber saldırıları ve artan düşmanlıkları azaltmak için uluslararası normlar geliştirmeye duyulan acil ihtiyacı ortaya koymaktadır.

Devletlerin çoğunun devlet destekli siber saldırılara doğru bir şekilde karşılık vermekte yeterli hazırlıkları olmadığı düşünülmektedir. Siber alanın stratejik önemi arttığında ve saldırgan siber faaliyetler daha yaygın hale geldiğinde, devletler bozucu veya yıkıcı saldırılara orantılı tepkiler vermek için siber politikalar geliştirme zorluğuyla karşı karşıya kalacaklardır. Saldırgan, bir devlet ise siber saldırılara nasıl bir karşılık verileceği konusunda net ve kesin bir cevap bulunmamaktadır. Siber saldırılara en iyi nasıl karşılık verilebileceği konusunda karmaşık sorulara cevap vermek gerekmektedir. Zamanında, orantılı, yasal ve ayırım gözetilen bir karşılık vermek ve saldırganın bunu bilmesini sağlamak saldırganlar için caydırıcı olacaktır.

Salırgan siber faaliyetler yaygınlaştıkça, devletler bozucu veya yıkıcı saldırılara orantılı tepkiler geliştirme zorluğuyla karşılaşmaktadır. Bununla birlikte, tepki

²² David E. Sanger, "Biden Hints U.S. Response to Russia for Cyberattacks," **New York Times**, October 15, 2016, (çevrimiçi) <http://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html>, 26.08.2019

²³ White House, **Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment**, December 29, 2016, (çevrimiçi) <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity>, 27.08.2019

vermeden önce bazı değişkenler göz önünde bulundurulmalıdır. Devlet destekli siber bir saldırıya orantılı karşılığı bir belirlerken, saldırıyı atfetme derecesini, saldırının etkisini, kullanılacak araçları, politik seçenekleri ve riskleri dikkate almak gerekecektir.²⁴

4.4.2.1.Saldırıyı Atfetme Derecesi

Bir siber saldırıyı saldırının arkasındaki devlet veya devlet dışı aktöre atfetmek etkili önlemler ve saldırının arkasındaki failleri belirleme yeteneği gerektirdiğinden önemli bir zorluk olmaya devam etmektedir. Atfetme sorunu son derece karmaşıktır ve her zaman çözülmesi mümkün değildir. Siber alan, saldırıların menşeinin tespitini engellemek için tüm dünyadaki sunucular üzerinden yönlendirilme imkânı sağlamaktadır. Bir siber saldırıyı yanlış atfetmek, yanlış bir hedefe yönelik bir karşılığa yol açabilir. Saldırı doğru atfedilmemişse saldırıya verilecek karşılığın orantılı olup olmamasının hiçbir önemi olmayacaktır. Bu nedenle atfin doğru yapılması çok kritiktir. Atfetmenin kesinliği düşükse, devletler saldırının ciddiyeti ne kadar yüksek olsa bile, verilecek karşılığın seçiminde daha sınırlı ve dikkatli hareket etmelidir. Devletlerin, yanlış bir saldırı yapmaları halinde ortaya çıkacak sonuçlar ile olası krizin tırmanması durumunda ortaya çıkabilecek maliyetleri göz önünde bulundurmaları gerekmektedir. Bu nedenle atfetme derecesi verilen karşılığı etkileyecektir.

Bir saldırıyı belirli bir kaynağa atfetme yeteneği, güvenilirliği korumak ve yurtiçi ve yurtdışında meşruiyet sağlamak için önemlidir. Atfetmek için yeterli kanıt, istihbarat veri kaynakları aracılığıyla toplanabilir veya dost ülkelerden elde edilebilir ancak devletlerin bu kaynakları kamuya açıklamak istememesi önemli bir zorluk içermektedir. Devlet, yürüttüğü misilleme eylemleri için uluslararası meşruiyet oluşturmak istiyorsa, en azından bazı atfetme kanıtlarını kamuoyu ile paylaşması gerekmektedir.

Atfetmenin teknik, yasal ve politik dâhil olmak üzere birçok yönü bulunmaktadır. Atfetme, adli, insan istihbaratı, sinyal istihbaratı, tarih ve jeopolitik gibi birçok bilgi

²⁴ Jarno Limnéll, **Developing a Proportionate Response to a Cyber Attack**, Aalto University Publication Series Science+Technology, 2016, s.9

kaynağının analizini gerektiren çok boyutlu bir konudur. Atfetme, üç seviyedeki belirsizliği en aza indirme uygulamasıdır. Taktik olarak, atıf bir bilim kadar bir sanattır, operatif olarak, atıf ince ayrımlı bir süreçtir ve stratejik olarak, atfetme politik riskleri ve maliyeti olan karardır.

Başarılı bir atfetme, her seviyede bir dizi beceri, dikkatli yönetim, zaman, liderlik, stres testi, ihtiyatlı iletişim ve sınırlamaları ve zorlukları tanımayı gerektirmektedir. Her üç seviyede de güvenlik uzmanlarının yoğun ilgisine bağlı olarak atfetme kabiliyetleri artmış olsa bile, atıfta bulunmak için atfetmenin sonucu her zaman politik bir karardır. Önceki bölümde ayrıntılı olarak incelendiğinden atfetme ile ilgili burada daha fazla açıklama yapılmayacaktır.

4.4.2.2 Siber Saldırının Etkisi

Devletler siber saldırılara verilecek karşılığın türünü ve seviyesini belirlerken, siber saldırıların meydana getirdiği etkileri çok iyi değerlendirmelidir. Saldırının etkilerini tespit etmek için; saldırının devletin güvenliğine ve topluma ne kadar zararlı olduğu, ne tür hizmetlerin etkilendiği ve saldırının ülkenin itibarında önemli bir güven kaybına neden olup olmadığı, gibi soruların cevabı aranmalıdır. Bilgisayar uzmanlarının, hedef kurumun bilgisayar ağlarına verilen zararın kapsamını doğru ve kesin olarak tespit etmesi haftalar hatta aylar sürebilir. Örneğin, Suudi yetkililerin Suudi petrol şirketi Aramco'nun otuz bin bilgisayarından verileri silen saldırı zararının kapsamını anlamaları kabaca iki hafta sürmüştür. Bir saldırının fiziksel etkisini değerlendirmek çok kolaydır ancak iş siber saldırılara gelince şirketler veya devlet kuruluşları bazen saldırıdan aylar veya yıllar sonra saldırıya uğradıklarını fark etmektedirler.

Bir siber saldırının etkileri her zaman net olmadığından, devletlerin siber düşmanlığın bir saldırı düzeyinde olup olmadığını ve bir müdahale gerektirip gerektirmediğini belirlemeleri oldukça zordur. Birçok siber saldırı örneği incelendiğinde, bunları saldırı veya casusluk olarak nitelendirmek için bu saldırıların amaçları yetersiz kalmaktadır. Siber bağlamda orantılılığın hesaplanmasındaki zorluk, siber saldırıların hızlı ve gizli doğasından kaynaklanmaktadır. Etkilerin anlaşılması için bilgi edinilmesi de zor olabilir; örneğin, finansal kuruluşlar ve özel şirketler, ticari gizlilik nedeniyle yaşadıkları zararlar hakkında bilgi vermek istemeyebilirler.

4.4.2.3.Verilecek Karşılıkta Kullanılacak Araçlar

Siber saldırılara orantılı bir karşılık vermek konusunda karar vermek gerektiğinde devletin elindeki mevcut seçenekler dikkate alınmalıdır. Her devlet, diplomatik, ekonomik ve askeri olmak üzere bu seçeneklerden birini veya birkaçını birlikte kullanarak karşılık verebilir. Devletler diplomatik bir yaptırımdan askeri bir saldırıya kadar tüm karşılıkları göz önünde bulundurmalıdırlar. Siber düşmanlıkların tamamı doğrudan orantılı bir siber müdahaleyi gerektirmeyecektir. Verilecek karşılık, siber alanla sınırlı olmak zorunda da değildir, çünkü devletin her biri kendi politik risklerini taşıyan başka imkânları kullanmasına hiçbir engel yoktur. ABD Savunma Komisyonu, mümkün olan en büyük siber saldırıya maruz kalması durumunda, ABD'nin nükleer bir karşılığı dışlamaması gerektiğini bile belirtmiştir.²⁵ Buna rağmen kinetik tepkilerin ancak saldırı ölümcül etkilere neden olmak üzere yapılmışsa, insanların yaralanmasına veya ölümüne neden oluyorsa veya insan hakları doğrudan ihlal ediliyorsa izin verilebileceği tartışılmaktadır.²⁶ Ancak şu anda, konvansiyonel anlamda fiziksel zarara neden olmayan bir siber saldırıya kinetik askeri müdahaleyi haklı çıkarmak oldukça zordur.

En önemli konu, devletin elindeki imkânların bir parçası olarak hangi siber veya fiziksel karşı önlemlerin kullanılabileceğine ve her durumda hangi önlemlerin kullanılması gerektiğine karar vermektir. Bu konu, bir devletin milli güç unsurları ve bu unsurları kullanma kararlılığıyla ilgilidir. Siber saldırılara verilecek karşılık, açık veya gizli bir şekilde yapılabilir. Siber yöntemler kullanılırsa, siber casuslukla hedefin kırılganlıklarını tespit ederek önceden hazırlık yapılmadıysa, hızlı şekilde örtülü bir karşılığın geliştirilmesi zor olabilir. Örtülü bir yanıt verildiğinde diğer devletlerin yapılan saldırıdan haberdar olması mümkün olmayacaktır. Açık bir siber karşılık, diğer devletlerin başka hedeflere karşı benzer siber tepkileri başlatma imkânını kaybetmesine ve büyük olasılıkla tekrar bir karşılık verilmesine neden olabilecektir. Eğer verilecek karşılık halk tarafından görülecekse, verilen karşılığın adil olduğuna

²⁵ Department of Defense, **Defense Science Board**, “Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,” January 2013, (çevrimiçi)<http://www.dtic.mil/get-tr-doc/pdf?AD=ADA569975>, 05.09.2019

²⁶ Jarno Limnéll, The cyber arms race is accelerating what are the consequences?, **Journal of Cyber Policy**, s. 50-60,

ilişkin bir öyküsü de olmalıdır. Devletler, bazen verecekleri karşılık için devlet dışı korsan grupları vekil tutabilmektedirler. Ancak bu yöntem izlendiğinde devletlerin saldırıya verilen karşılık üzerindeki kontrolleri sınırlı olacağından krizin tırmanma ve meşruluğunun sorgulanması riski bulunmaktadır.

Müdahale için hangi araçlar kullanılabilir? Siber saldırılara orantılı bir karşılık düşünüldüğünde, karar her zaman devletin elindeki mevcut olan seçeneklerle ilgilidir. Geçmiş uygulamalara bakıldığında her devlet en azından diplomatik, askeri ve ekonomik araçları kullanarak karşılık verebilecektir. Devletler, sessiz bir diplomatik kınamadan askeri saldırıya kadar, ellerindeki bütün karşılıkları göz önünde bulundurmalıdır. Siber saldırıya doğrudan orantılı bir siber tepki vermek gerektiğine ilişkin bir sınırlama yoktur. Yanıtın siber alanla sınırlı olması zorunluluğu yoktur, çünkü her biri kendi politik risklerini taşıyor olsa da, hiçbir şey devletin başka araçlar kullanmasını engelleyemez. Genellikle, saldırı ölümcül etkilere sebep olmuş, insanların yaralanmasına veya ölümüne yol açmışsa veya insan haklarını doğrudan ihlal edilmişse, kinetik tepkilere izin verilebileceği savunulmaktadır. Giderek sayısallaşan toplumlarda, daha önce tartışıldığı gibi, bu yaklaşım oldukça sınırlayıcı kalmaktadır. Bununla birlikte, şu anda, geleneksel anlamda fiziksel zararlara, insanların yaralanmasına veya ölümüne neden olmayan siber bir saldırıya kinetik askeri bir karşılık vermeyi haklı çıkarmak oldukça zordur.

Siber güvenlik, günümüzün güvenlik, savaş ve politikasının ayrılmaz bir parçası haline gelmiştir. Bu nedenle, siber saldırıların ve siber alandaki diğer faaliyetlerin daha geniş politik, stratejik ve jeopolitik bağlamda değerlendirilmesi gerekmektedir. Carl Von Clausewitz'e göre savaş politikanın başka araçlarla devamından başka bir şey değildir. Bu kapsamda devam etmekte olan savaşta, artık siber bileşen de genellikle siyasetin başka yollarla devamı olarak savaşın ayrılmaz bir parçası olmuştur.

Devletler milli güvenliklerini sağlamak için önce milli güvenlik politikasını oluşturmakta ve buna yönelik hedeflerini belirlemektedir. Bu politikanın uygulanması ve hedeflerin elde edilmesi için elde mevcut araçlara uygun olarak stratejiler, harekât ve taktikler geliştirmektedir. Bu faaliyetlerin hepsi önemlidir, ancak güvenlik uzmanları siber güvenikte çoğu zaman teknolojik bakış açısıyla sadece taktik ve araçlara odaklanmaktadır. Günümüzün internet ağıyla birbirine bağlı dünyasında ve

uluslararası politikada siber işlerin artan önemi nedeniyle siber işlere öncelikle politik bakış açısıyla yaklaşmanın daha sonra stratejilere, harekâta, taktik ve araçlara odaklanmanın uygun olacağı değerlendirilmektedir. Örneğin, NATO siber alanı, NATO'nun kendisini havada, karada ve denizde olduğu kadar etkili bir şekilde savunması gereken bir faaliyet alanı olarak kabul etmiştir.²⁷ NATO Genel Sekreteri Stoltenberg İngiltere'de yayımlanan Prospect dergisi için kaleme aldığı makalede *"Ciddi bir siber saldırı NATO için kuruluş anlaşmamızdaki 5'inci maddeyi tetikleyebilir. Bu, bir müttefikimize yönelik saldırının herkese karşı yapılmış sayılmasına yönelik ortak taahhüdümüzdür. Siber dünyayı NATO'nun havada, karada ve denizde olduğu gibi etkin biçimde operasyon yapacağı ve kendisini savunacağı bir alan olarak belirledik. Bu, müttefiklerimize yönelik herhangi bir saldırıyı, ister fiziki ister sanal dünyada olsun, caydıracağımız ve karşısında kendimizi savunacağımız anlamına geliyor."* demiştir.²⁸ NATO Genel Sekreterinin bu beyanı siber saldırılara karşı NATO'nun politik yaklaşımının ne olduğunu ortaya koymuştur.

Birleşik Krallık 2015 Stratejik Savunma ve Güvenlik Gözden Geçirme Belgesi siber saldırıları, terörizm veya uluslararası askeri çatışma ile aynı düzeyde birinci sırada bir tehdit olarak sınıflandırmıştır. Belgede özet olarak; siber uzayda güç şebekelerini ele geçiren bir saldırıya karşılık verilmezse yıkıcı sonuçların ortaya çıkabileceği bu yüzden siber uzayda sadece savunma yapılmayacağı saldırıya uğrandığında aynııyla mukabele edileceğini, ayrıca, saldırgan siber yeteneklere yatırım yapmaya devam edileceği zira tespit etme, izleme ve misilleme yeteneği en iyi caydırıcılık imkânını sağladığı ifade edilmiştir.²⁹

4.4.2.4.Verilecek Karşılık İçin Dikkate Alınması Gerekli Politika Kuralları

Devletlerin, saldırıya vereceği karşılığın nasıl olacağına karar verirken mevcut milli güvenlik ve siber güvenlik stratejilerini göz önünde bulundurmaları gerekmektedir. Devletler belirli dönemlerde milli güvenlik ve siber güvenlik politikalarını

²⁷ NATO, **Warsaw Summit Communiqué**, July 9, 2016, (çevrimiçi) http://www.nato.int/cps/en/natohq/official_texts_133169.htm, 27.08.2019

²⁸ Jens Stoltenberg, *Nato will defend itself*, **Prospect Magazine**, (Çevrimiçi) <https://www.prospectmagazine.co.uk/world/nato-will-defend-itself>, 27.08.2019

²⁹ United Kingdom, **National Cyber Security Strategy 2016 to 2021**, (çevrimiçi) <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>, 09.09.2018

yayımlamaktadır. Son dönemlerde başta Birleşik Krallık olmak üzere birçok ülke siber güvenlik stratejilerinde siber saldırılara karşı aynıyla mukabele edileceğini ve saldırgan siber yeteneklere yatırım yapmaya devam edeceklerini beyan etmişlerdir.

Eğer devlet NATO gibi uluslararası bir ittifaka ve kuruluşa üye ise, orantılı karşılığı oluştururken üye olduğu ittifak ve kuruluşun politik prensiplerini mutlaka dikkate almalıdır. Aksi takdirde, devlet kararlaştırılan ve paylaşılan politikalara uymamakla suçlanabilir. Daha önce de belirtildiği gibi, siber alan, devletlerin yapılan siber bir saldırıya orantılı bir karşılık vermesini gerektiren uluslararası hukuk kuralları dışında değildir.

Son yıllarda yapılan siber saldırıların analizi, devletlerin tepkilerinin büyük ölçüde değiştiğini göstermektedir.³⁰ Bir şeyler yapmak için devletler üzerinde önemli bir siyasi baskı bulunmaktadır ancak politik yanıtların birçoğu geçici karşılıklardır. Bu durum siber saldırılara verilen karşılığın hala aşırı denlenmemiş bir olgu olduğunu, siber alanın özellikle devletler için nispeten yeni bir çatışma alanı olduğunu göstermektedir. Devletler siber düşmanlıklara en iyi şekilde nasıl karşılık verebileceğini ve kullanılması gereken araçları tespit etmek için önceden hazırlıklı olmalıdır.

4.4.2.5. Aşırı Tepki Riski

Bir siber saldırıya karşı devletler aşırı tepki gösterebilirler. Devletler saldırıların tırmanma ihtimalini dikkate alarak verilecek karşılığı oluşturmalı ve karşılık vererek kazanmayı umdukları şeyle neleri tehlikeye attıklarını çok iyi değerlendirmelidir. Bir siber saldırının ardından büyük bir siyasi baskı ortaya çıksa bile, politik sağduyuya ihtiyaç olacaktır. En azından, belirli bir kısıtlama yapılmalıdır. Kendine hâkim olma, özellikle kinetik bir tepki göz önüne alındığında, durumun sakinleşmesini beklemektir. Durumu tırmandırmaktan caydırmak için, rakibin tırmanma sonucunun kendine hâkim olmaktan daha kötü olacağına inanması gerekir ki bu da bazen ulusal gücü tezahür ettirmenin daha güçlü bir yolu olabilir.

³⁰ Sico Van der Meer, "Signaling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors," **Clingendael**, December 2015,(Çevrimiçi)https://www.clingendael.nl/sites/default/files/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf, 29.08.2019

Devletler verilecek her karşılıkla ilgili maliyetleri hesaplamalıdır. Her bir yanıt, devletin diplomatik ilişkileri, itibarı, gücü ve askeri ve istihbarat operasyonları üzerinde etkili olacaktır. Bir karşılık seçilmeden önce ne anlama geleceğinin ve sonuçlarının neler olabileceğinin çok iyi hesaplanması gerekmektedir. Seçenekler değerlendirilirken, ilgili devlet kurumlarının yanı sıra verilecek karşılıktan etkilenebilecek özel sektör şirketleri de bu değerlendirme sürecinin içinde olması günümüz güvenlik anlayışının ve refah toplumunun bir gereğidir.

Devletler uğrayabilecekleri siber saldırılarla ilgili kırmızı çizgiler belirleyebilir ancak bu belirlemeyi yaparken karşı taraf da dikkate alınmalıdır. Devletin siber saldırılarla ilgili kırmızı çizgilerini belirleyip ilan etmesinin faydaları olduğu gibi birtakım sakıncaları da bulunmaktadır. Kırmızı çizgileri belirlemenin hem saldırganlar ve hem devletler açısından sakıncaları vardır. Saldırganlar dokunulmazlık ya da düşük politik risk içerdiğini düşünerek bu kırmızı çizgilerin altında kalan saldırılar yapmaya devam edebilirler. Devletler açısından ise devletler güvenilirliklerini korumak için bu çizgiler geçildiğinde otomatik olarak karşılık vermek zorunda kalabilirler.

Ayrıca devletler saldırılara verilebilecek potansiyel karşılıkların tamamını kamuoyuna açıklamak istememektedir. Öte yandan, kırmızı çizgiler belirlemek, bir devletin rakiplerine karşı caydırıcılık mesajıdır ve bu çizgiler geçilirse rakiplerin karşılık verileceğini bilmelerini sağlar. Devletlerin potansiyel karşılıklar ile ilgili belli bir derecedeki belirsizlik politik olarak en iyi çözüm olarak ortaya çıkabilir. Böylece devlet bazı ayrıntıları kamuoyuyla paylaşmak zorunda kalmayacaktır. Örneğin devletin kırmızı çizgiyi belirleyip bu çizginin aşılması durumunda bir karşılık verileceğini açıklaması, ancak detayları önceden açıklamaması yani verilecek karşılığın kapsamının ne olduğunun belirsiz olması devletin arzu ettiği gizliliği sağlayabilecektir.

4.4.2.6.Verilecek Karşılık için Angajman Kurallarının Belirlenmesi

Küresel güvenlik ortamını ve devletlerle diğer aktörler arasındaki güç dinamiklerini şekillendirmede siber alanın rolü giderek artmakta, aynı zamanda, siber kabiliyetler gittikçe daha fazla gelişmektedir. Günümüzün öngörülemeyen hibrit güvenlik ortamında devletlerin güvenliğini sağlaması, siber konularda daha fazla siyasi

uzmanlık ve hazırlık gerektirmektedir. Yeterince test edilmiş politik temelleri ve net bir yol haritası olmadığından siber alanla ilgili izlenecek politikalar konusunda kararsızlık ve şüphe bulunmaktadır. Devletler, karşılaşılabilecekleri muhtemel siber saldırılara orantılı bir karşılık vermek için öncelikle politik bir bakış açısına ihtiyacı vardır. Siber güvenlik alanında, politik bağlamı anlamadan çok fazla teknik detaylara odaklanmak hatalı sonuçlara neden olacaktır. Sonuçta, siber saldırıların devletin varlığını sona erdirmeye çalışan bir savaş eylemi mi veya sadece zorluk çıkaracak basit bir eylem mi olduğuna ilişkin karar, politik bir karardır. En baştan bu tespit yapılmazsa verilecek karşılık istenen etkiyi yaratmayacaktır.

Devletlerin çoğunun siber saldırılara karşılık verme protokolleri belirsizdir ve bu belirsizlik saldırganlar tarafından güç eksikliği olarak anlaşılmaktadır. Siber saldırılar karşısında pasif kalmanın rakipleri daha saldırgan olmaya teşvik etme ihtimali oldukça yüksektir. Devletler, saldırılara karşı verilecek uygun karşılık seçeneklerini ve karşılık olarak kullanılabilecek kinetik ve kinetik olmayan araçları önceden belirlemelidir. Siber saldırılara karşılık vermek için angajman kuralları geliştirmek, karar vericilere olası sonuçları önceden belirlenmiş seçenekleri hızlı bir şekilde değerlendirme imkânı sağlayacaktır. Angajman kuralları devletlere, atfetme düzeyini ve saldırının ciddiyetini anlamaktan, verilecek orantılı karşılığa ve belirli eylem planlarını uygulamanın risklerini tespit etmeye kadar alacağı bir dizi karmaşık karara hazır olma imkânı sağlayacaktır. Önceden uygun karşılığın belirlenmesi devletin istemeden siyasi, ekonomik, istihbari ve askeri çıkarlarını tehlikeye atabilecek hatalar yapmasını engelleyecektir. Verilecek her karşılık her duruma göre değişecek olsa da, tespit edilecek angajman kuralları karar vericilerin seçenekleri hızlı bir şekilde değerlendirmelerini sağlayacaktır.

Atfın derecesi, saldırının etkileri, politika seçenekleri, riskler, güvenlik stratejileri, uluslararası hukuk, ivedilik ve orantılılık birleştirilerek, gerginlik seviyesine ve siber saldırıların ciddiyetine karşılık olarak uygulanması gereken farklı angajman kuralları tespit edilebilir. Angajman kuralları tespit etmenin amacı devletin, hiçbir şey yapmama kararı da dâhil olmak üzere siber bir saldırıya karşı verilecek karşılığa karar verirken, karar vericilerin dikkate alması gereken hususların göz ardı etmesine engel olmaktır. Angajman kurallarını tespit ederken dikkat edilmesi gereken husus siber

saldırı ne kadar şiddetli olursa, verilecek karşılığın da o kadar şiddetli olması gerektiğidir. Siber saldırılar sonucunda bir web sitesinin bozulması gibi çok düşük bir zarar meydana gelebileceği gibi yaşam kaybına sebep olacak çok ciddi sonuçlar da ortaya çıkabilir. Verilecek karşılık, diplomatik bir uyarıdan askeri müdahaleye kadar basitten karmaşığa doğru derecelendirilmelidir. Verilecek karşılığın kamuoyuna açıklanıp açıklanmayacağı beklenen fayda dikkate alınarak belirlenmelidir. Verilecek karşılık sonrasında çatışmanın tırmanma riski mutlaka değerlendirilmelidir.

Angajman kuralları aynı zamanda politik bir karşılık çerçevesi de oluşturmalıdır. Ancak böyle bir çerçeve oluşturulmuş olsa bile, doğru kullanılacağı anlamına gelmeyecektir. Çünkü siber alanı kullanmaya yönelik yeni yöntemler sürekli gelişmektedir. O yüzden politik karşılıklar durumun belirsizliğine bağlı olarak esnek olmalıdır. Her devletin kendine özgü kültürel, politik ve askeri özelliklere sahip olması nedeniyle, tüm devletlerin kendi politik karşılık çerçevesini geliştirmeleri gerekecektir.

4.5. İVEDİLİK VE YAKINLIK

Bir devletin meşru müdafaa kapsamında güç kullanabilmesi için, o devletin silahlı saldırı seviyesine ulaşmış olan siber saldırı da dâhil olmak üzere silahlı bir saldırıya maruz kalmış olması ya da çok yakında maruz kalacak olması durumunda ve bu saldırıyı defetmek için ivedi bir karşılık vermesi gerekmektedir.³¹

Birleşmiş Milletler Anlaşması'nın 51. maddesi silahlı bir saldırının gerçekleşmiş olduğu durumu ifade etmektedir. Bu durum, silahlı saldırının etkilerinin ortaya çıktığı, yani siber silahlı saldırının neden olduğu hasar ya da yaralanma olaylarını kapsamaktadır. Ayrıca siber saldırının silahlı saldırı başlatılmasında ilk adım olduğu durumları da kapsamaktadır. Örneğin bir hava harekâtı yapmadan önce siber saldırılarla ilgili devletin hava savunmasını etkisiz hale getirmek Birleşmiş Milletler Anlaşması'nın 51. Maddesi kapsamında değerlendirilecektir.

³¹ Terry D. Gill , “The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy”, **International Law And Armed Conflict: Exploring The Faultlines**, Martinus Nijhoff, Boston 2007, s.113-120

4.5.1.Yakınlık

Yakınlık, silahlı saldırının gerçekleşebileceği düşüncesiyle meşru müdafaa hakkının kullanılabilmesini ifade eden önleyici meşru müdafaa kavramı ile ilgili bir kriterdir. Birleşmiş Milletler Anlaşması'nın 51. maddesi silahlı saldırının gerçekleşebileceği düşüncesiyle meşru müdafaa hakkının kullanılabilmesini açıkça ifade etmese de düşman saldırıya hazırlanırken devletin boşta beklemesinin de uygun olmayacağı yönünde görüşler bulunmaktadır. Aksine, yakın bir silahlı saldırıya karşı devletin meşru müdafaa hakkının doğacağı ağırlıklı bir görüş olarak ortaya çıkmaktadır. Bu görüş, önleyici meşru müdafaa kavramını ortaya çıkarmıştır. ABD, 2003 yılında Irak'a düzenlediği saldırıyı meşru hale getirmek için bu müdahalenin önleyici meşru müdafaa kapsamında yapıldığını ileri sürmüştür.³² Bu kavram uluslararası hukuk çevrelerinde çokça tartışılmış ve bu hakkın güçlü devletler tarafından kötüye kullanılmaya elverişli olduğu sonucuna varılmıştır.

Tezin önceki sayfalarında değinildiği gibi Birleşmiş Milletler Anlaşması'nın 51. Maddesini dar yorumlayan bazı hukukçulara göre meşru müdafaa sadece bir saldırı başladığında izin verilebilir; önleyici meşru müdafaa hukuka aykırıdır. Bu yaklaşımın farklı bir biçimi, hedefine ulaşmamış yeni başlayan bir saldırı karşısında, meşru müdafaa eylemine izin verilebileceğini ileri sürmektedir. Ancak siber alanın kendine has özellikleri ve siber saldırıların hızı böyle bir değerlendirmeyi imkânsız kılmaktadır.

Birleşmiş Milletler Anlaşması'nın 51. Maddesini geniş yorumlayan ve önleyici meşru müdafaa hakkının olduğunu savunanlar arasında da birtakım görüş farklılıkları bulunmaktadır. Önleyici meşru müdafaa hakkını savunanlar bu hakkın doğması için silahlı saldırının başlatılmak üzere olmasının gerektiğini ifade etmektedirler. Önleyici meşru müdafaa hakkını savunanlar saldırıya uğrayan devletin etkin şekilde kendini savunma imkânını kaybetmeyecek bir zamanda bu hakkı kullanması gerektiğini ileri sürmektedirler. Bu kapsamda saldırıya uğrayan devletin önleyici meşru müdafaa

³² Terry D. Gill , a.g.e., s.142-147

hakkını etkin şekilde kullanabilmesi imkânı son fırsat penceresi standardı olarak adlandırılmıştır.

Bu standart uyarınca, saldırgan açıkça silahlı saldırı başlatmaya karar verdiğinde devlet ister siber ister kinetik olsun silahlı bir saldırıya karşı önleyici meşru müdafaa eylemi yapabilir aksi takdirde saldırıya uğrayan devlet etkin bir şekilde kendini savunma hakkını kaybedecektir. Başka bir deyişle, devlet yaklaşmakta olan silahlı bir saldırıya karşı kendisini savunmak için yalnızca son fırsat olarak önleyici bir eylemde bulunabilir. Bu son fırsat, söz konusu saldırıdan hemen önce veya bazı durumlarda gerçekleşmeden çok önce kendini gösterebilmektedir.³³

Burada dikkat edilmesi gereken meşru savunma eyleminin muhtemel silahlı saldırıya zamansal yakınlığı değil devletin, saldırgan devlete karşı kendisini etkili bir şekilde savunma imkânını yitirmeyecek bir zamanda meşru savunma eylemini yapmış olmasıdır.

Örneğin X devletinin istihbarat servisi, Y devletinin önümüzdeki bir hafta içinde X devletinin uluslararası bir havaalanındaki hava trafik kontrol sistemine zarar vermek için bir siber saldırı başlatmaya hazırlandığına ilişkin kesin bir bilgi aldığını varsayalım. Siber saldırı, X devletinin havaalanındaki hava trafiğini kontrol eden bilgisayar sistemlerini bozarak havadaki uçakların yanlış yönlendirilmesine havadaki ve yerdeki uçakların zarar görmesine ve insanların ölmesine ve yaralanmasına neden olacak sonuçta bir dizi karışıklık meydana gelecek şekilde planlanmış olsun. X Devletinin istihbarat servisi, saldırının gerçekleştirilmesinde yer alan kişilerin belirli bir yerde ve zamanda toplanacağı bilgisine sahip olsun. Diğer tedbirlerin yetersiz kalması durumunda X devleti, etkili bir meşru müdafaa imkânını yitirmenin an meselesi olduğu ve saldırı hazırlığı yapan bireylere yönelik saldırının, orantılı olacağı sonucuna varırsa önleyici meşru müdafaa hukuka uygun olacaktır.

Bu gibi vakaları değerlendirirken, hazırlık eylemleri ile bir saldırının ilk aşamasını oluşturan eylemler arasında bir ayrım yapılmalıdır. Saldırganların çok kritik bir bilgisayar sistemini ele geçirmiş olduğu durumu ele alalım. Eğer saldırgan

³³ Micheal N. Schmitt, **Talinn Manual on The International Law Applicable to Cyber Warfare**, Cambridge University Press, 2013, s.61

bilgisayar sistemine girerek sadece gelecekte bu bilgisayarları botnet olarak kullanarak silahlı bir saldırı başlatma kabiliyeti kazanmak istiyorsa, yakınlık kriteri karşılanmayacaktır. Bununla birlikte, eğer saldırgan ele geçirdiği bilgisayarları botnet olarak kullanarak silahlı bir saldırı gerçekleştirmeye karar verdiğyse, saldırıya uğrayan devletin etkili bir şekilde kendini savunma hakkını kaybetme ihtimaline karşı hareket geçmesi gerekecektir. Bu durumda silahlı saldırı yakın hale gelecektir. Uygulamada bu ayrımı yapmak şüphesiz çok zor olacaktır. Herhangi bir savunma müdahalesinin hukukiliği, saldırıya uğrayan devletin durum değerlendirmesinin makul olup olmadığına göre belirlenecektir.

Silahlı bir saldırı gerçekleştirme niyeti veya aracı bulunmayan muhtemel bir saldırıya karşı yapılan önleyici saldırılar, hukuksal olarak önleyici meşru müdafaa olarak nitelendirilmeyecektir. Ayrıca düşman bir devletin siber saldırı yapabilme kapasitesinin bulunması tek başına potansiyel olarak saldırıya uğrayabilecek devlete kuvvet kullanarak meşru müdafaa yapma hakkı vermeyecektir. Saldırıya uğraması muhtemel devlet ilk önce, düşman devletin fiili bir saldırı kararına vardığı sonucuna ulaşmak zorundadır. Bu sonuca varıncaya dek, saldırıya uğraması muhtemel olan devletin vereceği karşılık, kuvvet kullanmayı gerektirmeyen tedbirlerle veya konunun Birleşmiş Milletler Güvenlik Konseyi önüne getirilmesiyle sınırlı olacaktır. Bir devletin başka bir devlete karşı silahlı saldırı yapma niyeti ve fırsatı olsa bile, saldırıya uğraması muhtemel olan devletin meşru müdafaa hakkı kapsamında güç kullanması, saldırgan devlet harekete geçtiğinde saldırıya uğrayan devletin etkin savunma imkânını yitireceği anda başlayacaktır.

4.5.2.İvedilik

İvedilik, yakınlıktan farklı olarak, meşru müdafaa eylemini misilleme eyleminden ayırmaktadır. İvedilik, saldırıya uğrayan devletin meşru müdafaa sırasında makul bir şekilde tepki verebileceği silahlı saldırıların gerçekleştirilmesini takip eden dönemi ifade etmektedir.³⁴ Saldırı ve müdahale arasındaki zamansal yakınlık, saldırganı tanımlamak için gereken süre ve karşılık vermek için gereken süre gibi faktörler

³⁴ Terry D. Gill , **a.g.e.**, s.151-154

ivedilik kriterinin karşılanıp karşılanmadığının değerlendirilmesinde dikkate alınmaktadır.

ABD ile İngiltere arasında Caroline olayı nedeniyle ortaya çıkan uyuşmazlık taraflarca hakeme götürülmüş ve hakem kararı meşru müdafaa'nın kullanılabilmesi için belirli şartların gerçekleşmiş olmasının gerektiğine karar vermiştir. Caroline olayı³⁵, 1837'de Kanada'nın İngiltere'ye karşı verdiği bağımsızlık savaşı sırasında çıkmıştır. Savaş sırasında Kanadalılar ihtiyaç hissettikçe yakındaki ABD eyaletlerine sığınmakta ve onlardan yardım almaktaydı. ABD Hükümeti tarafsızlık politikası izliyordu. Kanadalılar, Kanada'daki Navy adasından İngiliz gemilerine saldırıyor ve ihtiyaç duydukları silah yardımını Caroline adlı bir Amerikan bandıralı gemi vasıtasıyla temin ediyorlardı. İngilizler Caroline adlı gemiyi bir Amerikan limanında ele geçirmiş, ders olsun diye de Niagara Şelalesinden aşağı atmıştır. Bu olayda bazı ABD vatandaşları yaşamını yitirmiş, bunun üzerine sorumlu görülen bir İngiliz tutuklanmıştır. Olay sonrasında İngiliz Dışişleri Bakanı, İngiltere'nin meşru müdafaa ve kendini koruma hakkına dayanarak bu eylemi gerçekleştirdiğini ifade etmiştir. Bu olayda İngiltere, gemiyi yok ederken meşru müdafaa hakkı çerçevesinde hareket ettiğini ileri sürmüştür. İngiltere'ye göre Caroline korsan bir gemiydi ve ABD kendi sınır hattında kendi yasasını uygulayamadığına göre İngiltere meşru savunma için gerekli önlemleri almıştı. ABD, İngiltere'nin bu görüşünü reddetmiş ve sorun hakemliğe götürülmüştür. Hakemlik kararına göre meşru müdafaa hakkının kullanılması için **tehlikenin o an ortaya çıkmış, ani, karşı konulmaz ve başka hiç bir korunma yoluna başvurmaya imkân bırakmayacak nitelikte** olması gerektiği belirtilmiş ve bu olayda İngiltere'nin meşru müdafaa boyutlarını aştığı ortaya çıkmıştır.³⁶

İvedilik kriteri açısından en önemli sorun meşru müdafaa hakkının temelini oluşturan bir olayın tamamlanmasının ardından meşru müdafaa hakkının hangi süre içinde kullanılacağına nasıl saptanacağıdır. Örneğin, bir devlete karşı çok kademeli siber saldırılar planlanmış ve ilk aşamasında devletin kritik siber altyapılarından bir

³⁵ Michael Wood, **The Use of Force in International Law: A Case-Based Approach**, Oxford Public International Law, s.15 (çevrimiçi) <https://opil.ouplaw.com/view/10.1093/law/9780198784357.001.0001/law-9780198784357-chapter-2>, 02.09.2019

³⁶ Maria Benvenuta Occelli, "Sinking" the Caroline: Why the Caroline Doctrine's Restrictions on Self-Defense Should Not Be Regarded as Customary International Law", **San Diego International Law Journal**, Volume 4, 2003, s.468-490

kısmına silahlı saldırı seviyesine ulaşan siber saldırılar başlatılmış olabilir. Meşru müdafaa durumu bu ilk dalga siber saldırıların sona ermesiyle ortadan kalkmayacaktır. Daha fazla siber saldırının takip edebileceği sonucuna varılması makul ise, saldırıya uğrayan devlet bu saldırılara bir siber savaş olarak bakabilir ve kendini savunmaya devam edebilir. Bununla birlikte, böyle bir sonuç makul değilse, kinetik veya siber olsun, başka herhangi bir güç kullanımı, misilleme olarak nitelendirilebilir. Son tahlilde, ivedilik gerekliliği, o zamanki geçerli olan koşullar ışığında bir makullük testini içermektedir.

Bazı durumlarda, bir siber saldırı gerçekleştiği veya gerçekleşmekte olduğu gerçeği bir süre için belirgin olmayabilir. Saldırı sonucunda ortaya çıkan hasar veya yaralanmanın sebebi veya saldırının başlatıcısı saldırının sonuna kadar tespit edilememiş olabilir. Her iki duruma verilecek klasik örnek Stuxnet gibi bir solucanın kullanılmasıdır. Bu gibi durumlarda, o zamanki geçerli olan koşullar ışığında bir makullük testini geçerli olmadıkça, ivedilik kriteri karşılanmayacaktır.

Yukarıda bahsedilen bütün kriterler, geçmiş ve mevcut uygulamalar dikkate alındığında siber bir saldırıya karşı verilebilecek karşılıkların aşağıdaki gibi olabileceği değerlendirilmektedir.

- a) Pasif caydırıcılık: doğrudan hiçbir şey yapmamak.
- b) Diplomatik Protestolar: Neredeyse hiç yükselme riski olmayan büyük ölçüde sembolik bir tepki.
- c) Yasal Tedbirler: şirketlere ve bireylere karşı yasal işlem.
- ç) Ekonomik yaptırımlar
- d) Siber alanda misilleme: misilleme yapmak, gelecekteki siber saldırılara tolerans gösterilmeyeceğini gösterecektir.
- e) Siber alanda örtülü misilleme.
- f) Askeri misilleme: Bu tür bir eylem muhtemelen karşı askeri müdahaleyi tetikler ve tehlikeli bir tırmanma süreciyle sonuçlanabilir.

Mevcut jus ad bellum(haklı savaş) paradigması içinde siber savaşı tanımlamaya yönelik mevcut girişimler, siber saldırılardan yeterli koruma sağlamamaktadır. Siber

savaşın doğasında var olan teknoloji, saldırıyı belirli bir kaynağa atfetmeyi veya bunun arkasındaki amacı tanımlamayı neredeyse imkânsız hale getirmektedir. Ayrıca, siber savaş eylemleri neredeyse eş zamanlı gerçekleşmektedir. Saldırganın kimliğinin ve amacının belirlenmesini gerektiren mevcut hukuk sistemi, dijital çağın bu tür özelliklerini hesaba katmamaktadır. Bu nedenle mevcut uluslararası paradigma, devletlerin kullanabileceği seçenekleri sınırlandırmakta ve uluslararası hukuku ihlal etmeden etkili bir şekilde karşılık vermeyi zorlaştırmaktadır. Bir devletin karşılık verme hakkını kısıtlamak, devletleri, terör örgütlerini ve bireyleri giderek daha şiddetli siber saldırılar yapmaya teşvik edecektir.

Birleşmiş Milletler Anlaşmasının 2. Maddesi 4. fıkrası uyarınca siber savaş analizi etmeye yönelik sonuç temelli yaklaşımlarda ciddi kusurlar bulunmaktadır. Sonuç temelli yaklaşımı; meşruiyet karinesini bir faktör olarak kullanarak, saldırının meşru olup olmadığını sorgulayarak uluslararası hukukta bir saldırının meşruiyetini belirlemeyi gerektirir. Aslında, yaklaşım gerçekleşmiş bir saldırıyı analiz etmek için geriye doğru işlemektedir. Ayrıca, diğer savaş türlerinden farklı olarak, siber saldırının büyüklüğünü ve meşru olarak verilebilecek karşılığı saldırı anında kolayca tespit etmek mümkün değildir. Bu sorun, yukarıda belirtilen sonuç odaklı yaklaşım da dâhil olmak üzere saldırının meydana gelmesinden sonra analiz yapmayı gerektiren bir çerçeveye ortaya çıkmaktadır.

Siber savaşın kendine özgü doğası nedeniyle uluslararası hukuk, siber bir saldırıya iyi niyetle karşılık veren devletler için koruma sağlamalı, saldırıyı atfetmeden ve tanımlamadan, önce saldırıya uğrayan siber meşru müdafaa yapabilmelidir. Devletin hayatta kalması derhal, güçlü ve saldırgan bir karşılık vermeye bağlı olabileceğinden, devlet hayati çıkarlarını korumak için meşru müdafaa hakkını kullanırken uyması gereken uluslararası hukuk kuralları daha esnek yorumlanmalıdır. Uluslararası hukuk, bir devletin siber saldırıya karşılık olarak, özellikle de saldırının kritik ulusal altyapısını hedef alması durumunda, önleyici meşru müdafaa dâhil meşru müdafaa hakkını sağlamaya yönelik olarak geliştirilmelidir.

Bir devletin, kritik ulusal altyapısına yapılacak siber bir saldırıya karşılık olarak herhangi bir sorumluluk yüklenmeden aktif savunma önlemleri almasına imkân vermek mevcut jus ad bellum paradigması altında siber savaşla mücadelede tercih

edilen bir yönetim prensibidir. Bu istisnayı, güç kullanımını düzenleyen olağan kurala uygulamak için, uluslararası toplum, bir devletin aktif savunma önlemleriyle koruyabileceği kritik bir ulusal altyapı listesi yapıp bu listeyi yayınlamalıdır. Son dönemde devletler siber güvenlik strateji belgelerinde ulusal kritik altyapı envanterini oluşturma gayreti içindedir. Listede tanımlanan kritik altyapı bir siber saldırıya maruz kaldıysa, devlet ilk önce saldırıyı teamül hukukunda istenen kesinlik seviyesinde bir devlete atfetmeden veya saldırıyı nitelendirmeden iyi niyetli bir şekilde meşru müdafaa hakkını kullanarak saldırıya karşılık verebilir. Böyle bir istisna, jus ad bellum çerçevesini kökten değiştirmeyecek, bunun yerine, devletin, meşru müdafaa hakkını, yeni bir tehdide yanıt olarak kullanmasına izin verecektir.

Birleşmiş Milletler Anlaşması, internet mevcut olmadan önce yazılmıştır. Bu nedenle, siber saldırı, geleneksel kuvvet kullanma tanımıyla nitelenemeyecek kadar karmaşıktır. Bu zorluğa rağmen, tehdidin ciddiyeti ve yaygınlığı, uluslararası toplumun hem jus ad bellum paradigması içindeki siber savaşın anlamı hem de siber saldırıya maruz kalan devletler için mevcut seçenekler konusunda fikir birliğine varmasını zorunlu kılmaktadır. Devletlerin siber saldırılara karşı güç kullanımını düzenleyen uluslararası hukukun eski yorumlarıyla sınırlanmamış meşru müdafaa hakkını kullanarak karşılık verme imkânı olmadıkça, uluslararası barışı tehdit eden ciddi tehditler ortaya çıkacaktır.

4.7. Estonya Saldırısının Gereklilik, Orantılılık, Yakınlık ve İvedilik Kriterlerine Göre İncelenmesi

Estonya saldırısı, altyapı boyutu ve saldırıların kapsamı göz önüne alındığında, dünya üzerindeki egemen bir devlete karşı en önemli koordine edilmiş siber saldırılardan birisi olarak bilinmektedir. Saldırganlar yenilmiş olmasına rağmen, internet bankacılığının kullanılamaması veya iletişim güçlükleri gibi Estonya halkını etkileyen bazı ani etkiler olmuştur. Banka işlemlerinin % 98'inin çevrimiçi yapıldığı ve vatandaşların çoğunluğunun vergi formlarını çevrimiçi doldurduğu bir ülkede, bu tür uzun süren olayların yaratacağı etki oldukça yıkıcı olabilmektedir.

Bu saldırılar uluslararası barış ve güvenliği potansiyel olarak tehdit ve BM Anlaşmasını ihlal etmiştir. Estonya'ya yapılan siber saldırılar Wingfield Analizi ile

değerlendirilmiş ve siber saldırıların güç kullanma seviyesine ulaşmadığı sonucuna varılmıştır. Bu nedenle Estonya devleti için meşru müdafaa hakkı doğmamıştır. Bu durum verilecek karşılığın askeri güçten başka bir araç olmasını gerektirmektedir. Bunlar meşru müdafaa yöntemleri değil verilebilecek diğer karşılıklardır. Bu karşılıkların bir dava, bir tutuklama, diplomatik bir taarruz veya gizli bir operasyon şeklinde olması mağdur devletin seçimi olacaktır. Ancak saldırıların silahlı saldırı seviyesine ulaştığı ve bir devlete atfedildiği varsayılarak gereklilik, orantılılık, yakınlık ve ivedilik kriterleri açısından incelenecektir.

Varsayımlar; saldırıların silahlı siber saldırı seviyesine ulaştığı ve Rusya'ya atfedildiği farz ve kabul edilmiştir.

Gereklilik; silahlı bir güç kullanımına varan siber saldırıları da kapsayan yaklaşmakta olan bir saldırıyı başarılı bir şekilde defetmek veya devam etmekte olan bir saldırıyı başarılı bir şekilde boşa çıkarmak için güç kullanımını gerektirmektedir. Estonya saldırısı saldırı başladıktan sonra yaklaşık bir hafta devam etmiştir, bu nedenle saldırıyı boşa çıkarmak için güç kullanımı gerektiğinden gereklilik kriteri karşılanmıştır.

Orantılılık; Estonya Devleti, Rusya'ya karşı önce açık veya örtülü siber misilleme yapmalı ancak Rusya siber saldırılara karşı göreceli olarak dayanıklı olduğundan meşru müdafaa'nın amacıyla orantılı olarak fiziki bir karşılık verebilir.

Yakınlık; Estonya, Rusya'nın açıkça silahlı siber saldırı başlatmaya karar verdiğini tespit eder etmez etkin bir şekilde kendini savunma hakkını kaybetmeyecek şekilde ister siber, ister kinetik olsun önleyici meşru müdafaa eylemi yapabilmeli. Ancak Estonya'nın böyle bir tespiti olmamıştır. Bu nedenle bu kriterin incelenmesi gerekli değildir.

İvedilik; kamu hizmetleri sekteye uğramış olan Estonya Devleti'nin bu hizmetleri etkin şekilde devam ettirmek için ivedi şekilde Rus saldırılarını durdurması gerekmektedir.

Sonuç olarak silahlı bir saldırı seviyesine ulaşmayan ancak meşru müdafaa kapsamında verilecek karşılıkla ilgili gereklilik, orantılılık ve ivedilik kriterleri açısından inceleyebilmek için silahlı saldırı seviyesine ulaştığı ve Rusya'ya

atfedildiği varsayımı altında Estonya'nın Rusya'ya meşru müdafaa kapsamında ivedilikle önce açık veya örtülü siber misilleme yapmasının yeterli olmadığı takdirde kinetik bir karşılık vermesinin orantılı olacağı sonucuna varabiliriz.

4.6. STUXNET Saldırısının Gereklilik, Orantılılık, Yakınlık ve İvedilik Kriterlerine Göre İncelenmesi

2009 yılında İran'ın Natanz nükleer yakıt zenginleştirme tesislerine yapılan ve kullanılan virüsün adıyla 'Stuxnet saldırısı' anılan bu saldırının ABD tarafından yapıldığına ilişkin yaygın bir kanaat vardır. ABD, bu saldırıyla ilgili olarak saldırıyla bir ilgisinin olduğuna veya olmadığına ilişkin resmi bir açıklama yapmamıştır.

Saldırı ve böyle bir virüsün varlığı hakkında kapsamlı bilgiye saldırıdan yaklaşık bir sene sonra ulaşılabilmiştir. Ukrayna bilişim şirketi Virusblokada, Mayıs 2010'da Microsoft Windows işletim sistemlerinde zararlı etki gösterme olasılığı bulunan bir virüs programı keşfetmiştir. Virusblokada, virüs programının o güne kadar rastlanılan tüm zararlı yazılımlardan daha karmaşık bir yapıya sahip olduğunu tespit etmiştir. Bunun üzerine yazılım şirketi Microsoft ile İsrail anti virüs program yazılım şirketi Kaspersky birlikte virüsün kaynağını bulmak üzere ortak bir araştırma başlatmıştır. Araştırmaya daha sonra Amerikan bilişim güvenlik şirketi Symantec de dâhil olmuştur.

Bulgulara göre Stuxnet saldırısı iki ayrı tarihte gerçekleştirilmiştir. İlk saldırı 22 Haziran 2009 tarihinde saat 16.30'da, ikinci saldırı ise 07 Temmuz 2009 tarihinde 17.00'de meydana gelmiştir. Saldırının hedefi 'Simatic WinCC Step7' isimli denetleme kontrol ve veri toplama sistemidir. SCADA (Supervisory Control and Data Acquisition) diye adlandırılan kontrol ve bilgi toplama sistemi elektrik üretim ve dağıtımının kontrolü ile su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesinde kullanılmaktadır.³⁷

Varsayımlar: Saldırının silahlı siber saldırı seviyesine ulaştığı ve ABD'ye atfedilmiş olduğu farz ve kabul edilmiştir.

³⁷ Stamatis Karnouskos, Stuxnet Worm Impact on Industrial Cyber-Physical System Security, **IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society**, (çevrimiçi) <https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/> , 08.04.2019

Gereklilik; silahlı bir güç kullanımına varan siber saldırıları da kapsayan yaklařmakta olan bir saldırıyı başarılı bir řekilde defetmek veya devam etmekte olan bir saldırıyı başarılı bir řekilde bořa çıkarmak için güç kullanımını gerektirmektedir. Stuxnet saldırısı yapıldıktan bir yıl sonra tespit edildiğinden bu kriteri karşılaması mümkün değildir.

Orantılılık; eğer saldırı zamanında fark edilmiş olsaydı saldırıyı uzaklařtırmak veya saldırıyı yenmek için İran'ın açık veya örtülü siber misilleme yapma veya askeri bir karşılık vermesi orantılı olabilirdi. Ancak verilebilecek karşılıkların bu saldırıyı uzaklařtırma imkânı olmadığı düşünölmektedir. Çünkü virüs harekete geçtikten sonra saldırıyı yapan devletin de kontrolünden çıktığı değerlendirilmektedir. Verilecek karşılık benzer saldırıların tekrarlanmaması için bir caydırıcılık sağlayabilir.

Yakınlık; önleyici meşru müdafaa ile ilgili bir kriterdir. İran'ın önleyici meşru müdafaa kapsamında karşılık verebilmesi için ABD'nin böyle bir saldırı yapmaya karar verdiğıne ilişkin sonuca ulaşmış olması gerekmektedir. Ancak İran'ın bırakın saldırı kararına ilişkin bilgiye sahip olmasını saldırının yapıldığından bile haberi olmamıştır. **Bu nedenle vakada yakınlık kriterinin incelenmesi gerekli değildir.**

İvedilik; saldırıya uğrayan devletin meşru müdafaa sırasında makul bir řekilde tepki verebileceğı silahlı saldırıların gerçekleştirilmesini takip eden dönemi ifade etmektedir. Saldırı ve müdahale arasındaki zamansal yakınlık, saldırıyı tanımlamak için gereken süre ve karşılık vermek için gereken süre gibi faktörler ivedilik kriterinin karşılanıp karşılanmadığının değerlendirilmesinde dikkate alınmaktadır. Stuxnet saldırısı için ivedilik kriteri de karşılanmamıştır.

Sonuç olarak meşru müdafaa kapsamında verilecek karşılıkla ilgili gereklilik ve ivedilik kriterleri karşılanmadığından orantılı da olsa saldırıya meşru müdafaa kapsamında bir karşılık vermek mümkün değildir.

SONUÇ

İnsan var olduğundan bugüne barutun icadından nükleer silahların kullanımına kadar meydana gelen gelişmeler kara, deniz, hava ve uzay alanlarıyla ilgili olmuştur. Ancak siber alan bu alanlardan çok farklı, insan yapımı ve suni bir alandır. Suniliği, siber alanı ve onun politikayla olan ilişkisini tanımlamakta soruna neden olmaktadır. Teknik düzeyde, siber alan, bir ağ, sosyal medya, iletişim kanalı ve bilgi deposu gibi yeni teknolojik gelişmeler için bir platformdur. Siber alanın özellikleri kara, deniz, hava ve uzay alanlarına özgü kriterlerle açıklanamayacak kadar karmaşıktır. Ayrıca siber alanda kullanılan araçlar diğer alanlardan çok farklıdır.

İnsanların davranışlarını düzenleyen bir takım kurallar olduğu gibi devlet davranışlarını düzenleyen kurallar da bulunmaktadır. Bu kurallara norm adı verilmektedir. Normatif uluslararası teori uluslar üstü alandaki aktör davranışlarını ve mevcut sistemin normlara uygun olarak düzenlenmesini öngörmektedir. Uluslararası ilişkiler mevcut normlar esas alınarak yürütülmekte, devletler uluslararası alandaki davranışlarını mevcut uluslararası normlara göre belirlemektedir. Norm teorisine göre uluslararası bir normun varlığı herkesin davranışını etkiler ve cesaret kırıcıdır veya norm tarafından teşvik edilen davranışlarda bulunmayı artırır. Mevcut uluslararası düzeni ve devlet davranışlarını belirleyen en önemli norm Birleşmiş Milletler Anlaşması'dır. Bu norma Birleşmiş Milletler teşkilatına üye olsun veya olmasın bütün devletler uymak zorundadır. Ayrıca yüzyıllar içinde değişip gelişerek oluşmuş teamül kuralları bulunmaktadır. Bu teamüller kara, deniz, hava ve uzay alanlarına ilişkindir. Siber alan yeni ortaya çıkan diğer alanlardan çok farklı bir alan olduğundan mevcut normların bu alana uygulanması sorunlara neden olmakta, mevcut ve gelecekte ortaya çıkması muhtemel sorunlara çözüm sağlamayacağı değerlendirilmektedir.

Siber alanla ilgili ortaya çıkan ve çıkabilecek sorunlara nasıl bir çözüm getirileceğine ilişkin iki yaklaşım bulunmaktadır. ABD'nin başı çektiği birinci yaklaşım mevcut hukuk kurallarının siber alana uyarlanmasını savunurken Rusya'nın desteklediği ikinci yaklaşım ise siber silahların yasaklanmasını içeren uluslararası bir anlaşmanın yapılması gerektiği yönündedir. Siber silahların yasaklanmasına ilişkin yaklaşıma, amacının ABD'nin siber üstünlüğünü bastırmak olduğu, teklif edilen antlaşmanın uygulanamaz olduğu, pratik olmadığı, sivil özgürlükleri ve ifade

özgürlüğünü ihlal ettiğine yönelik endişelerinden dolayı ABD tarafında itiraz edilmektedir. Bu nedenle siber silahların kullanımının yasaklayan bir anlaşmanın yapılması, pek olası görünmemekte, yapılsa bile belli bir devletin kabulünü gerektirdiğinden uygulanmaya başlamasının uzun süre alacağı düşünülmektedir.

Bütün bunların yanında bu yeni siber alanla ilgili normlar da henüz tam olarak ortaya çıkmamıştır. Siber savaşı düzenleyen çok az normatif kısıtlama olmasına rağmen siber savaş üzerine çekilen dikkat ve tartışmaların, siber savaş için çeşitli normlar üzerinde uzlaşmaya varmaya ve ortaya çıkan normları kodlamaya yardımcı olacağı düşünülmektedir. Norm evrim teorisi, normların ortaya çıkmasının özellikle örgütsel platformlara sahip norm girişimcilerinin ve liderlerinin kilit aktör olarak varlığı halinde daha muhtemel olduğunu belirtmektedir. Şu anda BM ve NATO, siber savaş için ortaya çıkmakta olan normları teşvik etmek için kullanılan iki temel uluslararası organizasyondur. Birleşmiş Milletler 'deki çalışma grupları, esas olarak Rusya önderliğinde, NATO'daki çalışma grupları ise ABD önderliğinde yürütülmektedir. NATO'nun bu çalışmadaki en önemli faaliyeti, Siber Savaşa Uygulanacak Uluslararası Hukukla ilgili Tallinn El Kitabının geliştirilmesi olmuştur. Tallinn El Kitabı, uluslararası çatışma hukukunun siber savaş için yeterli ve uygulanabilir olduğu görüşünü ortaya çıkarmakta ve siber savaşın yeni ve farklı uluslararası normlar ve anlaşmalar gerektirdiği yönündeki Rusya'nın tutumunu reddetmektedir.

Siber alanla ilgili normlar yaygınlaşıp içselleştirilinceye kadar bu ortamda yapılabilecek en iyi şeyin Talinn Belgesi ve Wingfield Analizi gibi yöntemlerden istifade ederek mevcut Silahlı Çatışma Hukuku kurallarını siber alana uygulamak olduğu değerlendirilmektedir. Ancak şimdiye kadar meydana gelen siber saldırılarla ilgili olarak Silahlı Çatışma Hukuku uygulamaları bir tespitten öteye geçmemiş, mağdur devletleri korumada başarısız olduğu gibi siber imkân ve kabiliyetleri fazla olan güçlü devletleri cesaretlendirmiştir. Bu nedenle birçok devletin ulusal güvenlik strateji belgesinde siber güvenliğini sağlamak için saldırgan siber yeteneklere yatırım yapmaya başladığı ve/veya devam ettiği görülmektedir. Silahlı Çatışma Hukuku kurallarının mevcut siber saldırılara tatbik edilmesi sonuçlarının ülkeleri saldırgan davranışlardan caydırıcılığının yeterli olmadığı düşünülmektedir. Bugünkü devlet

davranışları siber alanda yeni silahlanma yarışının başladığına veya başlayacağına işaret etmektedir.

Her ne kadar siber alanda normlar yaygınlaşınca kadar mevcut silahlı çatışma hukukunun bu alana uyarlanması en iyi çözüm olduğu konusunda taraflar hem fikir ise de Birleşmiş Milletler Anlaşmasının 2. Maddesi 4. fıkrası uyarınca siber savaşı analiz etmeye yönelik sonuç temelli yaklaşımlarda ciddi kusurlar bulunmaktadır. Sonuç temelli yaklaşım meşruiyet karinesini bir faktör olarak kullanarak, saldırının meşru olup olmadığını sorgulayarak uluslararası hukukta bir saldırının meşruiyetini belirlemeyi gerektirir. Aslında, yaklaşım gerçekleşmiş bir saldırıyı analiz etmek için geriye doğru işlemektedir. Bu nedenle tezin başlangıcında ortaya konulmuş olan hipotez doğrulanamamıştır.

Ayrıca, diğer savaş türlerinden farklı olarak, siber saldırının büyüklüğünü ve meşru olarak verilebilecek karşılığı saldırı anında kolayca tespit etmek mümkün değildir. Bu sorun, yukarıda belirtilen sonuç odaklı yaklaşım da dâhil olmak üzere saldırının meydana gelmesinden sonra analiz yapmayı gerektiren bir çerçeveye ortaya çıkmaktadır. Birleşmiş Milletler Uluslararası Adalet Divanı'nın Nükleer Silahların kullanımı ile ilgili tavsiye kararında, bir saldırının silahlı saldırı olarak nitelendirilip nitelendirilemeyeceği hususunda saldırı araçlarının seçiminin önemsiz olduğunu ısrarla vurgulamıştır. Bugüne kadar yapılan uluslararası siber saldırılardan birinin silahlı saldırı eşiğine ulaştığına yönelik uluslararası toplum tarafından bir açıklama ve tespit yapılmamıştır. 2009 yılında İran'ın uranyum zenginleştirme tesisine Stuxnet virüsü ile yapılan siber saldırılar sonucunda santrifüjlere verilen fiziksel zarar ışığında, siber saldırıların silahlı saldırı eşiğine ulaştığı yönünde güvenlik uzmanları arasında yaygın bir kanaat bulunmaktadır. Ancak Stuxnet operasyonlarının silahlı saldırı eşiğine ulaştığına ilişkin değerlendirme saldırıdan birkaç yıl sonra yapılabilmektedir. Çünkü saldırı ancak bir yıl sonra tespit edilmiştir. Saldırıya uğrayan devletin meşru müdafaa hakkının doğduğunu varsaysak bile meşru müdafaa kapsamında verilecek karşılıkla ilgili gereklilik ve ivedilik kriterleri karşılanmadığından orantılı da olsa saldırgana meşru müdafaa kapsamında bir karşılık vermek mümkün değildir.

Ayrıca, siber saldırılar birbiriyle neredeyse eş zamanlı gerçekleşmektedir. Saldırganın kimliğinin ve amacının belirlenmesini gerektiren mevcut hukuk sistemi,

dijital çağın bu tür özelliklerini hesaba katmamaktadır. Fakat taktik, operatif ve stratejik seviyede yapılacak değerlendirmelerle siber saldırının zor da olsa bir devlete atfedilebileceğine ilişkin çalışmalar bulunmaktadır. Atfin zorluğu nedeniyle mevcut uluslararası sistem, devletlerin kullanabileceği seçenekleri sınırlandırmakta ve uluslararası hukuku ihlal etmeden etkili bir şekilde karşılık vermeyi zorlaştırmaktadır. Bir devletin meşru müdafaadan doğan karşılık verme hakkını kısıtlamak, devletleri, terör örgütlerini ve bireyleri giderek hem daha şiddetli hem de daha fazla siber saldırı yapmaya teşvik edecektir.

Yapılan siber saldırının Birleşmiş Milletler Anlaşmasının 51. Maddesinde tanımlanan silahlı bir saldırı kriterlerini karşıladığı yönünde kanaat oluşması durumunda saldırıya uğrayan devletin meşru müdafa hakkı doğmaktadır. Meşru müdafa hakkının kullanılması için tehlikenin o an ortaya çıkmış, ani, karşı konulmaz ve başka hiç bir korunma yoluna başvurmaya imkân bırakmayacak nitelikte olması gerekmektedir. Ancak meşru müdafa hakkının kullanılması, aynı zamanda gereklilik, orantılılık, yakınlık ve ivedilik şartlarına tabidir. Estonya'ya yapılan siber saldırılar silahlı saldırı seviyesine ulaşmadığından Estonya devleti için meşru müdafa hakkı doğmamıştır. Bu durumda Estonya Birleşmiş Milletler Anlaşmasının 51. Maddesinden kaynaklanan meşru müdafa hakkını kullanamayacaktır. Meşru müdafa hakkı doğmuş olsaydı Estonya, gereklilik, orantılılık, yakınlık ve ivedilik şartlarına uygun olarak askeri güç de dâhil her türlü kuvvet kullanarak karşılık verebilirdi.

Meşru müdafa hakkı doğmadığına göre saldırıya uğrayan devlet hiçbir karşılık veremeyecek midir? Birleşmiş Milletler Anlaşmasının 2. Maddesi 4. Fıkrasına göre başka bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı tehdit veya kuvvet kullanmak yasaklanmıştır. Bu sefer saldırının tehdit veya kuvvet kullanma olarak değerlendirilip değerlendirilmeyeceği incelenmelidir. Birleşmiş Milletler Anlaşmasının 51. Maddesini tersinden yorumladığımızda saldırıya uğrayan devletin saldırgan devlete, siber alanda veya fiziksel alanlardan birinde silahlı saldırıya ve kuvvet kullanmaya varmayacak şekilde bir karşılık vermesi en doğal hakkıdır. ABD, Rusya'nın 2016 ABD Başkanlık Seçimlerine siber müdahale ve saldırılarına karşılık olarak ekonomik yaptırım uygulamış ve birçok Rus diplomatı sınır dışı etmesi meşru müdafa yöntemleri olmayıp verilebilecek diğer karşılıklardır.

Diğer bir sorun ise saldırıya uğrayan devletin meşru müdafaa hakkını kullanmasına imkân sağlayacak şartlar oluşmuş olsa da eğer saldırı bir devlete atfedilemiyor veya düşük bir dereceyle atfedilebiliyorsa bu durumda da saldırgana gereken karşılık verilemeyecektir. Bu sorunun üstesinden gelmek için siber alanın kendine özgü doğası nedeniyle uluslararası hukuk, silahlı saldırı seviyesine ulaşmış siber bir saldırıya düşük atfetme derecesi ile iyi niyetle karşılık veren devletlerin meşru müdafaa hakkının korunması için daha esnek yorumlanabilir. Çünkü devletin hayatta kalması ve hayati çıkarlarını koruması derhal, güçlü ve saldırgan bir karşılık vermesine bağlı olabilir. Ancak bu durumun da devletlerin bu imkanı suiistimal etme ihtimali bulunmaktadır.

Siber alanın doğasında var olan teknoloji, saldırıyı belirli bir kaynağa atfetmeyi veya bunun arkasındaki amacı tanımlamayı neredeyse imkânsız hale getirse de bazen fiziksel bir saldırının da bir saldırgana atfedilmesinde güçlükler yaşanmaktadır. Örneğin Yemen hükümetiyle çatışan ve İran'ın desteklediği iddia edilen Husi isyancıları Eylül 2019'da Suudi Arabistan petrol tesislerine yönelik saldırıları üstlenmesine rağmen saldırıların arkasında İran'ın olduğuna yönelik şüpheler bulunmaktadır. Bu örnekten de anlaşılacağı üzere atıf sorunu siber alanda büyük bir sorun olarak karşımıza çıkmış olsa da sadece siber alana ilişkin değildir. Bu sorunun somut olayın özelliğine bağlı olarak çözülmesi gerektiği düşünülmektedir.

Silahlı Çatışma Hukuku'nun siber alana uygulanması sonucunda ortaya çıkan sorunlara çözüm önerisi olarak getirilen diğer bir husus devletlerin kritik siber ulusal altyapılarını ve angajman kurallarını önceden beyan etmeleridir. Böylece devletin, kritik ulusal altyapısına yapılacak siber bir saldırıya karşılık olarak herhangi bir sorumluluk yüklenmeden aktif savunma önlemleri almasına imkân sağlanmış olacaktır. Bu istisnaya göre, Birleşmiş Milletler Anlaşmasının 51. Maddesinden kaynaklanan meşru müdafaa hakkının kullanılabilmesi için bir devletin aktif savunma önlemleriyle koruyabileceği kritik bir ulusal altyapı listesi yapıp bu listeyi Birleşmiş Milletler ve ilgili platformlarda paylaşması önerilmektedir. Bu önerinin birçok devlet tarafından benimsendiğine yönelik olarak son dönemde devletlerin siber güvenlik strateji belgelerinde ulusal kritik altyapı envanterini oluşturma gayreti müşahade edilmektedir. Listede tanımlanan kritik altyapı bir siber saldırıya maruz kalırsa, devlet

ilk önce saldırıyı teamül hukukunda istenen kesinlik seviyesinde bir devlete atfetmeden daha düşük seviyede bir atıfla veya saldırıyı nitelendirmeden iyi niyetli bir şekilde meşru müdafaa hakkını kullanarak saldırıya karşılık verebilecektir. Böyle bir istisna, mevcut Silahlı Çatışma Hukuku çerçevesini kökten değiştirmeyecek, bunun yerine, devletin, meşru müdafaa hakkını, yeni bir tehdide yanıt olarak kullanmasına izin verecektir.

Birleşmiş Milletler Anlaşması yapıldığında henüz hayatımızda internet mevcut değildi. Bu anlaşma yapılırken yüzyıllar içinde oluşmuş uluslararası teamüller esas alındığından henüz var olmayan siber alanla ilgili hiçbir teamül de yoktu. Birleşmiş Milletler Anlaşması metninde geçen birçok kavram geleneksel anlamları içinde kullanılmıştır. Bu nedenle, siber alanla ilgili kavramların özellikle de siber saldırı kavramının geleneksel kuvvet kullanma tanımıyla açıklanması mümkün değildir. Geçmişten günümüze saldırı araç ve yöntemleriyle savunma araç ve yöntemleri adeta birbiriyle yarış halinde gelişme göstermiştir. Kısa bir süre saldırı araç ve yöntemleri öne geçmiş daha sonra savunma araç ve yöntemleri öne geçmiştir. Doğadan buna bir örnek verecek olursak Heliconius kelebeği ile tutkulu asma arasındaki ilişki karşılıklı silahlanma yarışı kapsamında değerlendirildiğinde, bir türe ait genetik kompozisyonda bir değişiklik olduğunda karşılık olarak diğesinde de değişiklik meydana gelmektedir. Tutkulu asma kendini korumak için zehir geliştirirken Heliconius kelebeği ise zehri özümseme yeteneğini geliştirip bu zehri kendi düşmanlarına karşı bir silah olarak kullanmıştır. Benzer şekilde Heliconius asmayı yiyerek beslenirken asmanın üremesini ve hayatta kalmasını sağlamıştır.

Bu benzetmeden yola çıktığımızda devletlerin de çıkar ve menfaatlerini gerçekleştirmek için belirli şartlara bağlı olarak kullandıkları kuvvet kullanma yöntemlerinin benzer şekilde sürekli değişim ve gelişim içinde olduğunu söyleyebiliriz. Birleşmiş Milletler Anlaşmasıyla oluşturulan hukuki düzen siber alanın özellikleri nedeniyle saldırgan tarafa yani siber imkân ve kabiliyetleri gelişmiş devletlere avantaj sağlamaktadır. Devletlerarasındaki çıkar ve menfaat mücadelesinin daha adil ve hakkaniyetle devamı için Birleşmiş Milletler Anlaşmasıyla oluşturulan hukuki düzenin çıkar ve menfaatleri elde etme yöntemlerinde meydana gelen bu değişime ayak uydurması gerekmektedir. Özellikle siber imkân ve kabiliyetleri sınırlı

devletlere siber saldırılara karşı güç kullanımını düzenleyen uluslararası hukukun eski yorumlarıyla sınırlanmamış meşru müdafaa hakkını kullanarak karşılık verme imkânının sağlanması uluslararası barışın devamı için hayati öneme haizdir.



BİBLİYOGRAFYA / KAYNAKÇA

Alexander Klimburg	National Cyber Security Framework Manual , NATO CCD COE Publications, December 2012
Alexander Gostev	The Flame: Questions and Answers, Kaspersky Lab , 28 May 2012
Amir Lupovici	“The “Attribution Problem” and the Social Construction of “Violence””, International Studies Perspectives , 2014
Andress Jason, Winterfeld Steve	Cyber Warfare : Techniques, Tactics and Tools for Security Practitioners , 2011
Andrew Moravcsik	“The Origins of Human Rights Regimes: Democratic Delegation in Postwar Europe”, International Organization 54(2)
Andrew Blake	“Hillary Clinton: U.S. Will Treat Cyberattacks ‘Just Like any Other Attack,’” Washington Times , October 7, 2016, (çevrimiçi) http://www.washingtontimes , 24.07.2019
Ann Florini	“The Evolution of International Norms,” International Studies Quartetly 40, No:3, Eylül 1996
APT1, Alexandria	VA: Mandiant , 18 Feb. 2013
Azah Anir Norman et.al	Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review, Future Technologies Conference 2017 , (çevrimiçi) https://umexpert.um.edu.my/file/publication/00007219_156865_68443.pdf , 12.09.2018
BM Şartı Hazırlık Görüşmeleri,	BM Şartı Hazırlık Görüşmeleri , 1945, (çevrimiçi), https://digitallibrary.un.org/record/1300969/files/UNIO-Volume-21-E.pdf , 24.12.2018
Bilgi Teknolojileri ve İletişim Kurumu	2018 yılı 1. Çeyrek Pazar Verileri Raporu , (çevrimiçi) https://www.btk.gov.tr/uploads/pages/pazar-verileri/2018-1ceyrekraporu-kurumdisi.pdf , 13.09.2018
Bin Cheng	General Principles of Law , Cambridge University Press, 2006

Brown, Gary, and Keira Poellet	"The Customary International Law of Cyberspace." Strategic Studies Quarterly 6, No. 3 , 2012,
Catherine Lotrionte	"State Sovereignty And Self-Defense In Cyberspace: A Normative Framework For Balancing Legal Rights", Emory International Law Review , Vol.26,(çevrimiçi) http://law.emory.edu/eilr/_documents/volumes/26/2/symposium/lotrionte.pdf , 09.07.2019
Convention of Cybercrime	Convention of Cybercrime , (çevrimiçi), https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/8601684 , 09.09.2018
ÇÖLKESEN Rıfat, Bülent ÖRENCİK	Bilgisayar Haberleşmesi ve Ağ Teknolojileri , Papatya Yayıncılık, Haziran, 1999, s.345-358
David A. Sanger	"Obama Order Step Up Wave of Cyber attacks Against Iran", The New York Times , 1 June 2012, (Çevrimiçi) http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html , 25.11.2015 "Biden Hints U.S. Response to Russia for Cyberattacks," New York Times , October 15, 2016, (çevrimiçi) http://www.nytimes.com/2016/10/16/us/politics/biden-hints-at-us-response-to-cyberattacks-blamed-on-russia.html , 26.08.2019
David Kushner	The Real Story of Stuxnet , IEEE Spectrum, 26 Feb 2013, (çevrimiçi) https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet , 30.04.2016
Department of Defense	Defense Science Board , "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat," January 2013, (çevrimiçi) http://www.dtic.mil/get-tr-doc/pdf?AD=ADA569975 , 05.09.2019
Denise Garcia	Small Arms and Security New Emerging International Norms , Routledge; First Edition (November 1, 2006)
Dean Cheng	Cyber Dragon , Preager, Santa Barbara, California, 2017
Dwen-Ren Tsai et.al	"Optimum Tuning of Defense Settings for Common Attacks on the Web Applications", Security Technology ,

	2009, 43rd Annual 2009 International Carnahan Conference
Electricity Consumers Resource Council	The Economic Impacts of the August 2003 Blackout, February 9, 2004, (çevrimiçi) http://www.elcon.org/Documents/Profiles%20and%20Publications/Economic%20Impacts%20of%20August%202003%20Blackout.pdf , 30.04.2016
Emilio Iasiello	“Are Cyber Weapons Effective Military Tools?” , Military and Strategic Affairs 7 , No. 1, Mart 2015,
Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin	Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains , Bethesda, MD: Lockheed Martin Corporation 2010
Encyclopaedia Britannica	(çevrimiçi) https://www.britannica.com/topic/norm-society , 25.03.2019
Eneken Tikk,et.al	Cyber Attacks Against Georgia: Legal Lessons Identified , Cooperative Cyber Defence Center of Excellence, November 2008
Eric Cole,	Advanced Persistent Threat, (Çevrimiçi) http://index-of.es/Varios/Syngress.Advanced.Persistent.Threat.Nov.2012.ISBN.1597499498.pdf , s.19-21, 25.02.2019
Finnemore and Sikkink	“International Norm Dynamics,” International Organization , Vol. 52, No. 4, (Autumn, 1998), s.891.
Geoff McDonald, Liam O	Murchu, Stephen Doherty and Eric Chien, Stuxnet 0.5: The Missing Link, Version 1.0, Symantec , 26 Feb. 2013
George V. Hulme	“How Distributed Denial of Service Attacks are Evolving” , (çevrimiçi) https://www.csoononline.com/article/3222095/network-security/ddos-explained-how-denial-of-service-attacks-are-evolving.html , 11.09.2018
Hasan Çiftçi	Her Yönüyle Siber Savaş , TÜBİTAK, Ankara, 2013

Herbert S. Lin	“Offensive Cyber Operations and the Use of Force”, Journal of National Security Law & Policy , Vol.4, No.63, 2010
Hüseyin Pazarcı	Uluslararası Hukuk , Gözden Geçirilmiş 3.Bası, Turhan Kitabevi, Ankara 2014
Ian Brownlie	International Law And The Use Of Force Between States , Oxford Scholarship Online: March 2012, s.275-278
International Court of Justice	Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) , (çevrimiçi) https://www.icj-cij.org/en/case/1 , 21.02.2019
	Legality of the Threat or Use of Nuclear Weapons , (Çevrimiçi) https://www.icj-cij.org/en/case/93 , 29.01.2019
	Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.) , (Çevrimiçi) https://www.icj-cij.org/en/case/70 , 12.02.2019
	United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran) Case, 24 May 1980, (çevrimiçi) https://www.icj-cij.org/en/case/64 , 08.07.2019
	Nuclear Weapons Advisory Opinion , 08.07.1996, para.39, (çevrimiçi) https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf , 18.07.2019
	Oil Platforms Judgment 12.12.1996, paras.57,61, (çevrimiçi) https://www.icj-cij.org/files/case-related/90/090-19961212-JUD-01-00-EN.pdf , 23.07.2019
International Criminal Tribunal for the Former Yugoslavia	Tadic Case , Case No. IT-94-1-T, 07 May 1997, (çevrimiçi) http://www.icty.org/en/press/tadic-case-verdict , 08.07.2019
James Lewis	“Significant Cyber Events Since 2006,” Center for Strategic and International Studies , July 11, 2013,(çevrimiçi) http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf . 21.03.2019
James P. Farwell and Rafal Rohozinski	“Stuxnet and the Future of Cyber War”, Survival Global Politics and Strategy , Volume 53

James J. Wirtz	“Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy “, NATO Cooperative Cyber Defence Centre of Excellence Publications , Tallinn 2015, s.29-32
Jarno Limnéll	Developing a Proportionate Response to a Cyber Attack , Aalto University Publication Series, Science+Technology, 2016 The Cyber Arms Race is Accelerating What are The Consequences?, Journal of Cyber Policy ,
Jason Healey	A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 , Cyber Conflict Studies Association (June 1, 2013)
Jean-Marie Henckaerts and Louise Doswald-Beck	Customary International Humanitarian Law , Cambridge University Press, 2009,
Jeffrey W. Legro	“Military Culture and Inadvertent Escalation in World War II”, International Security 18, No. 4 (Spring 1994)
Jeffrey Carr	Inside Cyber Warfare: Mapping the Cyber Underworld , O'Reilly Media; 2. Edition (31 Dec. 2011)
Jelle van Haaster	Assessing Cyber Power, 8th International Conference on Cyber Conflict , (Çevrimiçi) https://ccdcoe.org/uploads/2018/10/Art-01-Assessing-Cyber-Power.pdf , s 7-21, 29.08.2019
Jens Stoltenberg	Nato will defend itself, Prospect Magazine , (Çevrimiçi) https://www.prospectmagazine.co.uk/world/nato-will-defend-itself , 27.08.2019
Jurriën Hamer, Rinie van Est & Lambèr Royakkers	Cyberspace Without Conflict , (çevrimiçi) https://www.rathenau.nl/sites/default/files/2019-08/Cyberspace%20without%20conflict.pdf , s.19-21, 30.08.2019
Jon R. Lindsay	‘Stuxnet and the Limits of Cyber Warfare’, Security Studies 22/3 (2013)
Joseph S. Nye	Cyber Power , Belfer Center for Science and International Affairs, 2010

Jim Finkle	“Exclusive: Insiders suspected in Saudi cyber attack”, Reuters , 7 Sept. 2012.
Katzenstein, Wendt, and Jepperson	Norms, Identity, and Culture in National Security , Columbia University Press, 1996
Keir Giles and William Hagestad	Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English , (Çevrimiçi) https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf , 06.09.2018
Kim Zetter	‘How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History’, Wired Magazine , 11 July 2011 Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Broadway Books; Reprint Edition (September 1, 2015),
Knapp Eric, Langill Thomas Joel	Industrial Network Security , Elsevier, Waltham, 2015
Leon Panetta	‘Remarks on Cybersecurity to the Business Executives for National Security’, (çevrimiçi) https://www.lawfareblog.com/secdef-panetta-speech-cybersecurity , 15.06.2019
Maria Benvenuta Occelli	"Sinking" the Caroline: Why the Caroline Doctrine's Restrictions on Self-Defense Should Not Be Regarded as Customary International Law”, San Diego International Law Journal , Volume 4, 2003,
Martha Finnemore and Kathryn Sikkink	“International Norm Dynamics and Political Change”, International Organization 52 (4),
Martin C.Libicki	Cyber deterrence and Cyber war , The Rand Corporation, Santa Monica 2009
Matthew Hoisington	Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, Boston College International and Comparative Law Review V.32

Matthew Crosston and Frank Valli	An Intelligence Civil War: “HUMINT” vs. TECHINT Cyber, Intelligence, and Security, Volume 1, January 2017
Matthew J. Sklerov	“Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect their Duty to Prevent”, Military Law Review , V.201, 2009,
Matthew Hoyer	“Trump on Iran: "We'll know for certain over the next very short period of time", CNN , (Çevrimiçi) https://edition.cnn.com/middleeast/live-news/saudi-oil-attack-dle-intl/index.html , 18.09.2019
Merriam-Webster Dictionary	Merriam-Webster Dictionary , (çevrimiçi) https://www.merriam-webster.com/dictionary/hacker , 31.07.2018
Mervyn Frost	Ethics in International Relations: A Constitutive Theory , (Cambridge: Cambridge University Press, 1996), s. 58.
Michael C. Long II	Attack and Defend: Linux Privilege Escalation Techniques of 2016 , s.6-16 (çevrimiçi) https://www.sans.org/reading-room/whitepapers/linux/attack-defend-linux-privilege-escalation-techniques-2016-37562 , 11.09.2018
Michael N. Schmitt, et.al	The Tallinn Manual on the International Law Applicable to Cyber Warfare , Second Edition, Cambridge University Press, New York, 2017
Michael N. Schmitt	Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Research Publication 1 Information Series , 1999 “Bellum Americanum: The U.S. View of Twenty-first Century War and Its Possible Implications for the Law of Armed Conflict,” Michigan Journal of International Law 19 (1998) “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” Columbia Journal of Transnational Law 37 1999
Mohn, Elizabeth	“Stuxnet”, Salem Press Encyclopedia of Science , 2015, (çevrimiçi) http://eds.a.ebscohost.com/eds/detail/detail?

	vid=4&sid=84b9a4f9-291d-45a2-ac7e-e76289b32b9%40sessionmgr4007&bdata=Jmxhbm9dHImc2l0ZT1lZHMtGl2ZQ%3d%3d#AN=87323878&db=ers, 14.09.2018
Muharrem Gürkaynak ve Adem Ali İren	“Reel Dünyada Sanal Açmaz:Siber Alanda Uluslararası İlişkiler”, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi , 2011,Cilt:16, Sayı:2,
Nathaniel Hartley	Hat-tribution to PLA Unit 61486, CrowdStrike , 09 June 2014
Nate Anderson, and Cyrus Farivar	‘How the feds took down the Dread Pirate Roberts’, Ars Technica , 3 Oct. 2013.
National Security Strategy of the United States of America 2017	National Security Strategy of the United States of America 2017 , (Çevrimiçi) https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ,s.8, 09.09.2018
NATO	Warsaw Summit Communiqué , July 9, 2016, (çevrimiçi) http://www.nato.int/cps/en/natohq/official_texts_133169.htm . 27.08.2019
Ned Moran, Joshua Homan and Mike Scott	Operation Poisoned Hurricane, FireEye , 6 Aug. 2014
Neil Robinson et.al	Data and Security Breaches and Cyber Security Strategies in The EU and Its International Counterparts , European Union, 2013,
Nicole Perlroth	‘Hackers Lurking in Vents and Soda Machines’, New York Times , 8 Nisan 2014
Oona A. Hathaway, et.al,	“The Law of Cyber Attack”, California Law Review , Vol. 100 , No.4,
Pauline C. Reich, v.d	” Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents- and the Dilemma of Anonymity”, European Journal of Law and Technology , Vol.1, Issue 2, 2010

Piret Pernik	"Improving Cyber Security: NATO and The EU", International Centre for Defence Studies , Talinn, 2014
Ralph Langner	Stuxnet's Secret Twin', Foreign Policy , 19 Nov. 2013
Richard K. Betts	'Analysis, War and Decision: Why Intelligence Failures Are Inevitable', World Politics , 31/1 (Oct. 1978)
Robert K. Knake	"A Cyberattack on the U.S. Power Grid", Contingency Planning Memorandum No. 31 , 2017, (çevrimiçi) https://www.cfr.org/report/cyberattack-us-power-grid , 12.09.2018
Ron Rosenbaum	'Cassandra Syndrome', Smithsonian Magazine 43/1, (April 2012)
Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata	'Cyclones in Cyberspace', Security Dialogue 43/1 (2012)
Rukondo Solomon	"Electronic protests: Hacktivism as a form of protest in Uganda", Computer Law & Security Review Volume 33, 2017,
Ruthmery Pillco Huarcaya	Passionflowers and Butterflies: A love-hate relationship, Osa Conservation , (çevrimiçi) http://osaconservation.org/2017/10/passifloras-butterflies-a-love-hate-relationship/ , 09.04.2019
Salih Bıçakçı	21. Yüzyılda Siber Güvenlik , Bilgi Üniversitesi Yayınları, İstanbul, 2013
Sarah Gordon, Richard Ford	"On the Definition and Classification of Cybercrime", J. Computer Virology , No:1, 2006
Sean Collins, Stephen McCombie	"Stuxnet: The Emergence Of a New Cyber Weapon And Its Implications" Journal of Policing, Intelligence and Counter Terrorism , Vol.7, No.1, 2012
Sico Van der Meer	"Signaling as a Foreign Policy Instrument to Deter Cyber Aggression by State Actors," Clingendael , December 2015,(Çevrimiçi) https://www.clingendael.nl/sites/default/fi

	les/PB_Signalling_as_a_foreign_policy_instrument_SvdM.pdf., 29.08.2019
Stamatis Karnouskos	Stuxnet Worm Impact on Industrial Cyber-Physical System Security, IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society , (çevrimiçi) https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ , 08.04.2019
Stephen Herzog,	“Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses”, Journal of Strategic Security , 2011, Cilt 4(2),
Susan Brenner	At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, The Journal of Criminal Law & Criminology . 97/2 (2007
Şener Çelik	Stuxnet Saldırısı ve ABD’nin Siber Savaş Stratejisi, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi , Cilt: 15, Sayı: 1, 2013, s.137-175 (Basım Yılı: 2014)
T. C. Wingfield, J. B. Michael, and D. Wijesekera	" Optimizing Lawful Responses to Cyber Intrusions ," (Çevrimiçi) http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf , 10.04.2019
Terry D. Gill	“The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy”, International Law And Armed Conflict: Exploring The Faultlines , Martinus Nijhoff, Boston 2007, s.113-120
The Epic Turla Operation	Kaspersky Lab , 7 Ağustos 2014
Thomas M. Franck	Terrorism and the Right of Self-Defense , The American Journal of International Law Vol. 95, No. 4 (Oct., 2001),
Thomas Schelling	The Nuclear Taboo,” MIT International Review(Spring 2007) , (çevrimiçi) http://web.mit.edu/mitir/2007/spring/taboo.pdf , 27.03.2019
Thomas Rid & Ben Buchanan	Attributing Cyber Attacks, Journal of Strategic Studies , 2015, Vol. 38

Thomas Rid	Cyber War will Not Take Place, Oxford/New York: OUP 2013
Threat Report: Beyond the Breach, Reston	VA: Mandiant , 18 Feb. 2014
Tim Maurer	Cyber Norm Emergence at the United Nations, Explorations in Cyber International Relations Discussion Paper Series , Belfer Center for Science and International Affairs, 2011
United Kingdom	National Cyber Security Strategy 2016 to 2021 , (çevrimiçi) https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 , 09.09.2018
Ulaştırma Denizcilik ve Haberleşme Bakanlığı	2016-2019 Ulusal Siber Güvenlik Stratejisi , (Çevrimiçi) http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf , 12.09.2018
United Nations	Declaration on Principles of International Law Friendly Relations and Co-Operation Among States in Accordance with The Charter of The United Nations , (çevrimiçi) https://www.un.org/ruleoflaw/files/3dda1f104.pdf , 27.12.2018
	United Nations General Assembly Resolution 3314 (XXIX) , (çevrimiçi) http://hrlibrary.umn.edu/instree/GAres3314.html , 14.02.2019
	Birleşmiş Milletler Anlaşması , (Çevrimiçi) https://www.un.org/en charter-united-nations/index.html , 02.02.2019
	Convention on the Law of the Sea, Article 19. Meaning of innocent passage
United Nations Security Council	Resolution 1368(2001) , (çevrimiçi) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement , 25.02.2019
United Nations General Assembly	56/83. Responsibility of States for Internationally Wrongful Acts , (çevrimiçi) https://undocs.org/en/A/RES/56/83 , 24.06.2019
	Implementation of the Declaration on the Strengthening of International Security , 18 December

	1973, (çevrimiçi), https://www.refworld.org/docid/3b00f1c754.html , 08.07.2019
UNIDIR Resources	Autonomous Weapon Systems and Cyber Operations , 2017
Unveiling “Careto”- The Masked APT	Version 1.0, Kaspersky Lab , 06 Feb. 2014
US Department of Defense	US Department of Defense Dictionary of Military and Associated Terms , November 2010,(Çevrimiçi) http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2810-13%29.pdf , 06.09.2018
U.S.-Canada Power System Outage Task Force	Final Report on the August 14, 2003 Blackout in the United States and Canada , 2004
United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Criminal	United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Criminal Nr 14-118, Erie, PA: US District Court Western District of Pennsylvania , 1 May 2014, 12–13, Exhibit F
Vitaly Kamluk	“ The Mystery of Duqu: Part Six ,” (çevrimiçi), https://securelist.com/the-mystery-of-duqu-part-six-the-command-and-control-servers-36/31863/ , 15.06.2019
Viyana Antlaşmalar Hukuku Sözleşmesi	Viyana Antlaşmalar Hukuku Sözleşmesi , 1969, (çevrimiçi), https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf , 24.12.2018
Walter Gary Sharp	Cyberspace and the Use of Force, Ageis Research Corp , 01.02.1999
W. Earl Boebert	‘A Survey of Challenges in Attribution’, in Committee on Deterring Cyberattacks (ed.), Proceedings of a Workshop on Deterring Cyberattacks (Washington DC: National Academies Press 2011)

White House	Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting, June 8, 2013, (çevrimiçi) https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china/.23.07.2019 Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, December 29, 2016,(çevrimiçi) https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity, 27.08.2019
William Broad et al	Israeli Test on Worm Called Crucial in Iran Nuclear Delay', New York Times , 15 Jan. 2011.
The White House Office of the Press Secretary	Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference, 25.09.2015 (çevrimiçi)https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint, 25.03.2019
'2014 Data Breach Investigations Report'	'2014 Data Breach Investigations Report', Verizon , 22 April 2014,

ÖZGEÇMİŞ

1965 yılında Yozgat'ta doğdu. 1980 yılında Kuleli Askeri Lisesi'nden, 1988'da Kara Harp Okulu'ndan (Lisans, İşletme) mezun oldu. 2002-2004 yılları arasında Kara Harp Akademisinde Kurmay Subaylık Eğitimi ile birlikte Ulusal ve Uluslararası Güvenlik Stratejileri Yönetimi Yüksek Lisans programını tamamladı. 2008 yılında Silahlı Kuvvetler Akademisi'nde Üst Düzey Yöneticilik Eğitimi aldı. 2014 yılında Stratejik Araştırmalar Enstitüsü'nde (SAREN) doktora eğitimine başladı. 2017 yılında İstanbul Hukuk Fakültesi'nden mezun oldu.

2017'den itibaren doktora eğitimine İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Ana Bilim dalında devam etti.

1989-2004 yılları arasında Kıta ve Karargâh Görevlerinde bulundu. 2006-2008 Yılları arasında Tabur Komutanlığı, 2009-2011 yılları arasında Afganistan Kabil Silahlı Kuvvetler Ataşeliği görevlerini icra etti. 2011-2013 yılları arasında Üst Düzey Yöneticilik (Tugay Komutan Yardımcısı) görevini icra etti. 2013 yılında İstanbul Üniversitesi Hukuk fakültesine kaydını yaptırdı. 2013-2014 yılları arasında Üst Düzey Yöneticilik (Kolordu Denetleme Heyeti), 2015-2016 yılları arasında Harp Akademileri Yüksek Sevk ve İdare Akademisi öğretim elemanlığı görevlerini ifa etti. Ağustos 2016'da Silahlı Kuvvetler 'den emekli oldu. 2017 yılında İstanbul Üniversitesi Hukuk fakültesinden mezun olmayı müteakip avukatlık stajını tamamlayarak serbest avukatlık ve Milli Savunma Üniversitesi Kara ve Deniz Enstitüleri ile Müşterek Harp Enstitülerinde öğretim elemanlığı yapmaktadır.

İngilizce bilen Can BOLAT, Fatma Arzu BOLAT ile evli olup iki çocuk babasıdır.