T.C

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU

ANABİLİM DALI

SİBER UZAYDA HASMANE "DAVRANIŞ" VE "NİYETİN" BELİRLENMESİ

Doktora Tezi

JACQUES KABANO

Ankara, 2022

T.C.

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU

ANABİLİM DALI

SİBER UZAYDA HASMANE "DAVRANIŞ" VE "NİYETİN" BELİRLENMESİ

Doktora Tezi

JACQUES KABANO

Tez Danışmanı

Doç. Dr. Ülkü HALATÇI ULUSOY

Ankara, 2022

T.C.

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

SİBER UZAYDA HASMANE "DAVRANIŞ" VE "NİYETİN" BELİRLENMESİ

Doktora Tezi

Tez Danışmanı

Doç. Dr. Ülkü HALATÇI ULUSOY

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı	İmzası
1. Doç. Dr. Ülkü Halatçı ULUSOY	
2. Prof. Dr. Cavid ABDULLAHZADE	
3. Doç. Dr. Mustafa ÇAKIR	
4. Doç. Dr. Uğur BAYILLOĞLU	
5. Dr. Öğr. Üyesi. Nasıh Sarp ERGÜVEN	

TEZ SAVUNMASI TARİHİ

30.06.2022

T.C.

ANKARA ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Doç. Dr. Ülkü Halatçı ULUSOY danışmanlığında hazırladığım **"SİBER UZAYDA HASMANE "DAVRANIŞ" VE "NİYETİN**" BELİRLENMESİ (Ankara.2022) " adlı doktora tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Tarih: **30.06.2022**

Adı-Soyadı ve İmza:

Jacques KABANO

İçindekiler

İKİNCİ BÖLÜM

ULUSLARARASI HUKUK KAPSAMINDA BAZI SİBER OPERASYONLARIN HASMANE OLARAK BELİRLENMESİNE İLİŞKİN KRİTERLER VE SİBER SALDIRILARIN GEREKÇESİ

ÜÇÜNCÜ BÖLÜM

ULUSLARARASI İNSANCIL HUKUKU SİBER UZAYA UYGULAMANIN ZORLUĞU

KISALTMALAR

AK: Angajman Kuralları

BM: *Birleşmiş Milletler*

BT: Bilgi teknolojisi

DdoS: *Distributed Denial of Service*

DEF CON: Defense Ready Condition

DoS: Denial of Service

EFF: Electronic Frontier Foundation

FBI: Fedral Bureau of Investigation

GGE: Group of Governmental Express

HTTP: Hyper Text Transfer Protocol

IAC: International Armed Conflict

IBM: International Business Machines

ICRC: *International Community for Red Cross*

IHL: International Humanitarian Law

IP: Internet Protocol

ITU: *International Telecommunication Union*

NIAC: uluslararası olmayan bir silahlı çatışma

NSA: National Security Agency

OECD: *Organisation for Economic Co-operation and Development*

PHP: Hypertext Preprocessor

PII: Kişiyi tanımlamak için kullanılan bilgiler

UİH: Uluslararası insancıl hukuk,

URL: Uniform Resource Locator

Vb: ve benzeri

TEŞEKKÜRLER

Bu tez, benim sıkı çalışmamın, azmimin ve hedef odaklı ruhumun sonucunda ortaya çıkmıştır diyecek olursam, bu teşekkür yazısının daha ilk cümlesinden sizlere yüzde yüz yalan söylemiş olacağım. Halbuki gerçek olan, bunu, devlerin omuzlarında cüce olarak yapabilmiş olmamdır.

Öncelikle, bütün saygım, şükranlarım ve minnettarlığımla danışmanım Doç. Dr. Ülkü Halatçı ULUSOY'a teşekkürlerimi sunuyorum. Ne zaman aklım karışsa, her zaman kendisine koşmuşumdur.

İkinci olarak, yüksek lisansıma başladığım andan bugüne kadar, bana büyük bir ilham kaynağı olduğu için Doç. Dr. Mustafa ÇAKIR'a çok teşekkür ediyorum.

Üçüncü olarak, hem bir ebeveyne hem de bir öğretmene duyduğum saygıyı kendisine borçlu olduğum Prof. Dr. İraz HASPOLAT KAYA'ya gerçekten minnettarım.

Dördüncü olarak, Ece YILDIRIM'a, ona ihtiyaç duyduğum her an çalışmamı iki kez kontrol edip bana destek olduğu için çok teşekkür ederim.

Ayrıca, Ankara Üniversitesi'ndeki öğretim görevlilerine, öğrencilere ve bu zaman kadar bana nazikçe hizmet etmiş olan okul personeline; bu yolculukta bana destek olan herkese çok teşekkür ederim.

Sonuncu ama son derece önemli olarak, Türk Bursu Programı aracılığıyla eğitimimi finanse ettiği ve hayallerimin gerçekleşmesine izin verdiği için Türkiye Cumhuriyeti Devleti'ne çok teşekkür ederim, gerçekten çok minnettarım.

Jacques KABANO

GİRİŞ

Bugün uluslararası kamu hukuku, İkinci Dünya Savaşı'ndan sonra son büyük gelişimini Birleşmiş Milletler'in (bundan böyle "BM" olarak anılacaktır) kurulmasıyla yaşamıştır. Şu anda tanınan 197 devletten 193 tanesi, bugün BM'ye üyedir. Temel amaçlarından biri, kuruluş belgesinin ilk maddesinde (Birleşmiş Milletler Şartı) öngörüldüğü üzere, uluslararası barış ve güvenliği sağlamaktır.

Uluslararası ilişkilerin anarşik bir modele dayandığını söylemek doğru olmasa da, yine de uluslararası toplumun bugün kırılgan kaldığı ve bu sistemin, şu anda çok olası olmasa bile, herhangi bir zamanda çökebileceği doğrudur. BM bu şekilde antlaşma kurma yetkisine sahiptir, ancak kabul edilip edilmeyeceğine dair karar, üye devletlerin takdirindedir.

Uluslararası hukukun inşasını çok genel bir şekilde çizdikten sonra, bugünün toplumunda giderek merkezi bir yer kaplayan dijital teknolojinin geliştirilmesi için aynı yollardan geçeceği söylenebilir. Bilgisayar tarihine çok fazla girmeden, konunun incelenmesi için, bugün dünyanın en büyük iletişim ağını oluşturan internetin gelişimini anlamak yararlıdır. İnternet sınır tanımıyor ve bu iletişim biçiminin fiziksel olmadığını ve sistemin, özellikle değiştirmeye çalışan belirli girişimler dışında Amerika değiştirmeyi deneyebilir, veri akışlarına öncelik vermesine izin vermediğini bilerek, temel tıkanıklıklar oluşturmak teknik olarak imkânsızdır.

Devletin önemli endüstrileri ve altyapıları, bu sistemleri değiştiren veya zayıflatan çoklu, bazen ciddi siber saldırılara maruz kalan bilgi sistemlerine dayanmaktadır. Devletlerin ve işletmelerin, genellikle kara, deniz, hava ve uzaydan sonra beşinci çatışma alanı olarak kabul edilen bu yeni alanda kendilerini korumalarına ve savunmasına olanak tanıyan teknik ve teknik olmayan önlemler geliştirmek zorunlu hale gelmiştir. Uluslararası düzeyde, çok sayıda saldırı, yeterli müdahale çözümlerini bulmak için gittikçe daha fazla yer alan politikacıların ve hukukçuların ilgisini çekmiştir.

Kamuoyunun çoğu bilinen saldırılardan biri, örneğin, bir bilgisayar solucanı kullanarak İran nükleer programının bilgisayar sistemine girdiği Stuxnet saldırısıydı. Saldırının İsrail veya Amerikan istihbarat servisleri tarafından gerçekleştirildiğine dair şüpheler var, ancak

kimse bunu şimdiye kadar kanıtlayamıyor. Bu saldırı, uluslararası hukukun bu tür saldırılara yanıt vermedeki zorluğunu açıkça göstermektedir. Eğer bu silahlı kuvvetlerin fiziksel saldırısı olsaydı, İran kritik altyapısını korumak için kendini savunmada hareket edebilirdi. Bu araştırmada, siber saldırılar sırasında uluslararası hukukun karşılaştığı bu tür zorluklara bir çözüm sunmaya çalışmak istenmektedir.

Kuşkusuz hem özel hem de kamu siber saldırıları çoğalmaktadır ve uluslararası hukuk henüz yeterli yanıt verememektedir. Uluslararası hukuk tarihi, hukukun her zaman müdahale ihtiyacını gösteren olaylardan sonra müdahale ettiğini göstermiştir. Hukuk genel olarak bu mantıkla çalışmaktadır. Başka bir deyişle, hukuk proaktif bir araç değil, mevcut bir duruma tepki veren bir araçtır.

Bu tezin başlığının gösterdiği gibi, bu araştırmanın iki ana amacı vardır: siber uzayda düşmanca bir "davranış" ve düşmanca bir "niyet"i belirlemeye çalışmaktadır. Bir savaşın gerçekleştirilebileceği beşinci alan olarak, siber alan diğer alanlarda (Kara, Hava, Deniz ve Uzay) belirlenen savaşın önemli özelliklerinden hala yoksundur. Bu perspektifte bu çalışmanın amacı, siber uzayda düşmanca davranışın ve düşmanca niyetin ne olduğunun geçerli bir değerlendirmesini oluşturmaktır.

Bu tez üç bölüm halinde tasarlanmıştır. Birinci bölüm, Siber Kavramı ve Siberuzaya Uluslararası Hukukun Uygulanabilirliği olacaktır. Bu bölümde iki önemli nokta ele alınacaktır; birincisi, konuyla ilgili önemli tanımları ve edebiyat incelemesini tartışan kavramsal kısım ve egemenlik, yargı yetkisi ve devletlerin siber uzaya karşı yükümlülükleri gibi uluslararası hukuk konularının ilgisini inceleyecek ikinci kısım olacaktır.

İkinci bölümde, Bazı Siber Operasyonların Hasmane Olup Olmadığını Belirleme Kriterleri ve Uluslararası Hukuk Kapsamında Siber Saldırıların Gerekçelendirilmesi tartışılacaktır. Bu bölümde uluslararası siber saldırı sırasında meşru müdafaanın hukuki dayanağı ele alınacaktır. Bu bölümde, konuya ilişkin güç kullanımı, uluslararası barış ve güvenlik gibi konular ele alınacaktır. Bu bölümde, BM Şartı'nın 51. maddesi siber perspektif içinde incelenecektir.

Üçüncü bölüm Uluslararası İnsancıl Hukuk ve Siber Hukuk arasındaki sinerjiyi analiz edecektir. Uluslararası insancıl hukuk, silahlı çatışma yöntemlerinin düzenlenmesinde ve sınırlanmasında önemli bir rol oynamaktadır. Bu tez için çok önemli olduğu için,

uluslararası insancıl hukukun siber savaşa ilişkin çözümlerini incelemek gerçekten de bu araştırmaya daha fazla katkı sağlayacaktır. Bu bölümde, genel değerlendirme ve tartışmalardan oluşacaktır. Bu bölümde, tüm bölümlerin bulgularının değerlendirilmesini ele alınacaktır.

BİRİNCİ BÖLÜM

SİBER KAVRAMIN TEORİK TEMELLERİ
VE
ULUSLARARASI HUKUKUN UYGULANABİLİRLİĞİ

I. SİBER KAVRAMIN TEORİK TEMELLERİ

Siber uzay, soyut ve fazlasıyla teknik olan yapısı ve literatürdeki büyük anlamsal belirsizliği nedeniyle anlaşılması zor bir gerçekliktir. Gerçekte siber uzayın nesnel ve uzlaşmaya dayalı bir tanımı yoktur; aksine disiplinlere, aktörlere ve ülkelere göre birden fazla tanımı bulunmaktadır. Bununla birlikte, siber uzayın hem İnternet hem de ürettiği alan olması tartışılabilir: Tüm ulusların vatandaşları arasında, tüm mesafe kavramını ortadan kaldıran anlık bir hızda, yersizyurtsuzlaştırılmış değiş tokuşların meydana geldiği soyut bir alandır.

Bazen, siber uzayın farklı boyutları ve aynı zamanda onunla ilgili sorunların karışıklığı yeniden üretilmesine izin veren birkaç katmanda temsil bulmaktadır.[1]

İlk katman fizikseldir ve siber uzayın ürün olduğu birbirine bağlı ağlardan oluşan küresel bir ağ olan İnternet'in temelini oluşturur. Fiziksel ve siyasi coğrafya kısıtlamalarına tabi, yerelleştirilmiş, maddi mallar olan kablolar; düğümler, sunucular ve bilgisayarlardan oluşur. Bu katman, herhangi bir bütünleşmiş güvenlik olmadan, açıklık ve maksimum bilgi akışı ruhu ile tasarlanmıştır; bu durum, kablolar ve yönlendiriciler aracılığıyla açık (şifreleme olmadan) dolaşan verileri emmenin çok kolay olduğunu açıklamaktadır.

---

1 O. Kempf, ***In*troduction à la cyberstratégie**, Economica, Paris, 2012, s.176

İkinci katman mantıksal ve kullanışlıdır. Verilerin ağın iki noktası arasında iletilmesini, göndericisinden alıcısına küçük ayrı paketler halinde bilgi seyahatini sağlamayı mümkün kılan hizmetleri (uygulamalar, yazılımlar, arayüzler, programlar) içerir. Yine burada, bazı yönler coğrafi olarak yerelleştirilebilir (kullanılan yazılım, tedarikçi firma, alınan yollar, veri depolama, vb.). Bununla birlikte mantıksal mimari, ortak bir temele, dünyadaki tüm bilgisayarların birbirini anlamasına izin veren temel bir uyumlaştırma olan İnternet Protokolüne dayanır.

Üçüncü katman bilişsel ve anlambilimseldir; mantıksal katmanın kullanıcılarının dünyası, bilgi dünyası, sosyal ağlar, tartışmalar ve dünya çapında gerçek zamanlı alışverişlerdir. Bu, en soyut katmandır, coğrafi konum belirlenmesi en zor olan yine de en az alakalı olmayan katmandır. Bu katmandan aşağıdakiler belirlenebilir: Dünyanın farklı bölümleri tarafından erişilen içeriklerin çoğunluğunun hangi dilde olduğu, Facebook'ta en çok "arkadaş" olan ülkeler, bir harekete, bir devlete veya bir kuruma karşı düzenlenen yanıltma haber kampanyalarının veya komploların kaynağı.

Dolayısıyla siber uzay, hem yerelleştirilebilir bir maddi gerçeklik hem de kavranması gereken soyut bir değişim alanı karmaşıktır. Bir dizi bilgisayar ağını (ve tabletleri, akıllı telefonları, vb.), insan ağlarını, veri ve bilgi akışlarını, birbiriyle bağlantılı ve ortak dili kullanan bilgisayar ağlarından akan her şeyi belirleyebilir. Nesnelerin İnterneti'nin gelişmesiyle birlikte, her türden daha fazla cihaz ağlara bağlanmakta ve mevcut veri kütlesi sürekli genişlemektedir. Kimin neden kullandığına bağlı olarak, siber uzay terimi, belirli bir kavramsal bulanıklıkta tamamen farklı bir gerçekliğe veya hayal gücüne işaret edebilir.

Siber uzay, terimin coğrafi anlamında, yani " bir insan grubunun yaşadığı ve kolektif mülkiyeti olarak kabul ettiği bir alan"[2] veya Devletler için " karasal alanın sınırları ile sınırlandırılmış olan ve üzerinde yetki ve yargı yetkisinin uygulandığı"[3] bir bölge değildir.

Siber uzay kelimesi, ilk olarak, 1984 yılında *Neuromancer* adlı romanında anlattığı Kanadalı-Amerikalı bilim kurgu yazarı *William Gibson*'ın çalışmasında ortaya çıkmış olup burada siber uzay, elektronik olarak oluşturulmuş, karakterlerinin bilgisayarları birbirine bağlayarak girdiği üç boyutlu "*sonsuz karmaşıklık*" alanıdır. Böylelikle, tüm insanlığın bilgisayar sistemlerinin kalbinde depolanan veri ve bilgilerin, İnternet kullanıcılarının nesiller boyu el koyacağı zihinsel bir temsilini sunmaktadır.

Bu temsil, Net'in öncülerinin konuşmalarına ve hayal gücüne nüfuz etmektedir. 1990 yılında, İnternet hala sadece birkaç milyon kullanıcısı olan bir kulüpken Elektronik Sınır Vakfı (Electronic Frontier Foundation-EFF) kurulmuştur. Tarihçi Frederick Jackson Turner'ın tezine göre Amerikan demokrasisini oluşturan öncü cepheye doğrudan referans gösteren bu vakıf, dijital dünyadaki özgürlüklerin savunulması için savaşmaktadır. Görevleri, 1960'ların ve 1970'lerin Kaliforniya kampüslerindeki karşı kültür atmosferinde, bir açıklığın ruhu olmak, ağın yaratıldığı ruhu yansıtmak, değişim ve ifade özgürlüğü ve İnternet mimarisinin tam kalbine giden öz yönetimdir. Ağ, denetimden kaçmak için merkezi olmayan bir şekilde tasarlanmıştır, böylece bilgi her zaman tıkanıklığı atlayabilecektir. Elektronik Sınır Vakfı(EFF)'nın kurucu üyesi olan John Perry Barlow, 1996 yılında, hükümetlerin kanunlarının ve egemenliğinin onlar için geçerli olmadığını ilan ettiği bir "siber uzay bağımsızlık bildirgesi" yayınlamıştır. O sırada inanılmaz

---

2 Y. Lacoste, ***De la* géopolitique aux paysages**, *Dictionnaire de la géographie*, Armand Colin. Paris, 2003, s.413
3 ibid

iyimserliğinden ötürü eleştirilirken, bunu "hepimiz yaşlanıp daha akıllı hale geldiğimiz"[4] için kabul ettiği söylenmektedir. Bununla birlikte, birçok bilgisayar korsanı, hâlâ bu ifadeyi tam anlamıyla kabul etmekte ve siber uzayın düzenlenmesine ilişkin olan devlet müdahalesi ile aktif olarak mücadele etmektedir.

Siber uzay terimi, 2000'lerin ortalarından itibaren, hükümetlerin konuşmalarında, tehditler içeren, kontrol edilecek, denetlenecek, fethedilecek, sınırları aşmanın ve egemenliğini yeniden onaylamanın gerekli olduğu bir bölgenin temsili gibi paradoksal bir şekilde yeniden ortaya çıkmaktadır. 2007 yılında Estonya'ya yapılan, kamu idaresini, bankaları ve diğer Estonya servislerini felç eden siber ataklar, bilgisayar ağlarına olan bağımlılığın devletler için neden olabileceği güvenlik açıkları konusunda gerçek bir farkındalık yaratmıştır. Ertesi yıl Gürcistan'a yapılan saldırılar, siber saldırıların silahlı bir çatışma bağlamında askeri güçleri tetikleyebileğini göstererek, o zamana kadar esasen uzmanların ve teknisyenlerin sahip olduğu endişenin siyasi ve stratejik alanlarına girişini doğrulamıştır. Bunun sonucunda siber uzay, jeopolitik bir sorun haline gelmiştir.

Siber uzay, bir güçler rekabeti meselesi, bir yüzleşme harekât alanı ve jeopolitik çatışmalarda müthiş bir silahtır. Siber uzayın geniş bir insan faaliyetleri yelpazesi için neden önemli olduğunu tam olarak anlamak için farklı tanımlamalar ve analizler yapmaya çalışacağız. Hem sivil hem de askeri sorulara yaklaşacağız çünkü bunlar, genellikle çeşitli ve birbiriyle bağlantılı doktrinlerde ve hükümet yayınlarında birlikte sunulmaktadır.

Kanada, Siber Güvenlik Stratejisinde siber uzayı, bütün insan faaliyetlerini etkileyen bir alan olarak tanımlamaktadır. Kanada'ya göre siber uzay:

---

4 F. Turner, **From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism**, University of Chicago Press, Chicago, 2010, s.218.

"*Bilgi teknolojisi sistemlerinden oluşan birbirine bağlı ağların oluşturduğu elektronik dünya ve bu ağlarda bulunan bilgilerdir. Siber uzay, fikir ve hizmet alışverişinde bulunan ve arkadaşlıklar kuran 1,7 milyardan fazla insanı birbirine bağlayan ortak bir maldır*."[5]

Bu tanım biraz muğlak yönüyle sınırlı olsa da, ilginçtir ki, tarihsel olarak oldukça barışçıl ve militarizme pek az yönelmiş bir aktör olan Kanada için, siber uzay her şeyden evvel, askeri bir alan olmadan önce bir alışveriş ve temas alanı olarak görünmektedir.

Aynı şekilde Birleşik Krallık'ın stratejisi de siber uzayı ticareti ve ekonomik büyümeyi teşvik eden bir alan olarak tanımlamaktadır. Bu nedenle stratejik bir askeri avantajdan çok, Birleşik Krallık'ın emperyal ve kapitalist tarihine özgü ticari bir çıkar olarak görülecektir.[6]

Siber uzayın önemi ile de ilgilenen *Ekonomik İşbirliği ve Kalkınma Örgütü* (OECD), İnternet dâhil olmak üzere siber uzayın belirli bileşenlerinin, ekonomik gelişme ve uluslararası sistemdeki aktörler arasındaki ilişkiler için hayati önem taşıdığını düşünmektedir. 2008'de İnternet Ekonomisinin geleceği için Seul Bildirisi'nde imzacı ülkeler, interneti ve siber uzayda bulunan teknolojileri, üzerindeki çok sayıda insani ve ekonomik faaliyetin olduğu, her yerde mevcut olan bir unsur düzeyine yükseltecek kadar ileri gittiler.[7]

Dolayısıyla, OECD açısından İnternet, ekonomik alışveriş için hayati bir alandır ve artık sadece askerler veya bilimsel ağlar arasında bilgi alışverişine izin veren bir teknolojik platform değildir:

---

5 *Stratégie de cybersécurité du gouvernement du Canada (Kanada Hükümeti'nin Siber Güvenlik Stratejisi)* 2010, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf E.T 27 Şubat, 2020

6 The United-Kingdom Government-Cabinet Office, **The UK Cyber Security Strategy***,* **Protecting and promo ting the UK in a digital world***,* London, 2011.

7 OECD, "The Seoul Declaration for the Future of the Internet Economy", **OECD Digital Economy Papers**, 2008, s.4-5

İnternet, ilk önce, telefon ağı üzerinden farklı bilgisayarları birbirine bağlamanın bir yolu olarak tasarlanmış, ancak şimdi dünyanın her yerinden milyarlarca kullanıcıyı taşınabilir veya sabit cihazlar aracılığıyla birbirine bağlamaktadır. Su, elektrik veya diğer hizmetlere erişimi olmayan kişiler cep telefonlarından İnternet'e erişebilmektedirler. İnternet kendi başına milyarlarca dolarlık bir endüstridir, ancak aynı zamanda dünya ekonomisinin çoğu için yaşamsal bir altyapıdır.[8]

Siber uzayı anlamanın ve tanımlamanın farklı yolları, uluslararası sistemin aktörlerinin stratejik çıkarları ve öncelikleriyle yakından bağlantılıdır. Her ne kadar Fransa ve Çin orada stratejik ve askeri bir önem görüyor gibi görünse de, Anglo-Sakson ülkeleri daha Protestan bir çizgide[9] görünmekte, siber uzayın işle ve genel olarak pazarla ilişkisine değer vermektedir. Buna rağmen İngiltere gibi siber uzayı bir özgürlük alanı olarak tanımlayan bir ülke bile Facebook ve diğer elektronik medyaya müdahale etmek için "yıllık özel birimler" oluşturmaya karar vermiştir.[10]

Bu görevdeşlik, çeşitli politikalarda ve teknik incelemelerde sunulan siber uzayın devlet vizyonlarında da görülebilir. Gerçekten de farklı kamu politikaları (Fransa, Amerika Birleşik Devletleri, Çin), siber uzayın stratejik yönünü diplomatik ve politik bir alan olarak vurgularsa, diğer ülkeler (Birleşik Krallık veya Kanada) özel aktörler arasındaki alışverişlere veya hatta siber uzayın ekonomik önemine daha fazla vurgu yapacaktır. Bu nedenle, yapılandırmacı bir analizde, siber uzaya verilen önemin ve onun içinde teşvik edilen faaliyetlerin, söz konusu farklı aktörlerin söylemlerine ve ilgi alanlarına göre

---

8OECD, **OECD internet economy outlook**, Paris, 2012. http://public.eblib.com/choice/publicfullrecord.aspx?p=1057623 (27/02/2020).

9 M.Web, **The Protestant Ethic and the Spirit of Capitalism**, Courier Corporation, 2012

10 MacAskill, Ewen, "British army creates team of Facebook warriors", **The Guardian**, *2015.* http://www.theguardian.com/uk-news/2015/jan/31/britisharmy-facebook-warriors-77th-brigade (27/02/2020)

değiştiği görülebilecektir. Bu, uluslararası ilişkilerde önemli bir etkiye sahip olabilir, çünkü güvenlik nesnesi, aktörlere göre değişiklik gösterebilir ve bunların tümü, siber uzayda gerçekleşen veya gerçekleşmeyen diğer tüm faaliyetler üzerinde önemli bir etkiye sahiptir. Örneğin, Birleşik Krallık, İnternette bulunan ekonomik sektörün bir güvenlik nesnesi olması gerektiğini düşünürse, bu faaliyet alanına yönelik herhangi bir saldırı, müdahaleye konu olabilir ve bu durumun, hem siber uzaydaki hem de bu alanın dışındaki diğer faaliyetler için sonuçları olabilir. Bu nedenle, tehdidin inşası ve uluslararası sistemde alınan önlemler, aktörlerin siber uzaydaki çeşitli faaliyetlere verdikleri öneme bağlı olarak değişebilmektedir.

Siber uzayın insan faaliyetinin diğer alanlarına bu şekilde etki etmesi, insan faaliyetlerinin maddesel ve maddesel olmayan boyutları arasında belirli bir karşılıklı bağımlılık yarattığı için önemlidir. Siber uzaydaki herhangi bir güvenlik açığı, ona bağlı olan faaliyetlerin seyri üzerinde doğrudan bir etkiye sahip olabilmektedir.

A. SİBER UZAYIN TEMEL KAVRAMLARI

Siber uzaydaki farklı kavramları keşfetmeden önce, öncelikle internetin ne olduğunu ve nasıl çalıştığını anlamak çok önemlidir. Sosyal bilimlerde, interneti; bilgisayarları ve diğer cihazları birbirine bağlayan uluslararası bir ağ olarak anlamaktayız. Çalışmamızın bu kısmında, internetin nasıl çalıştığını açıklamak istiyoruz; bu kısım, araştırma konumuz altında, çalışmak istediğimiz tüm alanları anlamamıza yardımcı olacaktır.

Bilgisayarınız hücresel veri veya herhangi bir Wi-Fi yönlendirici aracılığıyla internete bağlanabilir, ancak yine bir noktada cihazınız fiber optik kablo ağına bağlanacaktır. Örneğin bir video izliyorsanız, o video bir veri merkezinde tutulur. Daha açık olmak gerekirse, veri merkezi içinde bir katı hâl sürücüsünde (SSD) depolanır. Bu SSD,

sunucunun iç belleğine erişir. Sunucu, işi istediğiniz zaman videoyu veya saklanan diğer bilgileri size ulaştırmak olan ve bunu komuta eden bir hizmet makinesidir. Şimdiki çekişme, veri merkezinde depolanan verilerin, fiber optik kabloların karmaşık ağları üzerinden aynen cihazınıza nasıl aktarılacağı olacak. Bu zorluğu anlamak için, önemli bir kavram olan internet protokol adresini (IP Adresi) anlamamız gerekir. İster sunucu, ister bilgisayar veya cep telefonu olsun, internete bağlı her cihaz, yalnızca IP adresi olarak bilinen bir sayı dizisi tarafından tanınır. IP adresini, evinizi benzersiz bir şekilde tanımlayan ev adresiniz gibi düşünebilirsiniz. Size gönderilen herhangi bir mektup tam olarak size ulaşır çünkü benzersiz bir ev adresiniz vardır. Benzer şekilde, internet dünyasında IP adresi, tüm içeriğin hedeflerine ulaştığı bir teslimat adresi olarak çalışır. İnternet servis sağlayıcınız (İSS) cihazınızın IP adresine karar verecek ve İSS'nizin cep telefonunuza veya bilgisayarınıza verdiği IP adresini görebileceksiniz. Veri merkezindeki sunucunun da bir IP adresi vardır. Sunucu bir web sitesini depolar, böylece herhangi bir web sitesine yalnızca sunucunun IP adresini bilerek erişebilirsiniz. Ancak, bir kişinin bu kadar çok IP adresini hatırlaması zordur. Bu sorunu çözmek için, google.com, youtube.com ve diğerleri gibi, hatırlanması uzun sayı dizisinden daha kolay olan IP adreslerine karşılık gelen alan adları kullanılmaktadır. Dikkat edilmesi gereken bir diğer nokta da, bir sunucunun birkaç web sitesini saklama yeteneğine sahip olmasıdır ve sunucu birden fazla web sitesinden oluşuyorsa, bütün bu web sitelerine sunucunun IP adresiyle erişilemeyeceğidir. Bu gibi durumlarda, web sitesini benzersiz şekilde tanımlamak amacıyla ek bilgi parçaları, ana bilgisayar başlıkları kullanılır. Bununla birlikte, facebook.com veya youtube.com gibi dev web siteleri için tüm veri merkezi altyapısı, belirli web sitelerinin depolanmasına tahsis edilecektir. Aslında karmaşık fiber optik kablo ağı, internetin omurgasıdır. Işığı taşıyan bu fiber optik kablolar, bir yönlendiriciye bağlandıkları deniz tabanından kapınıza kadar

getirilmektedir. Yönlendirici bu ışık sinyallerini elektrik sinyallerine dönüştürmektedir. Daha sonra elektrik sinyallerini bilgisayarınıza iletmek için bir internet kablosu kullanılmaktadır. Bununla birlikte, internete mobil hücresel verilerinizi kullanarak erişiyorsanız, optik kablodan elektrik sinyalinin bir hücre kulesine gönderilmesi gerekmekte ve hücre kulesinden sinyal, elektromanyetik dalgalar şeklinde cep telefonunuza ulaşmaktadır.[11]

İnternet dünya çapında bir ağ olduğundan, IP adresi atamaları, alan adı kayıtları vb. gibi şeyleri yönetmek için bir organizasyona sahip olmak zorunlu hale gelmiş, bunların hepsi İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) adlı bir kurum tarafından yönetilmektedir.[12][13]

Yukarıdaki sinyal yolculuğunda, internet kullanımınızla neyi başarmak istediğinize bağlı olarak belirli bir komuta ulaşmak için birçok protokolün kullanılması gerekir. Siber uzayda kilit rol oynayan diğer kavramları incelerken göreceğimiz gibi; İnternetin iyi işleyişini tehlikeye atmayı yönetmek, bilgisayar bilimi alanında büyük miktarda bilgi gerektirmektedir.

Burada bir soru sorabiliriz: Siber uzay failler için neden bu kadar çekici? Bilgi toplumunda pek çok şey siber uzay yoluyla hızlı ve ucuz iletişime bağlıdır çünkü gittikçe daha fazla iş ve sosyal süreç oraya kaymaktadır. Bu gelişme, siber uzayı saldırganlar için giderek daha çekici hale getirmiştir. Siber uzay, potansiyel bir saldırgan için uygun olan bir

---

11 R. Shuler, "How does the Internet Work?", **Pomeroy IT Solution** 2002. https://web.stanford.edu/class/msande91si/wwwspr04/readings/week1/InternetWhitepaper.htm (6/03/2020).

12 ICCAN Politikasi https://www.icann.org/policy#what_is_policy E.T (6/03/2020)

13 M. Mueller, D. Thompson, "ICANN and INTELSAT: Global Communication Technologies and their Incorporation into International Regimes", In: Braman, S. (eds) The Emergent Global Information Policy Regime. International Political Economy Series. Palgrave Macmillan, London. 2004, s. 65

dizi özelliğe sahiptir, uzamsal mesafeler neredeyse hiç rol oynamamaktadır. Saldırgan, kendisini sahada acil bir riske maruz bırakmadan uzaktan hareket edebilir. Ayrıca, İnternet'teki birçok hizmet kasıtlı olarak açık olacak şekilde tasarlandığından, fail için özellikle İnternette çeşitli kamuflaj seçenekleri vardır. Özellikle siber suçlular, siber uzayda özel saldırı teknikleri yardımıyla çok sayıda farklı hedefe paralel olarak saldırmanın mümkün olmasından yararlanmaktadır. Böyle bir saldırı yalnızca hedeflerin küçük bir yüzdesinde başarılı olsa bile, genellikle önemli hasarlara yol açmaktadır. Ancak, bu konu söz konusu olduğunda, siber uzaydaki bu düşmanca eylemlerin güç kullanımına yol açıp açmayacağını ve buna göre uluslararası hukukun tepkisinin ne olacağını incelemek için devlet çıkarlarını hedef alan saldırılara odaklanacağız.

1. Siber Güvenlik

Siber güvenlik, Devletlerin ve kuruluşların insanlarının ve bilgisayar ekipmanlarının korunması için dijital dünyaya uygulanan yasaları, politikaları, cihazları ve güvenlik mekanizmalarını bir araya getiren bir alandır**.**

Hızla değişen teknolojiler, endüstrilerin iş yapma şeklini değiştirmektedir. Nesnelerin İnterneti, Bulut Bilişim, Otomasyon ve Yapay Zeka gibi gelişmekte olan teknolojiler, yeni, açık ve veriye dayalı otomatik iş modellerinin benimsenmesini ve benzeri görülmemiş sayıda değer yaratma fırsatının gerçekleştirilmesini mümkün kılmaktadır. Ancak bu değer garanti edilmemektedir. Teknoloji ilerledikçe, kuruluşların karşı karşıya olduğu siber risk seviyesi de artmaktadır. Aslında, çözümleyiciler küresel siber risklerin "*2020 yılında üç trilyon ABD doları olarak tahmin edilen bir ekonomik kayba neden olarak teknolojik yeniliğin hızını yavaşlatabileceğini*"[14] tahmin ediyor olsalar da ne yazık ki, teknolojilerin

14 J. M., Kaplan ve ark., **Beyond Cybersecurity: Protecting your Digital Business,** Hoboken, NJ: Wiley, 2015.

hızlı gelişimi ve ilgili siber riskler, kuruluşların uyarlanabilirliğini aşıyor gibi görünmektedir. Son on yılda siber güvenliğe yapılan önemli yatırımlara rağmen, tüm sektörlerdeki kuruluşlar, siber risk geçitlerinin arttığını görüyor.

ABD ve Kanada gibi ülkeler aynı siber güvenlik çerçeve modelini paylaşmaktadırlar.[15] Bu model yedi siber güvenlik kişiliğine odaklanmaktadır: Stratejist, Danışman, Savunmacı, İtfaiyeci, Bilgisayar korsanı, Bilim Adamı ve Dedektif.

Stratejist kişilik; siber güvenlik çabalarını yönetir, yönlendirir ve teşvik eder. Danışman kişilik; güvenli sistemlerin ve ağların tasarımı ve oluşturulması konusunda tavsiyelerde bulunur. Savunmacı kişilik; sistemler, veriler ve ağlar için güvenliği destekler, yönetir ve korur. İtfaiyeci kişilik; dahili sistemlere, verilere ve ağlara yönelik tehditleri tanımlar, analiz eder ve azaltır. Bilgisayar korsanı; siber güvenlik risklerini belirlemek ve azaltmak için özel tehdit algılama ve kasıtlı aldatma faaliyetleri gerçekleştirir. Bilim adamı; güvenlik duruşunu iyileştirmek için tehdit istihbaratı, kriptografik veriler ve güvenlik bilgilerinin özel analizini gerçekleştirir. Dedektif; siber güvenlik ihlallerini veya sistemlerin, ağların ve dijital kanıtların ihlallerini araştırır.[16]

Zamanla, robotik süreç otomasyonu, yapay zeka ve bulut bilişim gibi yıkıcı teknolojiler nedeniyle diğer kişiliklerin gelişmesi daha olasıdır. Savunucular için bu, otomasyon ve yapay zeka yoluyla gerçekleştirilecek denetim değerlendirmelerinin sayısında azalma ve bulutla yönetilen hizmetlere geçiş anlamına gelebilir.

---

15 W., Newhouse, S., Keith, B., Scribner, & G., Witte, *NICE Cybersecurity Workforce Framework*, 2017, çevrimci : https://www.nist.gov/itl/appliedcybersecurity/nice/resources/nice-cybersecurityworkforce-framework

16 ibid

Görüldüğü gibi, yukarıdaki açıklama, siber güvenlik çerçevesinin nasıl yapılandırılabileceğine dair yalnızca bir örnekten ibarettir. Bununla birlikte, diğer ülke ve kuruluşların siber tehditlerle başa çıkmaya ilişkin kendi yolları vardır: İlerleyen alt-başlıklarda göreceğimiz gibi, özellikle siber güvenliğin tarihsel arka planı ve yeni tehditler ortaya çıktıkça, bunlarla savaşmak için alınan siber güvenlik önlemleri de bu yollardandır. Sorulması gereken mantıksal soru, mevcut siber güvenlik çerçevelerinin seviyesinin yeni tehditlerle karşı karşıya olup olmadığıdır.

2. Siber Terörizm

Düzensiz savaşların (gerilla savaşı, şehir çatışması, ordunun yokluğu, sivil savaşçılar vb.) ortaya çıkması, çatışmaların ve savaş hukukunun algılanma biçiminde birçok değişikliğe yol açmıştır. Siber uzay teknolojilerinin batı toplumlarında yaygınlaşmasıyla birlikte, siber terör faaliyetlerinin gerçekleştirilmesinin uygun olup olmadığının sorgulanması akıllıca olacaktır.

Bir araştırmacı olan Kramer ve ekibi (*Milli Savunma Üniversitesi Teknoloji ve Ulusal Güvenlik Politikası Merkezi*), siber terörizmi klasik terör eylemlerinin karşılığı olarak, ancak siber uzayda tanımlamaktadır. Bir saldırının siber terörizm olarak nitelendirilebilmesi için, bu saldırının geleneksel saldırılarla benzer etkilere sahip olması gerekir (örneğin yıkım, ölüm, suyun kirlenmesi).

"*Siyasi, dini veya ideolojik hedefler peşinde koşan hükümetleri veya toplumları sindirmeyi veya zorlamayı amaçlayan bilgisayar tabanlı saldırı veya saldırı tehdidi... Saldırı, fiziksel terörizm eylemlerinden kaynaklanan korkuya benzer bir korku yaratmak için yeterince yıkıcı veya bozucu olmalıdır. Ölüm veya bedensel yaralanmaya, uzun süreli elektrik kesintilerine, uçak kazalarına, su kirlenmesine veya büyük ekonomi kayıplarına yol*

açan saldırılar örnek olabilir ... Temel olmayan hizmetleri kesintiye uğratan veya esasen maliyetli bir baş belası olan saldırı, siber terörizm olmayacaktır."[17]

Bir yandan bu saldırıların gerçekleştirilmesi nispeten ucuz olacak, diğer yandan saldırganları yalnızca fiziksel bir tepkiye maruz bırakacağı için ilginç olacaktır. Terörist gruplar, uzaktan büyük saldırılar gerçekleştirerek, Devlet olsun ya da olmasın hedeflerine büyük zarar verebilecektir. Bu büyük saldırılar, siber uzaydaki siber saldırıların kaynaklarını başarılı bir şekilde belirlemek karmaşık olduğundan, kendilerini saldırganlar için güvenli kılarken, durdurulması ve karşı koyulması zor olma avantajını sunacaktır.

Siber saldırılar veya fiziksel altyapıya (denizaltı kabloları, veri merkezi, fiber optik röle, vb.) yönelik saldırılar yoluyla siber uzaya kuvvet yansıtmak oldukça basit olduğu için, terörist grupların büyük ölçekli saldırılarını gözlemlememiş olmak şaşırtıcıdır. Her şeye rağmen, terörist grupların bilgisayar korsanlarına veya suç gruplarına dönüşme riski azdır. Bunun nedeni ise, motivasyonları farklı olan gruplar oldukları ve bunun terörist gruplar için bir sızma ve sabotaj riski oluşturacağı içindir. Ama aynı zamanda, çünkü bu iki aktör kategorisi faaliyetlerini sürdürebilmek için mevcut altyapılara ihtiyaç duymaktadır.

Bu konuda pek çok yazar, terörist grupların devletlere karşı büyük ölçekli siber saldırılar düzenlemeye hiç yönelmediği konusunda hemfikirdir. Bir yandan, bu gruplar siber uzay teknolojilerinin suç (para toplama, organize suç vb.) ve medyanın (siber etki, propaganda vb.) kullanımından çok daha fazla yararlanmaktadır. Öte yandan, kitlesel saldırılar durumunda, hedef devletin başka bir devleti terörist gruba destek sağlamakla suçlaması muhtemeldir. Bu, yalnızca terörist grupların müttefik devletinin güvenliğini değil,

17 F.D, Kramer ve ark., **Cyberpower and national Security**, 1st ed. Washington, D.C: *National Defense University Press:* Potomac Books, 2009, s.438

aynı zamanda geleneksel bir askeri müdahale durumunda grupların kendilerini de tehlikeye atacaktır.

Siber terörizm eylemlerinin sembolik önemini nitelendirmek de bizim için önemli görünmektedir. Büyük ölçüde kaydileştirilmiş doğaları gereği, bu terörizm biçimleri muhtemelen konvansiyonel bir terör saldırısı kadar hayal gücüne çarpmayacaktır. Büyük bir siber saldırı, aynı zamanda örgütsel kaos yaratan bir dizi ağı ve hizmeti bozmadığı sürece, siber saldırılara maruz kalmak, bir bombayı patlatmak veya halka açık bir yere girip rastgele insanlara bomba yerleştirmekten daha az çarpıcıdır. Bu anlamda, siber saldırılar, onları gerçekleştiren gruplar için bir şekilde terörist saldırıların cazibesine sahip olmayacaktır: Hayal gücüne saldırmak, bir korku iklimi aşılamak ve çeşitli aktörlerin siyasi kararlarını etkilemeye çalışmak. Dolayısıyla, ekonomiye veya Devletin hizmetlerine zarar veren bir saldırı durumunda bile, siber terörizm muhtemelen geleneksel saldırılarla aynı sembolik güce sahip olmayacaktır.[18]

Terörist gruplar şimdiye kadar, çoğunlukla interneti ve siber alanı propaganda için kullanmışlar (bazen çok etkili bir şekilde, IŞİD örneğinde olduğu gibi, bkz. Farwell 2014) ya da orduları veya temel altyapıyı hedeflememek için kendilerini organize etmek için kullanmışlardır. Ayrıca, belirli durumlarda (örneğin Kolombiya'daki uyuşturucu kaçakçıları grupları) bu grupların faaliyetlerini finanse etmek için suç amacıyla yoğun bir siber alan kullanımı mevcuttur.

Birkaç drone kaçırma örneği olsa da, stratejik ve askeri önem açısından hala oldukça küçüktür. Diğer vakalar, uluslararası sistemde (örneğin "Suriye Elektronik Ordusu") daha geniş bir siber güç uygulamasının bir parçası olarak hükümet, siyaset ve medya web

18 F.D, Kramer ve ark., 2009, s. 448

sitelerinin hacklendiğini bildirmiştir.[19] Bu izole saldırılar, onları kullanan ordulara karşı teknolojik araçların kullanılmasına ya da temel altyapı ağlarına veya ordulara karşı gerçek terör saldırılarına yol açmamıştır.[20] Sonuç olarak, bize öyle geliyor ki, bugün olduğu gibi terörist grupların, suç veya propaganda amacıyla siber uzaya yatırım yaparak kazanacakları daha çok şey vardır. Bu çalışma söz konusu olduğunda, devlet tarafından desteklendiği iddia edildiğinde klasik terörizme kıyasla siber uzayda devlet destekli terörizmin akla yatkınlığını ve mevcut uluslararası hukuk araçlarının bu konuda ne söyleyeceğini görmek için ikinci bölümde daha fazla araştırma yapılacaktır.

3. Siber Savaş

"Siber savaş" kavramı, bilgi ve iletişim teknolojilerini kullanarak veya onları hedef alarak siber uzayda yürütülen savaşlar için geçerlidir.[21] Akıllı şebekelere ve diğer İnternet tabanlı izleme ve kontrol sistemlerine artan bağımlılık; enerji, ulaşım ve savunma kaynaklarının özüne, devletleri ve sivil nüfusu yok etmek isteyenlerin ulaşabileceği anlamına gelmektedir.[22] Aslında, savaş siciline bağlanabilen düşmanca eylemler (siber uzay içinde veya aracılığıyla), muhtemelen stratejik kapsamlarını sınırlandırma etkisine sahip iki ana özelliğe sahiptir.

---

19 A. Peterson, "The Post just got hacked by the Syrian Electronic Army. Here's who they are", **The Washington Post**, 15 Ağustos 2013.
20 O. Kempf, "Le cyberterrorisme : un discours plus qu'une réalité**", Hérodote**, vol. 152-153, no 1, 2014, s. 82-97
21 S. Elliot, "Analysis on Defense and Cyberwarfare", **Infosec Island**, 8 Temmuz 2010.
22 E. Messmer, "Cyberattack Seen as Top Threat to Zap U.S. Power Grid", **Network World**, 2 Temmuz 2010. Ona göre, fiziksel bir saldırı ile ilişkilendirilebilecek koordine edilmiş siber saldırı tehdidi, Kuzey Amerika elektrik şebekesine yönelik en endişe verici "yüksek etkili ve düşük frekanslı" tehdit olarak görülüyor.

Bu özelliklerden ilki, siber uzaydaki savaş eyleminin gizliliği açısından da gizli bir boyuttan ilerlemektedir[23]: Ya ışık hızında taşınmaktadır ya da uzun süre yüklü bir virüs tarafından tetikleniyorsa, saldırının geldiği görülmemekte ya da gerçekten nereden geldiği hemen görülmemektedir. Dahası, saldırganlığın kaynağını bir siber karşı saldırı ile yok etmeyi içeren herhangi bir ön tepki, saldırganın kimliğini belirleyebilmek açısından neredeyse imkansız olmakla kalmamaktadır, aynı zamanda saldırgana ele geçirdiği güvenlik açığını belirleme ve düzeltme fırsatı verdikten sonra saldırganın saldırı kapasitesinin hemen güncelliğini yitirdiği ölçüde faydasız olmaktadır. Buna ek olarak, siber uzayın evrimi devam ederken bir yandan da siber saldırganların zaten var olan güvenlik açıkları yerine yeni güvenlik açıkları bulmak için çok aktif olması gerektiği gerçeği göz ardı edilmemelidir. Son olarak, siber savaşa özgü harekat modu, herhangi birinin potansiyelini düşürmek hatta tamamen mahvetmek veya bu silahların hedeflediği güvenlik açıklarını ortadan kaldırma imkânı sunmak dışında, yaptıkları silahları caydırıcı amaçlarla keşfetmesini de yasaklamaktadır.[24]

İkinci özellik, karmaşık sistemlere nüfuz edebilen ve büyük hasarlara neden olabilecek gerçek keskin siber silahlar oluşturmak için gereken çok yüksek teknikte yatmaktadır.[25] Bu gerçeklik, bilgisayar teknolojilerinde ustalaşabilen ülkelerin kendileri için hayati öneme sahip sistemleri sağlamak adına çalıştıkları sürekli artan koruma seviyesinin karşılığıdır. Başka bir deyişle, siber uzayın üst katmanının büyük ölçüde açık olan kısmına saldırılar gerçekleştirmek çok zor görünmese de ("tüketici" sitelerinin sökülmesi, DoS veya Hizmet engelleme saldırısı); sonuçları yıkıcı olmaktan çok utanç verici olan saldırılar, karmaşık bir

23 J. Tournier, "*Les Deux Phases De La Cyberguerre",* **Annuaire Français de Relations Internationales,** Vol. XVII, Université Panthéon-Assas Centre Thucydide, 2016, s.643-644.
24 J. Tournier, 2016
25 J. Tournier, 2016

sistemde büyük hasara neden olabilecek bir saldırı gerçekleştirme olasılığı, çok yüksek düzeyde ve uzun vadeli bir uzman hazırlığı gerektirmektedir.

Bu nedenle, bu tür silahların üretimi için çok ağır bir yatırım ön şarttır; kullanımı genellikle belirli bir hedefle sınırlı olan ve tek bir kullanıma adanmış olan ve yayılmanın ve kirlenmenin ikincil etkilerine ilişkin mutlak bir garanti sunmayan uygulamanın doğal sonucu olabilir. Sonuç olarak, aktif ve etkili siber silahlar için önemli bir kapasite geliştirmek amacıyla, insan kaynakları da dahil olmak üzere kaynakların uygun potansiyelini yalnızca gelişmiş ülkeler hizalayabilecek gibi görünmektedir. Bir bakıma, bu ülkeler, genel işleyişlerinin bilgi sistemlerine karşı giderek artan bağımlılığı göz önüne alındığında siber saldırı riskleri sorunuyla en çok ilgilenen ülkelerdir.

Siber uzaydaki kritik altyapıya yönelik saldırılara karşı savunmasızlık, BİT'ye bağımlılıkla birlikte artmaktadır. Tam olarak "siber savaş" terimi hala tanımlanmamış olsa bile, son on yılda BT altyapılarına ve İnternet hizmetlerine yönelik şiddet içeren saldırılar, siber uzaydaki bir çatışmanın biçimini ve boyutunu göstermektedir. Gürcistan, Estonya, Güney Kore ve Amerika Birleşik Devletleri'ndeki saldırılar siber savaşla ilişkilendirilmiştir. Brezilya'da çok sayıda elektrik kesintisi siber saldırılardan sorumlu tutulmuş ve 2008'de bilgisayar korsanları hükümetin web sitesine girmiş ve bir haftadan fazla kontrol etmişlerdir. Yukarıda bahsedilen ikilik aslında, siber uzayda hangi önlemlerin düşmanca eylemi ölçtüğünün, zorunlu olarak "güç kullanımına" bağlı bir savaşı başlatan faktör olabileceğini bilme sorusunu gündeme getiriyor. İkinci bölümde buna geri döneceğiz, ancak ondan önce, bazı akademisyenler tarafından siber savaş statüsü kazanmış, halihazırda tamamlanmış siber operasyon örneklerinden bahsetmek gerekiyor.

İlk siber savaş eylemi olarak kabul edilen şeyi ilişkilendirmek için, Doğu Avrupa'da 2007'ye geri dönmek gerekmektedir. Estonya hükümeti, bir Sovyet askerinin heykeli olan Bronz Asker'den kurtulmaya karar vermiştir. İşgalin sembolü olarak görülen eser, başkent Tallinn'in merkezinden kaldırılmıştır. Bununla birlikte, bu karar ülkedeki Rusça konuşan azınlık tarafından kabul görmemiş ve daha sonra başkentte yapılacak olan isyanları tetiklemiştir. Yapılan isyanları da ardından hızla gelen, ülke çapındaki hizmetleri engellemek amacıyla yapılan saldırılar takip etmiştir.[26] Bankalar, medya, yönetimler, bazen birkaç günlüğüne olmak üzere, her şey kapalı kalmıştır. Bir dizi kanıt, daha sonra başka bir ülkeye büyük ölçekli bir bilgisayar saldırısı gerçekleştiren ilk ülke olan Rus hükümetini hızla tespit etmiştir.[27] Ancak bu tür saldırı, birçok bilgisayar korsanı tarafından kullanılan oldukça basit bir saldırıdır. Sunucuların bir süre çevrimdışı olmasına izin vermekte, ancak kalıcı hasara neden olmamaktadır.

Siber savaşa iki yıl sonra bir geri dönüş yapılmış, bu seferki saldırı, doğrudan fiziksel kurulumları etkilemiştir. 2009'da ülkenin nükleer programını yavaşlatmak için İran'daki Natanz uranyum rafinerisinin bilgisayarlarına Stuxnet adlı bir virüs yerleştirilmiştir.[28] Bu bilgisayar kurdu inanılmaz derecede karmaşıktır. Santrifüjlerin parametrelerini aşırı ısınmak ve kullanılamaz hale getirmek için ince bir şekilde değiştirmektedir.[29] Bush

---

26 D. McGuinness, "*How a Cyber-attack Transformed Estonia",* **BBC News**, 27 Nisan 2017. https://www.bbc.com/news/39655415 E.T (03/05/2020).

27 R. Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", **Cooperative Cyber Defence Centre of Excellence**, 2008, https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html

28 W. Broad, J. Markoff, ve D. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", **New York Times,** 15 Ocak 2011.

29 J. Benillouche, "Israël a lancé une attaque électronique contre l'Iran", **SLATE,** 26 Eylül 2010. http://www.slate.fr/story/27763/israel-attaque-electronique-iran erişim tarih 3 Mayıs 2020.

yönetimi altında İsrail'in yardımıyla NSA tarafından başlatılan, daha sonra Obama[30] döneminde devam eden programın birkaç yıl sürdüğü ve bin santrifüjü kapattığı söylenmektedir.

Sonraki yıllarda özellikle İran ve Kuzey Kore büyük çaplı siber saldırılarla öne çıkmıştır. İran, bir Suudi petrol şirketine[31] ve bir Las Vegas kumarhanesine[32] saldırmıştır. Bu arada Kuzey Kore, Sony Pictures[33] sunucularına girmiştir. Ancak, o zamandan beri en çok dikkat çeken bilgisayar korsanları, her şeyi başlatanlar, Ruslar olmuştur. En çok duyurulan eylemleri, şüphesiz, Hillary Clinton'ın kampanyasının belgelerini çalarak ve büyük bir dezenformasyon kampanyası yürüterek Amerikan başkanlık kampanyasını etkileme girişimleridir.[34] Ancak bu manevralar, Rusya ve Ukrayna arasındaki çatışmanın Donbass çevresinde başladığı 2014 yılından bu yana, Rusya'nın Ukrayna'ya yönelttiği saldırılara kıyasla hiçbir şey değildir.

Ukrayna, Ruslar için dijital silahlarını test edecekleri bir eğitim alanı haline gelmiştir. Kiev neredeyse her gün her tür saldırıya maruz kalmaktadır[35]: Yönetimler, işletmeler,

---

30 D. E. Sanger, "*Obama Order Sped Up Wave of Cyberattacks Against Iran"*, **New York Times,** 1 Haziran 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html erişim tarih 3 Mayıs 2020.

31 N. Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back", **New York Times**, 23 Ekim 2012

32 B. Elgin & M. Riley, "Sheldon Adelson's Las Vegas Sands Corp. was hit with a security breach in February. Is this the next frontier of cyberwarfare?", **Bloomberg,** 12 Aralık 2014. Çevrimci: https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas erişim tarih 5 Mayıs 2020.

33 M. Untersinger, "Les Etats-Unis inculpent un Nord-Coréen d'opérations de piratage sans précédent", **Le Monde**, 6 Eylül 2018, available https://www.lemonde.fr/pixels/article/2018/09/06/les-etats-unis-accusent-un-nord-coreen-d-etre-derriere-le-piratage-de-sony-pictures-et-wannacry_5351390_4408996.html

34 V. Lysenko& C. Brooks, "Russian information troops, disinformation, and democracy*"*, **First Monday**, vol. 23, 5 Mayıs 2018

35 M. Untersinger*, "*L'Ukraine, cible préférée des hackeurs russes"*,* **Le Monde**, 4 Nisan 2019*,* https://www.lemonde.fr/international/article/2019/04/04/l-ukraine-cible-preferee-des-hackeurs-russes_5445462_3210.html

bankalar, altyapı... Rusya hiçbir şeyden kaçınmamaktadır. Bilgisayar korsanları, elektrik şebekesine dokunarak büyük kesintilere neden olmuştur. Demir yolu ağı, yoğun sezonda saldırıya uğrayarak rezervasyonların kaydedilmesini engellemiştir. Bu, gerçek bir dijital yıpranma savaşıdır. Rusya, Ukrayna'ya karşı tarihin en iddialı bilgisayar saldırılarından biri olan NotPetya'yı[36] Haziran 2017'de başlatmıştır. Virüs bir "silici" dir, yani virüs bulaşmış cihazlardaki verileri silmektedir. Anında ülke bilgisayarlarının% 10'una yayılmış, ardından bölge dışına çıkmış ve dünyanın en büyük denizcilik şirketi olan Maersk dahil binlerce işletmeyi etkilemiştir. Beyaz Saray'a göre toplam sonuç on milyar dolar zarar olmuştur.[37]

Dünyanın dört bir yanındaki ülkeler çok eski zamanlardan beri birbirleriyle savaş halindedirler. Bu ya da bu türden eylemlerin tepki olarak neye yol açacağı bu nedenle bilinmekte, hatta kodlanmıştır. Siber savaş ise yenidir. Kırmızı çizgilerin gerçekte nereye yerleştirildiğini kimse bilmemekte ve hassas altyapılara saldırarak öldürme yeteneğine sahip bir kötü amaçlı yazılım olan Triton'un ortaya çıkması bu konuda yeni sorular ortaya çıkarmaktadır. Siber casusluk ve potansiyel hedeflerin tanınması savaş eylemleri olarak kabul edilir mi? Teminat hasarı saldırganlık mıdır? Sınırları belirlemek ve eylemlerini ve tepkilerini olabildiğince çabuk tartmak uluslara kalmıştır. Yine bu, ikinci bölümde dikkatlice inceleyeceğimiz bir tartışmadır.

4. Siber Saldırı

Eski FBI Direktörü (2001-2013) Robert Mueller bir keresinde şöyle demiştir: "*Sadece iki tür şirket olduğuna ikna oldum: Hacklenmiş olanlar ve olacak olanlar*".[38] Ancak, tüm

36 A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", **WIRED,** 22 Ağustos 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, Erişim Tarih 3 Mayıs 2020.
37 A. Greenberg, 2018
38 Robert S. Mueller III, Director of Federal Bureau of Investigation, *RSA Cyber Security Conference*, San Francisco, CA 1 Mart2012.

siber saldırılar bir siber savaşla sonuçlanmamaktadır. Bu nedenle siber saldırı kavramını incelemek gerekmektedir. Bilgi Teknolojisi Sistemleri (BT Sistemleri) günümüzde nadiren tek başına kullanılmaktadır, genellikle küresel ağa bağlıdır. BT sistemleri arasındaki iletişim genellikle yerel ve küresel ağlar aracılığıyla, örneğin İnternet veya mobil radyo ağları aracılığıyla gerçekleşir. Sürekli olarak bir veri ağına bağlı olmayan neredeyse tüm bilgisayarlar, örneğin yeni veri stokları veya yeni program sürümleri veri ortamı kullanılarak içe aktarıldığında zaman zaman yeni bilgiler sağlanır. Daha önce bahsettiğimiz gibi, küresel olarak iletişim kuran bu BT sistemlerinin tamamına siber uzay denilmektedir. Giderek daha fazla BT iletişim ilişkisinin kaydığı İnternet, siber alanın önemli bir parçasıdır. Bununla birlikte, diğer birçok ağ yapısı da dünya çapında yaygın olarak kullanılmaktadır. Bununla birlikte, küresel ağ olasılıkları da failler tarafından zararlı faaliyetler için kötüye kullanılmaktadır. Siber uzay birincil saldırı aracı olarak kullanılıyorsa veya kendisi bir saldırının hedefi ise bir siber saldırıdan söz edilir.[39] Çok sayıda farklı saldırı hedefi ve olası saldırı yöntemlerine rağmen, bir siber saldırının ardındaki motivasyon genellikle paraya, bilgi toplamaya, sabotaja, siyasi çıkarları etkilemeye veya savunmaya kadar dayanabilmektedir.[40]

Siber uzayda kasıtlı olarak hareket eden saldırganlar aşağıdaki gruplara[41] ayrılabilir:

- **Siber Aktivistler**: Politik, sosyal, ekonomik veya teknik bir kötü yönetime dikkat çekmek veya bu konudaki bir talebi ("hacktivizm") güçlendirmek için

---

Çevrimci: https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

39 F. Vince ve ark., *Cyber Attacks: Prevention and Proactive Responses*, Practical Law Publishing Limited and Practical law Company, 2011, s. 1.

40 Cyberattack definition, "what does cyberattack mean?" **Techopedia**. http://www.techopedia.com/definition/24748/cyberattack , erişim tarih 5 Mayıs 2020.

41 *Types of Cyber-attackers*, Çevrimci : https://www.javatpoint.com/types-of-cyber-attackers erişim tarih 5 Mayıs 2020.

siber saldırı kullanan saldırganlardır. Saldırının arkasındaki motivasyon etkilemektedir. Bir siber saldırının neden olduğu hasar kabul edilmekte veya daha fazla dikkat çekmeye zorlanmaktadır. Sosyal konulara odaklanan bir grup hacker, sözde etik korsanlardır (iyi niyetli bilgisayar korsanları).

- **Siber Suçlular**: Siber suçluların motivasyonu, bilgi teknolojisini kullanarak yasa dışı olarak para kazanmaktır. Yelpazesi, organize siber suçtan çok az hasarla basit suça kadar uzanmaktadır.
- **Siber Alandaki Ekonomik Casuslar:** İnternetin avantajları casuslar için yeni fırsatlar yaratmaktadır. Endüstriyel casusluk ve rekabetçi casusluk mali çıkarlara hizmet etmektedir. Rakipler ve ürünleri hakkında dahili bilgiler, küresel rekabette parasal faydalar sağlamaktadır.
- **Siber Uzayda Devlet İstihbarat Servisleri**: Endüstriyel casusluğun aksine, devlet istihbarat servislerinin siber saldırıları öncelikle mali çıkarlara hizmet etmeyip bilgi ve etki toplamaya hizmet etmektedir.
- **Siber Savaşta Devlet Aktörleri**: Askeri sektörde siber uzay, artık kara, deniz, hava ve uzay gibi klasik askeri alanların yanında bir başka önemli alan olarak görülmektedir.
- **Siber Teröristler**[42]: Teröristler, farklı hedeflere saldırmak için devlet aktörleri ve suçlular gibi siber saldırıları kullanabilir, böylece ideolojilerini yayabilir ve etkilerini artırabilirler.

42 S. M. Furnell & M. J. Warren, *Computer hacking and cyber terrorism: the real threats in the new millennium?,* 23 Mart 1999: https://www.sciencedirect.com/science/article/pii/S0167404899800066 erişim tarih 5 Mayıs 2020

- **Script Kiddies**[43]: Script Kiddies grubu, pratikte beceri ve bilgiyi test etmek için siber saldırılar gerçekleştirir. Hiçbir mali çıkar gözetilmemektedir. Hedeflerin seçimi spesifik değildir ve çoğu durumda yalnızca koruma düzeyine bağlıdır.

Bu fail grupları temelde motivasyonları, hedefleri ve kaynakları açısından farklılık göstermektedir. Teknik düzeyde ise, belirli bir siber saldırının arkasında hangi fail grubunun olduğunu doğrudan belirlemek her zaman mümkün değildir.

Yukarıdaki paragraflarda saldırganlardan bahsedilmektedir ancak siber saldırıların türleri (türlerin aksine, bu alt bölümden sonra doğrudan inceleyeceğimiz konu) nelerdir? Siber saldırılar genellikle saldırının amacına göre, yani saldırganların başlatılan hedefler üzerinde sahip olmak istedikleri etkiye göre bu doğrultuda; üç[44] grupta özetlenebilir:

- **Gizliliğe Yönelik Saldırılar:** Failler, örneğin bir radyo ağını dinleyerek veya silinen bilgileri kurtararak gizli bilgileri gözetlemeye çalışabilmektedir.
- **Bütünlüğe Yönelik Saldırılar**: Bilgi, yazılım veya arayüzler üzerindeki manipülasyonlar birçok siber saldırıda önemli bir rol oynamaktadır.
- **Kullanılabilirliğe Yönelik Saldırılar**: Failler, örneğin dağıtılmış hizmet engelleme saldırıları (DDoS saldırıları) yoluyla bilgileri veya BT hizmetlerini sabote etmeye çalışabilmektedir.

43 P. Putman, *Script Kiddie: Unskilled Amateur or Dangerous Hackers?, United States Cybersecurity Magazine, çevrimci:* https://www.uscybersecurity.net/script-kiddie/ erişim tarih 5 Mayıs 2020.

44 A. Ghahrai, "*Confidentiality, Integrity and Availability*", 24 Hazıran 2019. https://devqa.io/confidentiality-integrity-availability/ erişim tarih 5 Mayıs 2020

Burada, siber saldırıların genellikle birkaç saldırı adımı içerdiğine ve bu adımların farklı amaçlara sahip olabileceğine dikkat edilmelidir[45]. Bir casus yazılım programı aracılığıyla gerçekleştirilen bir siber saldırı, örneğin, en azından kötü amaçlı yazılım programının kurulumunu (bütünlüğe saldırı) ve gerçek bilgi akışını (gizliliğe yönelik saldırı) içermektedir. Saldırının amacına ek olarak, siber saldırılar, hedefli saldırılar (bir hedef veya birkaç seçilmiş hedef) veya büyük ölçekli saldırılar (mümkün olduğunca çok sayıda keyfi hedef) olup olmadıklarına göre de farklılaştırılabilmektedir. Bu iki tür saldırı, fail için belirli avantaj ve dezavantajlarla ilişkilendirilir. Avantajı, saldırının başarıya götürme olasılığının daha yüksek olmasıdır. Dezavantaj olarak ise; bu tür büyük ölçekli saldırılar genellikle daha belirgindir ve bu nedenle zamanında karşı önlemleri tetiklemektedir.[46]

Anlamamız gereken bir diğer önemli konu da siber saldırıların neden olduğu zararın boyutudur. Siber alandaki tipik hedefler; bilgi, BT hizmetleri ve BT sistemleridir. Siber saldırıların neden olabileceği olası hasar, bu hedeflerin vatandaşlar, kurumlar ve toplum için değerine bağlıdır.

Sıradan insanlar için, siber saldırılar sonucunda önemli mali kayıplara uğrama riski vardır. İnternet ödeme süreçlerini veya İnternet bankacılığını kurcalamak, paranın failin hesaplarına girmesine veya kurbanın hesabının silinmesine neden olabilmektedir. Endüstriyel casusluk ve rekabetçi casusluk, yenilikçi şirketler için özel bir risktir.[47] Örneğin, ürün stratejisi veya araştırma ve geliştirme alanlarından gelen gizli bilgilerin çalınması, bir

---

45 Mindcore, *Types of Cybersecurity Threaths and How they Will Impact your Business*, 1 Mayıs 2019, çevrimci: https://mind-core.com/types-of-cyber-security-threats-and-how-they-will-impact-your-business/ erişim tarih 5 Mayıs 2020.

46 W. Chen, Y. Liu and Y. Guan, "*Cardinality change-based early detection of large-scale cyber-attacks*," 2013 **Proceedings IEEE INFOCOM,** Turin, 2013, ss. 1788-1796.

47 S. Stephens, "Why companies underestimate the physical damage of cyber attacks", **AIRMIC**, *1 Mart 2016.* https://www.airmic.com/news-story/why-companies-underestimate-physical-damage-cyber-attacks e.t 5 Mayıs 2020.

rakibe belirleyici avantaj sağlayabilir. Bir ihale sürecindeki teklif hesaplamaları veya satış bilgileri de rakiplerin ilgisini çeker. Siber saldırılar da şantaj şirketlerinde rol oynayabilir. Örneğin, failler gizli bilgileri yayınlamakla tehdit edebilir veya şirketin müşterilerine veya ortaklarına daha uzun süre sunduğu önemli BT hizmetlerini bozabilir.

Çok önemli (kritik) altyapıların kullanılabilirliğine yönelik saldırıların gerçekleşmesi durumunda özellikle yüksek bir hasar potansiyeli vardır.[48] Kritik altyapılar, devlet toplumu için büyük öneme sahip kuruluşlar ve kurumlardır; bunların başarısızlığı veya bozulması sürdürülebilir arz tıkanıklıklarına, kamu güvenliğinde önemli kesintilere veya diğer dramatik sonuçlara yol açacaktır.

Olası hasarı değerlendirirken, siber saldırıların genellikle geleneksel bilgi teknolojisine (web sunucuları veya veritabanları) yönelik olduğu, ancak endüstriyel süreç kontrol otomasyonu ve teknolojisi ile dijital ölçümlerin de siber saldırılardan etkilendiği unutulmamalıdır. Bu tür saldırılar, bir endüstriyel tesisin güvenliği üzerinde doğrudan bir etkiye sahip olabilmektedir. Örneğin siber savaşla ilgili bir önceki bölümde tartıştığımız "Stuxnet" olayı bunun sadece teorik bir senaryo olmadığını göstermiştir.[49]

Siber saldırıları başarılı bir şekilde gerçekleştirmek için failler öncelikle aşağıdaki güvenlik açığı türlerinden yararlanmaktadır: Yazılım açıkları, tasarım açıkları, yapılandırma açıkları ve insan hatası. Prensip olarak, günümüzün bilgi işlem karmaşıklığı

48 CISCO, "Critical Infrastructure Cyberattacks a Greater Concern than Enterprise Data Breaches", **Security Magazine**, 26 Mart 2020, https://www.securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-concern-than-enterprise-data-breaches e.t 5 Mayıs 2020.

49 K. Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory", **Information Security Journal: A Global Perspective**, vol. 18, 2009, ss.1–7,

göz önüne alındığında bu tür zayıflıkların[50] tümü tamamen önlenemeyecektir. Genel olarak, siber saldırıların başarısı öncelikle aşağıdaki faktörler tarafından desteklenmektedir:[51]

- Çoğu durumda, failler teknik zayıflıkları kamuya açıklanmadan önce ("sıfır gün") istismar etmektedirler. Bu tür yeni güvenlik açıklarından (istismarlardan) yararlanan programlar, yer altı pazarlarında işlem görmektedir.
- Bir güvenlik açığının keşfedilmesi ile bir yamanın yayımlanması arasındaki dönemde, etkilenen birçok sistem korumasızdır. Geçici çözümler genellikle rahatsız edicidir veya kurumsal nedenlerle uygulanması zordur.
- Birçok kurumda, yeni yayınlanan güncellemeler ve yamalar ya günler, haftalar sonra içe aktarılmakta ya da hiç içe aktarılmamaktadır. Bu, örneğin kaynak eksikliğinden, organizasyonel sorunlardan veya farklı bileşenler arasındaki uyumsuzluklardan kaynaklanabilmektedir.
- Bilgi teknolojisi ve ilgili güvenlik unsurları bugün o kadar karmaşıktır ki, birçok kullanıcı farkındalık ve eğitime rağmen güvenlik kurallarına uymaktan bunalmıştır.

5. Siber Saldırı Türleri

En son IBM raporuna göre, 2019'da dünyadaki her işletmenin % 28'lik bir siber saldırıya maruz kalma olasılığı vardı. Ek olarak, bir veri ihlalinin ortalama maliyeti 3,92

50 J. Fruhlinger, *"What is a cyber-attack? Recent examples show disturbing trends"*, CSO Online, 27 February 2020. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html e.t. 5 Mayıs 2020
51 J. Fruhlinger, 2020

milyon dolardı.[52] Siber saldırı; bilgisayar sistemlerini, altyapıları, bilgisayar ağlarını veya kişisel bilgi işlem cihazlarını hedef alan her tür saldırgan eylemden oluşmaktadır. Siber suçlular, verileri veya bilgi sistemlerini çalmak, değiştirmek veya yok etmek için çeşitli yöntemler kullanmaktadır. Günümüzde siber suçlular, tespit edilmekten kaçınmak için çeşitli karmaşık teknikler kullanmakta ve çoğu zaman tehditleri şifrelenmektedir. Çoğu durumda, geleneksel antivirüs çözümlerinin bilmediği yeni kötü amaçlı yazılım çeşitlerini kullanmaktadırlar. İşte birçok bilgi sisteminin karşılaşabileceği en yaygın beş siber saldırı:

a. Hizmet Engelleme (DoS) veya Dağıtılmış Hizmet Engelleme (DDoS) Saldırısı

Hizmet reddi saldırısı, bir sistemin kaynaklarını aşırı yüklemektedir. Maksimum kapasitesinin ötesinde taleplerle doldurmaktadır. Sonuç olarak, sistem artık yetkili kullanıcılardan gelen servis taleplerine cevap verememektedir.

Hizmet engellemenin tatmini, bazıları için isteklendirme kaynağı olmaktadır. Bununla birlikte, saldırıya uğrayan kaynak bir rakibe aitse, saldırgan için avantaj oldukça gerçek olabilmektedir. Bununla birlikte, genellikle bir DoS saldırısının amacı, aynı anda başka bir saldırının başlatılabilmesi için bir sistemi çevrimdışı duruma getirmektir. DoS saldırısı, paralel olarak gerçekleşen gerçek saldırıyı maskelemek için kullanılmaktadır.[53]

b. Ortadaki Adam

İki taraf arasındaki iletişimi, ikisi de aralarındaki iletişim kanalının tehlikeye girdiğinden şüphelenmeden durdurmayı amaçlayan bir saldırıdır.[54] En yaygın kanal,

52 IBM, "How much would a data breach cost your business", 2019, Cost of a Data Breach Report https://www.ibm.com/security/data-breach e.t, 11 Mayıs 2020.
53 ibid
54 D. Swinhoe, "What is a man-in-the-middle attack? How MitM attacks work and how to prevent them", **CSO Online,** 13 Şubat 2019.

ortalama bir İnternet kullanıcısının İnternet bağlantısıdır. Saldırganın ilk önce bir kurbandan diğerine mesajları gözlemleyip yakalayabilmesi gerekmektedir. Bilgisayar korsanları, güvenli bir veriyi hedeflemek ve suç işlemek için e-postayı, internet tarama geçmişini ve sosyal medyayı ele geçirirler. Kullanıcıların korumalarını istemeden düşürmelerini ve savunma hattını açmalarını gerektiren e-dolandırıcılık saldırısından (*phishing attack*) farklı olarak, ortadaki adam adı verilen saldırı pasif bir siber saldırıdır. Onlar farkında olmadan yapılmaktadır.[55]

c. E-dolandırıcılık ve Mızraklı (Hedef Odaklı) Kimlik Ağı

E-dolandırıcılık, güvenilir kaynaklardan geliyormuş gibi görünen e-postalar göndermekten oluşan bir saldırıdır. Amaç, kişisel bilgi almak veya kullanıcıları bir şeyler yapmaları için etkilemektir.

Burada, e-postanın "Kimden" bölümündeki bilgiler, tanıdığınız birinden gelmiş gibi görünmektedir; göderen, yönetiminiz veya bir iş ortağınız gibi bile görünebilmektedir. Siber suçlular, hikâyelerine güvenilirlik kazandırmak için genellikle web sitesi kopyalamayı kullanmaktadır. Kişiyi tanımlamak için kullanılan bilgiler (PII) veya oturum açma kimlik bilgileri sağlayarak sizi aldatmak için meşru web sitelerini kopyalamaktadırlar.

d. Kaçak İndirme

Kaçak indirme saldırıları, kötü amaçlı yazılımları yaymanın yaygın bir yöntemidir. Siber suçlular güvenli olmayan web siteleri aramaktadırlar. Kaçak indirmeler, bir web

---

https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html E.T 11 May 2020.

55 D. Swinhoe, 2019.

sitesini ziyaret ederken veya bir e-posta iletisini veya bağlamsal pencereyi görüntülerken gerçekleşebilmektedir.[56]

Diğer birçok siber güvenlik saldırısı türünün aksine, bir kaçak indirme saldırısı, kullanıcının saldırıyı etkinleştirmesini gerektirmez. Dolayısıyla, bir düğmeyi tıklamamış veya kötü amaçlı bir eki açmamış olsanız bile, bilgisayarınıza yine de virüs bulaşabilir.[57]

e. Parola Kırma Saldırıları

Şifreler, bir bilgi sisteminin kullanıcılarının kimliğini doğrulamak için kullanılan en yaygın mekanizmadır. Bu nedenle şifrelerin elde edilmesi yaygın ve etkili bir saldırı yaklaşımıdır. Siber suçlular, birinin şifresine çeşitli yollarla erişebilmektedir. Genellikle kişinin ofisine bakmak, şifrelenmemiş parolaları elde etmek için ağ bağlantısını kurcalamak, sosyal mühendisliği kullanmak, bir şifre veri tabanına erişmek veya doğrudan tahmin etmek yeterli olmaktadır. Son yaklaşım rastgele veya sistematik olarak yapılabilir.[58]Bir parolayı kaba kuvvet yaklaşımı kullanarak tahmin etmek, birçok parolayı denemek ve bunun işe yarayacağını ummak anlamına gelmektedir. Siber suçlular daha sonra kişinin adı, işi, hobileri, akrabaları veya benzeri öğelerle bağlantılı şifreleri deneyerek belirli bir mantık uygulamaktadır.

Yukarıdaki saldırıların çoğu ve diğer türlü saldırılar, amaçlarına ulaşmak için kötü amaçlı yazılımlar kullandığından, bu alt bölümde kötü amaçlı yazılımdan bahsetmek gerekmektedir. Kötü amaçlı yazılımlar, özellikle Truva atı virüsleri, fidye yazılımı, virüsler,

---

56 J. Lake, "What is a drive-by download and how can it infect your computer?", **Comparitech**, 13 Aralık 2019. https://www.comparitech.com/blog/information-security/drive-by-download/ E.T 11 Mayıs 2020.

57 J. Lake, 2019

58 B. Vigliarolo, "Brute force and dictionary attacks: A cheat sheet", **Tech Republic**, 17 Aralık 2018. URL: https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/ E.T. 11 Mayıs 2020.

yazılım solucanları veya bankacılık kötü amaçlı yazılımları olarak bilinen her türden kötü amaçlı yazılımın bir koleksiyonudur. Kısacası, bunların bir çeşit silah olduğunu söylemek, pek de yanıltıcı olmaz. Bununla birlikte, kötü amaçlı yazılım teriminin ortak bir paydası vardır: Operatörlerinin ve yazarlarının mutlaka kötü niyetleri bulunmaktadır. Kötü amaçlı yazılım yazarları, kötü amaçlı etkinliklerinden para kazanmak için birçok numara kullanmaktadır. Bazı kötü amaçlı yazılımlar, olabildiğince çok hassas verileri çalmak için bir sisteme sızmaya çalışmakta, ardından operatörlerinin bunları satmasına veya kullanmasına izin vermekte ve ardından kurbanlarından para sızdırmaktadırlar. Siber suçluların iyi bilinen bir yöntemi, bir kullanıcının verilerini veya diskini şifrelemek ve daha sonra bilgilerini kurtarabilmeleri için büyük bir fidye istemektir.[59] Bununla birlikte, çok özel hedefler peşinde koşan ve en başından finansal kazançla motive edilmeyen siber suçlu grupları da bulunmaktadır. Faaliyetlerini finanse etmek için nasıl para kazandıklarını bilmek zor göründüğünden onlara; devletler, Dark Web girişimcileri veya diğer bilinmeyen kuruluşlar tarafından yardım edilebileceği söylenmektedir. Her halükârda kesin olan bir şey vardır ki bu operasyonlardan bazıları yüksek oranda finanse edilmiş, gelişmiş ve çok iyi organize edilmiştir.

Çoğu bilgisayar saldırısı oldukça önemsizdir. En kötü durumda, kullanıcı ekranında bir fidye notu görmekte ve bu, bilgisayarının şifrelenmiş olduğunu ve kullanıcının ödeme yaptıktan sonra kilidinin açılacağını açıklamaktadır. Ancak, olan şeyler genellikle görünmezdir. Çeşitli kötü amaçlı yazılım türleri, tespit edilmeden mümkün olduğu kadar fazla veriyi çalmak için olabildiğince dikkatli davranmaktadır. Bununla birlikte, belirli bilgisayar saldırılarının kapsamı veya karmaşıklığı kaçınılmaz olarak uluslararası topluluğun dikkatini çekmektedir. Bu durumda; yapılan WannaCry, NotPetya / ExPetr,

59 Check Point, "What Is the Purpose of Malware?", https://www.checkpoint.com/definitions/what-is-malware/ E.T. 11 May 2020.

Stuxnet, DarkHotel ve Mirai kötü amaçlı yazılımları, son on yılın en dehşet verici ve rezil bilgisayar saldırılarını şimdiden gerçekleştirmiştir.[60]

Bir bilgisayara virüs veya solucan yoluyla kötü amaçlı bir yazılım yüklendiğinde; bir botnet çalıştırılabilmektedir. Bir grup virüs bulaşmış bilgisayar olarak botnetler, birçok durumda DDoS saldırıları başlatmak için kullanılabilmektedir.[61] Konumuzun yönü göz önünde bulundurulduğunda, amacı özel maddi kazanç elde etmek olan saldırılar bizi ilgilendirmemektedir. Bu konu, devletlerin dikkatini çeken ve bu tür düşmanca eylemler onların siyasi veya bölgesel egemenliklerini zayıflattığı için kuvvet kullanma konusunu gündeme getiren siber saldırılarla ilgili olduğu sürece, ana odağımıza girecektir.

B. SİBER GÜVENLİĞİN TARİHSEL ARKA PLANI

Güvenlik, tarihin yıllıklarından bu yana var olmuştur ve onun gelişimi, tüm eylem kapsamı içinde bir şekilde insanoğlununkiyle bağlantılı olmuştur. Güvenlik hedeflerinin gelişmesi gibi, kuruluşlarda güvenliğin evrimi de geride bırakılmamış ve başlangıcından bu yana esas olarak maruz kaldığı teknolojik ilerlemelerin motive ettiği önemli bir değişime uğramıştır. "Siber güvenlik" teriminin en erken kaydedilen kullanımı, "siberporn" kelimesinin icat edildiği yıl olan 1989'da geldi. Ancak hiçbir terim baskın değildi.

60 J. Snow, "Top 5 most notorious cyberattacks", **Kaspersky Daily,** 6 Kasım 2018. https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/ E.T. 11 Mayıs 2020.

61 F. Pamela, "Computer malware and attacks", **Khan Academy**, URL https://www.khanacademy.org/computing/ap-computer-science-principles/the-internet/cybercrime-and-prevention/a/computer-vulnerabilities E.T. 11 Mayıs 2020.

1990'ların "bilgi otoyolu"nun hareketli günlerinde, insanlar alışverişin, flört etmenin ve çalışmanın çevrimiçi olabileceği fikrine alışmadan önce, bir şeye siber önekini eklemek, fütürist gençlik yaşadığı ışıltılı dünyada gerçekleşiyormuş gibi görünmesini sağladı.[62] Son 25 yılda, siber tehdit ortamı, herkesin hayal edebileceğinden çok daha hızlı değişmiştir. İnsanoğlu, bu tehlikelerin gelişmesine ve daha önceki alt bölümlerde bahsettiklerimiz gibi son yıllarda meydana gelen büyük siber saldırılara tanık olmuştur. Bununla birlikte, önemli odak noktası, kuruluşların her yeni nesil tehdidin planladığı zorlukların üstesinden gelmeyi zaman içinde nasıl seçtikleri üzerinde bulunmaktadır. Aşağıdaki zaman çizelgesi, siber güvenliğin gelişmesini anlamamıza yardımcı olabilir:

1. **Creeper Virüsün Keşfi**

"*Ben Creeperim... Yakalayabilirsen beni yakala*" Bu mesajın birkaç ARPANET bilgisayarında görünmeye başladığı yıl 1971'di. O zamanlar hiç kimse bilgisayar dünyasında böyle bir şey görmemişti: Kendini kopyalayan ve ağ üzerinden bir düğümden diğerine yayılan bir program. Programın adı Creeper idi ve bugün tarihteki ilk bilgisayar virüsü olarak kabul edilmektedir.[63] Kötü amaçlı bir program değildir ve kendini kopyalayarak ağ üzerinden dolaştı ve nereye giderse gitsin bu mesajı görüntülemiştir.

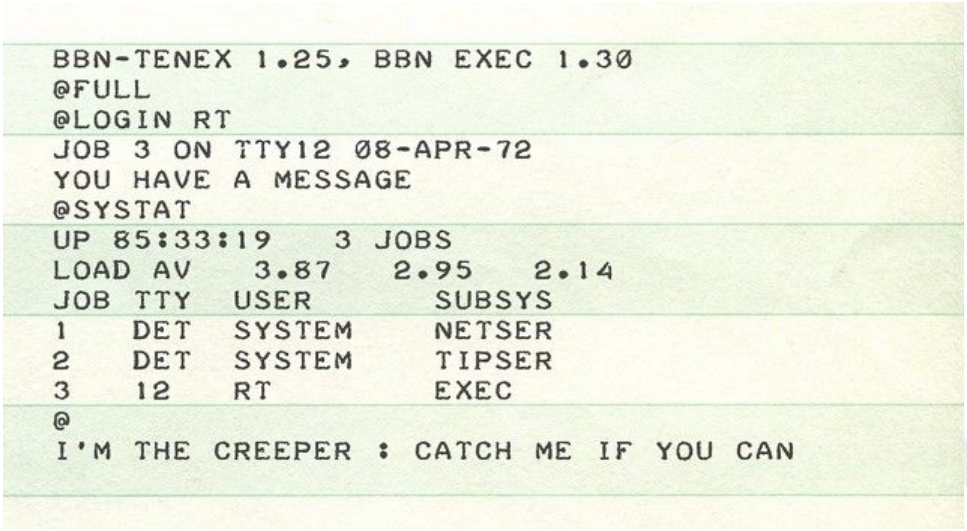
Kendilerini kopyalayabilen ilk bilgisayar programları, bilgisayar virüsü veya solucanına benzer bir şey hakkında kuram geliştiren ilk kişi olan matematikçi John von

---

[62] Annalee Newitz, The Bizarre Evolution of the Word "Cyber", Gizmodo, 2013, https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 E.T 30.06.2022

63 Scientific America, "When did the term 'computer virus' arise?", 19 Ekim 2001. URL: https://www.scientificamerican.com/article/when-did-the-term-compute/ E.T. 18 Mayıs 2020

Neumann tarafından 1949 gibi erken bir tarihte tahmin edilmiştir.[64] Ancak, 1971 yılına kadar mühendis Robert H. (Bob) Thomas teoriyi gerçeğe dönüştürerek kendi Creeper'ını yaratmıştır.[65] Creeper, bir programın belirli bir görevi yerine getirirken bir bilgisayardan diğerine atlayarak ağda geçiş yapabileceğini göstermek için tasarlanmış bir deneydir.



(Şekil.1: Creeper Virüsü ve Kaynak Kodu)[66]

Ancak tarihte ilk virüs olarak kabul edilmesine rağmen pratikte herkes bunun böyle tanımlandığı konusunda hemfikir değildir. Sadece bilgisayar virüsü kavramının 80'li yıllara kadar doğmaması nedeniyle değil, zarar vermesi amaçlanmadığı için yazılımın mobil uygulamalarını göstermesi amaçlanmıştır. Yine de, hala hızlı ve bulunması zor bir yazılım parçasıydı ve bu, zamanın geri kalan bilgisayar dehaları için bir zorluk teşkil etmekteydi.

64 Scientific America, 2001
65 Scientific America, 2001
66 Hackernoon, "Are We Ever Going to Solve Cybersecurity?", **Connexion3,** 5 Şubat 2020. https://connexion3.gr/are-we-ever-going-to-solve-cyber-security/ E.T 18 Mayıs 2020.

Bu, Creeper'ı bugün tarihin ilk antivirüs olarak tanımlayabileceğimiz şeyi yaratmamıza yardımcı olan bir meydan okuma haline getirmiştir.[67]

2. İlk ABD Siber Güvenlik Patenti, İlk DEF CON Konferansı ve Güvenli Yuva Katmanının Doğuşu (SSL) 2.0

Bilgisayarların gelişmesi nedeniyle, dünya çapında çeşitli teknoloji ve bilgisayar üreticileri, bilgisayar sistemlerinde yaptıkları yeni buluşlar için patent haklarını talep etmek için acele etmekteydiler. Eylül 1983'te MIT, "kriptografik iletişim sistemi ve yöntemi" için ilk ABD Bilgisayar Sistemi Patentini kazanmıştır. Bu patent ilk kez RSA (Rivest-Shamir-Adleman) olarak bilinen ve açık anahtarlı şifreleme sistemlerinin öncüsü olan bir algoritmayı sunmuştur.[68] Bir diğer açıdan kriptografi, modern siber güvenliğin temelidir.[69]

DEF CON, dünyadaki en bilinen siber güvenlik teknik konferanslarından biridir. Jeff Moss tarafından Haziran 1993'te Las Vegas'ta 100 kişilik bir konferansta başlatılmıştır. O zamandan beri, DEF CON konferansı bilgisayar korsanlarının, araştırmacıların, profesyonellerin ve hükümet temsilcilerinin bilgisayar güvenliğini tartışmak için bir araya gelebileceği bir yer olmuştur. 1993 yılından beri düzenlenen DEF CON konferansı, yeni teknolojilere ve BT güvenliğine adanmış, her yıl binlerce meraklıyı bir araya getirmektedir. Şimdiye kadar, bu etkinliğe katılanlar sadece bilgisayar korsanları değildi: DEF CON'un

---

67 D. Saltonstall, "The Creeper and The First Anti-Virus Program", **Ezine Articles**, 15 Nisan 2009. URL: https://ezinearticles.com/?The-Creeper-and-The-First-Anti-virus-Program&id=2224501 E.T. 18 Mayıs 2020.

68 R. Margret, "RSA Algorithm", **TechTarget Network,** Kasım 2018. https://searchsecurity.techtarget.com/definition/RSA E.T 18 Mayıs 2020.

69 T. Matthew, "A Brief History of Cybersecurity", **Cyberinsider,** 2019. https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/ E.T. 19 Mayıs 2020

kapıları, özel sektördeki profesyonellerden gazeteciler de dâhil olmak üzere araştırmacılara kadar daha geniş bir kitleye açık bulunmaktaydı.[70]

Güvenli Yuva Katmanı (SSL), bir bilgisayar ağı üzerinden iletişimin güvenliğini sağlamaya yardımcı olan kriptografik bir protokoldür. 1990'ların başında Netscape Communications araştırmacıları, korumasız bir ağ üzerinden istemciler ve sunucu uygulamaları arasındaki iletişimi güvence altına almak için bir protokol geliştirmek istemiştir. Bu girişim, 1994 yılında SSL'nin ilk sürümünü doğurmuştur. SSL, mesaj doğrulama kodu (MAC) adı verilen kısa bir bilgi parçasını kullanarak çalışmaktadır.[71] Bu nedenle bu MAC, bir mesajın bütünlüğünü ve gerçekliğini sağlamayı mümkün kılmaktadır. Şubat 1995'te Netscape, SSL'nin (SSL 2.0) ikinci sürümünü piyasaya sürmüştür ve bu, Güvenli Hiper Metin Aktarım Protokolü adı verilen web güvenliği dili haline gelmiştir. Günümüzde, bir web sitesi adresinde "HTTPS" görülürse, yetkisiz erişimi engellemek için, iletişimlerinin bir koda dönüştürüldüğü fark edilmelidir.[72]

3. Anonymous'un Doğuşu

Anonymous, sanal bir topluluk oluşturan, tanımlanamayan bir şekilde hareket eden ve kendilerini esas olarak internette, ama aynı zamanda sokaktaki belirli eylemlerle de gösteren bir grup aktivistin adıdır. Anonymous, kendilerini ifade özgürlüğü hakkının savunucuları olarak tanıtmakta, sivil itaatsizliği kışkırtmakta ve barışçıl davranmaktadır. Halka açık yerlerde, üyeleri "*V for Vendetta"* çizgi romanında ve sinemaya uyarlamasında V karakterinin kullandığı Guy Fawkes maskesini takmaktadırlar. Topluluk üyeleri,

---

70 C. Avey, “Historic Hacking: A Brief History of Cybersecurity”, 18 Ağustos 2019. https://www.secureworldexpo.com/industry-news/historic-hacking-brief-history-cybersecurity E.T 19 Mayıs 2020.
71T. Matthew, 2019
72 C. Avey, 2019

içlerinde oluşabilecek herhangi bir hiyerarşi biçimini ateşli bir şekilde reddetmektedir. Bir liderin yokluğu, aynı zamanda merkezi olmayan eylemlerini de desteklemektedir.[73]

Anonymous'un ilk izleri 2003 yılına kadar uzansa da, gerçek bir organizasyona tanıklık eden ilk eylemler, 2006 yılında Habbo'nun sosyal medya web uygulamasına karşı yönlendirilmiştir.[74] Anonymous, tam bir kışkırtmayla uygulamanın sanal dünyasını yüzlerce özdeş simgeyle istila etmiş ve oyunun belirli bölümlerini engellemiştir.[75] Sonraki aylarda, bilgisayar korsanları da dâhil olmak üzere Anonymous üyeleri, dinleyicilerinin gözünde onu itibarsızlaştırmak için bir Amerikan radyo sunucusu ve varsayılan bir neo-Nazi olan Hal Turner'a karşı bir bilgisayar baskını düzenlemiştir.[76] Yüzlerce kişinin katıldığı bu ilk ideolojik eylemle Anonymous, gerçekten aktivist olmuştur. Son olarak, 2008'den bu yana, dünya çapındaki şehirlerde düzenli olarak "fiziksel" etkinlikler düzenlenmektedir. Hedefleri, internette konuşma özgürlüğünü ihlal ettiğine inandıkları herkes, herhangi bir kuruluş veya hükümetlerdir.

Anonymous, 2008'deki "Chanology Project"[77] sırasında ilk kez küresel bir hareket olarak ortaya çıkmış ve modern siber aktivizmi doğurmuştur. Scientology Kilisesi'ne yöneltilen bu eylem, ikincisinin yanlışlıkla yayınlanan bir dâhili tanıtım videosunu her ne pahasına olursa olsun silme iradesini izlemektedir. Tarikatın onu eleştirenlere karşı şiddetiyle ilişkilendirilen bu içeriği sansürlemeye yönelik bu çabalar, hareketi kızdıracaktır.

---

73 N. Chandler, “How Anonymous Works”, **HowStuffWorks.com,** 12 Mart 2013. URL https://computer.howstuffworks.com/anonymous.htm E.T 20 Mayıs 2020

74 P. Shakarian ve ark, “Cyber Attacks and Public Embarrassment: A Survey of Some Notable Hacks”, **Introduction to Cyber Warfare: A Multidisciplinary Approach**, 2013, s.4. https://arxiv.org/ftp/arxiv/papers/1501/1501.05990.pdf

75 P. Shakarian ve ark, 2013

76 N. Rapold, “We are Legion: The Story of the Hacktivists,” Brian Knappenberger tarafından yönetilen belgesel, **New York Time-Movie Review**, 18 Ekim 2012. https://www.nytimes.com/2012/10/19/movies/we-are-legion-on-computer-hacker-activists.html E.T 20 Mayıs 2020.

77 P. Shakarian ve ark, 2013, s.6

Scientology Kilisesi web sitesi engellenmiştir. Bu eylemlere ek olarak Anonymous, dünyanın çeşitli şehirlerindeki tarikat karargâhı önünde gösteriler yapılması çağrısında bulunmuştur. Bu gösteriler sırasında Anonymous ve destekçileri, anonimliklerini garanti altına almak ve Scientology Kilisesi'nin misillemelerinden kendilerini korumak için Guy Fawkes'ın maskesini ilk kez takmışlardır.

2010 eylemlerinin de gösterdiği gibi, grup açıkça siyasallaşmıştır. Bunlardan en önemlilerinden biri, alternatif bir basın sitesi olan Wikileaks'e destek amacıyla yürütülen ve hükümetlerin gerçek eylemlerine ilişkin bilgi sızıntılarının yanı sıra siyasi ve sosyal analizlerin yayınlandığı operasyondur. Wikileaks'in bağış yapmasını önlemek için PayPal, Mastercard ve hatta Amazon gibi şirketler hizmetlerini geri çekmiştir. Mutsuz Anonymous üyeleri, bu çevrimiçi ödeme hizmetlerine karşı devasa bir saldırı başlatmış ve böylece faaliyetlerini engellemiştir.[78]

Anonymous, "Arap Baharı"[79] olaylarına katılımlarıyla da ünlüdür. Ocak 2011'de başlayan Tunus operasyonu sırasında grup, Tunuslu yetkililerin sitelerine saldırarak ve isyancıların sosyal ağlarda kendilerini ifade etmelerini engelleyip sansürü atlatmalarına yardımcı olarak Ben Ali hükümetine karşı mücadeleye katkıda bulunmuştur. Bu, Anonymous'un internet dışındaki hareketlere yaptığı yatırımın başlangıcını işaret etmektedir. Aynı dönemde Anonymous, Mısırlı devrimcilere Mübarek hükümetine karşı mücadelelerinde destek sağlamıştır. Yetkililer tarafından internetin bloke edilmesinin ardından, Mısırlılara yeniden bağlanmalarını sağlamak veya ilk yardım sağlamak için "ilk yardım çantası" göndermeye hak kazanmışlardır. Brian Knappenberger'in belgeselinde bazı

78 L. Turner, *Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and PayPal*, Independent 24 Ocak 2013. URL: https://www.independent.co.uk/news/uk/crime/anonymous-hackers-jailed-for-ddos-attacks-on-visa-mastercard-and-paypal-8465791.html E.T 20 Mayıs 2020.
79 P. Shakarian ve ark., 2013, s.7-8

üyelerin açıkladığı gibi, Anonymous, kendi ağlarını isyancıların kullanımına sunacak kadar ileri gitmiştir. Anonymous, sağlanan yardımla sosyal ağların yürüttüğü bu popüler hareketlerin sonuçlarında önemli bir rol oynamıştır. Bununla birlikte, Anonymous siber savaş dünyasına da girmiş bulunmaktadır. Topluluk, aynı yıl içinde, kendi üyelerini Occupy Wall Street hareketinin öfkeli üyelerine katılmaya da teşvik etmiştir.[80]

Anonymous, bir gruptan çok, internette vazgeçilmez hale gelen bir fikirdir. Her zamankinden daha büyük ve kontrol edilemez gücü, hükümetleri endişelendirmektedir; bu nedenle hareket, Amerika Birleşik Devletleri tarafından bir terör örgütü[81] olarak kabul edilmektedir. Bazı üyeler de yasal kovuşturmaya ve hatta mahkûmiyete maruz kalmıştır. En iyisini ve en kötüsünü yapabilen Anonymous'un eylemleri, kolektif ve küresel bir vicdanın sonucu ve sayısız isimsizin elinde bulunan korkunç bir silahtır. Anonymous, herkesin, ne yapmak istediğine ilişkin bir sestir.

4. Aurora Operasyonu ve Bir Ulusun Hacker Olarak Açığa Çıkması

Google, 13 Ocak 2010'da bir siber saldırının[82] kurbanı olduğunu duyurmuş ve Aralık ortasına kadar Adobe dâhil olmak üzere en az 20 başka şirket hedef alınmıştır.[83] Bu sayı daha sonra Yahoo, Symantec, Northrop Grumman ve Dow Chemical dâhil olmak üzere

---

80 B. Knappenberger, *We are Legion: The Story of the Hacktivists* (Belgesel) 2012, URL: https://g.co/kgs/JRSuWh

81 K. Rawlinson & P. Peachey, Hackers step up war on security services" 13 Nisan 2012. URL: https://archive.vn/20130629103235/http://www.highbeam.com/doc/1P2-31126850.html E.T.20 Mayıs 2020.

82 Google, A New Aprroach to China, 12 Ocak 2010, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html E.T. 20 Mayıs 2020.

83 The Coming Storm, *Google Hacked, Says it Will Stop Censoring Chinese Search Results,* 12 Ocak 2010. URL: https://krebsonsecurity.com/2010/01/hack-against-google-prompts-search-giant-to-stop-censoring-chinese-search-results/ E.T. 20 Mayıs 2020.

34’e çıkartılmıştır.[84] Google'a yapılan saldırı "fikri mülkiyete" yönelik doğrudan casusluktu, saldırıların bir diğer hedefi de Çinli insan hakları savunucularının Gmail hesaplarıydı.[85]

Saldırı, Internet Explorer'daki 0 günlük bir güvenlik açığı yoluyla gerçekleşmiştir. Saldırı için kullanılan ikili dosyalardan ikisinde de saldırganın bilgisayarında "Aurora" terimini içeren hata ayıklama bilgilerini yüklemek için bir yol bulunmuştur. Saldırı bu nedenle "Aurora Operasyonu"[86] olarak adlandırılmıştır.

Google, saldırıların arkasında Çin'in olduğundan şüphelenmiştir. Kötü amaçlı kodu analiz ederken, kaynak olarak Çin'e bir referans bulunmuştur: Kod, Çin'den gelen çok alışılmadık bir sağlama toplamı algoritması kullanmaktadır. Bu algoritmaya ilişkin tüm referanslar ve yayınlar Çin web sitelerinde bulunmuştur.[87]

New York Times, Şangay'daki Jiatong Üniversitesi'ne ve Lanxiang'daki meslek okuluna yapılan saldırıların izinin sürülebileceğini ve her ikisi tarafından reddedildiğini bildirmiştir. Ancak, bir siber saldırının kaynağı gerçekten kanıtlanamamıştır.[88] Aurora Operasyonu, ileri düzeyde kalıcı bir tehdidin tüm işaretlerini göstermektedir.[89] Saldırganların gerçekten bir devlet tarafından görevlendirilmiş olup olmadığı ya da normal siber suçlular olup olmadığı, hala, ileride olacak tartışmaların bir konusudur.

---

84 J. Scofield: Google, Yahoo, Adobe and who?, 14 Ocak 2010, The Guardian. URL: https://www.theguardian.com/technology/2010/jan/14/google-yahoo-china-cyber-attack E.T. 20 Mayıs 2020.
85 Google, 2010
86 CFR, Operation Aurora, Ocak 2010’deki Raporu. URL: https://www.cfr.org/interactive/cyber-operations/operation-aurora E.T. 20 Mayıs 2020.
87 Google, 2010
88 J. Markoff, *cyberattack on Google Said to Hit Password System*, 19 Nisan 2010, The New York Times. URL: https://www.nytimes.com/2010/04/20/technology/20google.html E.T. 20 Mayıs 2020.
89 N. Lord, *what is an Advanced Persistent Threat? APT Definition*, 11 Eylül 2018. URL: https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition E.T 20 Mayıs 2020.

C. GENEL DEĞERLENDİRME

İnternet, tarihi boyunca, kullanım açısından bazı önemli dönüm noktaları ile gelişmiştir. Böylece İnternet, uzun bir süre, kullanıcılarını önce üniversitede ve endüstriyel ortamda, sonra genel olarak kamusal alanda birbirine bağlamak olan "teknik" bir telekomünikasyon ağı olarak kalmıştır. 2000'lerin başlarında, ev içi ve profesyonel kullanımlarda ve hepsinden önemlisi büyük ölçekli demokratikleşmede patlama yaşanmıştır. Sosyal ağlar, e-ticaret ve genel olarak e-iş gibi yenilikçi kullanımlar ortaya çıkmıştır ve bu yenilikçi kullanımlar, bugün hala gelişmektedir. 2030'da ortaya çıkacak bir sonraki devrim, Nesnelerin İnternetive daha özel olarak M2M[90] (Makineden Makineye) olacaktır. Aslında, İnternet, artık yalnızca bireyler ve makineler arasında bir iletişim vektörü olmayacak ve bu durum, tamamen özerk ve giderek daha akıllı makineler arasına taşınacaktır.

Teknolojilerin ve kullanımların gelişmesiyle birlikte, bilgisayar tehditleri de İnternet'in başlangıcından bu yana gelişmektedir. Sivil İnternetin başlangıcında (askeri atasından bahsetmemekteyiz - Arpanet), ağlar ağına bağlantı, esas olarak akademisyenler, araştırmacılar ve büyük şirketler için ayrılmıştır. Birincil amaç (bugün neredeyse hayalî), farklı uzak ekipler arasındaki işbirliği ve nihayetinde bilginin yayılması yoluyla bilimsel araştırmanın iyileştirilmesiydi. Ağdaki ilk kabalık eylemleri yalnızca eğlenmeyi ve teknik yeteneklerin gösterilmesini hedeflenmekteydi. Bu bağlamda, 1988'de Morris solucanının yaratılışından veya bilgisayar virolojisi üzerine ilk kitaplardan alıntı yapılabilir. Verizon tarafından gerçekleştirilen izinsiz girişlerle ilgili yıllık çalışmanın[91] 2004'teki başlangıcından bu yana, bilgisayarların ve özellikle İnternet'in başlangıcından bu yana tehditlerin tipolojisinde değişiklikler olduğunu fark etmiş bulunmaktayız.

---

90 IoT vs M2M — What is the Difference? 16 Ocak 2019. URL: https://www.avsystem.com/blog/iot-and-m2m-what-is-the-difference/ E.T 22 Mayıs 2020.
91 Verizon - 2014 Data breach investigations report, 2014

Önceki saldırılar esas olarak fırsatçı olursa (kolay hedefler esas olarak hedef alınmış ve saldırıya uğramıştır), mevcut saldırılar gittikçe daha fazla hedeflenir, genellikle otomatikleştirilir[92], koruma mekanizmalarıyla[9394] ve mobil cihazlar (akıllı telefonlar) veya ödeme terminalleri gibi yeni saldırı vektörlerini kullanırlar. İnternet hâlihazırda bazı büyük ölçekli bilgisayar saldırılarının veya çökmelerinin kaynağı olmuştur. Etkiler, şu an için bir faaliyet alanı (2014'te DRAGONFLY)[95], bir coğrafi bölge veya bir ülke (2008'de Gürcistan) ile sınırlı kalmıştır. 2030'a kadar çok daha geniş bir tehdit beklenebilir; bazı analistler, tüm siber alanı (İnternet ağı, sunucular, terminaller, nesneler, vb.) etkileyecek küresel bir çökme ("cybergeddon")[96] olasılığını uyandıracak kadar ileri gidebilirler. Böyle bir senaryo, büyük veri kaybına neden olabilir ve veri hizmetlerini çok uzun bir süre kesintiye uğratabilecek, bu nedenle insani, endüstriyel, ekonomik ve sosyal sonuçlar, herhangi bir büyük krizde olduğu gibi dramatik olabilecektir.

II. ULUSLARARASI HUKUKUN SİBER UZAYA UYGULANABİLİRLİĞİ

Hukuk, kendisini hem bir tanık hem de sosyal bağların bir aracı olarak sunmaktadır. Maksim[97], "Toplumun olduğu her yerde, bir hukuk vardır." demiştir. Sonuç olarak, ağa bağlı bir toplumda sosyal bağın ne olacağı sorusu, kısmen, siber uzay gibi bir ortamda yasanın ne olduğunu sormak anlamına gelmektedir. Siber uzayın vaatleri ne olursa olsun,

---

[92] özellikle kötü amaçlı yazılım kullanılarak

93 F-Secure - Malwares analysis Report - Regin, 2014

[94] algılama ve analiz önlemeler

95 Dragonfly: *after Stuxnet, new successful attack against Scada systems*, 2014

96 C. Chan, Cybergeddon, Fiscal Crises and Natural Catastrophes - Global Risks 2014, 31 Temmuz 2014. URL: https://www.barnett-waddingham.co.uk/comment-insight/blog/cybergeddon-fiscal-crises-and-natural-catastrophes/ E.T 22 Mayıs 2020

97 A. X. Fellmeth and M. Horwitz, *Guide to Latin in International Law*, Oxford University Press, 2011, s.281.

insan etkileşimleri orada gerçekleştiği sürece, soru onları çerçevelemeye yönelik standartlarda ortaya çıkacaktır.[98]

Bilgi teknolojilerinin gelişimi, çeşitli faaliyetlerin hukuki çerçevelerini tanımlarken kullandığımız kategorileri sorgulayan dönüşümleri desteklemektedir. Bilgi alışverişi koşullarındaki bu değişikliklerin hukuka etkisi olamamaktadır. Siber uzay tarafından yaratılan koşullar, hukukun genel olarak dikkate alındığı paradigmaların gözden geçirilmesini gerektirmektedir. Siber uzay, sanal ve ağlar, sosyal ilişkileri yöneten standartları tanımlama ve uygulama yöntemlerini yeniden tanımlamaktadır.[99]

Böyle bir ortamda, Devletler sınırlı bir müdahale kapasitesine sahiptir. İnternet sınır tanımaz ve çoğu zaman sanal alandaki etkileşimleri tanımlayan özelliklere bakılmaksızın tasarlanmış devlet müdahalelerini anlamsız hale getirebilir.[100] Siber uzay, kendisini, normatifliklerin genel olarak dayandığı kriterlerin çoğundan yoksun bir ortam olarak sunduğundan, birkaç gözlemci, yasaların İnternete uygulanmasının zorluklarını ve hatta imkânsızlığını tartışmaktadır. Siber uzay, eyalet sınırlarının ölçütlerine, ayrıcalıklı hukuk çerçevelerine meydan okumaya devam etmektedir. Dolayısıyla, devletler hukukunun siber uzayda gerçekleşen faaliyetleri tek başına yönetemeyeceği gözlemi, aynı şekilde, çeşitli iletişim faaliyetlerini düzenleyen düzenlemeler için de geçerlidir.

A. SİBER UZAYI DÜZENLEMEYLE İLGİLİ SORUNLAR

98 E. Katsh, *The Electronic Media and the Transformation of Law*, Oxford University Press, New York, 1989, s.6.
99 A. D. Murray, *The Regulation of Cyberspace: Control in the Online Environment,* Routledge, 2007, s.136.
100 Y. Ling, "*Human Interactions in Physical and Virtual Spaces: A Gis-Based Time-Geographic Exploratory Approach*. " PhD diss., University of Tennessee, 2011. https://trace.tennessee.edu/utk_graddiss/1149 E.T 25 Mayıs 2020.

Hakim olan normatifliğin[101] ortaya çıkma ve uygulama yöntemlerini daha iyi anlamak önemlidir. Siber uzayda normatiflik koşullarının yeniden tanımlanması, diğerlerinin yanı sıra, ilk mesele olan egemenlik değişimiyle kendini göstermektedir. Ele almamız gereken ikinci konu, İnternet faaliyetlerindeki artışın getirdiği, standartların temellerinin yeniden tanımlanmasına yönelik baskıları yoğunlaştıran nicel ve nitel değişikliklerdir.[102]Üçüncü konuda, kuralların ifade biçimlerinden kaynaklanan mutasyonları açıklayacağız. Son olarak, çoğu faaliyetin "siber-mekânsallaştırılması"[103], dördüncü konuyu oluşturacak olan normatiflik kaynakları arasında yeni bir rol dağılımına yönelik eğilimi beslemektedir.

1. Bir Egemenlik Değişimi

İnternet açık bir ortam olduğundan, ağda aynı kuralların geçerli olması gerektiğini düşünmek imkânsızdır. Bu olay, devletlerden kaynaklanan normatifliğin sağladığı işaretçilerin giderek daha belirgin bir şekilde çözülmesinden rahatsızlık duyanların kafasını karıştırabilir. Siber uzaydaki egemenlik kavramı yeni epistemolojik zorluklar getirmektedir. Esasen kaydi bir alanda devlet egemenliğini düşünmek gerçekten zordur, ancak yerel düzeyde gerçekleşen geniş bir insan faaliyetleri dizisi için bir üstyapı işlevi görmektedir.[104]

---

101 S. Delacroix, *Legal norms and normativity: an essay in genealogy*. Oxford: Hart Publishing, 2006.

102 E. Tikk-Ringas, International Cyber Norms Dialogue as an Exercise of Normative Power, Upcoming in Georgetown Journal of International Affairs (2017). URL: https://ict4peace.org/wp-content/uploads/2017/02/Tikk-Normative-Power.pdf E.T 25 Mayıs 2020.

103 M. Dodge and R. Kitchin, *Atlas of Cyberspace*, Pearson Education, London, 2001, s.136

104 H. Yeli, *A Three-Perspective Theory of Cyber Sovereignty*, PRISM 7, NO. 2. P.109-115. URL: https://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/10-3-Perspective%20Theory.pdf E.T 26 Mayıs 2020.

Egemenlik, başka herhangi bir yüce otoriteye tabi olmayan bir varlığın tam gücü anlamına gelmektedir. Egemen varlık, standartların üretilmesiyle ilgilenildiği zaman önemli bir ölçüt olmaktadır. Pozitivist yaklaşımla anlaşılan hukuk çerçevesinde Devlet, bu egemen varlık ve hukukun neredeyse tartışmasız kaynağıdır.[105] İnternet dünyasında ise birçok bilim adamı, egemen varlık olarak kabul edilenin kullanıcı olduğunu iddia etmektedir. Bununla birlikte, İnternette farklı biçimler alan ağlar, kendilerini gerçek egemen varlıklar olarak sunmaktadırlar. Siber uzayın ortaya çıkışı, egemenlikte bir değişime dönüşmüştür[106]. Devlet tarafından ise, kullanıcı ve bu sanal alanı oluşturan ağların yararına bir miktar kayıp yaşanmıştır. Siber uzay için uygulanabilecek olan genel uluslararası hukuka ulaştığımızda, siber uzayda egemenliği neyin oluşturduğunu ayrıntılı olarak göreceğiz.

2. Standartların Temellerini Yeniden Tanımlamak

Elektronik ağların ademi merkeziyetçi organizasyonu, düzenlemeyi, çoğu yasal toplulukta yaygın olan reflekslerin komuta ettiğinden farklı paradigmalara göre düşünmeyi gerekli kılmaktadır. Hukukun siber uzayda etkin bir şekilde uygulanmasında karşılaşılan zorluklar, hukuki biçimciliğin terk edilmesini ve sadece dogma olarak kabul edilen kurallarla sınırlı kalmayıp, kuralların aradığı amaçları da vurgulayan bir yöntemin kullanılmasını gerektirmektedir. Hukuku, rasyonelliklerinden anlamak gerekmektedir. Siber uzayın getirdiği değişiklikler, çeşitli hukuk kurallarının altında yatan rasyonalitelerde bir değişikliğe neden olmaktadır. Ek olarak, kuralların oluşturulmasını veya kuralların

105 J. E. Núñez, *About the Impossibility of Absolute State Sovereignty*, International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, Springer Netherlands, 1 Aralık 2014, Cilt. 27, Sayı 4, s. 645-664

106 S. Woodhams, *The Rise of Internet Sovereignty and the End of the World Wide Web*? In Opinion 23 Nisan 2019. URL: https://theglobepost.com/2019/04/23/internet-sovereignty/ E.T 26 Mayıs 2020.

ortadan kaldırılmasını haklı göstermesi gereken rasyonaliteler etrafındaki tartışmalar, siber uzaydaki yeni durumları adlandırmak için uygun mecaz arayışı etrafında kristalleşmektedir.

Her bir kurallar külliyatının arkasında, onların meşruiyetinin temelini oluşturan ilkeler, değerler ve çıkarlar bulunmaktadır. Çoğu zaman, kural, farklı çıkarları ve değerleri uzlaştıran veya seçimleri yansıtan bir kararın sonucudur. Bir faaliyetin yasal çerçevesi, öncelikle, belirli yönleri çerçevelemek için taleplerin ortaya çıktığı değerlere dayanmaktadır. Politikaların uygulanmasına katkıda bulunmak amaçlandığında, yasal çerçeve, yansıtılmaya çalışılan, genellikle çelişkili olan değerlere bağlıdır. Bu nedenle bu değerler göz ardı edilerek analiz yapılamamaktadır. Bu değerler, bazen onları anlam ve hukuki sonuçlarla yüklü kavramlar haline getiren kanun tarafından bile tutulmaktadır. Siber uzay gibi bir olgunun yasal boyutlarını anlamak, öngörülen veya akla gelebilecek kuralların rasyonaliteleri ile ilgili konular hakkında bilgi sahibi olmayı gerektirmektedir. Bir olgunun hukuki boyutlarını ve büyük ölçüde, kuralların kabul edilmesini zorlayan nedenleri bilmek, onları "rasyonel"[107] kılmaktır.

Elektronik medyanın düzenlenmesinin altında yatan rasyonellikler gibi değişime uğrayan bazı rasyonellikler de mevcuttur. Siber uzay, ulusal bölgelerden gelen yöneticilere meydan okuyan medya ortamlarının bir temsilini sunmaktadır. Elektronik medyaya yönelik düzenleyici rejimler, genellikle devletin neyin yayınlanmasının yasal olduğunu belirleyebileceği öncülüne dayanmaktadır. Siber uzayın yapılandırması, neyin iletilmesi veya neyin iletilmemesi gerektiğini belirleme yerini birey düzeyinde konumlandırmaktadır; düzenlemede merkezi bir oyuncu olarak devleti yetersiz bulmakta, hatta meşrulaştırmaktadır. Savunmaya ve milli yaratıcılığın örneğine bağlı rasyonaliteler bu nedenle bir meşruiyet krizi yaşamaktadırlar.

---

107 P. Jestaz, Le *droit*, 2nd Edition, Paris, Dalloz, 1992

Rasyonaliteler dile; hukuki analizlerde düzenleme ve standart sorunlarını ortaya koyma biçiminde yansıtılmaktadır. Nesneleri adlandırmaya götüren süreçler sadece teknik değil, aynı zamanda gerçekliğin belirli yönlerini vurgulamaya ve diğerlerini belirsizleştirmeye de yardımcı olmaktadır. Bu nedenle, siber uzayı adlandırmanın farklı yollarını, dâhil olan rasyonaliteler hiyerarşisinin vizyonunu görmek gerekmektedir. Bu temsiller, siber uzayın normatifliği üzerinde bir etkiye sahiptir: Belirli rasyonaliteleri meşrulaştırmaya ve diğerlerini diskalifiye etmeye yardımcı olmaktadırlar. Aktörler, tercih ettikleri rasyonaliteleri meşrulaştırmak için çeşitli mecazlar öne sürmüşlerdir. Hukuk gibi, düzenleme de bu tür temsil sistemleri çerçevesinde düşünülmüştür. Elimizdeki siber uzay görüntüleri, orada gerçekleşen faaliyetlerle ilgili düzenlemeyi tasarladığımız öncülleri şekillendirmektedir. İnternetin ilk günlerinde, artık "bilgi parçaları"[108] olduğunun kabul edilmeye başlandığı zamanlarda, bu aşırı özgürlük evreninde yasaların hiçbir şey yapamayacağı ilan edilmiştir. Birçok aktör, barındırılan veya sunucularından geçen içerik için sorumluluk yüklemeye cezbedilebilecek rasyonaliteleri diskalifiye etmek için kendilerine "ağların manipülasyonunda ustalıktan"[109] başka bir şey olmayan basit aracılar demektedirler.

3. Kuralların İfadesinde Değişimler

İnternette, devletlerin ve aktörlerin faaliyetlerinden kaynaklanan çeşitlendirilmiş davranış kurallarının ortaya çıktığını görmekteyiz. İnternette geçerli olan birkaç kural, genellikle koordinasyonu sağlamayı amaçlayan düzenleyici süreçlerin bir parçası

---

108 P. Fox, *From electricity to bits*, Khan Academy. URL: https://www.khanacademy.org/computing/ap-computer-science-principles/computers-101/digital-data-representation/a/from-electricity-to-bits E.T 26 Mayıs 2020.
109 P. T. Metaxas, *Network Manipulation (with application to Political issues)*, URL: https://pdfs.semanticscholar.org/747e/34f71e1c255da36052b4ead9ec57b62fc9d7.pdf E.T 26 Mayıs 2020.

olmaktadır. Koordinasyon düzenlemesi, onsuz neredeyse imkânsız olacak bir faaliyeti kolaylaştıran bir düzenlemedir. Örneğin, yolun sağında araç sürmenin kuralı, riskli bir faaliyeti koordine etmektir. Bunun önsel ahlaki bir amacı yoktur. İnternet evreninde alan adlarının düzenlenmesi, iletişimi mümkün kılmak için gerekli koordinasyonu sağlamayı amaçlamaktadır. Belirli bir alan adına karşılık gelen yalnızca bir IP adresi olabileceğinden, alan adları üzerinde tahsis ve münhasırlık sağlayacak mekanizmaların devreye sokulması gerekmektedir.

İnternet kullanıcı gruplarındaki artış ve siber uzayda gerçekleşen faaliyetlerin çeşitliliği, basit koordinasyon soruları olarak değerlendirilebilecek soruların sayısının azaltılmasına yardımcı olmaktadır. İnternet kullanıcılarının karşılaştıkları zorluklar, ait oldukları kültürel evrenler içindeki farklı kapsam ve anlamdaki konuları ve sorunları giderek daha fazla ilgilendirmektedir. Bu nedenle, tüm bunların basit standartlarla çerçevelenmesini beklemek giderek zorlaşmaktadır. Konuyla ilgili bir fikir birliği olduğunda, belirli içeriğe sahip kavramları kullanarak kuralları belirtmek nispeten kolaydır. Hukuki metinlerin genel yorum ilkeleri, kelimelerin sıradan anlamlarına güvenmemizi gerektirmektedir. Bu, yorumlayıcıların metinle sınırlı olduğu anlamına gelmektedir. Hukuk veya yönetmelik metni, yasama iletişiminin genel amacını keşfetmeyi mümkün kılmakta ve her şeyden önce, yorumlayıcının ona verebileceği anlamların kapsamını sınırlamaktadır. Elektronik ortamlar, farklı kültürel geçmişlere sahip aktörleri bir araya getirmektedir. Ulusal, kültürel mekânlarda dayandıkları fikir birliği seviyeleri ve referans çerçeveleri artık sanal alanlarda zorunlu olarak işlevsel değildir. Kuşkusuz bu nedenle, belirli bir noktada, değişken içerikli standartlar ve kavramlar aracılığıyla normları formüle etme zorunluluğundan kaçılmamaktadır.

Siber uzay gibi değişken ortamlarda, kanunların veya düzenlemelerin neye izin verdiğini ve neyin yasaklandığını bir kez ve tamamen tanımlamasını beklemek gerçekçi değildir. Değerlere ve etiğe dayalı davranışları ve faaliyetleri çerçevelemek söz konusu olduğunda, koordinasyon zorunluluklarını karşılamak için uygulamaya konulan modellerin yetersizliği görülmektedir. Örneğin, temel haklar alanında, kısmen belirlenmiş bir içeriğe sahip kavramların anlamlarının, yalnızca örtük olarak da olsa etkin bir şekilde belirlenmesi, önemli zorluklar ortaya çıkarmaktadır.[110] Devletler tarafından kararlaştırılan yasal çerçeveler, kanun koyucular tarafından, standartlar, belirsiz kavramlar ve aktörlerin normatif uygulamalarına büyük bir yer bırakan diğer ifade stratejileri kullanılarak bir taslak şeklinde formüle edilmektedir. Devlet düzenlemesine ek olarak, bundan böyle, çok sayıda kaynaktan oluşan normatif bir çerçevenin diğer boyutlarını oluşturan düzenleme ve öz düzenleme eklenmiştir. Dolayısıyla normatifliğin farklı kutupları arasında yeni bir rol dağılımı gerçekleşmiş bulunmaktadır.

4. Normatiflik Kaynakları Arasında Yeni Bir Rol Dağılımı

Siber uzayın karakteristik özellikleri, özellikle devlet düzenlemesini daha az uygulanabilir kılanlar, diğer normatiflik kaynaklarının[111] göreceli ağırlığında bir artışa yardımcı olmaktadır. Birkaç yazar, siber uzayda eyalet hukukunun sınırlarını vurgulamıştır. Trotter Hardy, yasaların siber uzaydaki sorunlara verilebilecek olası çözümlerden sadece biri olduğunu belirtmiştir.[112] Olay bazında hüküm verilmesi ve bundan kaynaklanan kuralların aşamalı olarak oluşturulması, sözleşmeler, gelenekler, ağlar tarafından uygulanan

110 I. Manners, *Normative Power Europe: A Contradiction in Terms?* Journal of Common Market Studies 70, no. 2, 2002, s.253.

111 D. Hunter, Cyberspace *as* Place *and the Tragedy of the Digital Anticommons*, 91 Calif. L. Rev. 2003, s.43

112 T. I. Hardy, *The Proper Legal Regime for "Cyberspace*", University of Pittsburgh Law Review, no55, 1994, s. 993-1055.

kurallar ve hatta belirli bir anarşi, İnternetteki davranışları yönetmek için daha uygun olabilecektir.

Düzenlemesi teknik mimari, sosyal standartlar, öz denetim ve hukukun sinerjisinden kaynaklanan tek ortam kesinlikle siber uzay değildir. Ancak sunduğu özellikler, bu farklı normatiflik kaynakları arasında hâkim olan dağılımı değiştirmektedir. Teknik mimari, siber uzay kaynaklarına erişimi ve kullanma haklarını belirleyen donanım, yazılım, standartlar ve yapılandırmalar gibi tüm teknik öğeler veya yapılar anlamına gelmektedir.[113] İletişim ağları ve teknolojinin dayattığı bilgi akışını yöneten bu kurallar, artan sayıda faaliyetin düzenlenmesinde önemli bir rol oynamaktadır. Teknik nesnelerin çeşitli şekillerde düzenleyici bir etkisi bulunmaktadır. Birincisi, mimari öğeler, güvenlik duvarları veya vekil sunucuları gibi yazılım olabilmektedir. Bu tür kaynaklar, bazı Devletler tarafından, içeriğin yurt dışından kendi ulusal İnternet ağlarında dolaşımını kontrol etmek için kullanılmaktadır. İkincisi, mimari, ağların ustaları tarafından uygulanmaktadır. Özelliklerinin, neye izin verdiğinin veya neyin yasakladığının seçimi, bir düzenleme eylemi, hatta yasalardır. Bu nedenle, çeşitli şekillerde mimari, siber uzayda gerçekleşen faaliyetler için hukuki çerçevenin bir bileşenini oluşturmaktadır.

Birkaç çalışma, siber uzayda gerçekleşen faaliyetlerin düzenlenmesinde teknik mimarinin önemli rolünü vurgulamıştır. Teknik nesnelerin politik boyutu, bilim sosyologlarının çalışma alanlarından biridir.[114] Bu çalışma, teknik mimarisini hesaba

---

113 J. Faircloth, Introduction to Enterprise Applications Administration, Enterprise Applications Administration, Morgan Kaufmann, 2014, s. 1-26, https://www.sciencedirect.com/book/9780124077737/enterprise-applications-administration

114 L. Winner, Do Artifacts Have Politics? *Daedalus* 109, no. 1 (1980): 121-36. http://www.jstor.org/stable/20024652. E.T 12 September 2020.

katacak ve bundan yararlanacak siber uzayı düzenlemeye yönelik yeni bir yaklaşımın çerçevesini ana hatlarıyla açıklamaktadır. Siber uzayın teknik mimarisinin hukuk boyutlarının incelenmesi, şimdi internetin normatifliğini anlamamıza ve buna göre hareket etmemize izin veren yollardan biri olarak ortaya çıkmaktadır.

Otokontrol, bir faaliyete katılanlar tarafından gönüllü olarak geliştirilen ve kabul edilen standartları ifade etmektedir.[115] İnternette gözlemlenen uygulama, orada hâkim olan ana otokontrol modellerini ortaya koymaktadır. Böylece, bir yerin (bir sitenin) kontrolüne sahip olanlar, siteye erişim, kabul edilen davranışlar ve yasaklanmış eylemlerle ilgili politikaları benimseme olanağına sahiptir. İnterneti oluşturan farklı ağlarda uygulanan farklı davranış standartları vardır. Biçim ve yapı bakımından benzer olsalar da, bu politikalar bazen az ya da çok kısıtlayıcı yapıları ile birbirinden ayrılmaktadır. "Kabul Edilebilir Kullanım Politikaları"[116] ifadesiyle belirlenen bu kurallar, belirli bir ağa erişimi sürdürmek için kullanıcının uyması gereken davranış standartlarını oluşturmaktadır.

Siber uzayda davranış kuralları konusu ele alındığında, devletin kendiliğinden koyduğu yasalar, düzenlemeler ve kısıtlamalar düşünülmektedir. Ancak somut olmayan gerçeklerle ilgili olarak aktörlerin haklarını ve yükümlülüklerini belirtmek, hukuk için bir meydan okuma olmaya devam etmektedir. Bu nedenle devlet hukuku, uygulandığı zaman, genellikle bileşenlerinden yalnızca biri olduğu bir düzenleyici yaklaşımın parçasıdır; ilkeleri belirler, hedefleri formüle eder, kriterleri belirler, ancak güncellenmesini sağlamak için diğer standartlar için giderek daha fazla yer bırakır. Böylece hukuk, diğer normatiflik

115 P. Trudel, *Les effets juridiques de l'autoréglementation*, Revue de droit de l'université de Sherbrooke, no 19, (1989a), s. 251-286

116 Acceptable use policy (AUP), URL: https://whatis.techtarget.com/definition/acceptable-use-policy-AUP E.T 26 Mayıs 2020.

kaynaklarının az ya da çok yoğun bir rol oynayacağı ortak düzenleme sürecinin bir bileşeni biçimini alır.

Siber uzayın her yerde bulunmasının yanı sıra, bölgesel sınırlara duyarsız kalması, davranış kurallarının ortaya çıkması, formülasyonu ve uygulanmasının nasıl tasavvur edileceğine dair sonuçlara sahip bulunmaktadır. Elektronik ortamlar, hukuk sisteminin çoğulcu toplumlarda karşı karşıya gelen değerler arasındaki dengeyi korumaya çalıştığı müdahale tekniklerinde değişikliklere neden olmaktadır. Ulusal sınırlar ve hukuk kategorileri olan seküler yer işaretlerinden yoksun olan bu alanlardaki hukuku anlamak için, elektronik ortamlarda uygulanan normatifliklerin temellerini daha iyi konumlandırmak önemlidir. Bu yaklaşım önemlidir, çünkü bu temeller, özellikle siber uzaya müdahalelerini uygun bir şekilde tasarlama zahmetine girecek olan devlet yetkilileri tarafından bundan sonra uygulanabilecek olan düzenlemelerdir. Bu temeller, Devletlerin siyasi sınırlarının çizgileri boyunca değil, şu anda kendilerini siber uzayın kurucu birimleri olarak ortaya koyan ağlar arasındaki sınırlar düzeyinde yer almaktadır.

Siber uzayda hukuk, ulusal hukukla sınırlı olmayan tekniklerle ifade edilmektedir. Devlet hukuku, derecesi düşürülmek bir yana, farklı normatiflik kaynakları arasındaki sinerjilerden kaynaklanan bir düzenleyici sürecin bir bileşenidir. Bu normatiflikler, siber uzayı olduğu gibi yapan teknik mimariden, sözleşmeye dayalı uygulamalardan ve aktörler tarafından yerine getirilen öz düzenlemeden kaynaklanmaktadır. Bu, orijinal devlet standartlarının ağırlığının ve davranışı etkili bir şekilde etkileme kapasitesinin, diğer düzenleme kaynakları ile kurulan sinerjiye bağlı olduğu bir ortak düzenleme ile sonuçlanmaktadır. Hukuk, istenen dengeleri ve korumaları bu şekilde sağlamaktadır. Böylelikle öngörülen siber uzayın normatifliğine hâkim olmak, onun gelişimi için bir koşul olmaktadır. Siber uzayda egemen otorite, payına sahip olan aktörleri ilgilendirmektedir.

Böyle bir yaklaşımdan, normatiflik sorunu, siber uzay üzerindeki kamu ve özel politikaların zorluklarının merkezinde yer almaktadır, çünkü asıl zorluk, bu normatifliğin insan onuru ve kültürel çeşitlilik ile tutarlı değerleri yansıtacağını garanti etmektir.

B. BİLGİ SİSTEMLERİNE SALDIRILAR: DEVLET KAYGILARINI GEREKTİREN STRATEJİK BİR TEHDİT

İnternetin ve yeni teknolojilerin önemli gelişmeleri ile birlikte, bilgi ve iletişim sistemleri artık toplumlarımızın işleyişinde merkezi bir yer tutmaktadır. Bununla birlikte, günümüzde, bilgi ve iletişim sistemlerinin gelişimi ve bunların her türlü faaliyette artan ara bağlantılarının, bu alanda yadsınamaz bir kısıtlama oluşturan güvenlik gereksinimlerine zarar verecek şekilde sağlandığı görülmektedir.

Bilgi sistemlerine yönelik saldırılar sınırları ortadan kaldırmaktadır ve birden fazla devlete yönelik olabilmektedir. Ağları izlemek ve olaylara yanıtlar geliştirmek, uluslararası iş birliği ve yardımı haklı çıkarmaktadır. Daha genel bir şekilde ifade etmek gerekirse, bilgi sistemlerinin yasa dışı faaliyetlere karşı korunması bugün birçok Devlet ve birkaç uluslararası kuruluş tarafından paylaşılan bir endişe olmaktadır. Ancak, bu alandaki uluslararası işbirliği hala birçok engelle karşı karşıyadır.

Amerika Birleşik Devletleri, Birleşik Krallık, Almanya, Çin ve Rusya, birkaç yıldır siber güvenliği ulusal bir öncelik haline getirip bilgisayar saldırılarıyla mücadele için önemli önlemler almıştır.

1. Amerika Birleşik Devletleri

Soğuk savaş boyunca, teknik istihbarat ve bilginin korunmasına uzun süredir devam eden bir ilginin[117] ve bu konulardaki artan çabaların yanı sıra ABD, bilgi sisteminin korunmasına stratejik öncelik vermiştir.

Amerika Birleşik Devletleri, aslında, İnternet'e en fazla bağımlı ülkelerden biridir ve dünyadaki en çok bilgisayar saldırısını yaşamaktadır. Örneğin, hükümet düzeyinde, savunma bakanlığı, Pentagon ve silahlı kuvvetlerin sistemleri 15.000 ağı ve 7 milyon kullanıcıyı bir araya getirmektedir.[118] Emekli Siber komutanı General Keith B. Alexander bir keresinde bu sistemlerin, bir günde neredeyse altı milyon kez saldırıya uğradığını bildirmiştir. Son yıllarda Pentagon, Dışişleri Bakanlığı, İç Güvenlik Bakanlığı ve hatta NASA'nın bilgi sistemlerine ciddi bilgisayar müdahaleleri kaydedilmiştir.[119] 2008 yılında yayınlanan merkezi Komutanlığın bilgisayar ağına ilişkin bir raporda, Florida'nın Tampa kentinde bulunan Orta Doğu için ABD bölgesel stratejik komutanlığının, sınıflandırılmış ağların ve bilgilerin tehlikeye atılmasına sebep olan bir USB sürücü kullanılarak bir virüs bulaştırıldığı belirtilmiştir.[120]

Mayıs 1998'de, siber güvenlik sorununun erken değerlendirilmesinin bir işareti olarak, Başkan Bill Clinton tarafından, özellikle bilgisayar sistemlerinin hem siber tabanlı hem de fiziksel saldırılara ilişkin güvenlik açıklarını ortadan kaldırmayı amaçlayan kritik

---

117 V. Güntay , "SİBER UZAY VE GÜVENLİK POLİTİKASI ÜZERİNE TEORİK BİR YAKLAŞIM", *Cyberpolitik Journal*, vol. 2, no. 4, s. 9, Ocak, 2018

118 J. A. Winnefeld Jr, C. Kirchhoff and D. M. Upton, Cybersecurity's Human Factor: Lessons from the Pentagon, Security&Privacy Eylül 2015 Sayı. URL: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon E.T 12 Eylül 2020.

119 P. Rosenzweig, *Significant Cyber Attacks on Federal Systems* -- 2004-present, 7 Mayıs 2012. URL: https://www.lawfareblog.com/significant-cyber-attacks-federal-systems-2004-present E.T 29 Mayıs 2020.

120 W. J. Lynn III, *Defending a New Domain the Pentagon's Cyberstrategy*. September/ October 2010. URL: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain E.T 29 Mayıs 2020.

altyapıların korunmasına ilişkin Başkanlık Kararnamesi 63 imzalanmıştır.[121] Ocak 2008'de Başkan George W. Bush, hükümet bilgi sistemlerini bilgisayar saldırılarından korumak için bir dizi önlemi resmileştiren Başkanlık Ulusal Güvenlik Direktifi 54'ü onaylamıştır.[122] Son olarak, Başkan Barack Obama konuya büyük yatırımlar yapmış ve siber güvenliği döneminin önceliklerinden biri haline getirmiştir. Nitekim 29 Mayıs 2009'da yaptığı bir konuşmada, "s*iber tehdidin, ekonomik konularda ve ulusal güvenlik açısından Amerika Birleşik Devletleri'nin karşı karşıya olduğu en ciddi sorunlardan biri olduğunu"* ve *"Amerika'nın 21. yüzyıldaki refahının siber güvenliğe bağlı olacağını*"[123] söylemiştir. Aralık 2009'da görevinden yeni ayrılan Howard Schmidt'i hem Milli Güvenlik Konseyi'ne hem de ekonomik sorulardan sorumlu ekibe siber güvenlik raporlamasından sorumlu Beyaz Saray danışmanı olarak atamıştır. Howard Schmidt'in ana görevlerinden biri Amerikan ulusal doktrinini birleştirmek ve bu konudaki kurumlar arası koordinasyonu iyileştirmektir.

Temmuz 2011'de Pentagon, birkaç raporu takip eden yeni bir siber strateji ("Siber 3.0" olarak adlandırılır)[124] yayınlamıştır. Belgede, ağı elektronik istihbarat kullanmak gibi diğer yeteneklerle korumaya yönelik geleneksel önlemleri güçlendirmeyi amaçlayan "aktif savunma" konusuna odaklanılmaktadır. Bu yeni strateji aynı zamanda hem ulusal düzeyde,

---

121 The White House, *Presidential Decision Directive/ NSC-63: Critical Infrastructure Protection*, 22 Mayıs 1998. URL: https://fas.org/irp/offdocs/pdd/pdd-63.pdf E.T 29 Mayıs 2020

122 The White House, *National Security Presidential Directive/Nspd-54-Homeland Security Presidential Directive/Hspd-23: Cybersecurity Policy (U)*, 8 Ocak 2008. URL: https://fas.org/irp/offdocs/nspd/nspd-54.pdf E.T 29 Mayıs 2020.

123 Metin: *Obama's Remarks on Cyber-Security,* 29 Mayıs 2009. The New York Times https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html E.T 29 Mayıs 2020

124 Department of Defense, "*Strategy for Operating in Cyberspace*", Temmuz 2011 URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf E.T 29 Mayıs 2020.

hem farklı kurumlar arasında hem de kamu ve özel sektör arasında uluslararası düzeyde, olduğundan daha yakın işbirliğinin önemini vurgulamaktadır. Beş alan içerir:

- Savunma bölümünün siber uzayı operasyonel bir alan olarak ele alması ve sunduğu potansiyelden tam olarak yararlanabilmesi için organizasyon, eğitim ve teçhizat çabası;
- Savunma bölümü ağlarını ve bilgisayar sistemlerini korumak için yeni savunma sistemlerinin kullanılması;
- Diğer kurumlarla ve özel sektörle ortaklık;
- Müttefikler ve uluslararası ortaklarla güçlü ilişkiler;
- Siber uzmanlığı ve teknolojik yenilikleri artırmak.

Amerika'nın amacı yalnızca bilgi sistemleri için etkili koruma sağlamak değil, aynı zamanda ABD'nin siber uzaydaki üstünlüğünü garanti altına almaktır. Toplamda, 2010'dan 2015'e kadar, ABD hükümetinin siber savunma için 50 milyar dolar veya yılda yaklaşık 10 milyar dolar harcaması beklenmekteydi ve on binlerce görevli bu konular üzerinde çalışmaktaydı. Askeri harcamaların azalacağına dair genel bir tahmin olsa da, siber savunma departmanının bütçesi geçmiş yıllara göre büyümeye devam etmiştir. Örneğin, 2020'de Siber Güvenlik bütçesi 17 milyar dolardır.[125]

Son olarak, Amerikan ordusunun bilgisayar mücadelelerinde savunmayı ve saldırıyı birleştiren bir doktrini olduğunu bilinmektedir. Bu nedenle, böylesi bir doktrin, siber uzaya adanmış Kasım 2011 Kongresinde Savunma Bakanlığı'nın raporunda bulunmaktadır. Bu

125 The White House, Funding Cybersecurity, URL: https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf E.T 12 September 2020.

belgeye göre[126]: "*Başkan, milletimizi, müttefiklerimizi, ortaklarımızı ve çıkarlarımızı siber uzaydaki düşmanca eylemlerden korumak için gerekli tüm araçları kullanarak yanıt verme hakkını saklı tutmaktadır. Düşmanca eylemler, ABD ekonomisine, hükümetine veya ordusuna yönelik önemli siber saldırıları içerebilmektedir.*" ve aşağıda belirtilmektedir: "*Başkan tarafından yönlendirilirse, Savunma Bakanlığı, silahlı çatışma hukuku dâhil olmak üzere, kinetik yetenekler için bakanlığın izlediği politika ilkeleri ve yasal rejimlere uygun bir şekilde saldırı amaçlı siber operasyonlar yürütecektir*.

2. Birleşik Krallık

Birleşik Krallık, Birleşik Devletler ile birlikte siber güvenlik konularını ve bilgi sistemlerinin korunmasının önemini çok erken anlayan ülkelerden biri olarak kabul edilmektedir. Gordon Brown'un önceki İşçi Partisi hükümeti döneminde, Mart 2008'deki ulusal güvenlik stratejisi[127], bilgi sistemlerine yönelik saldırıları ülkenin güvenliğine yönelik bir tehdit olarak tanımlanmıştır.

İngiltere, 2011 yazında özellikle Dışişleri Bakanlığı'nı ve 2010'da önceki yılın iki katı olarak bin siber saldırıya uğradığı söylenen savunma bakanlığını hedef alan bir dizi siber saldırıya maruz kalmıştır. Eski Savunma Bakanı Liam Fox, Haziran 2011'de şunları söylemiştir: "*Sistemlerimiz suçlular, yabancı istihbarat servisleri ve insanlarımızı sömürmek, sistemlerimizi bozmak ve bilgi çalmak isteyen diğer kötü niyetli aktörler*

126 Department of Defense Cyberspace Policy Report*, "A Report to Congress Pursuant to the National Defense Authorization Act for fiscal Year 2011,* Section 934, Kasım 2011. URL: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-059.pdf E.T 29 Mayıs 2020.

127 Cabinet Office, *The National Security Strategy of the United Kingdom Security in an interdependent world,* Mart 2008. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf E.T 1 Haziran 2020.

tarafından hedeflenmektedir. Size zorluk hakkında bir fikir vermek için geçen yıl, Savunma Bakanlığı 1000'den fazla potansiyel olarak ciddi saldırıyı soruşturmuş ve engellemiştir.", "Savunma müteahhitlerine yapılan son yüksek profilli saldırıların gösterdiği gibi siber uzayda majino hattı yoktur. Savunma ve güvenlik endüstrilerindeki ulusal fikri mülkiyetimiz, sistematik bir yağmacılık nedeniyle risk altındadır."[128]

Birleşik Krallık'taki mevcut siber savunmanın kurumsal mimarisi, esasen İşçi Partisi hükümetinin ulusal bir siber güvenlik stratejisi benimsediği 2009 yılına dayanmaktadır. Bu strateji, Ekim 2011'de "Dönüştürücü Bir Ulusal Siber Güvenlik Programını"[129] benimseyen "Stratejik Savunma ve Güvenlik İncelemesinin" kabul edilmesinin bir parçası olarak gözden geçirilmiştir. Bu mimari, genel bakanlıklar arası koordinasyondan, hükümet stratejisinin geliştirilmesinden, bilgi güvenliğinin korunmasına ilişkin harcamaların yönetilmesinden ve özel sektör ve halk ile ilişkileri denetlemesinden sorumlu Kabine Ofisi'nin (Başbakanlık ofisi) "Siber Güvenlik ve Bilgi Güvence Ofisi" yetkisi altına yerleştirilmiştir.

İngiltere'nin Kasım 2011'de yayınlanan yeni siber güvenlik stratejisi[130], Birleşik Krallık yetkililerinin bu konuya olan bağlılığını göstermektedir. Bu yeni strateji kapsamında Birleşik Krallık Hükümeti, bilgi sistemlerinin karşılaştığı siber tehditlerle ilgili tüm

---

128 BBC News, *Ministry of Defence foiled 1,000 cyber-attacks says Fox,* 7 Haziran 2011. URL: https://www.bbc.com/news/uk-politics-13691375 E.T 1 Haziran 2020.

129 HM Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review,* Ekim 2010. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf E.T1 Haziran 2020

130 Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world,* 2011. URL: https://a51.nl/sites/default/files/pdf/uk_cyber_security_strategy_final.pdf E.T 1 Haziran 2020.

sorunların üstesinden gelmek için Ulusal Siber Güvenlik Programına 650 milyon sterlin tahsis etmiştir.

Uluslararası işbirliği açısından Birleşik Krallık, 1-2 Kasım 2011 tarihlerinde Londra'da 700'den fazla kişiyi bir araya getiren uluslararası bir siber uzay konferansı[131] düzenlemiştir. Bu konferansa 61 ülkeden (Amerika Birleşik Devletleri, Rusya, Çin vb.) çok sayıda temsilci, uluslararası kuruluşların temsilcileri (BM, AB, NATO), sivil toplum temsilcileri ve çeşitli sektörlerden temsilciler katılmıştır. Birleşik Krallık Dışişleri Bakanı William Hague bu konferansta İnternet özgürlüğü lehine konuşmuş ve İnternet'i düzenleme konusundaki isteksizliğini belirtmiştir. İngiltere Başbakanı ise İngiliz hükümetinin siber saldırılarla mücadele etme ve özel sektöre ilişkin siber güvenlik kapasitelerini güçlendirme konusundaki kararlılığını vurgulamış, siber saldırıların İngiliz ekonomisine maliyetinin yılda 27 milyar sterlinden fazla olduğunu tahmin etmiştir. 2016 yılında yeni bir siber strateji raporu yayınlanmıştır. Hükümet, 5 yıl (2016-2021)[132] içindeki tüm siber faaliyetleri kapsaması amaçlanan bu rapor kapsamında, esas olarak bilgi sistemlerini dış ve iç siber tehditlerden caydırmaya ve korumaya odaklanan hâlihazırda belirlenmiş 13 stratejik önlemi gerçekleştirmek ve siber uzayda yeni teknikler ve yenilikler geliştirmek için 1,9 milyar sterlin harcayacaktır. Buna ek olarak, Birleşik Krallık hükümeti, raporda belirtildiği gibi, askeri siber savunma yeteneklerine kesinlikle inanmaktadır, yalnızca birkaç ülke Birleşik Krallık'a karşı ulusal bir siber tehdit olarak nitelendirilebilecek bir siber saldırı

131 Foreign & Commonwealth Office and The Rt Hon William Hague, *London Conference on Cyberspace: Chair's statement,* 2 Kasım 2011. URL: https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement E.T 1 Haziran 2020.

132 HM Government, *The National Cybersecurity Strategy 2016-2020*, 1 Kasım 2016.

gerçekleştirebilmektedir. Ancak rapor, diğer birçok ülkenin yakın gelecekte İngiltere'yi tehdit edebilecek karmaşık siber teknoloji geliştirme yolunda olduğunu kabul etmektedir.[133]

3. Almanya

Alman yetkililere göre, Almanya'da bilgi sistemlerinin güvenliğine yönelik tehditler, bilgisayar saldırılarının sıklığı, çeşitliliği ve sayısı bakımından sürekli artmaktadır. Alman ekonomisi üzerindeki etkileri, 2009 yılına göre % 66 artışla 2010 yılı için 61,5 milyon Euro olarak tahmin edilmiştir. Federal hükümet, Şubat 2011'de "Almanya için yeni bir siber güvenlik stratejisi"[134] kabul etmiştir. Bu stratejinin temel amacı, hükümet içinde koordinasyon araçları geliştirerek, ancak her şeyden önce özel sektörle bağlantılar geliştirerek Almanya'nın bu risklere karşı genel direncini güçlendirmekti. Bu, ulusal düzeyde paylaşılan bir siber güvenlik kültürü geliştirmek anlamına gelmektedir.

Aslında Alman stratejisi, ulaşım, elektrik veya bankacılık sektörü gibi sektörlerde ve diğer özel sektör aktörleriyle gönüllü olarak kritik altyapı operatörlerinin düzenleyici veya denetleyici otoriteleri ile ilişkilerin sistematik bir şekilde yapılandırılmasını sağlamaktadır. Almanya 2016'da yeni bir siber güvenlik stratejisi başlatmıştır. Bu Siber Güvenlik Stratejisi[135], siber güvenliğe atıfta bulunarak Federal Hükümetin faaliyetleri için bölümler arası stratejik çerçeveyi oluşturmuş, 2011'den itibaren siber güvenlik stratejisini güncellemiştir. Bu rapor, Federal Hükümetin çabalarını bu dört alana odaklayacağını belirtmektedir:

---

133 *The National Cybersecurity Strategy 2016-2020*

134 Federal Ministry of the Interior, "*Cyber-Sicherheitsstrategie für Deutschland*". Şubat 2011. (Almanca versyonu) https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile E.T 1 Haziran 2020.

135 Federal Ministry of the Interior, "*Cyber-Sicherheitsstrategie für Deutschland*". 9 Kasım 2016 (DE)https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf E.T 1 Haziran 2020

- Sayısallaştırılmış Bir Ortamda Güvenli ve Kendi Belirlediği Eylem: Dijitalleştirilmiş bir ortamda güvenli ve bağımsız bir şekilde hareket edebilmek, siber güvenliğin temel bir esasıdır. Almanya'daki şirketler, devlet ve diğer aktörler gibi vatandaşlar da bilgi teknolojisinin kullanımıyla ilgili fırsatları ve riskleri kavrayabilmeli, bunları değerlendirebilmeli ve eylemlerini buna göre sıralayabilmelidir (değerlendirme yeterliliği).
- Devlet ve Ticari Siber Güvenliğin Ortak Misyonu: Almanya'da siber güvenliği yüksek düzeyde kalıcı olarak garanti altına alabilmek için, güvene dayalı bir işbirliği ve devlet ile ekonomi arasında yakın bir alışveriş şarttır. İşbirlikçi yaklaşımın bir parçası olarak, ilgili yetkinlikleri bir araya getirmenin ve kullanmanın yeni yolları da vardır.
- Devlet Çapında Verimli ve Sürdürülebilir Siber Güvenlik Mimarisi: Devlet, siber uzay da dâhil olmak üzere, ülkede güvenliği, adaleti ve özgürlüğü garanti etmelidir. Bu, çeşitli aktörleri federal düzeyde etkin bir şekilde birbirine bağlayan ve ayrıca eyaletleri (vilayetleri), belediyeleri ve ekonomiyi gözetleyen modern bir siber güvenlik mimarisi gerektirmektedir.
- *Almanya'nın Avrupa ve Uluslararası Siber Güvenlik Politikasındaki Aktif Konumu*: Sayısallaştırılmış bir dünyada ulusaşırı ağlar göz önüne alındığında yüksek düzeyde siber güvenlik, ancak ilgili Avrupa, bölgesel ve uluslararası süreçlere ulusal önlemlerin yerleştirilmesi ve güçlendirilmesi ile elde edilebilir.

Rapor, bu strateji kapsamında *Almanya'nın Avrupa ve uluslararası siber güvenlik politikasında aktif* bir rol oynamaya devam edeceğine odaklanmaktadır. Avrupa'da ve dünya çapında net bir hukuki çerçeve, güven oluşturma ve daha fazla dayanıklılık, Almanya için daha fazla koruma anlamına gelecektir.

4. Çin

1990'ların ortalarında İnternet geliştirme yarışının sonlarından başlayan Çin, bugün siber uzayda büyük ve önemli bir aktördür.[136] Web devlerinin (Baidu, Alibaba, Tencent, Sina) ortaya çıkışı, son derece dinamik bir iç pazarda kendisini yabancı platformlardan kurtarmasını sağlamıştır.

Asya'daki siber savunmanın jeopolitik durumu, açıkça Amerika Birleşik Devletleri ve Çin arasındaki rekabet tarafından yönetilmektedir.[137] Bununla birlikte, Asya ülkeleri ve iki büyük güç arasındaki ekonomik değişimlerin, diplomatik faaliyetlerin ve stratejik ortaklıkların yoğunluğu açısından medyada ve yeni bir soğuk savaş türünün siyasi söyleminde yinelenen analoji uygunsuz görünmektedir. Karşılıklı bağımlılık öyle bir şeydir ki, çoğu ülke taraf seçmek zorunda kalmamayı tercih eder ve hem Amerika Birleşik Devletleri hem de Çin açık çatışmanın ardışık sonuçlarından korkmaktadır. Bununla birlikte, siber uzayda ekonomik, politik ve stratejik konuların birbirine olan yakınlığı, başka alanlarınkinden daha fazladır. Tehditlerin analizi, Çin'in yükselişinin, çoğu ülkenin endişelerinin merkezinde yer alırken, ABD'nin bölgedeki gelecekteki rolünün üzerinde durduğunu göstermektedir.[138] Asya uluslarının hem seçkinleri hem de halkları, güçlü bir güvensizlik ve çözülmemiş bölgesel ve tarihsel anlaşmazlıklarla bağlantılı milliyetçiliğin şiddetlenmesi bağlamında bölgenin siyasi veya ekonomik istikrarını tehdit edebilecek

---

136 Editor’s note, Evolution of the Internet in China, URL: http://www.chinadaily.com.cn/china/2016even/index.html Accessed 15 September 2020

137 M. Schulze and D. Voelsen, Strategic Rivalry between United States and China. Causes, Trajectories, and Implications for Europe, SWP Research Paper 2020/RP 04, s.32

138 S. L. Kastner, The Global Implications of China's Rise, International Studies Review, cilt. 10, sayı. 4 (Aralık., 2008), ss. 786-794. JSTOR https://www.jstor.org/stable/25482025 E.T. 15 Eylül 2020.

çatışmalardan korkmaktadır. Bu bağlamda siber, Asya'da ve Çin ile ABD arasındaki ikili ilişkilerde önemli bir dava konusu haline gelmektedir.

Asya'daki siber tehdit ortamı, büyük ölçüde Çin'in yükselişi ve siber yeteneklerinin gelişimi tarafından yönetilmekte ve yapılandırılmaktadır. Çin, ekonomik alanlarda, akademik ve kültürel alışverişlerde yumuşak güç politikası yoluyla, Asya ülkeleri ile sık sık "sempati atağı"[139] olarak tanımlanan bir politika izlemektedir. Özellikle, altyapı geliştirme yatırımları yoluyla, güvenlik açısından sonuçları olabilecek önemli yardımlar sağlamaktadır. Alan Chong, şirketlerin ve Çin hükümetinin bu altyapı projelerinin kontrol sistemlerine doğrudan erişime sahip olduğunu ve bu da onları devre dışı bırakmalarına izin verebileceğini belirtmiştir.[140] Öte yandan, bu altyapıların kullanıcıları, hükümetler ve eğitim veya bakım sağlayan Çin şirketleri arasında teknolojik bir bağımlılık gelişmiştir.[141] Son olarak, bu projelerin tamamlanması veya tamamlanması sonrasında Çin'den çekilme tehdidi inandırıcıdır; Altyapılar aynı zamanda Çin'in izinsiz girişlerini kolaylaştırabilecek BT ürünlerine de bağımlıdır.

Siber uzay sorunları, Çin ile birçok ülke arasında en üst düzeylerde resmi tartışmaların konusu haline gelmiştir; bu nedenle, Amerikalı ve Çinli yetkililer, siber uzayda güvenlik kurallarını tanımlama ihtiyacı üzerine[142] siber uzay üzerinde tartışmaktadırlar. Bu alışverişlere, diplomatik ilişkilerin kalitesine göre örnek verilecek olursa: Siber Çalışma Grubu içindeki diyalog Mayıs 2014'te Çin tarafından askıya alınmıştır. Çin, sesini

---

139 J. KURLANTZICK, Charm Offensive: How China's Soft Power Is Transforming the World, Yale University, 2007, ss. 37-60. URL: http://www.nicoravanilla.com/uploads/2/4/1/1/24114923/kurlantzik2007.pdf E.T 15 Eylül 2020.

140 A. Chong, *China and Southeast Asia: Offline Information Penetration and Suspicions of Online Hacking.* A view from Singapore, 2013.

141 A. Chong, 2013

142 (örneğin, devletlerarasında şiddetin artmasına yol açabilecek herhangi bir yanlış yorumlanma riskinden kaçınmak için)

uluslararası ölçekte daha geniş bir şekilde dayatmak istemektedir, siber uzayın normalleşmesi ve yönetiminin zorlukları üzerine ikili diyaloglara açık olup, motiflerinden biri egemenliği savunmaktır. Bu nedenle, standardizasyon organlarında (ITU) bulunmakta ve yabancı ortaklarla anlaşmaları resmileştirmektedir.

Çin, her türlü yolla (istihbarat, izinsiz giriş, casusluk) üst düzey bilimsel, teknolojik, ekonomik, stratejik ve politik bilgileri toplamak için ağlar aracılığıyla saldırıya liderlik etmektedir. Anahtar kavram, ister askeri, ister politik veya ekonomik alanda olsun, Çin gücünün ifade edilmesi için tüm medyanın merkezine stratejik bilgi ustalığını yerleştiren bilgileştirme'dir.

Amerika Birleşik Devletleri'nin askeri üstünlüğüyle karşı karşıya kalan Çin, barış zamanında kapasitesini artırmak için uzun vadeli bir strateji üzerine oynamaktadır. Bilgi Harbı kavramı, Deng Xiaoping tarafından 1980'lerde başlatılan ve birden çok kaynaktan toplama, çapraz kontrol, bilgi doğrulama ve güvenilirliğini sağlama, aynı zamanda bilgiyi manipüle etme, deforme etme, aldatmaya dönüştürme veya rakibi şüpheye düşürmek için kapasitesini geliştirmeyi amaçlayan ordu modernizasyon politikasının merkezinde yer almaktadır.[143] Bu durum, tüm klasik literatürde oldukça mevcut olan stratejik ilkelere dayanmaktadır ve burada, büyük ölçüde, rakibi caydırarak savaşı tercihen savaşmadan kazanmak için üstün zekâ ve düşmanın bilgisinin rolünde ısrar eden Sun Tzu'nun öğretilerinden esinlenilmiştir.[144] Bu araçlar, askeri araçlarla sınırlı değildir, düşmanın çıkarlarını hesaba katması için tüm araçlar iyidir ve siber uzayda fırsatlar sonsuzdur.

143 Major General W. Pufeng, The Challenge of Information Warfare in M. Pillsbury (ed)., Chinese View of Future Warfare, National Defense University Press, Washington DC, 1998, ss. 317-326

144 M. McNeilly, *Sun Tzu and the Art of Modern Warfare*, Oxford University Press, 2001.

Bilginin manipülasyonu, fikirlerin etkisi, casusluk, saldırıların tanımlanmasındaki zorluklar, eylem beklentisi, kaynakların değerlendirilmesi vb.

Mark McNeilly, bu yaklaşımı, en az yatırımla olabildiğince fazla etkiye sahip olmak, savaşta kendi milletini kaybetmeden düşmanı kuşatmak olan go oyunuyla karşılaştırmaktadır.[145] Bu nedenle bu strateji, çatışma durumunda daha düşük maliyetle hızlı bir zafer sağlamak için zemini hazırlamak amacıyla uzun vadeli bir stratejidir.

Siber strateji ulusal önceliğe yükseltilmiştir; hükümet bunu sadece askeri değil, aynı zamanda ekonomik açıdan da ulusal kalkınma planının bir parçası olarak görmektedir. İçerik kontrolünün ötesinde, siyaset artık egemenlik gibi altyapı ve diplomatik konuları da içermektedir. Bütçe ve kaynaklar için bir rekabeti vurgulayan Profesör Yi'ye göre[146], siber güvenlik ve bilgisayarlaşma terimleri ilk kez kullanılacaktır. Bu karar, genellikle en yüksek hükümet ve askeri komuta düzeyinde koordineli ve merkezileştirilmiş olarak görülen Çin Siber Stratejisinin sınırlarını ortaya koymaktadır. Çinli uzmanlar, tersine, çok büyük bir bürokrasiye, bazen çelişkili çıkarlara sahip aktörlerin çoğalmasına ve karar alma süreçlerinin büyük bir parçalanmasına, ordunun büyük bir özerkliğe sahip ayrı bir birim oluşturduğuna işaret etmektedirler.[147] Bazıları, Halk Kurtuluş Ordusunun stratejik literatürde[148] savunulduğu gibi siber yeteneklerin kullanımını operasyonlarına nasıl

145 A.g.e
146 S. Yi, *Cyber security depends on US cooperation*, China Daily 16 Aralık 2015. URL: http://europe.chinadaily.com.cn/opinion/2015-12/16/content_22724400_2.htm E.T 5 Haziran 2020.
147 J. Goodrich, *Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy*, dans le cadre du workshop *China and Cybersecurity: Political, Economic, and Strategic Dimensions,* 2012: http://igcc.ucsd.edu/assets/001/503568.pdf
148 J. Deal, *Chinese Information War: Historical Analogies and Conceptual Debates*, dans le cadre du workshop *China and Cybersecurity: Political, Economic, and Strategic Dimensions,* 2012: http://igcc.ucsd.edu/assets/001/503568.pdf

bütünleşmiş edip yapılandırabileceğini sorgulamıştır. Asker yetiştirmek için hassas bilgilerin paylaşılması, kurumların gizliliğini geliştirmek için uzun bir yol kat etmektedir.

Çin, karmaşık ve çelişkili yasal ve siyasi parçalanma ile siber uzaydaki egemenliğini korumayı planlarken, gelişmekte olan ülkelerin büyümesi, doğrudan Amerikan egemenliğinin sorgulanmasına yol açmaktadır. Ayrıca, Amerika Birleşik Devletleri ile yoğun rekabet ve yüksek bölgesel istikrarsızlık bağlamında, siber uzayda toplu güvenlik standartlarının ve davranış kurallarının geliştirilmesine katılmayı amaçlamaktadır. İki büyük güç arasında artan gerilim, çapraz ateşe yakalanan diğer uluslar için bölgenin ekonomik ve siyasi istikrarı konusunda ciddi endişeler yaratmaktadır. Çin'in bakış açısına göre, tehdit meselesi Amerika Birleşik Devletleri ile sınırlı değilken, özellikle Japonya ve Güney Kore ile denizde egemenlik çatışmaları etrafındaki gerginlikler ortadadır. Asya'daki tehdit haritalaması, rekabet ve işbirliği dinamiklerinin ülkeler arasındaki siber uzayda ortaya çıktığı bağlamı anlamamıza yardımcı olmaktadır.

5. Rusya

Ukrayna'da ve Batı ülkelerinde siber saldırı şüpheleri, dünyanın dört bir yanındaki sosyal ağlarda fikirlerini değiştirmek için çalışan troller, Demokrat Parti'den e-postalar çalan bilgisayar korsanları, vb. Rusya'nın siber uzaydaki varlığı muhtemel göz korkutucu görünebilir. Rusya ile siber uzay arasındaki ilişkiye bakıldığında ilk bakışta dikkat çeken unsurlardan biri, 2007'den beri Moskova'nın karıştığı saldırıların sayısıdır. Böylelikle Rusya, şirketlere saldıran bilgisayar korsanları ve siyasi partiler ile forumlarda yanıltma haber yapan troller arasında, yeni bir evrensel siber düşman olarak yer almaktadır. Daha önce Çin'e devredilen bu yer artık Rusya'nın ayrıcalığıdır[149], öyle ki daha detaylı bir analiz

149 C. Radu, China, *Russia Biggest Cyber Offenders A new study attributes more than 200 cyberattacks to the two countries over the past 12 years,* 1 Şubat 2019. URL:

yapılması gerekmektedir.

Çelişkili etkilerden kaçmanın son derece zor olduğu siber uzaya karşı daha takıntılı bir yaklaşıma dayanarak, Rusya'ya atfedilen eylemlerin kaydını tutmak gerekli görünmektedir. Moskova, 2000'lerin ortalarından önce siber uzayda görece az görünürken, iki olay, Rusya'nın siber uzayda inandırıcı bir aktör olmasına katkıda bulunmaktadır: İlk olay 2007'de,[150] 2. Dünya Savaşı'nın Sovyet "kurtarıcılarına" adanmış bir heykelin cıvatasını açmaya karar veren Estonya hükümetini hedef alan büyük bir siber saldırı sırasında gerçekleşmiştir. Başlangıçtan beri Rus kökenli olduğu konusunda şüphe duyulmayan bu saldırının asıl özgünlüğü, heykelin kaldırılması için sembolik intikam talep eden vatansever bilgisayar korsanlarının ve *Russian Business Network* gibi siber mafyanın karışık bir koalisyonu aracılığıyla gerçekleşmesidir.[151] Rus devletinin rolü ile ilgili olarak, saldırıya doğrudan veya dolaylı olarak dâhil olduğunu destekleyen hiçbir kanıt yoktur, ancak siber saldırının Vladimir Putin'in ikinci döneminde Batı ülkelerinde jeopolitik yönelimine ve Rus milliyetçiliğinin iddiasına hizmet ettiği kesindir.[152]

İkinci büyük olay, Gürcistan'a karşı 2008 savaşından kısa bir süre sonra gelmiştir.[153] Bu vesileyle Rus ordusunun performansı, birçok sorunun devam etmesine rağmen Batılı

---

https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows E.T 3 Temmuz 2020.

150 Windrem, 2016

151 A. Kozlowski, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, European Scientific Journal Vol. 3 (Şubat 2014), s. 241.

152 9 Mayıs 2007: Rusya'nın Nazi Almanyası karşısındaki zaferini kutlamak için Rus askerlerine yapılan bir konuşma sırasında: "Bugün [...] savaş kahramanlarına anıtları kirletmeye kalkışanlar kendi halklarına hakaret ediyor, devletler ve insanlar arasında yeni bir güvensizlik ve uyuşmazlık ekiyor. . " Vladimir Putin (tercüme edildi), "Büyük Vatanseverlik Savaşı'nda Zaferin 62. Yıldönümünü Kutlayan Askeri Geçit Töreninde Konuşma", Kremlin.ru, 9 Mayıs 2007, http://en.kremlin.ru/events/president/transcripts/24238 E.T 4 Temmuz 2020.

153 Kozlowski, 2014

gözlemciler tarafından beklenenden daha iyi olmuştur. Siber konularda, Gürcistan'a karşı angaje olan Rus birimleri, Estonya'ya yapılan saldırıyı güçlü bir şekilde hatırlatan bölgedeki bilgilendirme çabalarından bahsetmek yerine, Gürcistan ordusunun iletişim ve komuta sistemlerini felç etmek için tüm elektronik savaş ve siber saldırı eylemlerini kullanmıştır.[154]

Her iki durumda da, 2014 yılında Ukrayna'ya[155] da genişletilebilecek olan Estonya ve Gürcistan, rakibin göreceli zayıflığı teknik açıdan dikkate alınmalıdır. Bu iki ülkedeki kamu altyapılarının veya askeri unsurların siber güvenliği Avrupa, Amerika veya Çin standartlarına kıyasla çok zayıf görünmektedir. Rusya'nın veya Rus uyruklu aktörlerin becerilerini en aza indirgemek istemeden, siber saldırıların sonsal olarak yapılabileceği analizde düşmanların veya muhaliflerin seviyesinin dikkate alınması gerekmektedir. Ancak bu eylemler, Rusya'nın hiçbir zaman beklendiği gibi olmadığını da göstermektedir. Estonya örneğinde, yalnızca bir dizi varsayım olsa bile, Moskova'ya göre hikâyeyi hiçe sayan bir hükümetin sembolik cezasının gerçekleştirilmesi için hackerların ve trollerin eylemlerinin koordinasyonu, özellikle gizleme kullanımında iyidir. Gürcistan örneğinde, Rusya, Gürcistan'ı geleneksel yöntemlere ek olarak siber uzay kullanan birleşik operasyonlarının düzeyi ile şaşırtmıştır.

Rusya, Amerikan-Japon-Avrupa siber uzay yönetiminden[156] daha küresel bir yönetime geçme ihtiyacı konusunda Çin'in pozisyonlarına yaklaşmaktadır. Bununla birlikte, teknik açıdan Çin'den daha az gelişmiş olduğu ortaya çıkmıştır. Pekin, 1990'lardan beri donanım katmanından başlayarak tüm katmanları kapsayan eksiksiz bir siber ekosistem geliştirmek

---

154 Kozlowski, 2014
155 Windrem, 2016
156 T. Renard, *EU Cyber Partnerships : Assessing the EU cyber strategic partnership with third countries in cyber domain,* European Politic and Society, 2018 http://aei.pitt.edu/94368/1/EPS-EU-cyber-partners_RENARD_AM.pdf

için çalışırken, Rusya, 1990'ların sonlarında antivirüs[157] alanında bir miktar başarı elde etmesine rağmen, teknik katmanlar üzerinde başkaları tarafından geliştirilen çözümlere bağımlı kalmıştır.

Eylül 2013'te Brezilya Devlet Başkanı Dilma Rousseff, Brezilya'yı Cape Town, güney Hindistan ve Tayvan Boğaz üzerinden Vladivostok'a bağlayacak olan, 2015 yılına kadar 34.000 kilometre uzunluğunda bir denizaltı kablo ağı oluşturmak amacıyla *BRICS Cable* olarak bilinen büyük bir projenin başlatıldığını duyurmuştur.[158] Bu, Snowden vakasının birkaç ay önce ortaya çıkardığı bir derecedir.[159] BRICS Cable projesi, diğerlerinin yanı sıra, Putin belagatının başka yerlerde yaygın olarak kullandığı temsiller ve duruşlar temelinde, Rusya'nın kendisini bu yeni evrende nasıl konumlandırma niyetinde olduğunun yalnızca bir örneğidir; yani Devletin iktidarının ve egemenliğinin kutlanmasına dayanan belirli bir vatanseverlik biçiminin gelişmesidir.

Nitekim bilgi alanı kavramı esas olarak karar çevreleri ve doktriner metinlerle sınırlıysa da bu, Rusya'da internetin temsil edilme şekli ile ilgili olarak yetkililer ve kullanıcılar arasında aşılamaz bir boşluk olacağı anlamına gelmemektedir. Aksine, başkalık ve bilgi alanının altında yatan belirli bir egemenlik biçimini savunma fikri, büyük ölçüde, siber

157 R. Messier, *Collaboration with Cloud Computing: Security, Social Media, and Unified Communication,* Syngress Publication, Massachusetts, 2014, s. 9.
158 N. Rolland, A fiber-optic Silk Road, 2 Nisan 2015. URL: https://thediplomat.com/2015/04/a-fiber-optic-silk-road/ E.T 30 Haziran 2020.
159 S. Davies (Compilation), A Crisis of Accountability A global analysis of the impact of the Snowden revelations, June 2014. Available at https://www.christopher-parsons.com/Main/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

uzayın bir bölümünü "bölgeleştirmeye" yönelik önemli bir girişimde, yani ağın bir kısmının anlatımında bulunmakta olup bu; bir dil, uygulama ve değerler topluluğu olan Runet'tir[160].

Nesnel olarak, Runet terimi bugün İnternet'in Rusça konuşulan bölümünü tanımlamak için yaygın olarak kullanılmaktadır. Bu, çok somut bir şekilde, bilgiyi yaymak için Rusça kullanan tüm web siteleri, tüm sunucular ve tüm e-posta adresleridir. Bununla birlikte, Rusça konuşulan İnternete özgü bir terimin zaten mevcut olması başlı başına güçlü bir işarettir: Bugün Rusça, İngilizce'den sonra (% 59,3) dünya trafiğinin % 8,4'ünü kaplayan ağda en çok kullanılan ikinci dildir, Fransızca gibi batı ülkelerinde popüler bir dil olmasına rağmen yalnızca % 2,8'dir.[161]

Rus siber uzayı, kökenleri Soğuk Savaş'a kadar uzanan belirli bir fiziksel ve insani organizasyon sayesinde yapılandırılan çok çeşitli hırsların ve jeopolitik temsillerin sahibi olma özelliğine sahiptir. Bilgi alanı gibi stratejik bir kavramın varlığı, yetkililerin kendilerini "batı" olarak nitelendirilen bir vizyonun hâkim olduğu bir tartışmadan uzaklaştırma arzusunu doğrulamaktadır. Runet fikri, Rus siber uzay segmentinin fiili bağımsızlığıyla desteklenen bu ayrışma arayışını da doğrulamaktadır. Yine de bu bağımsızlık, çağdaş Rusya'ya özgü tahakküm mantığına tabidir ve ne kayırmacı mekanizmalardan ne de ondan kaynaklanan kontrol etme iradesinden kaçmayacaktır. Bunlar, işleyiş mekanizmalarıyla ve ayrıca Federasyonun iç siyasi yaşamı ve Sovyet sonrası alanın tamamı üzerindeki etkisiyle (Kiev'deki son isyanlar ve bu durumda İnternet'in oynadığı rol düşünülmektedir), egemenlik ve düzenlemenin şimdiye kadar en önemli noktalar olduğu bir sistemin kalıcılığını sorgulamaktadır.

---

160 S. Ilona, Internet Governance in Russia – Sovereign Basics for Independent Runet (18 Temmuz 2019). SSRN: https://http://dx.doi.org/10.2139/ssrn.3421984

161 25 Mart 2020 itibariyle web siteleri için içerik dillerinin kullanım istatistikleri, https://w3techs.com/technologies/overview/content_language E.T 3 Temmuz 2020

C. GENEL ULUSLARARASI HUKUK VE SİBER UZAYIN YÖNETİMİ

Bazı büyük ileri teknoloji ülkelerinin siber stratejilerini analiz ettikten sonra, siber uzayın yönetimi ile ilgili uluslararası topluluk düzeyinde ortak bir payda gibi bir şeye sahip olunup olunamayacağını incelemenin zamanı gelmiştir.

Siber saldırıların artan önemi göz önüne alındığında mevcut kuralların uygun ve yeterli olup olmadığı merak edilebilmektedir. Siber uzay, kesinlikle bir "kanunsuzluk" alanı değildir, yine de kara, deniz veya hava çatışmalarını düzenlemek için tasarlanmış kurallar analojisi yoluyla uygulamanın her zaman basit olmadığını görmekteyiz. Bazı yazarların uluslararası hukukta çok az istismar edilen kavramlara başvurma konusundaki yaratıcı önerileri – gerekli özen ilkesi veya zorunluluk durumu gibi mevcut normatif çerçevenin tamamen uyarlanmadığını göstermektedir. Aslında, siber saldırılara verilen yanıtlar, özellikle siber saldırıları tanımlama ve ilişkilendirme sorunu nedeniyle sınırlı kalmaktadır. Gittikçe daha fazla sayıda devlet dışı aktörün yanı sıra Devletlerin de kullanması muhtemeldir ve kendini savunma veya karşı önlemlerin kullanılması yalnızca katı koşullar altında yapılabilecektir. Zorunluluk durumuna başvurma ilginç olsa bile, yalnızca istisnai durumlarla ilgili olduğu için çok sınırlı görünmektedir. Bu nedenle bu durum, devletleri bir siber saldırıyı bir devlete atfetmene kadar güç kullanımına veya karşı önlemlere başvuramayacakları için hassas bir durumda bıraktırmaktadır.

Bu sorunlarla karşı karşıya kalınca, Devletler için, kendi yasasını geliştirmek ve Devletlere uygun yanıtlar vermek için farklı olanaklar mevcuttur.

Bazıları, uluslararası hukukun siber uzaya uyum sağlamak için resmi olarak değiştirilmesine gerek olmadığını ve bunun yerine geçerli yasayı belirlemek için Devletlerin uygulamalarına dayandığını düşünmektedir. Bu, bir azınlık pozisyonudur; Devletlerin ve literatürün çoğu, devletlerin siber uzaydaki davranışlarını düzenlemeyi amaçlayan bir antlaşma kabul etmeyi önermektedir.[162]

Bu antlaşmanın, örneğin Cenevre Sözleşmelerinde olduğu gibi, tüm üyeler için geçerli olan uluslararası hukuk normlarından mı oluşması gerektiği veya bu antlaşmanın, Devletlerin iç yasalarında hükümlerini uyarlamasını gerektiren Budapeşte Sözleşmesi ile aynı modelde mi işlemesi gerekip gerekmediği görülecektir.[163] Diğer öneriler, devletler tarafından resmi olarak bağlayıcı olmayan davranış kurallarının benimsenmesini teşvik etmeyi amaçlamaktadır. Literatürün bir kısmı için, siber uzay ile ilgili yeni standartlar benimsemeye gerek yoktur veya en azından hemen gerekli değildir. Bazıları, hukukun devlet uygulamaları yoluyla gelişmesini beklemeyi tavsiye etmiştir.[164] Ancak, bu yaklaşımın bazı eksiklikleri vardır. İlk olarak, özel bir kuralın oluşturulması teoride anında (*instant custom*) yapılabilmesine rağmen, çoğu özel kural belirli bir süre sonra oluşturulmaktadır. Bu nedenle, "genel uygulamayı hukuk olarak kabul eden"[165] bir kurallar bütününe sahip olmak muhtemelen yıllar alacaktır. Son olarak, siber uzayda devletlerin sahip olduğu farklı çıkarlar düşünüldüğünde, uluslararası toplumun çoğunluğu tarafından kabul edilen birleşik bir kurallar bütününe ulaşma olasılığı düşüktür.

---

162 D. Andrew and J. Lech, Establishing Cyber Warfare Doctrine, Journal of Strategic Security 5, no. 1 (2012) : 31-48. URL: https://scholarcommons.usf.edu/jss/vol5/iss1/7 E.T 18 Eylül 2020

163 Avrupa Konseyi, Siber Suçlar Hakkindaki Sözleşmesi, ETS 185 – Cybercrime (Convention), 23.XI.2001, Budapeşte 2001, European Treaty series no 185 URL: https://rm.coe.int/1680081561

164 Örneğin Uluslararası Kızıl Haç Komitesi.

165 Uluslararası Adalet Divanı Statüsünün 38. maddesinin şartlarını kullanmak.

Bu sorun, bir antlaşma taslağı hazırlama fikrinden eksik değildir. Bununla birlikte, taslağın hazırlanması, amacı uluslararası toplumun çoğunluğu için tatmin edici bir orta değer bulmak olan her Devletin temsilcilerinden oluşan taslak hazırlama komitelerinin kurulmasını gerektirecektir. Görünüşe göre bir antlaşmanın kabul edilmesi iki yönü, uluslararası hukuku ve iç hukuku birleştirmelidir. Birincisi, bir anlaşmanın kabul edilmesi, bugün hüküm süren belirsizliği sona erdirmek için bir siber saldırıyı neyin oluşturduğuna dair ortak bir tanım benimsemek için bir fırsat olacaktır. Aynı zamanda uluslararası hukukun siber uzay için de geçerli olduğunu hatırlamak için bir fırsat olacaktır. Siber uzayda güç kullanımının yasaklanması metnin temellerinden biri olmalıdır. "Güç" teriminin hiçbir tanımı bulunamazsa, antlaşma, yine de saldırganlığın tanımında kullanılan yöntemi kullanarak, Devletlerin güç kullanımı olarak nitelendirebileceği eylem örneklerinin bir listesini içerebilir.[166] Özellikle bu, önemli ulusal altyapı hedeflendiğinde hangi gücün kullanılacağına göre kriterlerin ortaya çıkarılmasını mümkün kılacaktır. Devletler ayrıca, ekonomisine saldırarak veya geniş ölçekte propaganda yayarak, başka bir devleti istikrarsızlaştırmaya çalışmamayı da taahhüt etmelidir.

Metnin başka bir bölümü, imza sahibi devletlerin siber tehdidi daha iyi hesaba katmak için iç mevzuatlarını uyarlamalarını gerektirmelidir. Somut olarak, bu, devlet dışı aktörlerin eylemlerinden kaynaklanan siber uzaydaki düşmanca davranışları cezalandırmak, Devletlerarasında özellikle bir siber saldırının kurbanı olduktan sonra yaptıkları soruşturmalar çerçevesinde Devletlerarasındaki iş birliğinin teşvik edilmesi meselesi olacaktır.

Bunlar, 2015 GGE raporunda yapılan önerilerle aynıdır. Bazı devletler, önceki GGE raporlarına dayanarak uluslararası düzeyde çalışmaya devam etmek istediklerini

166 A/RES/3314.

açıklamıştır. Son çalışma grubunun 2017'deki başarısızlığına rağmen, önceki raporlarda belirtilen kurallar, uluslararası topluluk tarafından tanınmaya devam etmelidir. Bununla birlikte, bazı Devletler tarafından, özellikle gelişmekte olan ülkeler için temsil edilme eksikliğini eleştiren GGE'ye yöneltilen eleştirilere dikkat çekilebilmektedir.[167] Altıncı bir grup oluşturulmuştur[168]; görev 2021 yılına kadar yeni bir rapor elde etmektir.

Her şeyden önce, müzakerelere katılmamaya veya anlaşmayı onaylamaya karar veren ve bu nedenle siber uzayda "yalnız bir kurt" olarak hareket edecek ve sisteme zarar verme riski taşıyan devletler düşünülmelidir. Ek olarak, tüm yeni teknolojilerde olduğu gibi, kurallar hızla geçersiz hale gelebilmektedir. Bu nedenle, bir antlaşma taslağı, teknolojinin gelişmesi nedeniyle uygulanamaz hale gelme riski olmadan, siber saldırıların yol açtığı tüm sorunları ele alacak kadar hassas olmalıdır.

Bazıları, en güçlü siber yeteneklere sahip devletlerin, siber uzaydaki davranışlarını düzenlemek için bir anlaşma taslağı hazırlamayı kabul etmelerinin olası olmadığını iddia etmektedir. Yine de Hollis'in belirttiği gibi,[169] uluslararası hukuk bugün siber operasyonlara benzetilerek uygulandığı şekliyle oldukça kısıtlayıcıdır. Bir antlaşmanın kabul edilmesinin, düşmanca operasyonlar yürütmek için siber yöntemler kullanmaya devam edecek olan devlet dışı aktörlerin davranışlarını değiştirmesi olası değildir. Bununla birlikte, bir antlaşma, Devletlerarasında işbirliği için iyi bir temel oluşturabilir ve yazarların kovuşturulmasını kolaylaştırabilir.

---

167 Birinci Komite: delegasyonlar siber uzayda güvenliği güçlendirmenin yollarını düşünmektedir (*Première Commission: les délégations réfléchissent aux moyens de renforcer la sécurité dans le cyberespace*'den çevrilmiştir) 30 Ekim 2018 URL: https://www.un.org/press/fr/2018/agdsi3613.doc.htm E.T 6 Temmuz 2020.

168 A / RES / 73/226 Karar ile oluşturulmuştur.

169 D.B. Hollis, "Why states need an international law for information operations", Lewis & Clark Law Review, Vol. 11, 2007, s. 1039.

Her şeyden önce, bir antlaşma taslağının hazırlanmasının uzun süre devam etme dezavantajı vardır. Büyük uluslar, siber uzay gibi bir alanda çıkarlarını savunmaya ve vizyonlarını empoze etmeye çalışmaktadırlar. Bunun kanıtı, hükümetin uzmanlar grubunun 2017'deki son toplantısının, devletler bir anlaşma bulamadığı için bir raporun kabul edilmesine yol açamayacağıdır. Bu nedenle bazı devletler bunun yerine bağlayıcı olmayan davranış kuralları benimsemeyi önermektedir.[170] Bu davranış kurallarında yer alan kurallar nihayetinde uluslararası teamül hukukunda belirginleşebilmekte ve bu nedenle geleneksel hukukla aynı gücü elde edebilmektedir.

Bu üç yol aynı anda başlatılmalıdır. Devletler, muhtemelen Birleşmiş Milletler içinde, siber uzaydaki temel sorunları, özellikle de devlet dışı gruplardan gelen siber saldırıların ele alınmasını ve atıf yapma konusunu ele alan bir anlaşma taslağı hazırlamak için çabalarına devam etmelidir. Aynı zamanda, siber saldırılar çoğaldıkça örf ve âdet hukuku yavaş yavaş oluşacak ve Devletlerin uygulamaları siber uzayda geçerli standartları zenginleştirecektir. Son olarak, davranış kurallarının geçici olarak oluşturulması, kuralcı olmasa da devletleri siber uzayda barış içinde davranmaya teşvik edebilecek bir çerçeve sağlamaktadır.

Bununla birlikte, genel uluslararası hukukun bu bölümünü, egemenlik ve gerekli özen ilkeleri (siber-özen) olan iki önemli uluslararası hukuk kavramından bahsetmeden bitirmek eksik olacaktır. Bu çalışma kapsamında birçok kez bu kavramlara geri döneceğiz.

1. Egemenlik

170 *Internationale Sicherheit und Völkerrecht im Cyberespace*. Ekim 2014, (Almanca) https://www.swp-berlin.org/fileadmin/contents/products/studien/2014_S18_slr.pdf

Siber uzaydaki egemenlik kavramı yeni epistemolojik zorluklar getirmektedir. Esasen kaydi bir alanda devlet egemenliğini tasavvur etmek gerçekten zordur, ancak yerel düzeyde gerçekleşen çok sayıda insan eylemi için bir üstyapı işlevi görmektedir.

Diğer alanlarda olduğu gibi, temel altyapının korunması (elektrik şebekeleri, su dağıtımı ...) ve devlet ve askeri hizmetlerin devamlılığı meşru bir egemenlik meselesi olabilir, siber uzayda bu mesele genişletilmiş güvenlik meselesine de uzanmaktadır. Böylece egemenlik, Devletin ve aynı zamanda ekonomik sektörlerin ve İnternetin işleyişine izin veren fiziksel ve elektronik altyapılar düzeyinde bulunabilmektedir. Bu yelpazeyi, endüstriyel casusluğa veya diğer Devletlerin diplomatik veya sivil haberleşmelerinin kitlesel casusluğuna veya sadece ulusal güvenliği baltalamak amacıyla yapılan saldırılara karşı korumak için genişletmek mümkün olacaktır. Sivil, devlet veya askeri alanlar arasındaki gözeneklilik nedeniyle, egemenlik sorununu daha geniş bir şekilde yorumlama ihtiyacı vardır. Örneğin, siber uzaydaki bir faaliyet alanına yönelik tehditler, bir dizi başka faaliyet üzerinde etkili olabilmekte ve egemenliği garanti altına almayı amaçlayan bir devlet tepkisini tetikleyebilmektedir. Sistemlerin ve ağların birbirine bağlanması, egemenliği ve onun korunmasını daha karmaşık hale getirmektedir. Tehditler geliştikçe (hiç şüphesiz siber tehditlerin sıklığı ve şiddeti artmaktadır)[171], siber uzaydaki çeşitli faaliyetlerin (askeri, ticari, sivil, idari vb.) korunması, gelecekte ulusal güvenliğin temel unsurlarından biri olacaktır.

Devletlerin siber uzay ve güvenliği ile ilgili 'konuşma eylemi' sorununu incelemek de ilginçtir. İlkelerin beyanlarına rağmen, tekrarlanan saldırılara maruz kalan savunmasız unsurların gerçekten kamu yetkilileri veya siber uzaydaki diğer aktörler tarafından güvence

171 Public Safety Canada, *Department Performance Report 2012-2013*. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-prfrmnc-rprt-2012-13/dprtmntl-prfrmnc-rprt-2012-13-eng.pdf E.T 10 Temmuz 2020.

altına alınması nadirdir. Bu nedenle, tehdidin ifadesi ve bu sektörlerin önemi, bazen gerçek egemenlik sorunlarından çok iç veya uluslararası politika endişeleriyle bağlantılıdır.

Son olarak, siber uzayda egemenliğin bir başka yönü de, aktörlerin (bu durumda çoğunlukla devlettir), onun işleyişine izin veren fiziksel altyapıları etkisiz hale getirme yeteneğidir. Örneğin, belirli bir bölgede İnternetin kesilmesi (uluslararası fiber optikler tarafından veri aktarımının kesintiye uğraması yoluyla) bir devlet aktörünün egemenliğinin bir gösterisi olabilirse, bu eylemlerin diğer aktörler üzerinde yansımaları olabilir, çünkü tüm altyapı Devletlerarasında paylaşılır. O halde bu, devlet egemenliğinin kullanılması mı, uluslararası sistemin istikrarını sorgulayan bir eylem mi yoksa bir saldırı mı?

Bu özellikle Tallinn Kılavuzunu yazan uzmanların ilk kurallarında söylediği şeydir: "*Bir Devlet, egemen topraklarında bulunan siber altyapılar ve faaliyetler üzerinde kontrol uygulayabilir*."[172] Bu, bir Devletin, kendi topraklarında bulunan altyapıların kullanım ve erişimini dilediği şekilde düzenlediği anlamına gelmektedir. Bir siber altyapıyı hedef alan bir saldırı, o Devletin egemenliğinin ihlali anlamına gelmektedir. Tallinn El Kitabı, bir devletin başka bir devletin egemenliğini ihlal eden siber operasyonlar yürütmemesi gerektiğini iddia etmektedir. Bununla birlikte, bu kural yalnızca devletlerarasında geçerlidir ve uluslararası hukuk kapsamında bir devletin egemenliğini ihlal etme yasağına tabi olmayan devlet dışı aktörler için geçerli değildir. Eylemleri yasal değildir, ancak basitçe uluslararası hukuka tabi değildir, ancak Devletlerin iç hukukuna tabi olabilmektedir.

2. Gerekli Özen İlkesi

172 Tallinn El Kitabi – Kural 1

Çeşitli meydan okumalara rağmen, pozitif uluslararası hukukta siber uzayda gerekli özeni gösterme görevi olduğuna şüphe yoktur. Yukarıda gördüğümüz gibi, bir Devlet, yasaklanmış bir güç kullanımı oluşturan veya başka bir devletin iç veya dış işlerine müdahale oluşturan bir siber saldırıya başvurduğunda uluslararası hukuku ihlal edebilmektedir. Devlet, bir eylemin gerçekleştirilmesinden sorumludur. Bununla birlikte, bir devletin egemenliğini ihlal eden bir operasyon daha genel bir biçimde yasa dışıdır. Birleşmiş Milletler Şartı'nın 2 (1). Maddesi bu nedenle "örgütün, tüm üyelerinin egemen eşitliği ilkesi üzerine kurulduğunu" belirtir. Devletlerin siber uzayda da egemenliklerini sürdürdüklerini, en azından siber altyapıları üzerinde uyguladıklarını düşünebiliriz.

Bununla birlikte, uluslararası hukuk aynı zamanda devletlerin belirli bir davranışı benimsemelerini gerektirir; bu davranışa uyulmaması, yükümlülüklerinin ihmal edilerek ihlal edilmesi anlamına gelmektedir. Korfu Boğazı davasında, Uluslararası Adalet Divanı'nın yükümlülüklerinden biri, "kendi topraklarının diğer Devletlerin haklarına aykırı eylemler için kullanılmasına izin vermemesi"[173] olarak açıkça belirtilmiştir. Bu kural, temel devlet egemenliği ilkesinden kaynaklanmaktadır. Bağımsız devletlerarasında herkes kendi toprakları üzerinde egemenlik uygulamakta özgürdür, ancak diğer devletlerin egemenliğini etkilememeye dikkat etmelidir. Uluslararası Adalet Divanı, Uruguay Nehri üzerindeki selüloz değirmenleri ile ilgili davaya ilişkin son kararında, bu ilkeyi hatırlatmış ve teamül bir kural olarak önleme ilkesinin kaynağının devletin kendi topraklarında gerekli özeni olduğunu ilan ederek, bu ilkenin teamül doğasına açıklık getirmiştir.[174]

Gerekli özen, devletlerden beklenen bir davranış standardına karşılık gelmektedir. Bu iddia başka bir devletin çevresine verilen zarar bağlamında yapılsa da kural geneldir ve

173 Corfu Strait Case, Judgment of April 9, 1949, I.C.J. Reports 1949, s. 18.
174 Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, s. 14, §101.

siber operasyonlar için de geçerli olmalıdır. İşte bu ruhla, 2015 GGE raporunda, "Devletlerin, bilgi ve iletişim teknolojilerini kullanarak uluslararası haksız eylemlerde bulunmak için kendi bölgelerinin kullanılmasına bilerek izin vermemeleri gerektiği"[175] belirtilmektedir. Tallinn Manual 2.0, kural 6'da gerekli özen kavramını ele almaktadır: "*Bir devlet, kendi topraklarının veya siber altyapısının, diğer devletler için ciddi olumsuz sonuçlar doğuran ve haklarını etkileyen, üreten siber operasyonlar için kullanılmasına, kendi hükümet kontrolü altında izin vermemesi için gerekli özeni göstermelidir*."

Bu durum 3 tarafı içerir: Siber operasyonun mağduru olan devlet, topraklarında gerçekleştirildiği devlet, saldırının arkasında üçüncü bir şahıs; bir devlet, bir şirket, bir grup birey. Bir devletin egemenliğine zarar verme yasağı yalnızca devletler için geçerliyse, gerekli özen ilkesi, bir Devletin kendi topraklarını başka bir devlete karşı düşmanca siber operasyonlar yürütmek için engelleme yükümlülüğüne uymaması nedeniyle mümkün kılınan devlet dışı aktörlerin eylemleriyle ilgili olabilmektedir.

Operasyonun gerçekleştirildiği devletin gerekli özen yükümlülüğüne aykırı olması için neden olunan hasarın ulaşması gereken ağırlık seviyesi tartışmalı olmaya devam etmektedir. Tallinn El Kitabı, bazı uzmanlar bu eşiğin "önemli" veya "gerçek" sonuçlara düşürülmesini önermesine rağmen "ciddi sonuçlar" terimini kullanmaktadır.[176] Bir devletin gerekli özeni gösterme görevini ihlal etmesi için, topraklarının başka bir devlete düşman amaçlarla kullanıldığına dair bilgi sahibi olması gerekir. Bu bilgi durumu, örneğin özellikle diğer devletlerden veya istihbarat servislerinden elde edilen bilgiler dikkate alınarak öznel ve nesnel olarak ölçülmelidir. Bununla birlikte, mağdur bir devlet için, bir devletin, bir

175 UN GGE Report 2015 (A/70/174)
176 A.g.e

saldırının failleri tarafından kendi topraklarını kullandığının farkında olduğunu göstermesi zor olabilmektedir.

Bazı yazarlar, ağları tekrar tekrar düşmanca amaçlarla kullanılan devletin bilgi varsayımını veya belirli bir devletin topraklarında bir siber saldırının kökeninin izini sürmenin mümkün olduğunu iddia etmektedir[177] (bu konu, bu tezde daha sonra tartışılacaktır). Ancak bu varsayım tehlikeli olabilir. Uluslararası Adalet Divanı, Korfu Boğazı davasında bu riski zaten tespit etmiş ve bilginin yalnızca bir eylemin bir devletin topraklarından kaynaklanması gerçeğiyle oluşturulmadığını belirtmiştir.[178] Bununla birlikte, herhangi biri uluslararası hukukun genel bir ilkesi olarak siber uzaya gerekli özeni gösterme görevinin uygulanmasını çürütse bile, mantıksal olarak da siber uzaydaki güvenliği işaret eden ülkelerin güvenliğinin korunmasına ilişkin belirli bir alanda gerekli özen görevinin geçerli olduğu tartışılmazdır. Yabancı devletlerin güvenliğiyle ilgili konularda gerekli özeni gösterme yükümlülüğünün varlığı, Alabama davası[179], Korfu Boğazı davası[180] ve Bern'deki Romanya Elçiliğine karşı saldırı[181]; ilgili dava gibi doktrin[182], diplomatik ve hukuksal

177 Örneğin, R. Garnett & P. Clarke, « Cyberterrorism: a new challenge for international law » in Andrea Bianchi (ed), *Enforcing International Law Norms against Terrorism*, Hart Oxford, 2004, s. 479.
178 Corfu Strait Case, 1949
179 Alabama davasında, mahkeme bir durum tespiti yükümlülüğünün uygulanabilirliğini açıkça kabul etti ve İngiliz hükümetinin tarafsız yükümlülüğünü yerine getirirken gerekli özeni göstermediği ve özellikle de zamanında etkili önleyici tedbirler... almayı ihmal ettiği... sonucuna vardı » (Amerika Birleşik Devletleri'nin Büyük Britanya'ya Alabama ile ilgili iddiaları, 8 Mayıs 1871 Washington Antlaşması'nın 1. Maddesi uyarınca oluşturulan tahkim mahkemesi tarafından 14 Eylül 1872'de verilen karar, BM Tahkim Kararları Koleksiyonu, cilt XXIX , s. 130).
180 Mahkeme, “herhangi bir Devletin kendi topraklarının diğer Devletlerin haklarına aykırı eylemler amacıyla kullanılmasına izin vermeme yükümlülüğünün” genel bir ilke olduğunu teyit ederek, Arnavutluk'un mayınların Boğaz'da olduğunu bildiği ve harekete geçmesi (özellikle bu mayınların varlığını İngiliz gemilerine bildirme) anlamına gelmektedir, ancak felaketi önlemek için hiçbir şey yapmamıştır.
181 Bu davada İsviçre'nin görüşüne göre: "Devlet, kendi topraklarından yabancı Devletlerin iç ve dış bütünlüğüne karşı yöneltilen fiilleri önlemeli ve cezalandırmalıdır" (Swiss Yearbook of International Law, 1959, p. 225).

uygulamalarla defalarca teyit edilmiştir. Bu, Devletlerin, diğer Devletlerin güvenliğine yönelik bir saldırıyı önlemeye çalışmak için tüm makul önlemleri alma görevini hiçbir zaman geri çekmemiştir. Bu gerekli özen yükümlülükleri, özellikle 11 Eylül 2001 tarihinden itibaren, Devletlerin terörist faaliyetleri önlemek[183] ve bastırmak için aktif önlemler almaları gerektiğinin teyit edildiği tarihten itibaren, terörizmle mücadele bağlamında da önemli ölçüde güçlendirilmiştir.[184]

Bu nedenle, devletlerin, kendi topraklarının diğer devletlerin güvenliğini tehdit etmek için kullanılmasını önlemek için ellerinde bulunan tüm makul önlemleri almaktan oluşan bir gerekli özen yükümlülüğü olduğu açıktır. O halde siber uzay bu genel güvenlik kuralının uygulanabilirliğinden nasıl çıkarılabilir?

Siber uzayda durum tespiti ilkesi, Devletler için siber güvenliğin temel bir yönüdür. Bu nedenle, örneğin, Amerika Birleşik Devletleri ("siber titizlik" konusunda oldukça isteksiz olsa da), "siber güvenlik gerekli özen" kavramına göre "*devletlerin bilgi altyapılarını koruma ve ulusal sistemleri hasardan veya yanlış kullanımdan koruma sorumluluklarını*

182 Örneğin R. P. Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », ss. 31- 36.

183 G. Guillaume, Terrorism and international law, RCADI, 1989, III, vol. 215, s. 390-398; veya 71984 sayılı Uluslararası Hukuk Derneği'nin Uluslararası Terörizm Hakkindaki kararının 9. Maddesi'ne (Altmış Birinci Konferans Raporu, Paris, 1984, s. 6) göre: "Bir Devlet, kendi yetki alanında uluslararası terörizm eylemleri önlemek için yasal olarak gerekli özeni uygulamakla yükümlüdür."

184 Güvenlik Konseyi, 28 Eylül 2001 tarihli 1373 (2001) sayılı kararın önsözünde, bu nedenle, "her Devletin, başka bir Devletin topraklarında iç savaş veya terör eylemlerini organize etmekten ve teşvik etmekten, buna yardım etmek veya katılmak veya bu tür eylemleri işlemek amacıyla kendi topraklarında organize faaliyetleri tolere etmekten kaçınma yükümlüğü vardır ". Çok sayıda doktrinsel ifade arasındadır. Örneğin, F. Dubuisson, "*Vers un renforcement des obligations de diligence en matière de lutte contre le terrorisme* ? », J. Kendall, P. Barron, M. Allenbaugh, "The diligence due in the era of globalized terrorism", The International Lawyer, 2002, vol. 36, s. 49 ;

tanımaları ve buna göre hareket etmeleri gerektiğini kabul ederek"[185] onu siber uzay için uluslararası stratejisinin temel bir unsuru haline getirmiştir.

Siber gerekli özen kavramı, kendi topraklarında bulunan ve hem kamu hem de özel aktörler tarafından yönetilen faaliyetler adına uyanıklık için birincil sorumluluklarını ileri sürerek, devletlerin siber uzayda sorumlu davranışlarının ortaya çıkmasına katkıda bulunarak siber güvenlik alanında önemli bir role sahip olmaktadır. Böylelikle, devletler için, bilgi ve kapasite durumunda, kendi bölgelerinden veya kendi kontrolleri altında diğer devletlerin altyapılarına, şirketlerine ve bireylerine karşı başlatılan siber saldırıları önlemek ve sona erdirmek için makul ve sorumlu bir davranış standardı oluşmaktadır.

Gerekli özen kavramı kesinlikle ilginçtir, çünkü bu çalışmada göreceğimiz gibi, aktör kesin olarak tanımlanamadığında veya işlem doğrudan bir devlete atfedilemediğinde bile bir tehdit veya bir siber saldırıya karşı koruma sağlamak için önlemler almaya izin vermektedir. Ancak yine de, siber saldırının hangi bölgeden kaynaklandığını göreceli olarak kesin bir şekilde belirleyebileceğinizi varsaymaktadır. Teknik olarak karmaşık kalır, zaman ve kaynak gerektirir ve bir tanımlama hatası olasılığı göz ardı edilemezdir. Her şeyden önce, topraklarında siber operasyonların gerçekleştirildiği devletin bu eylemlerden haberdar olduğunu ve aynı koşullarda başka bir devletin makul olarak alacağı önlemleri almadığını kanıtlamak mümkün olmalıdır. Bununla birlikte, bugüne kadar, bir devletin siber uzay karşısında makul şekilde alması gereken önlemler oldukça belirsizdir.[186]

Uluslararası hukuk açısından, siber gerekli özen kavramının iki önemli çekiciliği vardır. Her şeyden önce, analiz ettiğimiz gibi, kısmen temel atıf problemini aşabilir. Ayrıca, bir

185 2011'deki Siber Güvenlik Raporu.
186 Geiss/Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.), 2013,* s. 653.

siber saldırının yasal niteliği meselesinin ve bunun "uluslararası hukuka aykırı bir eylem" oluşturup oluşturmadığına dair varoluşsal sorunun çözümüne de yardımcı olabilecektir. Siber saldırılar alanındaki uygulama, bir devletten başlatılan bir siber saldırıyı "uluslararası hukuka aykırı bir eylem" olarak nitelendirmenin bazen zor olduğunu, yani onu o duruma atfetmenin veya norm olarak hangisinin ihlal edildiğini veya her iki nedenden dolayı aynı anda kesin olarak belirlenmesinin, çok zor olduğunu göstermektedir.

D. GENEL DEĞERLENDİRME

Dünya, dijital teknolojinin bilgi paylaşımı veya ekonomik gelişme için bir fırsat olduğu ve toplumlarımızın, işlerimizin ve hatta yaşam tarzlarımızın işleyişini temelden değiştirdiği fikrinde hemfikirdir. Ticaret, enerji, ulaşım veya endüstri, elektronik iletişimden ve her zamankinden daha güçlü veri toplama ve işleme kapasitelerinden yararlanarak dönüşürken, insan ve teknolojinin birleştiği bir dünyaya yolculuk gibi görünmektedir.

Uluslar Birliği, bu konu ile doğrudan ilgilidir. Siber uzay, devletlere egemenlikleriyle ilgili önemli sorular soran yeni bir ortamdır, orada bulunmanın ve eylem özerkliğini sürdürmenin önemli olduğu, sibernetik operasyonların uluslararasındaki çatışmaları başlatmak için gittikçe daha fazla ortaya çıktığı bir çatışma yeridir. Bununla birlikte, dijital gelişmelerin toplumlarımız üzerinde başka etkileri de vardır, çünkü kamuoyunun manipülasyonu yeni bir görüngü olmasa da dijital teknoloji ve onun "sosyal ağları" tarafından sunulan yeni fırsatlar vatandaşları ve onların siyasi liderlerini düşük maliyetli bir oranla, istikrarsızlığın etkisine daha fazla maruz kalmaya bırakmaktadır.

Devletlerin ve devlet dışı aktörlerin dâhil olduğu bilgisayar saldırılarındaki dramatik artış, uluslararası barış ve güvenlik için gerçek bir tehdit oluşturmaktadır. 2015 raporunda, Birleşmiş Milletler Siber Güvenlik Hükümet Uzmanları Grubu, özellikle devletlerin kritik

altyapılarına yönelik kötü niyetli eylemlerin sayısındaki çarpıcı artışla işaretlenen "endişe verici eğilimlerden" duyduğu endişeyi dile getirmiştir.[187] Bu endişe verici gözlem artık devletler, uluslararası kuruluşlar veya özel aktörler olsun tüm dijital ve siber güvenlik aktörleri tarafından paylaşılmaktadır. Bu saldırılar yalnızca kritik (çok önemli) dijital altyapıları tehdit etmekle kalmamakta, aynı zamanda devletlerarasında büyük bir gerilim kaynağı olmaktadır.

Bu soruların uluslararası hukuk için getirdiği zorluklar ne olursa olsun, genel olarak devletler ve devlet dışı aktörler arasındaki ilişkiler, yalnızca devletler (egemenlik sahipleri ve önemli yetkiler) ve ikincisi (devletlere "tabi") arasındaki hukuki statü farklılığıyla değil, aynı zamanda fiili güç, kaynaklar ve birbirlerinin eylem kapasiteleri nedeniyle devletler lehine açık bir dengesizlikle işaretlenmiş olarak kalmıştır. Aslında, devlet hemen hemen her zaman benzersiz bir güce sahip gibi görünmüştür, bu da ona bazen kendi korunmasına bağımlı olan özel aktörler (bireyler, azınlıklar, yatırımcılar vb.) üzerinde bazen düzenleme, yargı yetkisi ve yürütme ile karşı karşıya kalan tartışılmaz bir üstünlük sağlamıştır.[188]

Bu çalışmada devletlere odaklandık ve yine devletlere odaklanmaya devam edeceğiz ancak büyük dijital şirketlerin siber uzay politikaları geliştirmedeki yerini göz ardı edilmeyecektir. Büyük dijital şirketler, farklı açılardan bakıldığında, devletler kadar güçlü ve bazen siber saldırıları önlemede, kötü niyetli eylemleri ilişkilendirmede ve bunlara yanıt vermede daha da güçlü görünmektedir. Michael N. Schmitt ve Sean Watts'ın belirttiği gibi: "*Klasik olarak, devletler ve devlet dışı aktörler, yalnızca yasal statüdeki eşitsizliklerle değil, aynı zamanda kaynaklar ve yeteneklerdeki önemli dengesizliklerle de farklılaşmaktaydı.*

187 Genel Sekreter'in notu, A / 70/174, 22 Temmuz 2015 (GGE 2015).
188 Devletler ve Devlet dışı aktörler arasındaki bu hukuk gücü eşitsizliği fenomeni, özellikle ulusal güvenliğin korunması, organize suçla mücadele veya dış politikaların yürütülmesi gibi doğası gereği "egemen" olan alanlarda belirgindir.

Şaşırtıcı olmayan bir şekilde, uluslararası hukuk bu dengesizlikleri hesaba katmak için devlet merkezli bir eğilim geliştirmiştir. Bununla birlikte, siber uzay ve siber operasyonlar, devletlerin ve devlet dışı aktörlerin uluslararası barış ve güvenliği tehlikeye atma yetenekleri arasındaki önceden önemli olan bazı boşlukları kapatmıştır. Aslında, bazı devlet dışı aktörler artık bu konuda birçok devletin siber yeteneklerini aşamasa bile yeteneklerini eşleştirmektedir ".[189]

Pozitif hukukun siber saldırıların önlenmesi ve bunlara verilen tepkilerle ilgili çeşitli sorunlara çözüm getirdiğini söylemek hiçbir şekilde devletlerin bağlantısının kesilmesi gerektiği anlamına gelmez. Bu analiz boyunca gördüğümüz gibi, sürekli olarak yeni sorular ortaya çıkarken, yine de uluslararası hukukta temel olan sorularla ilgili birçok gri alan kalmaktadır. Bu nedenle uluslararası topluluğun, koşullara göre uluslararası hukuk tarafından sunulan tüm uygun araçları kullanarak bu sorulara yanıt bulmak için yakın işbirliği yapması zorunludur: Yeni bağlayıcı belgelerin kabulü; yumuşak hukuk metinlerinin kabulü; mevcut kuralların dinamik ve gelişen yorumu vb.

Siber uzayın uluslararası yönetimi sorunundan bahsedersek, sorun şu ki, ülkeler tarafından çok çeşitli forumlarda kurulan girişimlerin çoğalması, dijital güvenliğin iyi yönetimine kesinlikle tanıklık etmemektedir. Bazı devletler bu dağılım için bir çare olarak, merkezi olarak hareket edebilecek dijital güvenlik konusunda uzmanlaşmış yeni bir uluslararası organizasyonun yaratılmasını önermişlerdir[190]. Bununla birlikte, uluslararası sahnede, çağ, aslında bazı devletler tarafından asla onaylanamayacak olan yeni kurucu

189 M.N. SCHMITT & S. WATTS, "Beyond State-Centrism: International Law and Non-State Actors in Cyberspace", Journal of Conflict & Security Law, vol. 21, n° 3, 2016, s. 1 https://doi.org/10.1093/jcsl/krw019
190 M.N. SCHMITT & S. WATTS, 2016

antlaşmaların zaman alıcı müzakereleri yoluyla elverişsiz yapıların benimsenmesi için gerçekten de bir dönem olmayabilmiştir.

Bu çağ, normatif güçlere ve evrensel bir mesleğe sahip yeni uluslararası örgütlerin yaratılma dönemi de değildir. Aksine, "fora", "ağlar", "gruplar", "ajanslar", "komiteler" ve diğer gayri resmi kurumların çoğaldığını gözlemlemekteyiz ki bunlar belki de klasik uluslararası örgüt tanımına tam olarak uymamakta, ancak işlevlerini bir miktar verimlilikle yerine getirmektedir. Bir yazarın özetlediği gibi: "*Uluslararası hukuka alternatifler, uluslararası hukukun konuları olan uluslararası örgütlerin kurulmasını içermeyen çeşitli hükümetler arası koordineli eylemler yoluyla yaratılmaktadır*".[191]

Böylelikle, siber-gayret kavramının siber saldırıları önlemede veya bunlara son vermek için hızlı hareket etmede yararlı olduğunu göstermiş bulunmaktayız. Devletlerin kendi topraklarında faaliyet gösteren Devlet dışı aktörlere (ister terörist gruplar, siber suçlular, işletmeler veya basit bilgisayar korsanları olsunlar) karşı uygulamak zorunda oldukları durum tespiti görevi, doğrudan herhangi bir devletin "*kendi topraklarının, diğer devletlerin haklarına aykırı eylemlerin amaçları için kullanılmasına izin vermeme yükümlülüğünden kaynaklanmaktadır.”*

Bu bölümün amacı, uluslararası hukukun siber âlemdeki kaygılarını sunarak ve bu çalışmanın konusuna çok faydalı olan önemli kavramları analiz ederek siber uzayı tanıtmaktır. İkinci bölümde, mevcut uluslararası belgelerin belirli hükümlerine atıfta bulunularak, uluslararası hukukun siber operasyonlara uygulanabilirliğine derinlemesine bakılacaktır. Bu tezin yazarına, uluslararası toplumun mevcut uygulamalarını siber savaşla

191 E. BENVENISTI, *Substituting International Law in The Move from Institutions*? **American Society of International Law Proceedings**, vol. 100, 2006, s. 289-290.

karşılaştırmak ve bu alandaki çeşitli akademik girdileri ve akademiye katkısını analiz etmek için bir fırsat olacaktır.

İKİNCİ BÖLÜM

ULUSLARARASI HUKUK KAPSAMINDA BAZI SİBER OPERASYONLARIN HASMANE OLARAK BELİRLENMESİNE İLİŞKİN KRİTERLER VE SİBER SALDIRILARIN GEREKÇESİ

Bu bölümün altında iki ana nokta tartışılacaktır: Siber uzayda düşmanca davranışların belirlenmesi ve bu alanda güç kullanımının gerekçelendirilmesi. Pek çok devlet, siber uzayda operasyonlar hazırlama ve yürütme kapasitesini geliştirmektedir. Bu bölümün başlığında da belirttiğimiz gibi bazı siber operasyonlar, diğer devletlerin haklarına zarar verecek şekilde gerçekleştirildiğinde, uluslararası hukukun ihlalini teşkil edebilir.

Saldırı dereceleri veya etkileri göz önüne alındığında, egemenlik, müdahale etmeme, hatta tehdit veya kuvvet kullanma yasağını[192] ihlal edebilirler. Bu tür siber saldırıların hedef aldığı devletler, uluslararası hukukun sunduğu olanaklar dâhilinde yanıt verme hakkına sahiptir. Bununla birlikte, siber operasyonun kökenini, niyetinin düşmanca durumunu ve hatta eylemin kendisini belirlemek her zaman kolay değildir. Bu nedenle, bu bölümde siber uzaydaki angajman kuralları, siber operasyonların tespitleri ve uluslararası hukuk kapsamında bunlara verilen yanıtlar tartışılacaktır.

I. BAZI SİBER OPERASYONLARININ HASMANE OLARAK TESPİT KRİTERLERİ

Siber silahlar bugün ülkelerin askeri planlamasına dahil edildiğinden, politikacılar ve saha komutanları, temel bir sorunla giderek daha fazla yüzleşeceklerdir: Bu tür silahları kullanabilecek askeri operasyonlarla ilgili olarak kendi askeri kuvvetleri için angajman kurallarının (AK) nasıl formüle edileceğidir. Her ülkenin ordusunun kendi angajman kurallarını kullanma şekli vardır. Örneğin ABD Savunma Bakanlığı, angajman kurallarını "*ABD kuvvetlerinin karşılaşılan diğer kuvvetlerle muharebe angajmanını başlatacağı ve / veya devam ettireceği koşulları ve sınırlamaları tanımlayan yetkili askeri otorite tarafından yayınlanan talimatlar*"[193] olarak tanımlamaktadır. Sanremo Angajman Kuralları El Kitabına göre: *AK, yetkili makamlar tarafından verilmekte ve hedeflerine ulaşmak için askeri kuvvetlerin kullanılabileceği koşulların ve sınırlamaların tanımlanmasına yardımcı olmaktadır. AK, yürütme emirleri, konuşlandırma emirleri, operasyonel planlar veya sabit direktifler dâhil olmak üzere ulusal askeri doktrinlerde çeşitli biçimlerde görünmektedir.*

192 1945 BM Şartı'nın 2. Maddesi.
193 Department of Defense, **Dictionary of Military and Associated Terms**, 2010–2016, s.207. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf E.T 23 Eylül 2020.

Biçimleri ne olursa olsun, diğer şeylerin yanı sıra güç kullanımı, kuvvetlerin konumlandırılması, pozisyonu ve belirli özel yeteneklerin kullanılması için yetki ve / veya sınırlar sağlamaktadırlar. Bazı ülkelerde AK, askeri güçlere rehberlik statüsüne sahiptir; diğer ülkelerde ise AK, yasal komutlardır.[194]

Yetkililer, komutanlara silahlı operasyonları yürütmeleri için gereken onayları sağlarlar. Bu tür yetkililer, AK'lerin ciddi bir bileşeni olduğu kuvvet kullanma iznine sahiptir. AK'ler, uluslararası insancıl hukukun dayattığı güç kullanımına ilişkin kısıtlamaları yansıtmaktadır. Bu kısıtlamalar şunlardır: Meşru askeri hedeflere ulaşmak için yalnızca gerekli kuvvet eylemlerine izin veren "askeri zorunluluk"; savaşçılar ve siviller arasında fark yaratan "ayrım"; ve sivillere yönelik, beklenen yaşam veya yaralanma ya da sivil nesnelere verilen zararın, belirli bir eylemden öngörülen askeri avantajları aşmamasını öneren "orantılılık".

Bununla birlikte, komutanlar, devreye girebilmek için, belirli bir eylemin varlığının, aktörün düşmanca bir niyetini temsil ettiğinden veya bunun sadece bir düşmanlık eylemi olduğundan emin olmalıdır.

Siber uzayda düşmanlık eylemi, bir Devlet veya eylemleri bu Devlete atfedilebilecek ajanlar veya kuruluşlar tarafından, başka bir Devletin BT sistemlerinin ağlarının birbirine bağlanmasından yararlanarak askeri, mali, sağlık veya sosyal olsun, o devletin temel yapılarını ciddi şekilde bozmak veya zarar vermeye amaçlanan bilgisayar zorlayıcı önlemlerin davranışı olarak tanımlanabilir.

194 A. Cole ve Ark, *SANREMO Handbook on Rules of Engagement*, International Institute of Humanitarian Law, Sanremo, Kasım 2009

Sanremo el kitabı[195], siber alanla ilgili angajman kurallarını belirlerken ülkelerin takip edebileceği yerleşik yasal hususlar şunlardır:

i. Yerel ve uluslararası medeni ve ceza yasaları ve ulusal politikalar, bilgisayar ağı işletiminin yasal yönlerine göre büyük ölçüde farklılık göstermektedir. Ayrıca, çok taraflı ve iki taraflı iletişim anlaşmaları, bilgisayar ağı operasyonlarının yürütülmesini etkileyen hükümlere sahiptir.

ii. Kinetik olmamasına rağmen, siber uzaydaki işlemler düşmanca bir eylem veya düşmanca bir niyet oluşturabilmektedir. Her ikisinin de belirlenmesindeki faktörler, operasyonun ciddiyetini, aciliyetini, doğrudanlığını ve etkilerini içermektedir.

iii. Dikkate alınacak ilk AK zorunlu kurallardır. Zorunlu kurallar, seçilen kural askeri faaliyeti yasaklayan bir kural olsa bile, herhangi bir misyon için temel olan ve her AK'de bulunması gereken konuları ele almaktadır. Bu durumda, bilgisayar ağı operasyonlarında AK, uydu iletişimine müdahale ve uyduların nötralizasyonu / imhası dikkate alınmalıdır.

Siber uzayın temel özelliği, tek bir ülkenin yetki alanına girmeyen teorik bir ortam olmasıdır. Bilgisayar Ağı İşlemleri, siber uzayda gerçekleştirilen birincil işlem türüdür ve doğası gereği kinetik değildir, bu da bir düşmanlık eylemi veya düşmanca bir niyet olup olmadığını belirlemeyi zorlaştırır. Doğası gereği kinetik olmasa da, siber uzay operasyonları bir düşmanlık eylemi veya düşmanca niyet teşkil edebilir. Bunun hasmane bir hareket veya hasmane bir niyet olduğunu belirlemek için kullanılan faktörler, operasyonun ciddiyetini, acil ve doğrudan doğasını ve etkilerini içermektedir.[196]

195 A. Cole, Sanremo Handbook, 2009
196 A.g.e

A. SİBER UZAYDA HASMANE DAVRANIŞ VE HASMANE NİYET

1. Hasmane Davranış

Uzun bir süre, silahlı bir çatışmanın varlığı, savaş ilanı veya bir savaş durumunun tanınması gibi resmi kriterlerin doğrulanması ile şartlandırılmıştır. Ancak bu kriterler, insancıl hukuka ilişkin uluslararası sözleşmelerin uygulanmasında kırılgan hale gelmiştir. Muhalif bir hükümetin meşruiyetine meydan okumak, hatta ilhak veya teslimiyetin ardından bir devletin ortadan kaybolması, sözleşmelerin uygulanabilirliğini reddetmek için gereken tüm bahaneler olarak kabul edilmiştir. Günümüzde, savaşan tarafların niyetini ifade etmesi gereken tek taraflı veya karşılıklı düşmanlık eylemlerinin gerçekleşmesi yeterlidir.

Bu nedenle, Birinci Cenevre Sözleşmesi'nin 2. maddesine ilişkin yoruma göre silahlı çatışmadan, "*iki devlet arasında çıkan ve silahlı kuvvetler mensuplarının müdahalesine neden olan herhangi bir anlaşmazlık ...*".[197] olarak bahsedilmiştir. Bu silahlı çatışmanın varlığı, uluslararası insancıl hukukun uygulanmasını gerektirmektedir. Ek Protokol I'e ilişkin yoruma göre, "*insancıl hukuk ayrıca iki Devlet arasındaki silahlı kuvvetlerin kullanımıyla ilgili herhangi bir anlaşmazlığı da kapsamaktadır*".[198]

Hukukun uygulanmasındaki bu gelişme, sözleşmelerin "*tarafların her birinin ulusal çıkarları için imzalanan karşılıklı sözleşmeler*" olarak görüldüğü devlet merkezli

---

197 Sahadaki Silahlı Kuvvetlerde Yaralı ve Hastaların Durumunun İyileştirilmesi'ne İlişkin Sözleşme (I) hakkında 1952'deki Yorumu. Cenevre, 12 Ağustos 1949.

198 1987'deki Yorumu, 2 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Mağdurlarının Korunmasına İlişikin Protokol (1. Protokol)'un Genel İlkeler ve Uygulama Kapsamı, 8 Hazıran 1977, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=7125D4CBD57A70DDC12563CD0042F793 E.T 29 Eylül 2020.

uluslararası hukuktan, daha yüksek ilkelerin kendileri de dâhil herkes için geçerli olduğu daha kozmopolit bir hukuka geçişi yansıtmaktadır.[199]

Daha özellikli olarak, uluslararası insancıl hukuk, bir çatışmada savaşan taraflar arasındaki düşmanlıkların yürütülmesini yönetmektedir. Bunlar esasen bir askeri öldürmek, yaralamak veya mülke zarar vermek gibi şiddet eylemleridir. Bu şiddet, Cenevre Sözleşmeleri ve Ek Protokollerinde tekrarlanan bir terim olan saldırı yoluyla uygulanmaktadır. Örneğin, ayrım ilkesine göre, "*ne sivil nüfus ne de siviller saldırının hedefi olmamalıdır*".[200] Ek Protokol I'in 49. maddesine göre saldırı, ister saldırma ister savunma amaçlı olsun, bir düşmana yönelik bir şiddet eylemi olarak tanımlanmaktadır. Ek Protokol I'in 48. maddesine yapılan açıklamaya göre operasyon, "*şiddetin kullanıldığı askeri operasyonlara*" atıfta bulunmaktadır. Bu nedenle, kinetik olmayan işlemleri konu dışı tutarlar. Saldırı kavramı propaganda operasyonlarını, ambargoları veya diğer ekonomik veya psikolojik savaş araçlarını içermemektedir. Bilgisayar saldırıları uluslararası hukukun kapsamı dışında bırakılmalı mıdır?

Hayır, çünkü uluslararası hukukta, bir sözleşmenin oluşturulması sırasında uygulanmasını engellemek için bir tekniğin var olmamasına karşı çıkılamaz. Bu durumda, Viyana Antlaşmalar Hukuku Sözleşmesi'nin 31. maddesine göre atıfta bulunulması gerekir. Bu maddeye göre, bir sözleşme, "*hükümlerine andlaşmanın bütünü içinde ve konu ve amacının ışığında verilecek alelade manaya uygun şekilde iyi niyetle yorumlanmalıdır".*

---

199 1949 Cenevre Sözleşmeleri ve Ek Protokoller, ve Yorumları. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp E.T 29 Eylül 2020

200 Kural 7. Sivil Nesneler ile Askeri Hedefler Arasındaki Ayırım İlkesi, Bölüm C. Genel olarak sivil nesnelere yönelik saldırılar, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule7_sectionc E.T 24 Şubat 2021

Uluslararası insancıl hukuk, nüfusu ve sivil nesneleri korumayı amaçladığı için, burada operasyonların kinetik olsun veya olmasın siviller üzerindeki etkilerine bağlı olarak sonuca odaklı bir yaklaşım benimsenmelidir. Bu nedenle, kimyasal veya biyolojik silahların kullanımı, zarar verici sonuçları nedeniyle kinetik olmasa da her zaman bir saldırı olarak kabul edildiğinden, bu yorum yeni yapılmamıştır.

Bu nedenle, bir bilgisayar saldırısı, şiddetli sonuçları nedeniyle, kendi içinde şiddet içermese bile, saldırı veya düşmanca eylem olarak sınıflandırılabilir. Örneğin, büyük bir havalimanındaki hava trafik kontrol sistemine yapılan bir bilgisayar saldırısı, uluslararası insancıl hukuka tabi olacaktır. Aksine, bir üniversiteye veya bir alışveriş merkezinin web sitesine saldırmak ise uluslararası hukukun ihlali olarak adlandırılmaya yetmeyecektir.

Görünür fiziksel hasara neden olmadan, bir nesnenin yalnızca işlevini bozan ve zarar vermeyen siber operasyonlar ne olacak? "Hasmane davranış" olarak etiketlenmeleri yeterli olacak mıdır? Verilerin manipülasyonu veya silinmesi, uluslararası insancıl hukukun uygulanabilirlik eşiğini tetiklemeye yetecek midir?

Sorun, UİH'nin uygulanmasını haklı çıkarabilecek siber uzaydaki bu önemli düşmanlık eylemlerini belirlemektir. Bir eylem, "*belirli bir saldırgan hareketi eşiğine*" ulaştığında veya "*eylemin bu tür etkilere neden olacağı nesnel bir olasılık olduğunda*" düşman olarak nitelendirilmektedir. Yani, bu durumda, bu düşmanlığın "*geçerli koşullarda belirli bir eylemden kaynaklanması makul olarak beklenebilir*".[201]

Burada iki düşünceye karşı çıkılmaktadır. Kısıtlayıcı olarak nitelendirilebilecek birinci düşünce, siber operasyonu tek saldırı ile sınırlamaktadır. Bu düşünce, diğer bir

201 ICRC, International humanitarian law and cyber operations during armed conflicts, Bu pozisyon belgesinde ICRC, siber operasyonlar ve uluslararası insancıl hukuk (UİH) hakkındaki görüşlerini sunmaktadır.

deyişle, yalnızca fiziksel sonuçlarla zarar veren, uluslararası insancıl hukuka tabi olma ihtimali olan düşmanca bir eylemdir. Tallinn El Kitabı, psikolojik operasyonlar veya siber casusluk operasyonları gibi şiddet içermeyen operasyonları, uluslararası insancıl hukukun geleneksel kurallarına uygun olarak reddederken, şiddet içermeyen sınır bazen çok fazla olabilmektedir. Kılavuzun geliştirilmesine katılan bazı (azınlık)[202] uzmanlar, bir bileşenin değiştirilmesini değil, verilerin restorasyonunu gerektiren bir nesnenin işlevselliğini yitirmesine neden olan bir siber operasyonun düşmanca bir eylem oluşturduğunu düşünmektedir. Bu uzmanlara göre, işlevsellik kaybının maddi veya manevi kökeni önemli değildir, hasarı oluşturan sonuncusu olmaktadır.

Bir siber operasyonun düşmanca bir eylem oluşturup oluşturmadığını incelerken atıfta bulunulması gereken ikinci husus, düşmanlık açısından akıl yürütmeyi içeren ICRC tarafından savunulan pozisyondur.[203] Doktrin ve antlaşmalar "düşmanlıkların" kesin bir tanımını sağlamamıştır ve silahlı çatışma durumunda kullanılabilecek araç ve yöntemlerin kapsamı göz önüne alındığında, bu kavramın yorumlanması belirli bir esneklik gerektirmektedir. Uluslararası Kızıl Haç Komitesi, Kasım 2019'da, bu rahatsızlık eşiğine "ya özel bir askeri karakterin zararlı etkilerine neden olarak ya da insan hayatını kaybetmek, kişilere zarar vermek veya yok etmek veya doğrudan saldırıya karşı korunan mülklere zarar vermek suretiyle" ulaşılabileceğini belirtmiştir.[204] Genel olarak, "düşmanlıklar", "*askeri operasyonlara veya başka bir kısmın askeri kapasitesine herhangi bir düzeyde doğrudan*

202 M. N. Schmitt (Ed.), Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't, 9 Şubat 2017. https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/ E.T 20 Şubat 2020.
203 C. Droege, Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), 2012, s. 533-578
204 ICRC, 2019

zarar vererek silahlı bir çatışmada bir tarafı desteklemek için özel olarak gerçekleştirilen, şiddet içeren ve içermeyen bütün faaliyetleri" içermektedir.[205]

Başka bir deyişle, düşmanlıklar, şiddetli sonuçları olan eylemlerin yanı sıra düşmanın askeri yeteneklerini engelleyenleri de içermektedir. Örneğin, güç kaynağını veya iletişimi kesmek ya da bir baraj kurmak düşmanlıkların bir parçasıdır. Öte yandan, muhalif savaşçıyı dolaylı olarak etkileyen her şey, savaş çabasının bir parçasıdır, ancak düşmanlık oluşturmamaktadır. Askerlerin eğitimi, savaş için seferber edilen mali kaynaklar veya silah üretimi de düşmanlık oluşturmayan eylemler arasındadır.

Bu nedenle, siber operasyonlar askeri bir hedefi etkisiz hale getirme etkisine sahipse eğer uluslararası insancıl hukuka tabi olabilmektedir. Bu anlayış, askeri hedefin "etkisizleştirilmesinden"[206] bahseden Ek Protokol I'in 52 (2) Maddesini doğrulamaktadır. Bu madde, aynı zamanda yıkımdan değil aşırı "hasardan" bahseden orantılılık ilkesine de uygundur. Bununla birlikte, ICRC için hasar, tanımı gereği operasyonları etkiler. Dahası, siber uzayın soyut içeriğiyle daha uyumludur; yalnızca fiziksel hasar açısından akıl yürütmek bir anlam ifade etmeyecektir. Bununla birlikte, bu tasarımın sonuçlarının, TV yayınının kesintiye uğraması veya bir üniversitenin sitesine erişememe gibi basit bir kesintinin ötesine geçmeyecek bir hizmete yönelik herhangi bir saldırıyı içermesi riski bulunmaktadır.[207] Öncelikle, bu eylemler uluslararası insancıl hukuk tarafından kapsanmamaktadır, ancak birbirine bağlılık, düşmanca eylem ile basit iletişim arasındaki ayrımı bulanıklaştırmaktadır. Siber operasyonların neden olabileceği ciddi ancak fiziksel

---

205 N. Melzer, Targeted Killing in International Law, *Oxford Monographs in International Law*-Oxford University Press, New York 2008, s. 243

206 K. Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, 19 Kasım 2004, s. 4,6,8 https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf E.T 22 Eylül 2020

207 M. N. Schmitt, Cyber Operations and the Jus in Bello: Key Issues, Naval War College International Law Studies, 2011 http://ssrn.com/abstract=1801176 E.T 22 Eylül 2020.

olmayan zararlar ışığındaki bu yaklaşım, mantıksız değildir. Diğer yaklaşımın kapsayıcı olmadığı yönündeki endişelere yanıt vermektedir. Ancak Dörmann'ın riski, aşırı kapsayıcılık[208] riskinin tam tersidir. Örneğin, bir televizyon yayınının engellenmesi durumunda olduğu gibi, yalnızca rahatsızlık verenler de dâhil olmak üzere, tüm hizmet reddi saldırılarını kapsayacaktır. Devlet uygulaması, rahatsızlık nedeninin UST'de yasaklanmasının amaçlandığı fikrini desteklememektedir.[209] Aksine, sivillerin günlük yaşamlarına rahatsızlık ve müdahale, sıkça yapılan silahlı çatışmaların bir sonucudur ve sivil nüfusa yönelik psikolojik operasyonlar yaygın hale gelmiştir. Dörmann, "saldırıları" ölüm, yaralanma, hasar veya yıkıma neden olan operasyonlarla sınırlamanın tatmin edici olmayan sonucunu tespit ettiği için takdir edilecek, ancak önerdiği çare çok ileri gidecektir.[210]

Bu çare, aynı zamanda doğrudan konu üzerinde olmayan hukuka da dayanmaktadır. Askeri hedefler, saldırıya uğrayabilecek nesnelerdir.[211] Ancak ilk soru, bir saldırının gerçekleştirilip gerçekleştirilmediği veya tasarlanıp tasarlanmadığıdır. Ancak, askeri hedef tanımı, bu soru olumlu yanıtlandığı zaman devreye girecektir. Askeri hedeflerin tanımlanmasıyla ilgili mesele, nasıl veya ne sonuçlarla değil, neye saldırılabileceği ile ilgilidir.[212] Dahası, taslağı hazırlayanlar bir saldırı bağlamında "nötralizasyonu" tasavvur etmişlerdir. Terim, "*bir nesnenin yok edilmesine gerek kalmadan, düşmana karşı kullanılmasının engellenmesi amaçlanarak yapılan bir saldırıyı*"[213] içeren durumları kapsayacak şekilde dâhil edilmiştir. Örnekler arasında, bir kara alanını geçilmez kılmak için kara mayınlarının kullanılması veya diğer hedeflere yönelik bir hava saldırısına devam

208 A.g.e
209 A.g.e
210 A.g.e
211 A.g.e
212 A.g.e
213 M. BOTHE ve Ark., New Rules For Vıctıms of Armed Conflıcts,(1982), s. 289

edilirken, silah ekiplerini siper almaya zorlamak için düşman karadan havaya, füze bölgelerine antipersonel mühimmat ateşlemek sayılabilir.[214] Düşmanca eylemler, siber uzayda kalıcı olmaktadır, çok çeşitli aktörlerden kaynaklanmaktadır ve bireyleri, işletmeleri, her türden organizasyonu ve eyaletleri hedef almaktadır. Bu istikrarsızlık, hiç kimsenin bağışıklık kazanmadığı bir durumdur. Uluslararası istikrar ise, özel hayata saygı, ifade özgürlüğü veya verilerin korunması[215] açısından soru işaretleri uyandıran bir "herkese karşı savaş" duygusu vermektedir.

2. Hasmane Niyet

Siber uzayın kendine özgü zorlukları vardır. Bir siber saldırıya atıfta bulunmak çok zordur, çünkü komutanlar nadiren bir saldırının veya izinsiz girişin kaynağından emin olurlar ve emin olmak için gereken adli kanıtları oluşturmak zaman alıcı ve çoğu zaman kesin olmayan bir bilimdir. Niyeti belirlemek ise daha da zordur.

Amerikan Müşterek Genelkurmay Başkanlarına göre, hasmane (düşmanca) niyet, *Amerika Birleşik Devletleri, ABD kuvvetleri veya diğer belirlenmiş kişi veya mülklere karşı yakın kuvvet kullanma tehdidi olarak tanımlanmaktadır.[216] Bir komutanın, bir düşmanın saldırmak üzere olduğunun göstergesi, inancıdır. Bu inanç, bir komutanın saldırıya uğramadan önce saldırmasına izin veren Amerikan hukuku kavramı olan "erken meşru müdafaa*" için zemin hazırlamaktadır.[217]

---

214 Ibid.

215 A. Cattaruzza & D. Danet, *La cyberdéfense. Quel territoire, quel droit ?* Paris, Economica, Collection Cyberstratégie, 2014, s.32.

216 Chairman of the Joint Chiefs of Staff Instruction 3121.01B, "Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces," Washington, DC, 13 Haziran 2005

217 International and Operational Law Department, *Operational Law Handbook* (Charlottesville, VA: U.S. Army Judge Advocate General's Legal Center and School, 2012).

Gördüğümüz gibi bu bir Amerikan yaklaşımıdır ve neyin düşmanca bir niyet olacağına dair geleneksel bir tanım olmadığından, siber uzay gibi soyut bir alanda bunun kolay olamayacağını görmek kolaydır. Öte yandan, daha belirsiz veya dolaylı tehditlere yanıt vermek, Avrupa ülkelerinin öz savunma doktrinlerinin sınırlarını aşma eğilimindedir; düşmanca eylemle haklı gösterilen kuvvet ve kasıtlı AK'ler, teknik olarak bir saldırı gücü türüdür (Fransız, Alman ve İngiliz askerleri için).[218] Bir Alman askerî avukatın açıkladığı gibi:[219]

Düşmanca niyet saldırgan hedefleme için temeldir. Meşru müdafaa duruşu değildir. Düşmanca niyetin bir çeşit meşru müdafaa olması düşüncesi, oldukça Amerikanvari bir bakış açısı içermektedir. Bu durum, meşru müdafaa konusunda Avrupa ülkeleri ve ABD arasındaki büyük farkı gözler önüne sermektedir. Avrupa'daki meşru müdafaa söylemi ise çok dardır. Sadece bir tehdit içeren veya doğrudan gerçekleşen eylemlere karşı kullanılmaktadır.

Her ülke, meşru müdafaa konusunu, kendi planına ve ulaşmak istediği hedefe göre tanımlamalıdır. Dinamik bir savaş ortamında, birliklerin kuvvet kullanıp maya karar verme anları olduğunda ve bu kararlılığı kendi öznel davranış yorumlarına dayandırmaları gerektiğinde, birlikler, bazı hatalar yapmak zorundadırlar. Bazı yorumcular, bu soruna olası bir çözüm olarak, kuvvet senaryolarının "kullanma" ve "kullanmama" yönlendirmeleri arasında parlak bir çizgi çizen, tamamen nesnel bir AK'ye geçmeyi önermektedir. Ancak isyanla mücadele ortamlarında, askerlerin sivilleri düşman savaşçılardan bir an önce

218 E. L. Gaston, "Reconceptualizing Individual or Unit Self-Defense," *Harvard National Security Journal, 2017,* 306-307

219 E. L. Gaston, Interview with German military lawyer, Berlin, Germany, February 13, 2015

ayırmak için davranış temelli bir hedefleme planına girmelerini gerektirdiği göz önüne alındığında, davranış temelli AK'den uzaklaşmak, pek olası görünmemektedir.

Düşmanca bir eyleme veya düşmanca niyete yanıt verme yetkisinin, temel savunma hakkının bir parçası olarak kabul edilip edilemeyeceği, askerlerin belirsiz tehditlere ne kadar kolay yanıt verebilecekleri konusunda önemli sonuçlara sahiptir. Meşru müdafaa, savaş veya barış zamanında, silahlı bir çatışma durumunda veya bir barışı koruma görevinde olan askerler için kullanılabilmektedir. Meşru müdafaa, genelde diğer taktik kurallarla, uluslar üstü angajman kurallarıyla veya politika kararlarıyla sınırlandırılamamaktadır, ancak (belki de aşikâr bir biçimde) bazı durumlarda, bir komutanın astına vereceği acil emirler, meşru müdafaa ile çelişebilecektir.

Meşru müdafaa paradigması, bağlayıcı yasanın yokluğuyla işaretlenmiştir. Hukuki tartışmalar, miyopik olarak, meşru müdafaanın yer almadığı UİH doktrininin geleneksel ana hatlarına odaklanma eğilimindedir. Sonuç olarak, meşru müdafaa veya düşmanca niyetin temeli, kapsamı veya standartları hakkındaki temel sorular belirsizliğini korumaktadır. Bu kavramların ne zaman uygulanacağını çevreleyen önemli bir gri alan ve devletlerin neye izin verildiğine ilişkin yorumlarında önemli farklılıklar bulunmaktadır.[220]

Düşmanca davranışı ve düşmanca niyeti belirlemek kolay değildir. Örneğin, cep telefonuyla konuşan bir adam, asker konumlarını iletiyor veya bir saldırıda arıyor, düşmanca bir niyet gösteriyor veya sadece evini çocuklarını veya karısını arıyor olabilir. Toprağı kazan bir adam, doğaçlama bir patlayıcı cihaz yerleştiriyor, açık bir düşmanca harekette bulunuyor veya ekinler için bir sulama hendeği kazıyor olabilir.[221] Jus ad bellum

---

220 D. H. Lee, "Operational Law Handbook 2015," *The Judge Advocate General's Legal Center and School* (June 15, 2015), 83, http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2015.pdf

221 E. L. Gaston, 2017.

paradigmasının mevcut içeriği, siber saldırılara tepki vermek için yanıtlar veya kabul edilebilir çözümler sağlamamaktadır ve teknoloji, belirli bir varlığa atanmaya veya failinin niyetini belirlemeye izin vermemekte veya zorlaştırmamaktadır.[222] Örneğin, Rusya'daki bir İnternet protokolü adresine kötü amaçlı yazılım gönderilmesi, veri çalma girişimini mi göstermektedir? Bir botnet kurmanın habercisi midir? Kötü amaçlı yazılım Rus yapımı olsa bile mi? Kötü amaçlı yazılım yerleştirmek bir güç kullanımı olarak kabul edilmeli midir? Ne yazık ki, siber uzayda güç kullanımını neyin oluşturduğu konusunda uluslararası fikir birliği ya çok azdır ya da hiç yoktur. Herhangi bir düşmanca niyetin belirlenmesi için gerçek test; operasyonel olarak nasıl çalıştığının, yani savaş alanında ne kadar kolay kullanılabileceğinin belirlenmesidir.[223] Siber savaş alanı fiziksel değildir; soyuttur, ancak etkilerinin fiziksel dünyada gerçek sonuçları vardır. Testlerin sonuçları hızlı bir şekilde görülebilmekte ve uygulanabilmekte ve yöntem kısa sürede geliştirilmektedir.[224] Bu nedenle siber atıfları tartışmak çok önemlidir. Siber atıflar, saldırganın gerçek kökenini ve de hukukun uygun yanıtlarını tanımaya yardımcı olacaktır.

B. SİBER ATIFETME

Herhangi bir zarar verici eylemden kaynaklanan herhangi bir yasal sorumluluk, bu tür zararlara neden olmaktan sorumlu olan aktörün varlığını gerektirmektedir. Devletlerin yükümlülüklerine ilişkin uluslararası hukuk, bu zarar verici fiillerin belirli bir devlete açıkça atfedilip atfedilemeyeceğine dair net bir kanıt gerektirmektedir. Aynı durum, güç

222 M. Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense,* Boston College International and Comparative Law Review, Volume 32, Issue 2, 2009, s. 448.
223 R. A. Torruella, Determining Hostile Intent in Cyberspace, JFQ 75, 4th Quarter 2014, s.115
224 R. A. Torruella, 2014

kullanımına ilişkin uluslararası hukuk için de geçerlidir. Birleşmiş Milletler Şartı'na göre, güç kullanımı kuralının kapsamı şu şekilde özetlenebilir:

- Genel olarak, ulusların diğer uluslara karşı kuvvet kullanması yasaktır.
- Bazı koşullarda, devletlerin kuvvet kullanmasına izin verilmektedir: BM Güvenlik Konseyi tarafından kuvvet yetkisi verilirse veya eylem bir devlete atfedilebilir ise başka bir devlet veya devlet dışı bir aktör tarafından yapılan silahlı saldırıya karşı meşru müdafaada güç kullanılabilecektir.
- Güç kullanımı, Uluslararası İnsancıl Hukuk ilkelerinin belirlediği sınırlara uymalıdır.
- Ev sahibi devlet, devlet dışı aktörlerin silahlı saldırılarını önleyemiyorsa (çoğunlukla Amerikan doktrininde), kuvvet, doğrudan devlet dışı aktörlere karşı meşru müdafaada kullanılabilecektir.

Son olarak, hasmane bir siber eyleme uygun bir yanıtın belirlenmesi, aktörün kim olduğunun araştırılmasını gerektirmektedir (devlet, devlet dışı, bilinmeyen).

Fail atfedilmesi, hasmane bir siber eylemden kimin sorumlu tutulacağını belirlemektir. 2011 *ABD Savunma Bakanlığı'nın Siber Uzayda Faaliyet Gösterme Stratejisi'*nde belirtildiği gibi, hasmane siber eylemlere girişteki düşük engeller, yaygın olarak kullanılan bilgisayar korsanlığı araçlarıyla birleştiğinde, küçük grupların ve hatta bireylerin ulusal güvenliği etkileyebileceği anlamına gelmektedir.[225] Bununla birlikte, müdahale açısından önemli bir konu da aktörlerin kimliği değil, hasmane siber eylemlerin belirli bir devlete atfedilebilir olup olmadığıdır. Çeşitli aktörler tarafından oluşabilecek risklerin giderek daha fazla dikkate alınması ve savunma araçlarının çoğalması, siber saldırıların zararlarını azaltmaya katkıda bulunurken, saldırıların sürekli artması, tamamen savunma amaçlı bir

yaklaşımın, siber saldırganları saldırıya uğramaktan caydırmadığını göstermektedir. Bu nedenle, sibernetik, politik veya yasal tepkilerin tetiklenmesine izin vermek için saldırıların faillerini tespit edebilmek gerekli görünmektedir. Bu ayrım, uygun yanıtın, yanıt verenin ve angajman kurallarının belirlenmesine yardımcı olmaktadır.

Düşmanca siber eylemler, doğrudan veya dolaylı olarak bir devlete atfedilebilmektedir. İki devlet atıf yöntemi aşağıda kısaca açıklanabılır:

- **Doğrudan Atfetme:** Devletler, eylemleri devlet tarafından verilen yetkiyi aşsa bile, devletin yetki ve otoritesini kullanan bireylerin eylemlerinden veya ihmallerinden sorumlu tutulacaktır.
- **Dolaylı Atfetme:** Devlet dışı aktörlerin eylemleri veya ihmalleri genellikle devlete atfedilemeyecek; ancak, devlet bu tür eylemleri veya ihmalleri önlemede veya bunlara tepki göstermede gerekli özeni gösteremezse sorumluluk alabilecektir.[226]

Uluslararası hukukta evrensel olarak kabul görmese de, pratikte genel olarak bir devletin meşru müdafaada kuvvet kullanma hakkının bir devlete atfedilemeyen silahlı saldırılar tarafından tetiklendiği kabul edilmektedir.[227] Örneğin, silahlı bir saldırı, bir devletin onu önleme bilgisi veya yeteneği olmadan ortaya çıkabilir. Bu tür durumlarda, silahlı saldırı doğrudan saldırganlara atfedilecek ve mağdur devlet, tarafsız ve hatta müttefik bir devlette bulunmalarına rağmen, devlet dışı aktörlere karşı doğrudan kuvvet kullanarak savunma yapabilecektir. Yakın zamanda *Journal of Conflict and Security Law*

226 J. A. Hessbruegge, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law," ***New York University Journal of International Law and Politics*** 36 (Winter/Spring 2004): s.268.
227 E. F. Mejia, 2014, s. 118.

(Uyuşmazlık ve Güvenlik Hukuku Dergisi)'da belirtildiği gibi, meşru müdafaa hakkını tetikleyen şey, aktörünün doğası değil, düşmanca eylemin doğasıdır.[228]

Siber saldırılarda, bir kişinin, örgütün veya bir ulus devletin şüpheli olarak tanımlanması, özellikle bireysel saldırılar için son derece zordur. Bununla birlikte, bir siber saldırının failini tespit etmek imkânsız değildir ve ister devletler ister özel şirketler olsun, giderek daha fazla sayıda aktör, bir siber operasyonun kökenine kadar giden gelişmiş teknik kapasitelere sahiptir. Devletler genellikle yanlışlıkla devlet dışı aktörler olarak tanımlanmaktadır ve bunun tersi de geçerlidir. Manuel olarak tanıtılan yazılım durumunda, Stuxnet'te olduğu gibi, yazılımın yapısını, kullanılan kodları veya hatta insan zekâsı yardımıyla faili belirlemeye çalışılabilir. Saldırının kaynağı "teknik olarak" izlendikten sonra, bu davranışın bir devlete atfedilebilir olup olmadığı sorusu meydana gelecektir.

Her arama yapıldığında, gerekli hizmetin kullanılması için ücretlendirme ihtiyacıyla bağlantılı olan kullanıcıları tanımlamak ve bulmak için etkili bir sisteme sahip olan geleneksel telefon şebekesinden farklı olarak İnternet ağı, santralleri ve bunların tahsisini belirlemek amacıyla tasarlanmamıştır. Bu ağ, tamamen lojistik amaçlarla, başlangıçta kullanımı ücretsiz bir ağ olarak yapılmıştır. Ek olarak, işbirlikçi bir araştırmacı topluluğuna hitap edildiğinden, ARPANET spesifikasyon aşamasında güvenlik ihtiyaçları belirtilmemiştir. Bu, ağı dâhili siber saldırılara karşı değil, harici fiziksel saldırılara karşı korumaktı; bu nedenle, güvenlik pahasına ayrıcalıklı olan, sağlamlıktır.[229]

---

228 N. Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (Yaz 2012): s. 7, http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html E.T 29 Eylül 2020.

229 U.H. Rao and U. Nayak, *History of Computer Security In: The InfoSec Handbook*, Apress, Berkeley, CA, 2014 https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_2 8 Mayıs 2020.

İnternet protokolünde yerleşik olarak bulunan güvenlik açıkları nedeniyle, bireyler kimliklerini görece kolaylıkla gizleyebilmektedirler.[230] Saldırıların motivasyonu düşünüldüğünde atıf daha da karmaşık hale gelmektedir. Saldırı modelleri, etkileri ve belirsizlik düzeyleri, suçlu, terörist veya devlet destekli siber saldırılar arasında farklılık göstermektedir. Bu zorluklar, küresel siber güvenlik politikasının oluşturulmasıyla aşılabilecektir. Atfetmeye yönelik olan mevcut hukuk uygulama paradigması, saldırıları atfetmek için sağlam bir temel sunmamaktadır. Bunun yerine, ulus devletler, kendi sınırları içindeki bilgi sistemlerinden kaynaklanan veya bu sistemlerden geçen veya kayıtlı tüzel kişiliklerine ait olan kötü niyetli eylemlerden ve diğer siber tehditlerden sorumlu tutulmalıdır. Bu, siber uzayda açık ve kabul edilmiş sorumlu devlet davranışı normları olmadan yapılamayacaktır.

Bu normları oluşturma süreci, Birleşmiş Milletler ve Uluslararası Telekomünikasyon Birliği (ITU) ile ilişkili forumlarda başlamıştır, ancak Amerika Birleşik Devletleri, diğer forumlarda küresel siber güvenlik girişimlerinin gelişimine liderlik etmeye çalışmaktadır. Bunun yerine, Amerikan müttefikleri ve bazı Amerikalı ortaklar da dâhil olmak üzere ulus devletlerin çoğu, ITU çerçevelerini desteklemek için Rusya ve Çin'in liderliğini izlemeyi tercih etmektedir. ITU'dan çıkan küresel normların Amerikan sponsorluğu, daha güvenli bir siber ekosistem oluşturmak ve hegemonik bir Amerika Birleşik Devletleri'nin korkularını yatıştırmak için devletlerarasındaki işbirliğini derhal artıracaktır.[231]

---

[230] S. Korhan, "SİBER UZAYDA AKTÖR- GÜÇ İLİŞKİSİ", *Cyberpolitik Journal*, vol. 2, no. 4. s.98, Ocak. 2018

231 R. Hill, Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT, 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace,

2011'de Beyaz Saray, ABD hükümetinin siber uzayın nasıl güvenli hale getirileceğine ilişkin vizyonunda kalkınma, diplomasi ve savunmayı vurgulayan Uluslararası Siber Uzay Stratejisi'ni yayınlamıştır. Strateji, "*yeni ve mevcut dijital sistemleri kurmak ve güvence altına almak için bilgi ve kapasite sağlamada aktif bir rol oynamak" için çalışarak ABD'nin kalkınma taahhüdünü vurgulamaktadır".*[232] Bu unsur, kötü niyetli aktörlerin saldırılarını başlattığı veya siber uzayda geçtiği güvenli sığınakların sayısını azaltmaya yardımcı olmak açısından önemlidir. İkincisi, Amerika Birleşik Devletleri, diplomasi yoluyla, "*devletlerin açık, birlikte çalışabilir, güvenli ve güvenilir bir siber alanın içsel değerini tanıyan ve sorumlu paydaşlar olarak hareket ettiği uluslararası bir ortam için teşvikler yaratmaya ve bunun etrafında fikir birliği oluşturmaya*" çalışacaktır.[233] Dışişleri Bakanlığı ve Federal Soruşturma Bürosu, yabancı hükümetlerle ilişkiler geliştirmede rol oynamakta, böylece bir siber saldırı kendi bölgelerinde ortaya çıktığında veya bölgeden geçtiğinde, yanıt verme ve sorumlu davranma mekanizmaları devreye girmektedir. Bu temel işbirlikleri, siber suçluları ve teröristleri tespit etmek ve kovuşturmak için mevcut bulunmaktadır. Ayrıca, diplomasi, Amerika Birleşik Devletleri'nin siber uzaydaki kötü niyetli eylemlere karışan yabancı hükümetlere karşı endişelerini dile getirebileceği bir kanal sunmaktadır. Hükümetler bunu gerçekleştirmeye yanaşmazsa eğer, kötü niyetli siber faaliyetleri engellemek için daha zorlayıcı diplomatik

---

NATO CCD COE Publications, Tallinn, s. 119-134 https://www.ccdcoe.org/uploads/2018/10/Art-09-Dealing-with-Cyber-Security-Threats-International-Cooperation-ITU-and-WCIT.pdf E.T 03 Mart 2021

232 S. Schjolberg, Proposals for New Legal Mechanisms on Combating Cybercrime and Global Cyberattacks, *A presentation at the United Nations - ISPAC International Conference on Cybercrime: Global Phenomenon and its Challenges Courmayeur*, Italy, 2011

233 JCS, The National Military Strategy of the United States of America 2015, s. 11 https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf 29 Eylül 2020.

önlemler kullanılabilecektir. Son olarak, diğer her şey başarısız olduğu takdirde, Savunma Bakanlığı'nın "*siber uzaydaki düşmanca eylemlere, ülkeye yönelik herhangi bir başka tehdide olduğu gibi karşılık verme*"[234] görevi bulunmaktadır.

Hem eylem hem de aktör niteliğinin değerlendirilmesi, düşmanca bir siber eyleme karşı uygun tepkinin belirlenmesi konusunda merkezidir. Bir hükümet; izleme, pasif savunmaları iyileştirme, siyasi baskı uygulama, aktif savunma kullanma ve hem siber hem de konvansiyonel silahlarla karşı grev yapma gibi çeşitli şekillerde yanıt verebilir. Pasif Savunma, *"öncelik alma niyeti olmaksızın, düşmanca eylemin neden olduğu hasarın olasılığını azaltmak ve etkilerini en aza indirmek için alınan önlemler*"[235] olarak tanımlanmaktadır. Siber âlemdeki pasif savunma, sistemlere antivirüsler ve güvenlik duvarları yoluyla saldırılmasını daha zor hale getirmeyi, kullanıcıları güvenlik bilincine daha fazla sahip olacak şekilde eğitmeyi ve fazlalık ve yedekleme sistemleri aracılığıyla saldırı sonrası kurtarma sürelerini azaltmayı içermektedir. Aksine, aktif savunmalar, "*düşmana karşı bir çekişme alanı veya pozisyonunu reddetmek için sınırlı saldırı eylemi ve karşı saldırıların kullanılması*" olarak tanımlanmaktadır.[236]Siber âlemde bu, düşmanca bir siber saldırıya karşı savunmacı bir yanıt olarak bir siber karşı saldırı başlatmak anlamına gelmektedir. Savunma amaçlı siber saldırılar iki türe ayrılabilir. Amaç, yalnızca sistemi daha fazla hasardan korumak için gereken kuvvet miktarını kullanarak hedeflenen bir sisteme verilen zararı azaltmaksa, bu bir "hafifletici karşı saldırı" olarak kabul edilmektedir. Hafifletici bir karşı saldırının amacı, acil bir tehditten kaynaklanan hasarı azaltmak olmalıdır. Karşı saldırının amacı saldırganı cezalandırmaksa, bu, "denkleştirici bir karşı

234 R. A. Clarke ve R. K. Knake, Cyber War: The Next Threat to National Security and What to Do About It.", New York, NY: Ecco, 2010, s. 251-53

235 Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 Kasım 2010 (değişiklikler 15 Ağustos 2012), s. 237.

236 JP 1-02, *Department of Defense Dictionary*, s.2.

saldırı" olarak kabul edilmektedir. Uluslararası hukuka göre, yalnızca hafifletici karşı saldırı gerçekten savunmaya yöneliktir, çünkü amacı acil bir tehdide karşı savunma yapmaktır.[237]

Fail ve eylem atfı, düşmanca bir siber eyleme yanıt verirken hangi devlet kurumunun öncülük etmesi gerektiğini belirlemede de kritik öneme sahiptir. Bazı devlet kurumları, siber operasyonlar ve sorumluluklarla görevlendirilmiştir. Örneğin, ABD Siber Komutanlığı (CYBERCOM) komutanı Gen Keith B. Alexander'a göre ABD hükümeti aşağıdaki kurumları kullanmaktadır:[238]

- Savunma Bakanlığı / İstihbarat Topluluğu / NSA / CYBERCOM: Yabancı alanda tespit, önleme ve savunma, yabancı siber tehdit istihbaratı ve atıf, ulusal güvenlik ve askeri sistemlerin güvenliği ve aşırı durumlarda, ulusun tam kapsamlı bir siber saldırıya uğraması halinde memleketin savunmasından sorumludur.
- İç Güvenlik Bakanlığı (DHS): ABD kritik altyapısının siber güvenliğini artırmaya yönelik genel ulusal çabayı koordine etmek ve sivil federal hükümet (.gov) ağlarının ve sistemlerinin korunmasını sağlamak için liderlik etmektedir.
- Federal Soruşturma Bürosu (FBI): Kolluk kuvvetleri, iç istihbarat, karşı istihbarat ve terörle mücadele yetkileri altında yerel arenada tespit, soruşturma, önleme ve müdahaleden sorumludur. Daha da önemlisi, ev içi

237 J. P. Kesan ve C. M. Hayes, "Mitigative Counter striking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law and Technology* 25, no. 2 (Spring 2012): s. 420–21.
238 Gen Keith B. Alexander, 2012, supranote 131

alanda kötü niyetli siber faaliyet tespit edildiğinde, FBI bunu önlemek, araştırmak ve azaltmak için başı çekmektedir.

Teknik bir bakış açısına göre, bir siber saldırının kökenini belirlemek için çeşitli teknikler bulunmaktadır. Özellikle, her teknik birçok farklı ağ protokolüne uygulanabilmektedir. Atfetmeyle ilgili olarak, kamu literatürünün çoğu İnternet Protokolüne (IP) odaklanmaktadır.[239] Bu odaklanmanın bir nedeni, IP'nin İnternet standartlarına dayalı herhangi bir ağın merkezinde olmasıdır, bu nedenle IP'ye odaklanan herhangi bir uygulama birçok durumda yararlı olmaktadır. Bununla birlikte, atıf, Ethernet, Basit Posta Aktarım Protokolü (SMTP, e-posta için İnternet standardı), anında mesajlaşma protokolleri, Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) ve benzerleri dâhil olmak üzere diğer protokollerde de desteklenebilmektedir.[240] Her protokol için aynı genel tekniği yeniden tanımlamak yerine, birçok protokol için geçerli olabilecek tek bir teknik tartışılmaktadır. Bu genelliği vurgulamak için, "paket" yerine "mesaj" terimi kullanılmaktadır. Bir "mesaj", ilgili protokol için bir bilgi birimidir. Her "mesajın" bir "mesaj başlığı" ve "mesaj içeriği" vardır:[241]

1. Mesaj başlığı: Mesajın kaynağı ve hedefi gibi mesajla ilgili bilgiler sağlar. Bu bilgi, mesajı hedeflenen alıcıya ulaştırmak için kullanılmaktadır.
2. Mesaj içeriği: Gerçek mesajı içerir. Bu içerik daha da parçalanabilir (ör. İnternet posta mesajı içeriğinin birden fazla MIME bölümü olabilir).

İletişimin uç noktalarında (ana bilgisayarlarda), mesaj yönlendiricilerinde veya ağ trafiğini gözlemleyen ayrı monitörlerde birçok teknik uygulanabilmektedir. Bunlar ayrı

239 David A. Wheeler, Gregory N. Larsen and Task Leader, “Techniques for Cyber Attack Attribution”, Institute for Defense Analysis, Ekim 2003, s.21 https://apps.dtic.mil/dtic/tr/fulltext/u2/a468859.pdf E.T 15 Ağustos 2020.
240 Ibid.
241 David A. Wheeler, Gregory N. Larsen and Task Leader, 2003

teknikler olarak kabul edilmez, ancak farklı uygulamaların etkisi not edilebilir.[242] Birçok teknik manuel veya otomatik bir şekilde uygulanabilir. Manuel bir tekniğin otomasyonu farklı bir teknik olarak kabul edilmemektedir. Saldırıların hızı, manuel bir tekniğin destekleyebileceğinden çok daha fazla olabileceğinden, manuel tekniklerin genellikle başarısız olduğunu unutulmamalıdır.[243]

David A. Wheeler, Gregory N. Larsen ve Görev Lideri siber atıf için farklı teknikleri tartışmıştır, bunlar arasında şunlar yer almaktadır: Ana Bilgisayar İzleme İşlevlerini Ekleme (ör. "Geri Kırma"), Maç Akışları (başlıklar, içerik ve / veya zamanlama yoluyla), Saldırganın Kendi Kendini Tanımlamasını İstismar / Zorla Girdi Hata Ayıklama Gerçekleştirme, İletilen Mesajları Değiştirme, Ayrı Mesajları İletme (örn. İTrace), Ağı Yeniden Yapılandırma ve Gözlemleme, Sorgu Sunucuları, Honeypot / honeynet'i Gözlemleme, İleri Konuşlandırılmış Saldırı Tespit Sistemlerini (IDS'ler) Çalıştırma, Filtreleme (örneğin, Ağ Giriş Filtreleme), Sahte Önleme Uygulama, Güvenli Ana Bilgisayarlar / Yönlendiriciler, Gözetleme Saldırgan, Ters Akış Çalıştırma, Birleştirme Teknikleridir.[244]

Bu tezin amacı, saf bir bilgisayar bilimi konusuna dönüşeceği için, her tekniği tartışmak değildir. Bununla birlikte, hem eylemin hem de aktör atfının temelini bilimsel kesinlik ile kanıtlamak zordur. Bilgisayar ağları, atfetmeyi kolaylaştırmak için tasarlanmamıştır ve düşman aktörler, gerçek kimliklerini gizlemek için bu zayıflığı kullanmaktadırlar. Örneğin, İnternet, tipik olarak bir iletim işlemi sırasında gönderen kimliğini kullanmamakta, bu nedenle kaynak bilgileri kolayca taklit edilebilmektedir.

242 A.g.e, s.6
243 A.g.e
244 David A. Wheeler, Gregory N. Larsen and Task Leader, 2003, s.9-11

Gönderen bilgilerini bu şekilde maskelemek, genellikle "yanıltma ve aldatma" olarak adlandırılır. Hasmane siber aktörler, verileri bir şekilde dönüştüren ve "aklayan ana bilgisayar" olarak bilinen bir sistem kullanarak kimliklerini ve konumlarını gizleyebilmektedir. Siber aktörler, milisaniyeler içinde tamamlanan veya alternatif olarak aylara yayılmış bir saldırı uygulayabilmektedirler. Tüm bu faktörler, siber aktör atfetmeyi zorlaştırmaktadır.[245]

Ekim 2012'de bir ABD Savunma Bakanlığı yetkilisi, siber uzayda gerçekleşen bir saldırıyı bir bireye veya belirli bir devlete atfetmenin imkânsız olduğuna dair yaygın olarak paylaşılan inanca rağmen, departmanının bu kapasitenin geliştirilmesine önemli ölçüde yatırım yaptığını ve önemli ölçüde iyileştiğini söylemiştir. Zamanın Amerika Birleşik Devletleri Savunma Bakanı Leon Panetta, ABD Ordusunun artık siber saldırıların kökenini belirleme yeteneğine sahip olduğunu eklemiştir.[246] Böyle bir ağırlığın beyanı, tartışmaları da beraberinde getirmiştir. Birincisi, bu ifade, yeteneklerin doğru bir değerlendirmesi midir yoksa potansiyel düşmanları caydırmak için bir duruş sergilemeye mi daha yakındır? İkincisi, eğer bu ifade teknolojik olarak doğruysa, bu yeteneği kabul etmek ve daha sonra bunu belirli bir aktöre düşmanca bir eylemi atfetmek için kullanmak, süreçte kullanılan yöntem ve tekniklerden ödün verme riskini taşıyacaktır. Son olarak, siber savaşın son derece uyarlanabilir doğası göz önüne alındığında, adli tıp dâhil bütün siber savunmalar kaçınılmaz olarak sürekli gelişen siber tehditler tarafından engellenecektir. Atfetme konusundaki teknik sorun aşılsa bile, bir devletin uluslararası hukuktan sorumlu olduğu

---

245 D. A. Wheeler, "Planning for the Future of Cyber Attack Attribution," 15.07.2010, s. 3,http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/071510_Wheeler.pdf

246 C. Caroll, *US can trace cyberattacks, mount pre-emptive strikes, Panetta says*, 12 Ekim 2014, https://www.stripes.com/news/us-can-trace-cyberattacks-mount-pre-emptive-strikes-panetta-says-1.192789 E.T 8 Mayıs 2020.

bulgusunu desteklemek için ne derece güven sağlanmalıdır? Belirli? Çok belli? Bunlar, kesin nicel analize izin vermeyen öznel siyasi belirlemelerdir.[247]

Bu aynı sorun, eylem atfını değerlendirmeye çalışırken de ortaya çıkmaktadır. Düşmanca bir siber eylemin silahlı bir saldırıya eşdeğer olup olmadığını belirlemek için Schmitt modelini[248] kullanmak, öznel bir analizin uygulanmasını gerektirmektedir. Peki, şiddeti ne kadar şiddetlidir? Burada aciliyetten kasıt nedir? Hasmane bir siber eylem ile bu eylemin sonuçları arasında doğrudan bir bağlantı oluşturan nedir? Tüm bu sorular öznel, bilimsel olmayan bir değerlendirme gerektirmektedir.

Neyse ki, hukuk topluluğu öznel aktör ve eylem atıf sorunuyla uğraşmaktadır ve öznel atıfla ilgili kavramları ve sözlüğü kapsamlı bir şekilde geliştirmiştir. Bu, en çok hukuk ve ceza davalarıyla ilgili kanunda belirgindir. Hukuk uzmanları bu öznel kriterlere "ispat standartları" olarak atıfta bulunmaktadır. Kesinlik derecesine göre en yaygın olanlardan birkaçı: Kanıtın zerresi (mümkün olan en az kanıt miktarı), kanıtın üstünlüğü, açık ve ikna edici kanıt (sağlam bir inanç veya kanaat yaratma) ve makul bir şüpheden ötesi (bilimsel bir kesinlikten daha azdır).[249]

Devletin sorumluluğu ile ilgili taslak maddelerinin 4. maddesi uyarınca, bir siber saldırı, bir Devletin organlarından biri veya 5.madde uyarınca kamu otoritesi yetkilerini kullanmaya yetkili olduğu organların eylemi tarafından gerçekleştirilmesi durumunda devlete atfedilebilecektir.[250] Bu, askeri veya istihbarat servisleri tarafından gerçekleştirilen

247 E. F. Mejia, 2014, s. 120.
248 M.N. Schmitt/BT O'Donnell (eds), *Computer Network Attacks and international Law,* 2002
249 *Black's Law Dictionary*, s.147.
250 Uluslararası Hukuk Komisyonu, Devletin Haksız Fiilden Kaynaklanan Milletlerarası Sorumluluğu Üzerine Taslak Maddeler, yorumlarla birlikte 2001, oturum (A / 56/10), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf E.T 10 Temmuz 2020

siber saldırılar için geçerli olacaktır. Ayrıca bazı devletlerin siber alanda hükümete bağlı eylemlerinin de devlete atfedilebilecek özel birimler oluşturduğunu bilmekteyiz. Bir Devlet, organlarının işlevlerinin ötesinde hareket ettiğini iddia ederek sorumluluğundan kaçamaz; uluslararası hukuk, organları aşırı derecede davransa bile devletin sorumlu olduğunu düşünmektedir.

Yasal öznel standartları kullanmak, yeni bir fikir değildir. 2009 tarihli bir Microsoft teknik incelemesinde yazar, siber atfetme için benzer bir öznel değerlendirme önermekte ve şunları belirtmektedir:

Kesin atıfta bulunmanın aksine, doğru atıf olasılığına odaklanmak önemlidir. Elbette birçok alanda mutlak kesinliğe nadiren ulaşılabilir. Bu nedenle, bir dizi farklı standart geliştirilmiştir (örneğin, makul bir şüphenin ötesinde kanıt, kanıtların üstünlüğü) ve bireyler ve kuruluşlar, kritik kararlar alırken (örneğin, bir tıbbi tedaviyi başkasından görmeyi tercih ederken olduğu gibi) genellikle olasılıklara güvenmek zorundadırlar. Kuşkusuz, kesinlik ne kadar yüksek olursa, bir hareket tarzı seçmek o kadar kolay olabilir, ancak bu, makul önlem alınmadan önce kesinliğin gerekli olduğu anlamına gelmemektedir.[251]

Siber atıfları değerlendirmek için mahkeme temelli atıf kavramlarının tamamının ithal edilebileceğini varsaymak saflık olsa da, birkaç kilit nokta açık bulunmaktadır. İlk olarak, atıf için bilimsel kanıt gerekli değildir.[252] Bilimsel kesinlik, ispatın "altın standardı" olsa da, nadiren elde edilebilir ve tarihsel olarak, atıf kurmak için gerekli olmamıştır. İkincisi, daha önce belirtildiği gibi, atfetme, rutin olarak öznel belirlemelere dayanmaktadır.

---

251 S. Charney, "Rethinking the Cyber Threat: A Framework and Path Forward," Microsoft white paper (Redmond, WA: Microsoft Corp., 2009), s.9.
252 E. F. Mejia, 2014, s. 124

Üçüncüsü, öznel bir atıf değerlendirmesi kullanılırken, sonuçların ciddiyeti güven derecesine bağlıdır. Bir mahkeme, mali sorumluluğu, kanıtların üstünlüğüne dayalı olarak değerlendirebilir, ancak cezai suçun tespiti için çok daha yüksek bir güven derecesi gereklidir. Son olarak, birçok teknik uzman öznel bir değerlendirmeyi kullanırken tereddütlü veya rahatsız olabilir, ancak hükümet, hukuk topluluğu aracılığıyla, öznel atıfta yerleşik uzmanlığa sahiptir.[253]

Atfetmenin kurulmasında ve yeterli bir yanıtın önerilmesinde hukuki bilgi önemlidir. Siber alan yeni olmasına rağmen, aktör ve eylem atfetme sanatı Hukuk alanında uzun süredir devam eden bir uygulamadır. Şimdiye kadar meydana gelen her cezai kovuşturma, zorunlu olarak suçluluğun (aktör atıf) ve suçun (eylem atıf) öznel bir belirlenmesini gerektirmekteydi. Hukuk pratisyenleri, siber alanın teknik yönlerinden genellikle habersiz olsalar da, atıf yapma sanatında çok bilgilidirler. Gerçek şu ki, hepsi olmasa da çoğu siber operasyon, devlet organları tarafından alenen yürütülmektedir. Genellikle bir siber operasyonun faili kimliğini gizlemeye çalışmaktadır. Devletler bu iddiada bir istisna değildir ve mağdur Devletin herhangi bir şekilde yanıt vermesini önlemek için çoğu zaman anonim kalmaya çalışacaklardır. Bir siber saldırının failleri talimatlara veya direktiflere göre veya bir devletin kontrolü altında hareket ederse, davranışları o duruma atfedilecektir.

Son olarak, bir siber saldırı, eğer Devlet, bu eylemleri kendi başına kabul edip benimserse bir Devlete atfedilebilecektir. Somut olarak, eğer bir grup birey X devletine karşı siber saldırılarda bulunursa ve Y devleti bu saldırıları zımnen onaylarsa, buna atfedilemezler. Öte yandan, Devlet, saldırıların gerçekleştirilmesine yardımcı olmak veya karşı operasyonlara karşı korumak amacıyla hizmetlerini (istihbarat, askeri veya siber birim) bu gruba açık hale getirirse, bu eylemleri kendisinin gerçekleştirdiği kabul edilir ve bu

253 Id.

nedenle, bu eylemleri, sanki açıkça onaylarmış gibi ona atfedilebilir. Hâlâ çözülmesi gereken bir sorun mevcuttur: Bir eylemin bir devlete atfedilmesi için gereken kesinlik derecesi. Bu, siber saldırıların niteliğini analiz ederken özellikle önemli olan bir kanıt sorunudur.

Uluslararası hukukta veya Devlet sorumluluğuna ilişkin taslak maddelerde belirli bir eşik belirlenmemiştir. Bununla birlikte, İran-ABD İddialar Mahkemesi (IUSCT) tarafından 1987 yılında alınan bir kararla geliştirilen bir standart, doktrin tarafından genel olarak benimsenmiştir.[254] Mahkeme, bir eylemi bir devlete atfetmek için, failleri ve bunların devletle olan bağlantılarını "makul bir kesinlikle" tespit etmek gerektiğini söylemiştir. Lahmann ve Geiss'in belirttiği gibi, söz konusu eylem ne kadar ciddiyse ve bu nedenle daha şiddetli tepkilerin meydana gelme olasılığını ne kadar çok arttırırsa, gerekli kanıt standardı o kadar yüksek görünecektir.[255] Bu nedenle, bir başkasını silahlı saldırıya varan bir eylemde bulunmakla suçlayan bir devlet, kendi egemenliğini yalnızca asgari düzeyde ihlal ettiğini iddia etmesine kıyasla iddialarını daha kesin bir şekilde kanıtlamak zorunda kalacaktır. Bu nedenle, Tallinn El Kitabı, bir siber operasyonun başlatıldığı veya kaynağının bir Devletin siber altyapılarından geldiği gerçeğinin; bu durumun, devletin söz konusu operasyonla ilişkisine dair bir gösterge oluştursa bile operasyonu o Devlete atfetmek için yeterli kanıt oluşturmadığını ileri sürer. Böyle bir ipucu hala yetersizdir ve bir siber operasyondan şu veya bu devletin sorumlu olduğu iddiasını desteklemek için daha fazla kanıta ihtiyaç duyulacaktır. Siber uzmanlar teknik olarak bu atıfları tespit edebilirler, ancak genellikle öznel atıfların ayrıntılarından habersizdirler. Hem hukuk uzmanlarının

254 Yeager v. Iran, *IUSCT*, Case No. 10199, section.37.
255 R. Geiss & H. Lahmann, "Freedom and security in cyberspace: shifting the focus away from military responses towards non-forcible countermeasures and collective threat prevention" *in Peacetime Regime for State Activities in Cyberspace, K. Ziolkowski (ed.),* International Relations and Diplomacy, Tallinn *2013,* s. 624.

hem de teknik siber uzmanların yakın uyum bütünleşme, uygun bir siber politika ve belirli hasmane siber eylemlere uygun yanıtlar oluşturmak için kritik öneme sahiptir.

II. ULUSLARARASI HUKUK KAPSAMINDA SİBER SALDIRILARIN GEREKÇESİ

Yüksek yoğunluklu çatışmalarda yer alan tehlikelerle yüzleşmek için kurulan Birleşmiş Milletler Şartı, ilk bakışta, yeni teknolojilerin ortaya çıkması ve hızla gelişmesiyle ortaya çıkan hukuki zorlukları karşılayabilecek gibi görünmemektedir. BT altyapıları çağdaş toplumlarımızın sıcak noktaları haline geldikçe, devletler artık yeni bir değişken ve gizli bir tehdide karşı savunmasızdır: Devletlerarası siber saldırılar. Bu başlığın ilk kısmında, uluslararası barış ve güvenliğin korunmasında eyaletler arası siber saldırıların yarattığı zorlukları tartışılacaktır. İkinci kısımda, bir devlet siber saldırısının, Birleşmiş Milletler Genel Kurulu Saldırı Tanımı'nda sağlanan analitik çerçeveye dayalı olarak bir saldırı eylemi olarak nitelendirilip nitelendirilmediği ve buna yanıt vermek için BM Şartı'nın güç kullanımına ilişkin hükümlerinin uygulanıp uygulanmayacağı incelenecektir.

A. ULUSLARARASI BARIŞ VE GÜVENLİĞİ TEHDİT OLARAK SİBER SALDIRILAR

2010 raporundan bu yana ve özellikle 2013 ve 2015 raporlarında,[256] Birleşmiş Milletler ‘de uluslararası güvenlik bağlamında Bilgi ve Telekomünikasyon Alanında

256 Tüm bu raporlara BM Dijital Kütüphanesi aracılığıyla erişilebilir: https://digitallibrary.un.org/search?f1=author&as=1&sf=title&so=a&rm=&m1=e&p1=UN.%20Group%20of%20Governmental%20Experts%20on%20Developments%20in%20the%20Field%20of%20Information%20and%20Telecommunications%20in%20the%20Context%20of%20International%20Security&ln=en E.T 30 Aralık 2020

İlerleme Üzerine Devlet Uzmanları Grubu (daha çok Devlet Uzmanları Grubu (GGE) olarak bilinmektedir.) siber güvenlik konusunda, bilgi teknolojilerinin uluslararası barış ve güvenlik üzerindeki etkisi hakkında doğru bir teşhis sunmuştur. Bu grup, bir yandan dijital teknolojilerin yoğun kullanımını içeren yeni tehditleri ve yeni riskleri belirlerken diğer yandan da Devletlerin kendi yerel bağlamlarına göre uygulayabilecekleri bir dizi eylem ve önlem önermektedir.

Dünya düzeninin dönüşümü ve yeni tehditlerin ortaya çıkması veya silahlı çatışmalar, suç veya terörist ağlar, siber veya nükleer saldırılar gibi mevcut tehditlerin ortaya çıkması, uluslararası barış ve güvenlik stratejilerini oldukça etkilemiştir. Bu perspektifte, öncelikle uluslararası güvenliğin ne olduğu ve bunun siber tehditlerle bağlantılarının tartışılması gerekecektir. Ardından siber barışçıl çözümün yanı sıra siberle ilgili çatışmalarda müdahale etmeme ilkesinin uygulanması tartışılmaya devam edilmektedir. Ardından siber barışçıl çözüm ve siber ile ilgili çatışmalara müdahale etmeme ilkesinin uygulanması üzerine bir tartışma yapılmaktadır.

1. Uluslararası Güvenlik Nedir?

Öncelikle, uluslararası güvenliğin geniş çapta kabul görmüş bir tanımının olmadığını açıklığa kavuşturmak gerekir. Aslında, onu tanımlamak akademik tartışmaların ana eksenlerinden biri olmuştur.[257] Bununla birlikte, bu tartışmalar etrafında bazı fikir birlikleri mevcuttur: Ulusal güvenlik ve savunmaya yönelik eylemlerle bağlantılı, teorik

[257] J. BAYLIS, ‘’Uluslararası İlişkilerde Güvenlik Kavramı’’, Uluslararası İlişkiler, Cilt 5, Sayı 18, Yaz 2008, s. 69 - 85 Makalenin şngilizceden Türkçeye tercümesi Burcu Yavuz tarafından yapılmıştır. Orijinal metin için bkz. Brauch et. al., Globalization and Environmental Challanges, s. 495-502.

olarak gerçekçilik (realizm) tarafından desteklenen geleneksel bir güvenlik görüşü.[258] Bu görüşle karşı karşıya kalan ve son otuz yıl boyunca dünyada gerçekleşen değişimler göz önüne alındığında, sorun hakkında düşünmek için uluslararası güvenlik kavramı güçlenmeye başlamıştır. Olasılıkları, esas olarak güvenlik görüşünü katı, askeri olanın ötesine genişletmeye çalışan rasyonalist ana akıma meydan okuyan çok çeşitli yaklaşımlarda ortaya çıkmaktadır.[259]

Genel olarak güvenliği, insan grupları ve özneler için, değer verdikleri görevleri ve isteklerini tehdit edilmeden yerine getirebilecekleri bir koşul olarak anlamak mümkündür.

Güvenlik dörtkenardan oluşur:[260] Nesnel, öznel, statik ve dinamik. Nesnel olarak, güvenliğin, bir topluluğun değerlerine ve varlıklarına yakın belirli bir tehdit veya tehlike olmadığında elde edildiği anlaşılır. Öznel olarak, ulaşıldığını ya da ulaşılmadığını hissettiği sürece bu durumla ilgili mevcut algıları anlaşılır. Statik boyut, güvenli olsun ya da olmasın, gerçekte elde edilen güvenlik koşulunu ifade eder. Bunun için, bunu başarmayı mümkün kılan veya başarılması / sürdürülmesi için kullanılan bir dizi eylem, politika ve program vardır, bu durumda uluslararası toplum her zaman elde etmek için yaptıklarının dinamikleri, güvenli bir duruma daha yakın olmak için (bir kişinin yaşamı için, bir topluluk için veya bir sosyal grup için, bir Devlet için, bir bütün olarak dünya için) geleceği ile karşı karşıya

---

258 A. G. Stolberg, "Crafting National Interests in the 21st Century", Chapter 1 in, J. B. Bartholomees, Guide to National Security Issues, Volume II: National Security Policy and Strategy, Strategic Studies Institute, Carlisle, PA, 2012, s.8. *http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1110* E.T 3 Eylül 2020.

259 D. C. Copeland, Rationalist Theories of International Politics and the Problem of the Future, Security Studies, no. 20, sa. 3, 2011, s. 441-450. https://www.tandfonline.com/doi/abs/10.1080/09636412.2011.600144?src=recsys&journalCode=fsst20 E.T 3 Eylül 2020

260 A. G. Stolberg, 2012

kalmaktadır. Bu temel fikirler, Wolfers tarafından ulusal güvenlikten bahsederken verilen tanımlardan ortaya çıkmaktadır:

[…] Güvenlik, nesnel anlamda, elde edilen değerlere yönelik tehditlerin yokluğunu, öznel anlamda, bu tür değerlerin saldırıya uğrayacağına dair korkunun yokluğunu ölçmektedir. […] Gelecekteki saldırı şansı asla "nesnel olarak" ölçülemese de, uluslararası ilişkilerde terimin nesnel ve öznel çağrışımı arasındaki olası tutarsızlık önemlidir; her zaman öznel bir değerlendirme ve düşüntü meselesi olarak kalmalıdır.[261]

Güvenlik hakkında konuşurken söz konusu olan sadece tehditlerin varlığı değil, aynı zamanda bunların algılanması ve tehlike veya risk seviyesidir. Her iki kavramsallaştırma da öznel unsuru, yani güvenlik dinamiklerini alan deneklerin yaşamlarında veya bütünlüklerinde var olan hasar olasılığı hakkında sahip oldukları algıyı içermektedir.

Güvenliğin uluslararası bileşeni hakkında konuşmak için, ortak bir aygıtlar kümesi altında bulunan olası tanımların ve yorumların sıralanmasına izin veren değişkenleri (referans nesne, tehditler veya tehlikeler, korunacak nesnenin temelleri ve değeri ile güvenlikten sorumlu özel eylem araçları) dikkate almak gerekmektedir. Bunun için, uluslararası güvenlikle ilgili güncel çalışmaların bölündüğü iki ana yaklaşım, sorunun analizinin içinde yer aldığı genel çerçeveyi belirterek sunulmuştur. Uluslararası güvenliğe ilişkin iki büyük perspektiften her biri belirli bir dünya düzeni vizyonu üzerinde

261 A. Wolfers, "National Security as an Ambiguous Symbol" in Discord and Collaboration: Essays on International Politics, Johns Hopkins Press, Baltimore, 1962, s. 481-502.

düşünmektedir. İlk olarak, geleneksel, kısıtlı ve akılcı bir yön tanımlanır; öte yandan, genişletilmiş ve çok boyutlu bir güvenlik görünümü ortaya çıkmaktadır.[262]

Bahsedilen değişkenlere göre dikkate alınması gereken ilk nokta, referans nesnedir. Geleneksel yön, devlet merkezli bir uluslararası gerçeklik görüşünü sürdürmektedir: Devlet, uluslararası sistemin ana aktörüdür ve vatandaşlarına refah sağlama yeteneğine sahip tek kişidir; bu nedenle sigortalanacak ayrıcalıklı nesne haline gelmektedir. Bu görüş, uluslararası güvenlikten çok ulusal güvenliğe odaklanmaya devam etmektedir. Neden? Çünkü farklı ulusal çıkarlara sahip egemen ve bağımsız Devletlerden oluşan uluslararası sistemin birimleri arasında her zaman bir çatışma durumunda (gerçek veya potansiyel) olduğunu ve bu çerçevede güvenliğin her birinden dış politika için ana referans noktası olduğunu düşünerek başlamaktadır.

Devletin karşı karşıya olduğu tehditler esas olarak dışsaldır, sistemdeki diğer Devletlerden gelmektedir ve nesnel olarak tanımlanabilirler, somuttur ve onların algılarıyla oluşturulmamaktadır. Güvenliğin garanti edildiği araçlar temelde askeri niteliktedir; analiz, olası dış saldırılara karşı savunmaya odaklanmaktadır ve bundan sorumlu olanlar silahlı kuvvetlerdir. Başka mekanizmalar da vardır, ancak bunlar, her zaman, saldırganı olası bir saldırıdan caydırmak için güç gösterme olasılığıyla ilişkilidir, eğer bunu yaparsa yüzleşmek zorunda kalacağı sonuçlar göz önüne alındığında; genel olarak, savunma için tehlikede olan unsurlar kümesi maddi, yani askeri, ekonomik ve politik kaynakların birikimi olarak

262 D. BALDWIN, The concept of security" in Review of International Studies, British International Studies Association No. 23., Review of International Studies, 1997, s. 5-26. https://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf E.T 3 Eylül 2020.

tanımlanacaktır. İç düzen ve uluslararası düzen keskin bir şekilde ayrılmıştır, her düzlem için farklı mantık ve çıkarlar hâkimdir ve bu bölünmenin belirleyici faktörü Devlet'tir.[263]

Genişletilmiş ve çok boyutlu olarak adlandırılan ikinci güvenlik eylemi,[264] bu klasik görüşe karşı çıkmaktadır. Vurgu, Devlete, onun iç siyasal düzenine veya hayatta kalmasına değil, Devletler ve diğer sınır ötesi, üst ve alt ulusal aktörler arasında bir dizi ilişki ve uygulamanın kesiştiği arenada uluslararası / ulus ötesi üzerindedir.[265] Soğuk Savaş'tan sonrasına özgü bu ikinci özellik, güvenliğin ve uluslararası gerçekliğin dinamik ve heterojen olarak yorumlanmasına yönelik bir çerçeveyi desteklemektedir.[266] Bu anlamda, bazı uzmanlar "esnek" post-Westfalyan veya Westfalyan bir uluslararası sistemle karşı karşıya olduğumuzu anlamaktadırlar.[267]

Bu uluslararası gerçeklikten yola çıkılarak yeni güvenlik çalışmalarında artık ulusal güvenliği değil, daha çok uluslararası güvenliği sağlamayı amaçlayan bir odak hâkim olmaya başlamıştır.

Uluslararası gerçeklik daha karmaşık hale geldikçe, yeni güvenlik yaklaşımlarında aktörlerin ve dolayısıyla hasar kaynaklarının da değiştiği anlaşılmaktadır. Dikkatin odağı, geleneksel perspektifin dış devletlerarası mantığının yerini alan, küresel ve ulusötesi olarak anlaşılan sözde "yeni tehditler"[268] olacaktır. Bu çerçevede, güvenliğin; orduyu aşan ve

---

263 Baldwin, 1997, s.5
264 Baldwin, 1997, s.23
265 A. Blackwell, Multidimensional Security Perspective, OAS, 2013, https://www.oas.org/es/ssm/docs/speeches/speechAB_Calgary_5-1-2013_final.pdf E.T 12 Ocak 2020.
266 M. BARTOLOMÉ ''*Una visión de América Latina desde la perspectiva de la agenda de la Seguridad Internacional contemporánea*", **Journal of International Relations**, No. 23, *Autonomous University of Madrid*, Eylül 2013. s. 35-64.
267 Id.
268 IEEE, *The Evolution of The Concept of Security*, Framework Document 05/2011, the Spanish Institute of Strategic Studies, Haziran 2011, s.4

çevresel, sosyal, ekonomik ve sağlık yönlerini içeren önemli sayıda kenarı kapsayan birçok boyuta sahip olduğu anlaşılmaktadır.

Küreselleşme ve tehditlerin doğası göz önüne alındığında, bunlarla başa çıkmanın somut yolları net olmayacak ve ilgili özel yaklaşıma bağlı olacaktır. Ancak geleneksel güç kullanımının yanı sıra önleme, diplomasi, kalkınma, işbirliği gibi eylemler uluslararası güvenlik için uygun araçlar olarak gösterilebilmektedir. Uluslararası barış ve güvenliği garanti altına almak için sorumlulukların nasıl belirleneceğine ilişkin değişkenle ilgili olarak, gerçek şu ki, tüm gezegeni etkileyen sorunları çözebilecek tek bir Devlet olmayacaktır. Bu tür barışa ulaşmak adına; devletler, uluslararası kuruluşlar, şirketler ve sivil toplumlar işbirliği yapmalıdır.

Küresel olarak etkileyen ve tüm paydaşları ilgilendiren sorunların olduğu, ancak hepsinin güvenlikle ilgili aynı öncelikleri paylaşmadığı açıktır ve bu nedenle, anlayışlarının çoğul terimlerle sağlanması gerektiği anlaşılmaktadır. Uluslararası güvenliğin tüm önemi, her bir ajanın hayatta kalması ve sürdürülebilirliğinin korunması adına birincil veya en alakalı değerlerinden kaynaklanacaktır; buradan, medyanın da neyi sağlamak niyetinde olduğu anlaşılabilecek ve işbirliği yapmak veya birlikte çalışmak istediği aktörlere göre farklılaşacağı sonucuna varılabilecektir.

Tek bir bakışı kabul etmek, dünyanın karmaşıklığını ve çeşitliliğini inkâr etmeyi, yani uluslararası gerçekliğin çoklu etkileşimlerini ve çelişkilerini yalnızca tek yönlü olarak azaltmayı ima etmektir. Savunma açısından, her bir Devlet eylemlerinde bağımsızlığını güvence altına almıştır: Dâhili olarak, yüce ve münhasır güç olarak toprakları üzerinde, tam egemenlik içinde; siyasi gerçekliğin dış düzeyinde, içten keskin bir şekilde ayrılmış her

---

http://www.ieee.es/en/Galerias/fichero/docs_marco/2011/DIEEEM052011_EvolutionConceptSecurity_ENGLISH.pdf E.T 2 Ekim 2020.

Devlet, kendisini savunmak ve ulusal çıkarlarını korumak için (güç kullanımının keyfi olarak yetkilendirilmesi) gerekli gördüğü araçları kullanma gücüne sahip olacaktır. Güç dengesine dayalı bir uluslararası düzen hâkim olmuştur, böylece tek bir Devletin diğerlerinden daha güçlü olmasından ve bu sayede devlet egemenliğini bozmasından kaçınılmıştır.

Uluslararası güvenlik üzerine yukarıdaki analiz ve güvenlikle ilgili bilimsel teoriler, devletlerin çıkarlarını korumak için ne kadar ileri gidebileceklerini göstermiştir. Ancak, siber uzay söz konusu olduğunda çok boyutlu bir yaklaşım izlenmelidir çünkü siber uzay tam anlamıyla devletlerin kontrolü altında değildir, bu alanda özel şirketler büyük bir paya sahiptir.[269] Teknolojik eşitsizlikleri göz önüne alındığı zaman devletleri ilgilendiren şeyin, "ortak çıkarların o kadar yaygın olmadığı durumlarda bir fikir birliğine varmaya gerek olmaması" olduğu düşünülebilir. Bununla birlikte, uluslararası güvenliğin nesnel amacının uluslararası barışı sağlamak olduğu hiçbir ülke, kritik altyapıları siber saldırıya uğradığında, hizmetleri reddedildiğinde, bilgileri manipüle edildiğinde, işlevsel kimlik bilgileri hacklendiğinde vb. huzurlu hissedemeyecektir; bu nedenle uluslararası barış ve güvenliğin siber uzaya yayılması gerekmektedir.

2. Anlaşmazlıkların Barışçıl Çözümü Zorunluluğu

18 Ekim 1907'de Lahey'de imzalanan Uluslararası Çatışmaların Çözümü Sözleşmesi'nin ilk maddesi, Devletlerarasındaki ilişkilerde güç kullanımının "mümkün olduğunca" önlenmesi çağrısında bulunmaktadır. Birleşmiş Milletler Şartı'nın 33.

---

[269] J. Goldsmith, T. Wu, **Who Controls the Internet?: Illusions of a Borderless World**, Oxford University Press, 2006, s.65

Maddesi'nde (Bölüm VI) yer alan ihtilafların barışçıl yollarla çözülmesi ilkesi, daha ihtiyatlı bir tavır içermekte ve bir yandan Devletler ve diğer yandan BM gibi başlıca uluslararası aktörlerin sorumluluğunu Güvenlik Konseyi aracılığıyla teşvik etmektedir.[270] Barışın korunmasından, esasen BM Güvenlik Konseyi sorumludur. Gerçek şu ki, Devletler, ilk etapta, örgüt üyeleri arasındaki savaşın yasaklanmasına ilişkin kurallara saygı duyarak çok önemli bir rol oynamaktadır. Uyuşmazlığın çözümü için güç kullanımını dışlayan bu anlaşmazlıkları çözme yönteminin teşviki, Şart'ın 2. Maddesinin 3. ve 4. paragraflarında temel bir ilke olarak ortaya konmuştur.

Ayrıca, 1982 yılında Genel Kurul tarafından onaylanan Anlaşmazlıkların Barışçıl Çözümüne İlişkin Manila Deklarasyonu'nun[271] bu çeşitli yollara başvurma yükümlülüğünün tüm uluslararası anlaşmazlıklar için yer çekimi ve doğası ne olursa olsun geçerli olması açısından özel bir önem taşıdığını belirtmek önemlidir. Uluslararası ilişkilerin hukuki aracı olarak ilkenin doğrulanması, kuvvet kullanma yasağının genel bir emredici standart düzeyine yükseltilmesi anlamına gelmektedir. Aynı zamanda, anlaşmazlıkları barışçıl yollarla çözme yükümlülüğünün sonucunda, aynı zorunlu karakteri kazanmaktadır.[272]

Güvenli, istikrarlı ve müreffeh bir siber uzay, her ülke ve tüm dünya için büyük önem taşımaktadır. Her şeyin birbirine bağlı olduğu bir siber uzayda, tüm ülkeler birbirine bağlıdır ve birbirine bağımlıdır ve çıkarlarının giderek daha fazla iç içe geçtiğini

---

270 Bu ilke, Birleşmiş Milletler Şartı uyarınca Devletler Arasında Uluslararası Hukuk Dostu İlişkiler ve İşbirliği İlkeleri Bildirgesinde daha da güçlü bir şekilde teyit edilmiştir. GA Res. 2625 (XXV), Doc. Off. AG NU, 25th sess., Supp. n ° 28, Doc. NU A / 8028 (1970) [Dostluk Anlaşması] https://www.un.org/ruleoflaw/files/3dda1f104.pdf E.T 13 Ekim 2020.

271 A/RES/37/10, Manila Declaration on the Peaceful Settlement of Disputes, 1982. https://peacemaker.un.org/sites/peacemaker.un.org/files/GARES_ManilaDeclaration_ARES3710%28english%29.pdf E.T 13 Ekim 2020.

272 Bknz Ü. Halatçı Ulusoy, "Uluslararası Hukuk Açısından Libya ve Suriye Örneğinde, Koruma Sorumluluğu", TAAD, Yıl 4, Sayı 14, Temmuz 2013, s. 288

görmektedir. Huzurlu ve sakin bir siber, herkesin yararına olacaktır. Uluslararası toplum, siber uzayda barış ve güvenliği sağlamak için Birleşmiş Milletler Şartı'nın amaç ve ilkelerini, özellikle kuvvet kullanmama veya zorla tehdit ve anlaşmazlıkların barışçıl çözümüne ilişkin ilkeleri dikkatle gözlemlemelidir.[273]

Anlaşmazlıkların ciddiyeti ve niteliği ne olursa olsun, söz konusu anlaşmazlık birden fazla ülkenin çatışmasını içerdiği sürece, devletler güç yerine barışçıl mekanizmalara başvurmak zorundadır. Manilla Deklarasyonu'nun bu mantığı ve BM Şartı'nın ruhuyla; devletlerin siber nitelikteki bir çatışmada bu mekanizmaları kullanmasını hiçbir şey kısıtlamamaktadır. Aksine, uluslararası toplumun refahı için, barışçıl yerleşim, her durumda, mümkün olan her durumda teşvik edilmektedir.

*Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanında Kalkınma üzerine 2015 BM Hükümet Uzmanları Grub*u'nun raporu, siber uzaydaki devletlerin davranışını düzenlemek için 11 norm ortaya koymuştur.[274] Tüm bu normların ortak yönü, barışçıl bir siber uzay kurmaktır. Meşru müdafaa hakkına yalnızca, geleneksel silahlı çatışmalarla aynı seviyede, önemli ölçüde ulusal güvenlik tehdidine neden olma kapasitesine sahip bulunan siber saldırılarda izin verilse de, bu hakkın konusu olabilecektir, aksi takdirde şiddete başvurmadan her zaman anlaşmazlıkları çözüme kavuşturmaya çalışmak zorunludur. Diğer konularda olumlu sonuçlar sağlama konusundaki uzun süredir devam eden itibar göz önüne alındığında, bu barışçıl mekanizmalar arasında, aynı yolda

---

273 Çin Dışişleri Bakanlığı, *Stratégie de la Coopération internationale dans le Cyberespace,* 1 Mart 2017. Politics and Activities, https://www.fmprc.gov.cn/fra/wjdt/wjzc/ty/t1442395.shtml E.T 13 Ekim 2020.

274 N. G. Miralis, International Norms Governing Behaviour in Cyberspace: The UN's Charter, Australia Global. 1 Haziran 2020. https://www.lexology.com/library/detail.aspx?g=86aabb3f-f4df-4ea4-b540-e13350c7ace8 E.T 13 Ekim 2020.

siberle ilgili konularda başarılı olacakları gibi, mevcut çevrimiçi anlaşmazlık çözümlerinin yanı sıra tahkim ve arabuluculuk gibi diğer barışçıl çözümler önerilebilir.

3. Diğer Devletlerin İç Meselelerine Müdahale Yasağı

Yukarıda tartışıldığı gibi, tüm siber saldırılar düşmanca bir eylem veya sadece silahlı bir saldırı bir yana düşmanca bir niyet oluşturmamaktadır. Ancak bu fiiller uluslararası hukuk hükümlerine uygun olmayabilirler. Siyasi veya ekonomik sonuçları olan siber saldırılar, şu anda, Birleşmiş Milletler Şartı'nın 2(4) Maddesinde kullanılan "güç" kavramı ekonomik veya siyasi kısıtlamaları kapsamadığı için özellikle endişe vericidir.

Şiddeti güç kullanımının eşiğine ulaşmayan bu eylemler için literatür "*düşük yoğunluklu siber saldırılar*" veya "*tahribatsız siber saldırılar'' '* dan bahsetmektedir.[275] Bazı yazarlar, literatürün esas olarak felaket etkileri üreten büyük ölçekli siber operasyonlara odaklanmış olmasına rağmen, mümkün olsa da, bunların nadir olduğunu belirtmektedir. Aksine, "düşük yoğunluklu" siber saldırılar, bir devletin kuvvet kullanmakla suçlanmadan uluslararası ilişkilerin yürütülmesini etkilemesine izin verdiğinden, çok az kaynak gerektirdiğinden ve misilleme riskini azalttığından, güçlü bir büyüme yaşayabilecek gibi görünmektedir.

Bu saldırılar, güç kullanımından başka bir kategoriye, yani uluslararası hukuk tarafından yasaklanan müdahale kategorisine girebilir. Güç kullanımını yasaklama ilkesine odaklananlara kıyasla, çok az yazar siber saldırılara uygulanan müdahale etmeme ilkesine odaklanmıştır. Genel olarak, müdahale etmeme ilkesinin neleri içerdiğine ve siber bağlamda nasıl uygulanacağına dair daha fazla inceleme yapılmadan, kuvvet kullanımına

---

275 W. Mattessich, **Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage**, *Columbia Journal of Transnational Law, Sa. 54 (3)*, 2016, s. 876.

karşılık gelmeyen siber saldırılar için bir kategori oluşturması önerilmektedir. Bununla birlikte, Russel Buchan'ın da işaret ettiği gibi, "*müdahale etmeme ilkesi, Devletleri siber saldırılardan koruyabilen yasal bir çerçeve oluşturur; bu, fiziksel hasar üretmemelerine ve dolayısıyla yasaklı bir güç kullanımı olarak nitelendirilememelerine rağmen, yine de bir Devleti, özgürce belirleyebilmesi gereken bir davranışı benimsemeye zorlama etkisine sahiptir*."[276]

Başvuruyu, bir Devletin egemenliğini ve tam bağımsızlık içinde hareket etme kapasitesini zayıflatma etkisine sahip siyasi veya ekonomik kısıtlamalarla sınırlandırmak için, uluslararası hukuk, diğer devletlerin iç ve dış meselelerine müdahale etmeme ilkesini geliştirmiştir. Uluslararası Adalet Divanı'nın defalarca işaret ettiği gibi, bu ilke artık geleneksel bir değer kazanmıştır.[277]

Birleşmiş Milletler Şartında açıkça bulunmayan ilke, 1970 yılında Birleşmiş Milletler Genel Kurulu'nun 2625 (XXV) kararıyla kabul edilen *Devletler Arasında Birleşmiş Milletler Şartı'na Uygun Şekilde Dostane Münasebetler Kurma ve İşbirliği Yapmaya Dair Milletlerarası Hukuk İlkeleri Hakkında Bildiri*'de önemli bir metin temeli bulmaktadır. Şu hususları belirtmektedir:[278]

"Hiçbir Devlet veya Devletler grubu, doğrudan veya dolaylı olarak, herhangi bir sebeple, diğer herhangi bir Devletin iç işlerine veya dış işlerine müdahale etme hakkına

---

276 R. Buchan, **Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions**? *17 Journal of Conflict & Security Law 211*, 2012, p. 226. https://www.jstor.org/stable/26296227 E.T 14 Ekim 2020.

277 Örneğin, *Kongo Topraklarındaki Silâhlı Faaliyetler Davası, 162; Nikaragua'da ve Nikaragua'ya Karşı Askerî ve Paramiliter Faaliyetler Davası*, 202

278 *Devletler Arasında Birleşmiş Milletler Şart 'na Uygun Şekilde Dostane Münasebetler Kurma ve İşbir ği Yapmaya Dair Milletleraras Hukuk İlkeleri Hakkında Bildiri,* 1970, s.5 https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095256bm_30.pdf E.T 11 Mart 2021

sahip değildir. Bundan dolayı silahlı müdahale ve diğer bütün müdahale çeşitleri veya Devletin şahsiyetine karşı veya siyasi, ekonomik ve kültürel unsurlarına karşı tehdit teşebbüsleri milletlerarası hukuku ihlâl etmektedir.

Hiçbir Devlet, diğer bir Devletin egemen haklarını kendisine bağımlı şekilde kullanmasına ve ondan diğer herhangi bir menfaat sağlamayı temin etmek amacıyla, onu zorlayacak ekonomik, siyasi veya diğer herhangi bir tipteki tedbirleri kullanamaz veya kullanılmasını teşvik edemez. Yine, hiçbir Devlet, diğer bir Devletin rejimini zorla devirmeye yönelik yıkıcı, terörist veya silahlı faaliyetleri örgütleyemez, yardım edemez, teşvik edemez, finanse edemez, tahrik edemez veya müsamaha edemez veya diğer bir Devletteki iç savaşa müdahale edemez."

Bu hükümler, *Devletlerin İçişlerine Müdahale ve Karışmanın Kabul Edilemezliği Bildirgesi*yle tekrarlanmıştır ve ayrıca şunları da kabul eder:[279]

"Devletlerin ve halkların bilgiye serbestçe erişme ve bilgi ve kitle iletişim sistemlerini tam ve müdahale olmaksızın geliştirme ve siyasi, sosyal, ekonomik ve kültürel çıkarlarını ve özlemlerini desteklemek için bilgi medyalarını kullanma hakları… "

"İç veya dış işlerine" atıfta bulunulması, müdahale yasağı ilkesiyle korunan faaliyetlerin kapsamını tanımlamayı mümkün kılar. "İçişleri" kavramı, ayrılmış alan teorisinden, yani prensipte uluslararası hukuk tarafından düzenlenmeyen faaliyetlerden türemiştir. Diğer bir deyişle bunlar, devlet egemenliği ilkesinin her birinin özgürce karar vermesine izin verdiği konulardır. Bunlar, "*siyasi, ekonomik, sosyal ve kültürel sistem*

279 *BM Genel Kurul'un 1981 tarihli Devletlerin İçişlerine Müdahale ve Karışmanın Kabul Edilemezliği Bildirgesi,* A / RES / 36/103

seçimini ve dış ilişkilerin formülasyonunu" içermektedir.[280] Bu seçim, bir Devlet tarafından uygulanan bir kısıtlama nedeniyle artık özgür değilse, uluslararası hukuku ihlal edecektir. Bu, özellikle, hem güç kullanımını yasaklama ilkesini hem de müdahale etmeme ilkesini ihlal eden askeri harekâta başvurduğunda böyledir.

"Dış" ilişkiler diplomatik ve konsolosluk ilişkilerinin seçimini, bir devletin başka bir devleti veya hükümetini tanımasını, uluslararası bir örgüte üye olma seçimini, vb. içermektedir.

Müdahale etmeme ilkesi uzun uzadıya tartışılmış ve Nikaragua'daki Askeri ve Paramiliter Faaliyetlere İlişkin Uluslararası Adalet Divanı'nın kararında açıklığa kavuşturulmuştur. Bu kararda Nikaragua, Amerika Birleşik Devletleri'nin kendisine karşı aldığı bazı ekonomik önlemlerin "iç işlerine dolaylı bir müdahale biçimi" oluşturduğunu öne sürmeye çalışmıştır.[281]

Mahkemenin açıkladığı gibi, Birleşmiş Milletler Şartı'nın 2. (4) maddesi anlamında güç kullanımı oluşturan eylemler ve daha ziyade silahlı saldırganlık, ağırlıkları nedeniyle, müdahale etmeme ilkesinin de ihlalini teşkil etmektedir.[282] Bu yargıdan, isyancıları finanse etmek, desteklemek ve eğitmek, silahlanma veya lojistik destek sağlamak[283] gibi uluslararası hukuk tarafından yasaklanmış bir müdahale oluşturduğu sonucuna da varılabilir.[284] Dolayısıyla, bir Devletin siber yollarla faaliyet gösteren bir grup aktivisti

---

280 *Nikaragua'da ve Nikaragua'ya Karşı Askerî ve Paramiliter Faaliyetler Davası*, (Nikaragua / Amerika Birleşik Devletleri), UAD, Raporlar 1986, s. 14, §205.

281 *Ibid*, §123.
282 *Ibid*, §205.
283 *Ibid*, §195.
284 *Ibid*, §247.

finanse etmesi, eğitmesi ve desteklemesi gerçeği ya da yazılım ya da lojistik yardım sağlaması, doğrudan harekete geçmese bile, o Devletin müdahalesi olabilir.[285]

Ekonomik zorlamanın kullanılması uluslararası hukukta açıkça yasaklanmamıştır ve bundan, Birleşmiş Milletler Şartında bahsedilmemiştir. Bazı yazarlar, bir devlet için mevcut olan diğer çözüm askeri kuvvet kullanmak olduğunda ekonomik kısıtlamanın gerekli bir araç olduğunu da vurgulamaktadır.[286] Gerçek şu ki, ekonomik kısıtlama sınırlı kalmalı ve bir Devletin egemenliğini baltalayan bir baskıya dönüşmemelidir. Bir devletin ekonomisi üzerinde siber yollarla uygulanabilecek baskıların genel olarak benimsenenlerden tamamen farklı nitelikte olduğu unutulmamalıdır. Aslında, bir ambargo gibi ekonomik yaptırımlar ile bir devletin bankacılık ve finansal sistemine yönelik bir siber saldırı arasında çok az benzerlik vardır.

Uluslararası hukuk tarafından yasaklanmış bir müdahale olarak nitelendirilebilecek tipik bir siber saldırı örneği, söz konusu operasyon bir Devleti bu veya benzeri bir davranışı benimsemeye zorlamayı hedefliyorsa, bu, bir devlet borsasının bilgisayar sistemlerini hedefleyen bir operasyondur. Bu senaryo, özellikle insan hayatını kaybetmeden veya doğrudan mülkün tahrip edilmesine neden olmadan gerçekleştirilebileceğinden ve aynı amaca yönelik kinetik bir operasyonla mutlaka kaçınılamayacağı için düzenli olarak değerlendirilmektedir. Etkileri ekonomik alanla sınırlı olduğu için güç kullanımı veya silahlı saldırı teşkil etmemektedir. Öte yandan, mağdur devletin ekonomik ve mali sistemini baltalamak, içişlerine müdahale teşkil ettiğinden, uluslararası hukuk tarafından yasaklanmış bir müdahale olacaktır.

---

285 Ayrıca, Tallinn El Kitabı 2.0'ın pozisyonu, Kural 66'ya ilişkin Yorum, §23.
286 M. Gervais, **Cyberattacks and the laws of war**, *Berkeley Journal of International Law, Vol. 30 (2)*, 2012, s. 551.

İdeolojik baskı, bir devletin iç politikasını etkileme girişimini ifade etmektedir. İnternet herkesin erişebileceği bir alan olduğundan ve yapısı büyük ölçekli mesajlaşmayı düşük maliyetle mümkün kıldığından, siber uzay, iyice savunmasız hale gelmektedir. Birleşmiş Milletler Şartı, ideolojik aracın bir zorlama aracı olarak kullanılması konusunda sessiz kalsa da, bazı uluslararası anlaşmalar onun düşmanca amaçlarla kullanımını sınırlamaktadır.[287]

Genel Kurul, 110 (II)[288] kararında propaganda kullanımının yasallığına ilişkin görüşlerini ifade etmiştir. Barışa yönelik herhangi bir tehdidi, barışı bozmayı veya saldırı eylemini kışkırtma veya teşvik etme niyetinde olan veya olması muhtemel propagandayı kınamaktadır. Bununla birlikte, devlet uygulaması, bu beyanların etkisizliğini göstermektedir. Gerçekten de devletlerin, özellikle soykırım bağlamında şiddeti teşvik eden propaganda yaymaktan mahkûm edildiği bazı durumlar bulunmaktadır.

Bu durumların dışında, uluslararası hukuk, ideolojik aracın kullanımını, müdahale etmeme ilkesinin ihlali olarak tanımlama konusunda isteksiz görünmektedir. Bu nedenle, görüşleri etkilemeyi amaçlayan siber saldırılar, örneğin propaganda yayarak veya onları radikal konumlarla ilişkilendirmek için parti sayfalarını hackleyerek bugüne kadar müdahale etmeme ilkesinin ihlali, uluslararası hukuk çerçevesinde (iç hukukta olsa bile) yasadışı sayılmayacak gibi görünmektedir.

Bununla birlikte, propaganda yaymayı amaçlayan siber saldırılar, seçmenlere uygulanan baskı ve mağdur Devletin siyasi sistemi kanıtlanırsa, uluslararası hukuk tarafından yasaklanmış bir müdahale olarak kabul edilebilecektir. Yasaklanmış bir müdahale oluşturmak için, yalnızca seçmenlerin seçimini ikna etmeyi veya etkilemeyi

287 M. Gervais, 2012, s. 552.
288 Birleşmiş Milletler Genel Kurulu Kararı 110 (II), Yüzüncü Genel Kurul Toplantısı, 21 Ekim 1947.

amaçlayan operasyonlar değil, gerçekten bağlayıcı eylemler olmalıdır. Zorlayıcı bir propaganda eylemini, basitçe izleyiciyi ikna etmeyi amaçlayan bir eylemden ayırmak için, literatür, özellikle izleyicinin bilgi elde etmek için alternatif araçlara sahip olup olmadığına veya propaganda eylemlerinin erişilebilir bilgiyi kısıtlayıp kısıtlamadığına bakmayı önermektedir.[289]Bu nedenle, belirli internet sitelerinde yayılan propaganda, uluslararası hukuk tarafından yasaklanmış bir müdahale teşkil etmeyecektir; tüm haber medyasında propaganda yaymayı ve diğer bilgilerin dolaşımını engellemeyi amaçlayan siber saldırılar, müdahale etmeme ilkesinin ihlali olarak nitelendirilecektir.

Son olarak, gizli bilgileri kamuya açıklamadan önce çalmak için bir hükümetin bilgisayar sistemine girmeyi veya hükümeti devirmek isteyen bir isyancı gruba iletmeyi amaçlayan bir siber saldırı, diplomatik bir müdahale teşkil edebilmektedir.[290] Bununla birlikte, mağdur devlete herhangi bir baskı uygulanmadığından, bilgi çalmak için bir sisteme sırf izinsiz girmek müdahale teşkil etmeyecektir. Bu devletin egemenliğinin ihlali söz konusu olabilir, ancak operasyon herhangi bir baskı unsuru içermemektedir. Tallinn El Kitabı uzman grubu, bu analizi doğrulayarak, bir sisteme izinsiz giriş, güvenlik duvarları veya şifreleri "kırma" gibi savunma engellerini aşmayı gerektirse bile, herhangi bir kısıtlama unsuru olmadığı için bir müdahale olmadığını eklemektedir.[291]

Bir siber operasyon, ekonomik, ideolojik ve / veya diplomatik olarak da zorlama etkisine sahip olabilmektedir. Örneğin, Estonya'yı hedef alan siber saldırılar söz konusu olduğunda, hizmet reddi operasyonları esas olarak medya sitelerini hedef alıp siyasi liderleri itibarsızlaştırmayı amaçlayan bilgileri yaymıştır; ancak aynı zamanda birçok internet sitesi, özellikle bankacılık siteleri, erişilemez hale getirilmiştir. Bu yaşanan

289 S. Watts, 2014, s.14
290 M. Gervais, 2012, p. 552.
291 Tallinn Kılavuzu, Kural 10 §8'e ilişkin yorum.

olaylardan çok azı, yasaklanmış güç kullanımı olarak nitelendirilebilmektedir. Öte yandan, birçok yazar, ülke üzerinde bir etkiden daha fazlasını amaçlayan ve baskı kurmaya çalışan saldırıların süresi (birkaç hafta) ve ciddiyeti göz önüne alındığında, hükümete, Sovyet anıtını kaldırma kararını tersine çevirmeye zorlaması için müdahale etmeme ilkesinin ihlali olduğunu düşünmektedir.[292] Ülkenin iletişim ve bankacılık sistemlerine yaptıkları müdahalenin, özellikle ülkenin yeni teknolojilere bağlılığı göz önüne alındığında,[293] bunun uluslararası hukuk tarafından yasaklanmış bir müdahale olarak kabul edilmesi için yeterli etkisi olmuştur.[294]

Aynı durum 2008'de Gürcistan'daki olaylar için de geçerlidir. İletişim altyapısını, bankacılık bilişim sistemlerini ve medyayı hedef alan siber saldırılar, Gürcistan hükümetinin bir kriz döneminde iletişim kurmasını engellemiştir. Bu saldırılar, bir Devlete atfedilseydi, büyük olasılıkla müdahale etmeme ilkesinin ihlali olarak nitelendirilirdi.[295]

Müdahale etmeme ilkesi, bu nedenle, güç kullanım eşiğine ulaşmayan siber saldırıları uluslararası hukuk kapsamında yasa dışı eylemler olarak nitelendirmeyi mümkün kılar. Bununla birlikte, müdahale etmeme ilkesine bağlı netlik eksikliği, ancak her şeyden önce atıf problemleri göz önüne alındığı zaman, siber uzayda uygulanması zor olmaya devam etmektedir. Nitekim devlet dışı bir grup tarafından yürütülen bir operasyonu niteleyememek ya da tamamen basitçe bir operasyonu bir devlete atfedememek nedeniyle bu ilke uygulanamayacak ve mağdur devlete bir yanıt hakkı sağlanamayacaktır. Buna ek

---

292 R. Buchan, 2012, s.225
293 G.D. Brown and O.W. Tullos, **On the spectrum of cyberspace operations**, *Small Wars Journal*, 2016, s. 6.
294 Mattessich, 2016, s. 895.
295 I*d,* s. 6

olarak, bazı yazarlar[296], bazı siber operasyonların gerçekten uluslararası hukuk tarafından yasaklanan bir müdahalenin ciddiyet eşiğine ulaşacağını, ancak birçoğunun özellikle özel şirketleri hedeflediklerinde "gri bir alan"da kalacağını ve aynı zamanda bu operasyonların çok yerelleştirildiğini ve sadece nadiren devlet işlerinin yürütülmesi üzerinde bir etkiye sahip olduğunu vurgulamaktadır.

B. ULUSLARARASI SİBER SALDIRILARA KARŞI KUVVET KULLANMA OLASILIĞI

51. maddedeki "silahlı saldırı" kavramı, 39. maddedeki "saldırganlık" kavramından çok daha sınırlıdır. Silahlı saldırı eylemi, saldırganlıktır, ancak bunun tersi önerme her zaman geçerli değildir. Benzer şekilde, herhangi bir silahlı saldırı Madde 2 (4) 'nin ihlalini oluştursa da, her yasadışı tek taraflı güç kullanımı, bir silahlı saldırı değildir.[297] Özel Komite'nin silahlı saldırının tanımına ilişkin çalışmasında, delegelerin çoğu, sırasıyla Şartın 2 (4), 39 ve 51. maddelerde kullanılan "kuvvet", "saldırganlık" ve "silahlı saldırı" sözcüklerinin ciddiyeti meselesinde bir ilerleme olduğunu kabul etmiştir.[298] Bir uzlaşma bulmak için, Tanımda yer alan "saldırganlık" teriminin şartın 39. Maddesinde atıfta bulunulanla aynı anlama sahip olduğu kabul edilmiştir.[299] Bununla birlikte, Tanımın bağlayıcı bir hukuki gücü yoktur.

---

296 B.A. Walton, **Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law**, *Yale Law Journal, Vol. 126 (5)*, 2017, s. 1473.

297 Bkz. Nikaragua Davası, paragraf 101.

298 N. Melzer, **Cyberwarfare and International Law**, UNIDIR Resources 2011, s. 11 https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf E.T 20 Ekim 2020.

299 **Saldırganlığın Tanımı,** Genel Kurul Kararı 3314 (Xxix), paragraf 2. Birleşmiş Milletler Uluslararası Hukuk Görsel-İşitsel Kütüphanesi, https://legal.un.org/avl/pdf/ha/da/da_ph_e.pdf E. T 20 Ekim 2020.

Tanımın 1. Maddesi uyarınca, herhangi bir saldırganlık eylemi ve dolayısıyla Şart'ın 2(4). Maddesinin ihlali, hesap verebilirlik açısından, uluslararası devletin sorumluluğunun yasal kuralları dahilinde, bir Devlete atfedilebilir olmalıdır. Bir Devletin siber saldırısının, tanım kapsamında bir saldırganlık eylemi oluşturup oluşturmadığını belirlemek için, mağdur devlet, BMGK'yi siber saldırının veya sonuçlarının yeterli ağırlığa sahip yasadışı bir güç kullanımı oluşturduğuna ikna etmelidir.[300]

UAD'nin Madde 2 (4) 'ü yorumlamasına göre, "*başka bir devlet içinde yıkıcı veya terörist silahlı faaliyetler"* [301]için devlet desteği, kuvvet kullanma yasağının ihlali anlamına gelmektedir. Genelde yerleşik bir hükümetin istikrarsızlaştırılması olan yıkmanın amacı, hedef devletin "*toprak bütünlüğüne veya siyasi bağımsızlığına*" karşı bir eylem olarak yorumlanabilmektedir. Estonya ve Gürcistan hükümetlerinin yetki alanlarındaki siber uzayın parçası üzerinde yetkilerini kullanmaları engellendiği için, 2007 ve 2008'deki hizmet reddi, burada yıkıcı eylemlerle eşleştirilebilecektir. Müdahaleye ilişkin analizimizde daha önce gördüğümüz gibi yıkım, yalnızca, Şartın 2 (4) ve 51. maddeleri kapsamında tartışılacak bir konu olmayacaktır. Peki devletler siber saldırıları, saldırganlık yapmak amacıyla mı işlemektedir?

Saldırıların gizli niteliği nedeniyle, bir devletin siber saldırısının ardındaki niyetin ancak hasar yapıldıktan sonra ve muhtemelen siyasi bir bakış açısıyla saldırıdan hangi devletlerin yararlandığının araştırılmasıyla takdir edilebileceği görülmektedir. 2008 Rus-Gürcü çatışması örneğini ele alırsak; Rus askeri kara saldırısı olmasaydı ve öncesinde dağıtılmış hizmet reddi olmamış olsaydı, Rusya'ya askeri bir avantaj sağlayan Gürcistan'a

300 Saldırganlığın Tanımı Genel Kurul Karar 3314 (Xxix), madde 2
301 Nikaragua Davası, paragraf 196 ("*subversive or terrorist armed activities within another state*")

yönelik siber saldırıların askeri nitelikte sibernetik operasyonlar olduğu düşünülemezdi.[302] Yukarıda belirtildiği gibi, ayrı olarak ve herhangi bir uluslararası silahlı çatışmanın dışında değerlendirildiğinde, etkileri, tanımın 2. Maddesi uyarınca saldırı eylemleri olarak kabul edilebilecek düzeyde değildi.

2003 yılında, Petrol Platformları davasında UAD, *"tek başına veya bir Devlet tarafından başlatılan" saldırı dizisinin "bir parçası olarak gerçekleştirilen □ bir□ saldırının" □ buna□ karşı "silahlı saldırı"*[303] olarak nitelendirilip nitelendirilemeyeceği sorusunu incelemiştir. Bu, meşru müdafaa hakkını değerlendirmek için birkaç küçük olayın bir araya getirilebileceğini öne süren olaylar birikimi teorisinin bir uygulamasıdır. Bu teori, daha önceki birkaç küçük saldırıya dayanan kapsamlı ve sürekli bir planın parçası olarak birkaç ardışık saldırının kurulabileceği durumları ele almaktadır. Olayların biriktirilmesi doktrini, uluslararası hukukun bir kuralı olmamasına ve bazı yazarlar tarafından tartışılmasına rağmen, silahlı çetelerin veya askeri olmayan grupların saldırılarını değerlendirmek söz konusu olduğunda yararlıdır.[304] Birçok yazar, faillerin niyetinin düşmanca doğasını belirlemek için devlet siber saldırılarını analiz ederken bunun dikkate alınması gerektiğini önermektedir. Bu durumda teori, yalnızca hukuka aykırı güç kullanımı olarak nitelendirilebilen ve güvenilir bilgilere dayanarak muhtemelen diğer benzer siber saldırıların izlediği siber saldırılar için geçerli olmalıdır.

Uluslararası hukuk, siber yollarla gerçekleştirilsin veya gerçekleştirilmesin, düşmanca bir eylemin mağduru olan Devletlere bir dizi yanıt sunmaktadır. Bunlar, eylemin

---

302 P. Shakarian ve ark., 2013, s. 68

303 UAD, Petrol Platformlarına ilişkin dava (İran İslam Cumhuriyeti / Amerika Birleşik Devletleri), 2003, para. 64 https://www.icj-cij.org/public/files/case-related/90/090-20030307-ORA-01-00-BI.pdf E.T 19 Ekim 2020

304 T. Ruys, ***"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice***, New York, Cambridge University Press, 2010, s.169

ciddiyetine bağlı olarak değişmektedir. Öncelikle, yasaklanmış güç kullanımına eşdeğer bir siber saldırıya karşı mevcut olan yanıtlara odaklanmaktadır. Bir siber saldırı, silahlı saldırının ciddiyet düzeyine ulaştığında, mağdur Devletin belirli koşullar altında meşru müdafaaya başvurma hakkı vardır. Bu davalar bir istisna olup, yine bu alt bölümde incelenecek olan belirli koşullar altında ve çoğu zaman devlete yalnızca karşı önlemlere başvurma veya gereklilik temelinde savunma yapma izni verilecektir. Bir Devlet, Birleşmiş Milletler Şartı ile kurulan toplu güvenlik sistemine ve önlem almak için de Güvenlik Konseyi'ne başvurabilmektedir.

Birleşmiş Milletler Şartı, güç kullanımının yasaklanması ilkesini Devletlerarasındaki ilişkilerin temellerinden biri haline getirmektedir. Bu ilke uluslararası teamül hukukunda da tanınmaktadır ve uluslararası topluluğun büyüyen bir bölümü onu jus cogens olarak kabul etme eğilimindedir. Gerçek şu ki, şart, iki durumda kendisinin güç kullanımının yasaklanması ilkesine istisnalar sağlamaktadır. Güvenlik Konseyi, yedinci bölüm uyarınca, askeri tedbirler dâhil barışa yönelik bir tehdit, barışın ihlali veya bir saldırı eylemi söz konusu olduğunda bir Devlete karşı tedbirler alabilmektedir. İkinci istisna ise, meşru müdafaa hakkının kullanılmasıdır.

1. Siber Saldırının Silahlı Saldırı Olarak Nitelendirilmesi

Bir önceki alt bölümde silahlı saldırı kavramının ne anlama geldiğini daha iyi belirlediğimize göre, yazının bu kısmında bir siber saldırının bu şekilde nitelendirilip nitelendirilemeyeceği incelenecektir.

Madde 51 herhangi bir silaha atıfta bulunmamaktadır; yani saldırının geleneksel yollarla mı yoksa siber yöntemlerle mi gerçekleştirildiği konusunda hiçbir fark yok gibi

görünmektedir.[305] Bu aynı zamanda, bir siber saldırının ne zaman silahlı bir saldırı anlamına geldiğini bilmek için boyut ve etki kriterlerini kullanmayı öneren Tallinn El Kitabı editörlerinin çıkardığı sonuçtur. Bu El Kitabının 13. kuralı aşağıdaki gibidir: "*Silahlı saldırı düzeyine yükselen bir siber operasyonun hedefi olan bir Devlet, özünde var olan meşru müdafaa hakkını kullanabilir. Bir siber operasyonun silahlı saldırı teşkil edip etmediği, ölçeğine ve etkilerine bağlıdır."*[306]

Grup, silahlı bir saldırının zorunlu olarak askeri bir silahla gerçekleştirilmesi gerektiği şeklindeki araçsalcı yaklaşımı büyük ölçüde reddedip Uluslararası Adalet Divanı'nın nükleer silah tehdidi veya kullanımının yasallığı konusundaki görüşünü yinelemiştir.[307] Araç seçimi, silahlı saldırganlığın niteliği ile ilgisizdir. Grup, kimyasal, biyolojik veya radyolojik silahların kinetik araçlar olmasa bile silahlı saldırı olarak nitelendirilmesine engel olmadığını ve siber araçların kullanımı için de aynı olması gerektiğini vurgulamaktadır.[308] Bir aygıtı silah yapan şey, onun adı ya da normal kullanımı değil, kullanıldığı amaç ve açığa çıkardığı etkidir. Bu nedenle, insan hayatının kaybına ve / veya mülkün tahrip olmasına neden olan herhangi bir cihazın kullanımı, silahlı saldırı için yeterli kabul edilmelidir.[309]

Uygulamada, mülkün tahrip edilmesine veya can kaybına yol açmadan önemli rahatsızlıklara neden olan bir siber saldırı, güç kullanımı teşkil edebilir, ancak silahlı saldırı olarak nitelendirilmemektedir. Yalnızca bu etkilere ulaşan bir siber saldırı silahlı saldırı

---

305 M. Roscini, **World Wide Warfare - *Jus ad bellum* and the Use of Cyber Force,** *Max Planck Yearbook of United Nations Law, Vol. 14*, 2010, s. 106.
306 Tallin Manual, Kural 13.
307 Tehdit veya yasallığı Nükleer Silahların Kullanımı Danışma Görüşü, UAD. Raporlar 1996, s. 226, §39.
308 Tallinn Kılavuzu, Kural 13'e İlişkin Yorum, §3.
309 K. Zemanek, **Armed attack**, in Rüdiger/Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law*, 2013, § 21.

olarak nitelendirilebilmekte ve mağdur devletin meşru müdafaada güç kullanımına başvurma hakkını tetikleyebilmektedir. Bu, aynı zamanda Birleşik Devletler tarafından da kabul edilen görüştür. CIA ve NSA'nın eski Genel Danışmanı Daniel Silver, bir siber saldırının, "*öngörülebilir sonucu yalnızca fiziksel yaralanmaya veya mülke zarar vermekse ve o zaman bile, yalnızca bu öngörülebilir sonuçların ciddiyeti silahlı zorlamayla ilişkili sonuçlara benziyorsa"*[310] bir silahlı saldırı olabileceğinden bahsetmektedir.

Bu nedenle, kazalara neden olmayı amaçlayan hava trafik kontrol sistemlerine yönelik bir siber saldırı, silahlı saldırı olarak kabul edilecektir, çünkü böyle bir saldırı, insan hayatının ve mülkün yok edilmesinin öngörülebilir sonuçlarına sahiptir. Bir siber saldırının, sonuçları fiziksel nitelikte olmadığında 51. madde anlamında bir silahlı saldırı oluşturup oluşturmadığı tartışmalıdır. Örneğin, finans merkezlerini hedef alan bir siber saldırı, dolaylı yoldan, siber saldırıların bir sonucu olarak ortaya çıkabilse de, doğrudan mülke veya bireylere fiziksel zarar vermeyecektir.

Saldırının hedefine dayalı bir yaklaşımı destekleyenler için, bir siber saldırı kritik bir altyapıyı hedeflediği ve onu kullanım dışı bırakmaya çalıştığı andan itibaren, fiziksel hasara yol açsın ya da açmasın, silahlı saldırı olarak nitelendirilebilecektir.[311] Bununla birlikte, yukarıda açıklandığı gibi, hedef tabanlı yaklaşımın, bir siber operasyonu silahlı saldırı olarak nitelendirmeye çalışırken de ortaya çıkan birçok dezavantajı vardır; sonuçları yeterince ciddi ve doğrudan olmayan çok fazla operasyonu kapsama riski taşımaktadır. Örneğin, doğrudan sonuçları yalnızca ekonomik olacak bir siber saldırı, silahlı saldırı

310 D. B. Silver, **Computer Network Attacks as a Use of force under Article 2(4) of the United Charter**, in M. Schmitt/BT O'Donnell (eds), *Computer Network Attacks and international Law,* 2002, s.90
311 D. B. Silver, 2002

olarak nitelendirilmemeli ve mağdur Devletin meşru müdafaasında bir tepkiye izin vermemelidir.

2007'de Estonya'yı hedef alan saldırılarla ilgili olarak hükümet, 51. madde anlamında silahlı saldırı saldırılarını karakterize etmekten vazgeçmiş,[312] ancak Kuzey Atlantik Antlaşması'nın 5. maddesinin fıkrasını da devreye sokmaktan vazgeçmiştir. Bu madde, *NATO üye devletlerinden birine yönelik bir silahlı saldırının tüm üyelere yönelik silahlı bir saldırı oluşturduğunu* belirtirken; 51. maddede de belirtildiği üzere, devletlerin bireysel ve kolektif meşru müdafaa hakkı çerçevesinde güç kullanımına başvurma olasılığını tetiklemektedir. Bu, büyüklük ve etki kriterleriyle tutarlı görünmektedir[313]; saldırılar nihayetinde yalnızca "rahatsızlığa" neden olmuş ve mülke veya bireylere herhangi bir zarar vermemiştir. Bu nedenle siber saldırılar, meşru müdafaa hakkını tetikleyecek kadar ciddi bir boyuta ulaşmamıştır.

Ancak mesele, daha çok İran'ı hedef alan Stuxnet virüsü ile ilgili olarak tartışılmıştır. Elbette, virüs insan hayatının yok olmasına veya can kaybına neden olmamıştır; yalnızca ilgili nükleer santrallerin düzgün çalışmasını engellemiştir. Yine de, Tallinn El Kitabı'nın editörleri de dâhil olmak üzere bazı yazarlar,[314] virüsün karmaşıklığının bir askeri silah zirvesine eşdeğer olduğunu düşünmektedir. Ayrıca saldırı, ulusal güvenlik için kritik olarak

---

312 M.YAYLA, "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", TBB Dergisi 2013 (107), s.214

313 Capt Hiller Silva eneterio ve ark, *Risk Management in Military Operations: An application of the Mosler Method*, JOURNAL OF THE AMERICAS, 2. Baskı, Brazilian Air Force Academy, 2020, s. 227 https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%202%20Issue%202/07-Silva_eng.pdf E.T 13 Mart 2021

314 Tallinn Kılavuzu, Kural 13'e İlişkin Yorum, §13.

kabul edilebilecek bir altyapıyı hedef almıştır. Bununla birlikte, Şart'ın hedefleriyle tutarlılık adına, Stuxnet kullanımı, silahlı bir saldırı olarak nitelendirilmemelidir. Yazılımın ağır ve ciddi bir hasar verme potansiyeli olmasına rağmen, bu sonuçlar meydana gelmemiştir. Silahlı saldırının niteliğini, "potansiyeli olan" ancak can kaybına veya önemli hasara neden olmayan olgulara kadar genişletmek, bu kavramı çok fazla esnetecek ve buna yanıt olarak kuvvet kullanımı dâhil tedbirler alınırsa bir tırmanma riski oluşturacaktır.

Bugüne kadar hiçbir saldırı, bir devletin meşru savunma önlemleri almasına izin veren silahlı bir saldırı olarak karakterize edilmemiş olsa da, bu senaryo tamamen gerçeküstü değildir. Bu nedenle aşağıdaki gelişmeler, siber uzayda meşru savunma hakkının kullanılmasıyla ilgilidir.

2. Siber Uzayda Meşru Savunma Haklarının Kullanımı

Şart'ın 51. Maddesi, "*Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkını*"[315] belirlemektedir. 11 Eylül 2001 saldırılarına tepki olarak Güvenlik Konseyi'nin 1368 sayılı kararından bu yana doktrin, devlet dışı aktörler tarafından işlenen eylemlere yanıt olarak meşru müdafaa kullanımını geniş çapta kabul etmiştir.[316] Meşru müdafaa hakkı, Uluslararası Adalet Divanı'nın, 51. maddenin normuyla birlikte var olan ve içeriği özdeş olmayan Nikaragua'daki Askeri ve Paramiliter Faaliyetleri hakkındaki kararında yeniden teyit ettiği gibi, teamül hukuku olarak da tanınmaktadır.[317]

---

315 BM Şartı, madde 51, 1945.
316 N. TSAGOURIAS, **Self-Defence against Non-State Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule**, Leiden Journal of International Law 29, no. 3, 2016, s.801-825.
317 Nikaragua Davası, 1986, s. 14. §176.

Meşru müdafaa kavramının arkasındaki fikir, bir devletin bir saldırıyı durdurmak için gerekli önlemleri almasına izin vererek, bu önlemler güç kullanımını gerektirse bile uluslararası hukuk düzeninin korunmasıdır. Bu nedenle silahlı saldırganlığa tepki olarak kuvvet kullanmak mümkündür. Uluslararası hukuk, kuvvetin kullanıldığı yöntemlerle ilgilenmediğinden; geleneksel, kimyasal, biyolojik veya siber silahlar olduğundan, silahlı saldırılara yanıt olarak siber saldırılara başvurmak a priori olarak mümkündür.

Buradaki güç kullanımı, saldırının arkasındaki devletin yasadışı eylemleri ve mağdur devletin buna son verme ihtiyacına ilişkindir. Literatür, meşru savunma hakkının uluslararası teamül hukuku olarak 1837'deki Caroline Olayına dayandırılmasının izini sürmektedir. Bu olay, İngiltere Büyükelçisi ve ABD Dışişleri Bakanı Daniel Webster arasındaki yazışmalarda gösterildiği gibi, Birleşik Devletler ve Birleşik Krallık arasında diplomatik bir krize yol açmıştır. İngilizlerin önleyici meşru müdafaa içinde hareket ettiklerine dair argümanına cevaben Webster, meşhur bir şekilde, egemen devletin meşru müdafaa ihtiyacının "*ani, çok kuvvetli, başka herhangi bir seçenek ve müzakere için zaman bırakmayan*"[318] bir durumda olduğunu kanıtlayabilmesi gerektiğini söylemiştir.

Bu formül, silahlı saldırı karşısında meşru müdafaa hakkının uygulanmasına yönelik yöntemlerin temellerini atacaktır. Silahlı saldırı gözlemlendikten sonra, güç kullanarak tepki vermek isteyen devlet iki şartı yerine getirmelidir: Cevabı gerekli ve orantılı olmalıdır.[319] Bunun bir zaman boyutu da vardır; silahlı saldırı devam etmeli veya yakın olmalıdır. Bu tezde, bu modaliteler siber uzay bağlamında incelenmektedir.

---

318 Daniel Webster'dan Lord Ashburton'a Mektup (27 Temmuz 1842), in Diplomatic and Official Papers Of Daniel Webster While Secretary of State 104 (New York, Harper & Brothers 1848)

319 S.Dönmez., Kuvvet Kullanma Kapsamında Ön alıcı ve Önleyici Saldırı kavramları, Balkan and Near Eastern Journal of Social Sciences, 8-15, 2017: 03 (03)

Silahlı saldırıya yanıt olarak, meşru müdafaada siber yollarla güç kullanıldığında, yukarıda ayrıntıları verilen koşullara, müdahalenin geleneksel yöntemlerle yapıldığı gibi aynı şekilde uyulması gerekir. Dolayısıyla, güç kullanımına eşdeğer nitelikteki siber operasyonlar, ancak gerekli ve orantılı olmaları halinde meşru olacaktır. Silahlı saldırıya yanıt olarak siber güç kullanımı, ancak saldırganlığa son vermeyi amaçladığı zaman, mağdur Devletin kendisini yeterince savunmasına izin veren barışçıl bir önlem yoksa veya bunlar uygulanıp başarısızlıkla sonuçlanırsa meşru olacaktır.[320]Dolayısıyla, bir devlet, güvenlik duvarları gibi pasif siber koruma önlemleriyle kendini savunabilirse veya kuvvet kullanma eşiğinin altındaki aktif tedbirleri alabilmesi yeterli olacaksa, meşru müdafaada güç kullanılması haklı değildir.

Orantılılık ilkesi gereği güç kullanımının kapsamı; süresini ve yoğunluğunu, silahlı saldırıyı sona erdirmek için gerekli olanla sınırlandırmaktadır.[321] Bu, kullanılan gücün meşru müdafaa durumuna yol açan eylemle aynı büyüklükte veya nitelikte olması gerektiği anlamına gelmemektedir. Aslında, bir Devletin kendisini saldırganlığa karşı savunmak için daha fazlasını yapması gerekebilir; ya da tam tersine, silahlı saldırganlığa son vermek için asgari düzeyde güç kullanımı yeterli olabilir. Buna ek olarak, hiçbir şey mağdur Devletin aynı yollarla yanıt vermesini gerektirmez; bir kinetik saldırıya siber yollarla yanıt vermek veya bunun tam tersi, ancak meşru müdafaa uygulamasını düzenleyen koşullara saygı duyulduğu sürece mümkündür.[322] Bazı durumlarda, Devletlerin meşru müdafaa haklarını kullanmak istediklerinde siber önlemler almaları gerekeceği düşünülebilir, çünkü bunlar

320 Y. Dienstein, **Computer Network Attacks and Self-defence**, *International Law Studies*, Vol. 76, s. 109.
321 Tallinn Kılavuzu, Kural 14'e İlişkin Yorum, §5.
322 H.H. Koh, **International law in cyberspace**, *Harvard International Law Journal*, Volume 54, 2012, s. 4.

muhtemelen “geleneksel” önlemlerden daha az zarar vererek silahlı saldırganlığa son verebilecektir.

Hukuk, soruya tamamen sabitlenmemiş olsa bile, yazarların çoğunluğu, düşmanca eylemlerin birikiminin, bağımsız olarak silahlı bir saldırı oluşturmadığını, ancak katlanmış olarak düşünüldüğünde bu eşiğe ulaşılmasının tek bir meşru müdafaa eylemine yol açabileceğini düşünüyor gibi görünmektedir.[323] Örneğin, tek başına silahlı saldırı anlamına gelmeyen çok sayıda dağıtılmış hizmet reddi saldırılarından oluşan bir siber kampanya, birlikte silahlı saldırı olarak nitelendirilebilir. Mağdur devlet, sorumlu devlete karşı tek bir siber saldırı başlatarak yanıt verebilir.

Meşru müdafaa uygulaması ayrıca, silahlı saldırının etkilerini çoktan ürettiğini veya ortaya çıkma sürecinde olduğunu varsaymaktadır. Bu nedenle, bir siber saldırı zaten silahlı bir saldırıya eşdeğer etkiler ortaya çıkardığında veya bunlar mevcut durumda konuşlandırılırken güç kullanılması meşrudur.

Saldırının yakın olma kriteri, siber saldırılar bağlamında belirli bir esneklikle yorumlanmalıdır, çünkü bir siber operasyonun mağduru olan bir Devletin, kendini savunma önlemlerini uygulamak için biraz zamana ihtiyacı olabilmektedir. Ayrıca saldırgan mantık bombası kullanırsa, hasar, operasyon başladıktan uzun süre sonra meydana gelebilecektir.[324]

Bazen bir operasyon kendi başına bir silahlı saldırı anlamına gelmemektedir, ancak muhtemelen siber operasyonlar yoluyla gelecekteki silahlı saldırılara hazırlanmayı

---

323 Y. Dienstein, supranote 343

324 M. Roscini, supranote 334, s.120

amaçlamaktadır. Bunun tipik bir örneği, bir hava saldırıları kampanyası başlatmadan önce hava trafik kontrol sistemlerini devre dışı bırakmayı amaçlayan bir siber saldırıdır.[325]

Bu durumda, bazı yazarlar (Tallin El Kitabında), üç kriter karşılandığında, erken meşru müdafaanın mümkün olduğunu savunmuştur: "S*iber operasyonun, silahlı saldırıya eşdeğer küresel bir operasyonun parçası olması; siber operasyonun, yakın ve muhtemelen kaçınılmaz bir saldırı için geri alınamaz bir adım olması; savunan devletin, son olası pencerede silahlı saldırıya erken tepki vermesi*."[326] Son olası fırsat penceresi standardı (last feasible window of opportunity standard)'na göre,[327] saldırgan açıkça saldırıyı başlatmaya kararlıysa ve mağdur devlet belli bir anda harekete geçmezse kendisini etkin bir şekilde savunma fırsatını kaybedecekse, bir devlet silahlı bir saldırıya karşı erken bir meşru müdafaa ile hareket edebilecektir. Belirleyici nokta, belirli bir zamanda harekete geçmemenin, devletin saldırı başladığında kendisini etkili bir şekilde savunamamasına yol açıp açmayacağıdır.

Erken meşru müdafaa sorunu, özellikle geleneksel yollarla güç kullanımından önce bir operasyon oluşturulduğunda, siber saldırılar bağlamında mutlaka ortaya çıkacaktır. Bir virüsün izinsiz girişi veya bir ağa sızması, silahlı saldırı ile aynı değildir. Siber saldırıya yanıt verme olasılığı, koşullara ve devletin elindeki bilgilere bağlıdır, ancak bu ilk adım, saldırının sadece bir olasılık olduğunu değil, kesin olarak gerçekleşeceğini göstermelidir.[328] Bu kriter belirleyicidir. Tallinn El Kitabı örneğini ele alacak olursak, bir sisteme mantıksal bir bombanın yerleştirilmesi, ancak etkinleştirme koşulları yerine getirilirse ve bomba

---

325 Tallinn El Kitabı, 15. Maddeye İlişkin Yorum, §1.

326Ibidem

327 George Brandis , The Right of Self-Defence Against Imminent Armed Attack In International Law, 25 **Mayıs 2017,** EJIL: Talk!, https://www.ejiltalk.org/the-right-of-self-defence-against-imminent-armed-attack-in-international-law/ E.T 15 Mart 2021

328 Y. Dienstein, supranote 334, s.111

gerçekten de hemen harekete geçirilirse, yakın bir silahlı saldırı olarak nitelendirilecektir. Öte yandan, mantık bombasının bir ağa basitçe yerleştirilmesi, sahibinin onu tetikleme olasılığını bırakması veya yakınlık koşulunu karşılamaması, bir saldırının başlatılıp başlatılmayacağına dair hala çok fazla belirsizlik barındırmaktadır. Bu nedenle mağdur devlet, kendisini ancak son olası pencerede, yani, kendisini savunamamanın gerçek bir risk oluşturduğu zaman savunabilecektir. Bununla birlikte, ayrımın pratikte uygulanması her zaman kolay değildir. Bu duruma iyi bir örnek olarak, uzmanların başlangıçta İran sanayi kompleksini gözetlemeyi amaçladıkları, yıkıcı yeteneklerinden habersiz bir yazılım olduğuna inandıkları Stuxnet verilebilir.

Buna ek olarak, bazı yazarlar, Webster formülünün, Devletlere, siber uzay çerçevesinde öngörülen meşru müdafaa için önlemler alma seçiminde çok geniş bir takdir alanı sağladığını ve bu durumun kötüye kullanım durumlarına yol açabileceğini düşünmektedir.[329] *"Ani, çok kuvvetli, başka herhangi bir seçenek ve müzakere için zaman bırakmayan*" koşullar, siber saldırıların değerlendirilmesini nesnel olarak sınırlandırmak için çok geniş bir şekilde formüle edilecektir.[330]

Düşman bir devletin siber saldırılar düzenleyebilmesi, meşru müdafaa adı altında kuvvet kullanmak için bir sebep oluşturmamaktadır. Mağdur devlet, öncelikle tehdidin gerçek bir saldırı kararına dönüştüğü sonucuna varmalıdır. Ayrıca, elindeki diğer hukuk yollarını, özellikle diplomatik olanları tüketmiş ve muhtemelen durumu Güvenlik Konseyi'ne bildirmiş olmalıdır. Siber saldırının ancak mümkün olduğu durumlarda önlem

329 T. D. Gill & P. A. L. Ducheine, Anticipatory Self-Defense in the Cyber Context. International Law Studies (Naval War College), 89, 438-471. (2013). s.454-56 https://pure.uva.nl/ws/files/1727492/135180_395103.pdf E.T 21 Ekim 2020.
330 T.D. Gill & P.A.L. Ducheine, 2013, s.443

alınması halinde, şimdiye kadar önleyici meşru müdafaa uluslararası hukukta tanınmadığından, güç kullanımının yasaklanmasına ilişkin olan kurallara aykırıdır.

Meşru müdafaanın kullanılması bir aciliyet durumuna saygı göstermelidir, yani meşru müdafaada güç kullanımı silahlı saldırganlığın hemen ardından gerçekleşmelidir. Bu kriter, misilleme önlemlerinden kaçınmayı amaçlamaktadır. Tallinn El Kitabı, art arda siber saldırı dalgaları gören "siber kampanyaları" da hesaba katmaktadır. Bir devlet, kendisini hedef alan saldırılar sona erdikten sonra, tekrarlama ihtimali varsa, meşru müdafaaya başvurabilir. Son olarak, meşru müdafaa tedbirleri, ancak silahlı saldırı devam ettiği veya daha fazla düşmanlığın geleceği kesin olduğu sürece haklıdır.

Uluslararası Adalet Divanı, Birleşmiş Milletler Şartı Madde 2 (4) ve ayrıca 51. Maddesine ilişkin olarak, Tehdit veya Nükleer Silahların Kullanımının Yasallığına ilişkin görüşünde "bu hükümlerin belirli silahlardan bahsetmediğini" beyan etmiştir. Kullanılan silahlardan bağımsız olarak her türlü güç kullanımına uygulanır. Bu tipik tepki güç yasağı kurallarını ihlal etmediği sürece, hiçbir şey bir devletin silahlı bir saldırıya yanıt olarak siber araçları kullanmasını engelleyemez. Ayrıca, siber yollarla yapılan bir yanıtın, geleneksel yollarla gerçekleştirilen bir saldırıdan potansiyel olarak daha az yıkıcı olduğu da tartışılabilir. Bu argüman tersine çevrilebilir ve siber yollarla güç kullanımı daha felaket olabilir; ancak bu durumda, yukarıda tartışılan meşru savunmaların yasallık gerekliliklerini karşılamayacaktır.

3. Birleşmiş Milletler Güvenlik Konseyi ve Siber Düşmanlık Eylemleri

"*Barışa yönelik tehditler, barışın ihlali ve saldırganlık eylemleri durumunda*" uluslararası toplumun eylemlerine ilişkin VII. Bölüm, üç aşamalı bir prosedür öngörmektedir.

Birinci aşamaya göre, Güvenlik Konseyi, barışa yönelik bir tehdit, barışın ihlali veya bir saldırı eyleminin varlığını tespit eder ve gerekirse geçici önlemler alır (Madde 39 ve 40). Schmitt'e göre, eğer sibernetik saldırı bir silahlı kuvvet kullanımı içermekte ise (yani, bu âlime göre, bu eylem doğrudan mülkün veya kişilerin fiziksel olarak yok edilmesini hedefliyorsa), güvenlik Konseyi, bu üç durumdan biri varlığını bulmakta haklı olacaktır.[331] Ancak, kanıtlanmış güç kullanımının yokluğunda bile, Konsey bu siber saldırıyı barışa bir tehdit olarak görebilecektir.[332]

İkinci aşamada, Şart'ın 41. maddesinde belirtildiği üzere: *"Güvenlik Konseyi, kararlarını yürütmek için silahlı kuvvet kullanımını içermeyen ne gibi önlemler alınması gerektiğini kararlaştırabilir ve Bileşmiş Milletler üyelerini bu önlemleri uygulamaya çağırabilir. Bu önlemler, ekonomik ilişkilerin ve demiryolu, deniz, hava, posta, telgraf, radyo ve diğer iletişim ve ulaştırma araçlarının tümüyle ya da bir bölümüyle kesintiye uğratılmasını, diplomatik ilişkilerin kesilmesini içerebilir." "Diğer iletişim araçları"* na yapılan atıf, şüphesiz İnternet ağını içerebilir ve uluslararası toplum tarafından kapsanan olası bir bilgisayar, "abluka" nın yolunu açıyor gibi görünmektedir.[333] Bununla birlikte, 41. maddede belirtilen yöntemler burada büyük ölçüde yanıltıcı görünmektedir; bu bağlamda bir Devletin yapabildiği kadarıyla, maddi olmayan ve küreselleşmiş bir ağı "kesintiye uğratamadığı" müddetçe, 39. maddede sayılan eylemlerden birinden suçlu olan Devlete karşı deniz veya hava haberleşmesini kesintiye uğratabilecektir. Bununla birlikte bu hüküm, bazı uzmanlara göre ölümcül veya yıkıcı sonuçları olmayan ve devlet topraklarının işgaline yol açmayan tedbirler anlamına gelen "silahlı kuvvet kullanımını içermeyen" siber

331 M.N. Schmitt/BT O'Donnell (eds), *Computer Network Attacks and international Law,* 2002, supranote 339, s.935. (Saldırganlığa ve barış tehdidine atıflar, Rusya, Çin ve iki müttefiki tarafından 2011 yılında önerilen bilgi güvenliği hakkında uluslararası davranış kuralları taslağında bulunmaktadır.)
332 Ibid.
333 N. Melzer, 2011, supranote 321, s. 19.

önlemlere kapıyı tamamen kapatmamaktadır;[334] ancak 2008'deki Rus-Gürcü çatışması örneği, bir devletin bilgisayar sisteminin herhangi bir nötralizasyonunun veya ele geçirilmesinin zorunlu olarak bir düzeyde "yıkımı" içerdiğini kanıtlamaktadır.

Son aşama, bunu Şart'ın 42. maddesinde bulmaktadır: *"Güvenlik Konseyi, 41. maddede 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 bulunabilecektir. Bu girişimler gösterileri, ablukayı ve Birleşmiş Milletler üyelerinin hava, deniz ya da kara kuvvetlerince yapılacak başka operasyonları içerebilecektir."* Yine burada, Güvenlik Konseyi'nin tepkisinin fazlasıyla "fiziksel" boyutu, "diğer operasyonlara" atıfta bulunulması, bu önlemlerin "Birleşmiş Milletler Üyelerinin kuvvetleri hava, deniz veya kara yoluyla gerçekleştirilmesi" koşuluyla, bu olasılığı tamamen dışlamasa bile, siber önlemlere başvurmayı dışlıyor gibi görünmektedir. Yine bu bağlamda, bazı hukukçular bu nedenle Şart'ın 42. maddesinin uluslararası toplumun siber uzaya müdahalesini dışlamadığını düşünmüşlerdir.[335]

Gerçek şu ki, beş Devletin daimi üye olarak yer aldığı Güvenlik Konseyi'ndeki yavaşlık ve elverişsiz karar alma süreci, inkâr etmelerine rağmen, siber saldırıların en büyük aktörleri arasında yer alırken; Konseyin tepkisini BM Şartı'nın VII. Bölümü temelinde çok varsayımsal kılmaktadır.[336]

---

334 G. Grove, S. Goodman & S. Lukasik Cyber-attacks and international law, Survival, 42:3, 89-104, (2000), s.93. https://www.tandfonline.com/doi/abs/10.1093/survival/42.3.89?journalCode=tsur20 E.T 27 Ekim 2020.

335 N. Melzer, 2011, supranote 321, s. 19.

336 T. C. Huntley**, Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare,** 60 Naval L. Rev. 1 (2010), s. 27. this author criticizes the approach by M.

4. Siber Karşı önlemler

Gördüğümüz gibi, meşru müdafaaya başvurmak kesinlikle mümkündür, ancak çok sınırlıdır. Buna ek olarak, siber operasyonların gerçekleştirilme hızı ile bir Devletin, saldırının kaynağını belirlemek ve bunu bir Devlete atfetmek için ihtiyaç duyduğu kaynaklar göz önüne alındığı zaman, bu durum, siber uzay için uygun olmayabilir. Son olarak, bugüne kadar hiçbir siber saldırının silahlı saldırı olarak sınıflandırılmamış olması, bunların çoğunun yanıt olarak silahlı kuvvete başvurmak için gerekli şiddet eşiğine ulaşmadığını göstermektedir. Bununla birlikte, siber saldırıların mağduru bir devletin başka çözümleri olmadığını hayal etmek zordur. Bu nedenle, uluslararası hukukun bu düşük yoğunluklu siber saldırılara verdiği tepkiler analiz edilmelidir.

Uluslararası hukukta, bir uluslararası hukuka aykırı fiilin mağduru olan bir Devletin, karşı önlemlere başvurabileceği kabul edilmektedir.[337]

Karşı önlemler, başka bir devletin uluslararası hukuk kapsamındaki yükümlülüklerine uygun hale getirmek için işlediği hukuka aykırı bir fiile yanıt olarak alınan güç kullanımını içermeyen fiillerdir. Bu fiiller normalde hukuk dışıdır, ancak mağdur devlet, başka bir devletin yasadışı davranışına son vermek için bunları kullanma hakkına sahiptir. Bu bağlamda, karşı önlemler, düşmanca olmakla birlikte her koşulda yasal olan sözde misilleme önlemlerinden farklıdır.

Schmitt with regard to Chapter VII of the Charter. https://heinonline.org/HOL/LandingPage?handle=hein.journals/naval60&div=4&id=&page= E.T 27 Ekim 2020.

337 Schachter, Oscar, "Dispute Settlement and Countermeasures in the International Law Commission." *The American Journal of International Law*, vol. 88, no. 3, 1994, s. 471–477. *JSTOR*, www.jstor.org/stable/2203714 E.T 19 Mart 2021.

Hukuka uygun olmak için, karşı önlemlerin belirli koşulları karşılaması gerekir: Bir Devletin bir uluslararası hukuka aykırı fiil gerçekleştirmesine yanıt olarak alınmalı ve belirli sınırlamalara saygı gösterilmelidir.

Karşı önlemler, ilk olarak uluslararası hukuka göre hukuka aykırı olan fiillerdir, ancak kendisi de hukuka aykırı olan uluslararası bir fiilin işlenmesine son vermeyi amaçladıklarında hukuka aykırılıkları ortadan kaldırılmaktadır. Bir fiilin uluslararası hukuka göre haksız olması için, bir Devlete atfedilebilir olması ve ister bir antlaşmadan ister uluslararası teamül hukukundan kaynaklansın, o Devletin uluslararası bir yükümlülüğünün ihlalini teşkil etmesi gerekir. Özellikle bunlar, yukarıda görüldüğü gibi müdahale etmeme ilkesini ihlal eden işlemler olabilmektedir. Örneğin casusluk, uluslararası hukuk açısından yasadışı olmadığı için devlete karşı önlemler alma hakkı verilmemektedir.

Güç kullanımı, silahlı saldırının eşiğine ulaşsın ya da ulaşmasın, aynı zamanda açıkça haksız bir uluslararası eylemdir; keza, bir devletin egemenliğini ihlal eden bir fiil veya bir devletin bakım görevini yerine getirmemesi de böyledir.

Karşı önlemler belirli sınırlamalara tabidir. Her şeyden önce, devletin uluslararası hukuk kapsamındaki yükümlülüklerini ihlal eden haksız davranışına son vermek amacıyla ele alınmalıdır. Doğası gereği cezalandırıcı olmamalıdır ve ilke olarak, hukuka aykırı davranış sona erdiyse kullanılamayacaktır. Ayrıca statükoya dönmeyi mümkün kılmalı ve bu nedenle prensipte tersine çevrilebilir olmalıdır. Devletin sorumluluğu hakkındaki taslak maddelerin 50. Maddesi aynı zamanda belirli temel kurallara, özellikle de temel insan haklarını koruyan kurallara, insancıl hukuk kurallarına ve uluslararası hukukun emredici normuna (jus cogens) karşı gelemeyeceklerini belirtmektedir. Son olarak, bir Devleti,

diplomatik ajanlarla ilgili uyuşmazlıkların barışçıl çözümüne ilişkin yükümlülüklerinden veya kurallarından muaf tutamamaktadırlar.

Karşı önlemlerin bir orantılılık koşulunu karşılaması gerektiği genel olarak teamül hukukunda kabul edilmektedir. Bu, 51. maddede "*Karşı tedbirler, uluslararası haksız fiilin ciddiyeti ve söz konusu haklar dikkate alınarak, uğranılan zararla orantılı olacaktır."* [338]Şeklindeki Devlet sorumluluğu taslak maddelerinde yankılanmaktadır. Usule ilişkin olanlar da dâhil olmak üzere, uluslararası hukuka aykırı fiiller için Devletin sorumluluğu hakkındaki taslak maddelerde başka koşullar belirtilmiştir. Uluslararası hukuka aykırı fiilin mağduru olan Devlet, bunu yapan Devletten buna bir son vermesini ve yükümlülüklerine uymasını istemelidir. Bu yetersizse, karşı önlemler alma niyetini belli etmelidir.

Tallinn El Kitabını hazırlayanlar, bir devletin, kendisine borçlu olunan uluslararası *bir yükümlülüğün başka bir devlet tarafından ihlal edilmesine cevaben, siber ile ilgili olsun ya da olmasın karşı önlemler alabileceği* konusunda da hemfikirdir.[339] Ancak, karşı önlemlerin yalnızca bir devlete karşı alınabileceği vurgulanmaktadır. Karşı önlemler, fiillerinin bir duruma atfedilebildiği durumlar dışında, devlet dışı bir aktöre karşı olası bir yanıt olarak kabul edilmemektedir. Bununla birlikte, bu fiiller, özellikle mağdur Devletin iç hukukuna göre, kesinlikle hukuka uygun değildir.

Siber uzaydaki karşı önlemler aslında ne oluşturabilir? Devletlerin kendilerini siber saldırılardan korumak için güvenlik duvarları gibi pasif savunmalara sahip oldukları kabul edilmektedir. Bir Devlet bir siber operasyonun mağduruysa, karşı önlem rejimi altında sözde "aktif" savunmaları uygulamaya yetkili olabilecektir. Bu savunmalar, saldırının başlangıcındaki devleti, davranışına son vermeye teşvik etmek için saldırıların failini

338 BM sozlesmeler, 51.md
339 Tallinn Kılavuzu 2.0., Kural 20

kullanımdan çıkarmayı veya karşılıklı saldırıları uygun şekilde gerçekleştirmeyi amaçlamaktadır.[340] Daha sert bir şekilde, bir siber saldırının mağduru olan bir devlet, siber saldırılar sona erene kadar sunucularına ve bilgisayar sistemlerine erişimi kesebilmektedir.

Bununla birlikte, siber uzayda karşı önlemlerin kullanılmasının önünde hala birçok engel vardır. İlk olarak, etkili olabilmesi için, karşı önlemin yasadışı eylemi başlatan devletin üzerinde yeterli baskı oluşturması gerekir. Bununla birlikte, siber bağlamda, bir karşı önlemle hedef alındığını bilen bir Devlet için, özellikle mağdur Devlet karşı önlemlere başvurma konusundaki dikkatini açıklarsa, kendisini korumak için önlemler alması çok kolaydır. Ek olarak, siber karşı önlemler, uluslararası haksız bir fiilde bulunanlar dışındaki devletleri etkileme riskini de beraberinde getirmiştir. Örneğin, amacı bilgisayar sistemlerini ve ağları devre dışı bırakmak olan bir karşı önlem, hiçbir şekilde sorumlu olmayan aktörleri etkileme ve böylece Devleti her şeyden önce bir mağdur ve nihayetinde üçüncü bir Devlete ilişkin yasadışı bir uluslararası fiilden sorumlu kılma riski taşımaktadr.[341] Son olarak, karşı önlemlere uygulanabilen rejimle ilgili önemli bir sorun, bunların ancak bir Devletin haksız bir uluslararası fiilde bulunması halinde kabul edilebilmesidir; bu nedenle, devlet dışı grupların neden olduğu eylemlere yanıt vermemektedirler ve uluslararası haksız fiili bir devlete atfetme yeteneğini varsaymaktadırlar.

Devlet dışı bir grup tarafından gerçekleştirilen bir siber saldırının mağduru bir Devlet yine de elinde başka olasılıklara sahiptir; bu olasılıklar, ilgili saldırılar bir silahlı saldırının eşiğine ulaştığında meşru müdafaa hakkının kullanılması veya zorunluluk halinin çağrılmasıdır. Nitekim bir Devletin, bir grup aktivist, bir şirket veya terörist gibi Devlet dışı

340 O.A. Hathaway & R. Crootof, "The Law of Cyber-Attack", *California Law Review*, *Vol. 100*, 2012, s. 858
341 O.A. Hathaway & R. Crootof, supranote 374, s. 859.

bir aktörün eylemi olan ve yukarıda açıklanan ciddiyet eşiğine ulaşan bir siber operasyonun kurbanı olması, bir seçenek teşkil etmektedir. Bununla birlikte, gereklilik durumunun istisnai operasyonlarla sınırlı olduğu ve siber saldırılara karşı bir savunma "stratejisi" olarak kabul edilemeyeceği bir gerçektir.[342] Ayrıca, gereklilik haline dayalı eylemler, bir devletin mağduru olduğu eylemleri atfetme zorunluluğunu ortadan kaldırdığı için, istismara uğrama riskini de beraberinde getirmektedir.

C. GENEL DEĞERLENDİRME

Farklı aktörler arasında yeni bir etkileşim alanı olarak siber uzay, aynı zamanda bir diplomasi, yüzleşme ve savaş alanıdır. Hava, uzay, deniz ve hatta kara gibi klasik mekânlarla karşılaştırılabilir ve üst üste bindirilir. Siber teknolojilerin kullanımıyla siber uzayda operasyonlar yürütmek, uluslararası sistemde oldukça yeni bir uygulama olsa da, devletler ve askeri alan yine de bu alana hızla girmiştir.

Siber uzayda, aktörlerin gücü yansıtma şekli geleneksel alanlara kıyasla daha farklıdır. Daha önce de gördüğümüz gibi, siber uzay oldukça erişilebilirdir ve eylem ve saldırı araçları etkili olmakla birlikte ucuzdur. Diğer alanlarda olduğu gibi, temel altyapının (elektrik şebekeleri, su dağıtımı vb.) korunması ve Devlet ve askeri hizmetlerin sürekliliği meşru bir egemenlik sorunu olduğu takdirde, bu konu, siber uzayda genişletilmiş güvenlik sorunuyla örtüşür. Böylece egemenlik, Devletin ve aynı zamanda ekonomik sektörlerin ve İnternetin işleyişine izin veren fiziksel ve elektronik altyapılar düzeyinde bulunabilmektedir. Bu yelpazeyi, endüstriyel casusluğa veya diğer Devletlerin diplomatik veya sivil haberleşmelerin kitlesel casusluğuna karşı korumak için genişletmek mümkün olacaktır.

342 R. Geiss & H. Lahmann, 2013, supranote 214, s. 645.

Genel olarak İnternet ve siber uzay teknolojilerinin anlıklığı, ilgili çeşitli aktörleri bir saldırı veya bilgisayar korsanlığı durumunda yanıtlarını ve yanıt stratejilerini değiştirmeye zorlamaktadır. Aslında, siber uzayın işleyiş hızı önemli bir unsurdur, çünkü bir saldırı yalnızca birkaç dakika gerçekleştirilse bile feci sonuçlara yol açabilir ve kendini korumak veya yanıt vermek için çok az zaman bırakır.[343] Bu anlıklık, saldırıların kökenini hedeflemenin ve bunlara yeterince hızlı yanıt vermenin zor olduğu bir alanda angajman kuralları hakkında sorular da ortaya çıkarmaktadır. Siber uzayın son derece gözenekli olduğu gerçeği, yalnızca hedefler ve yan yana olan mağdurlar arasında farklılaşma sorunları yaratmakla kalmaz, aynı zamanda bilgi savaşı ile geleneksel savaş arasındaki kavşak noktalarına saldırılar (ve daha ziyade siber savaş) da yapar. Bu saldırılar, askeri veya sivil faaliyetlerin geri kalanını etkilerken, öncelikle teknolojik ağları ve bilgi ağlarını hedef alan bir alanda gerçekleşecektir.

Siber çatışma ve konvansiyonel savaş arasındaki farklar dikkat çekicidir ve kullanılan 'silahlarda' var olan bariz farklılıkların çok ötesine geçmektedir. Bu bölümde ileri sürülen argümanları özetlemek gerekirse, ilk ayrım, olası misilleme veya karşı önlemlerin hedefi hakkında belirsizlik yaratan siber saldırıların faillerini kesin olarak tespit etmenin, başka bir deyişle bu önlemlerin meşru olarak kimleri vurabileceğinin belirlenmesinin zor olmasıdır. İkinci ayrım, ağların ve dijital sistemlerin her yerde bulunması ve karşılıklı bağımlılığı nedeniyle, elektronik karşı önlemlerin sonuçlarını tahmin etmenin imkânsızlığı ve sonuç olarak, bu tür karşı önlemlerin artan etkisini ölçmenin zorluğudur. Üçüncü ayrım, bir siber çatışmanın koordineli bir saldırı olabilmesi ve bu nedenle yıkıcı olabilmesi veya

343 F. D. Kramer., S. H. Starr and L. K. Wentz., **Cyberpower and National Security**, Washington, D C: Center for Technology and National Security Policy; National Defense University Press: Potomac Books, 2009, s. 267.

çeşitli derecelerde altyapıların önemli ölçüde parçalanmasına yol açabilen sınırlı kapsamda tekrarlanan tehditlerin (siber casusluk, tanınmayan botnetlerin oluşturulması vb.) tehlikeli biçimini alabilmesidir. Dördüncü ayrıma göre, Devletlerarasında bir çatışma olması durumunda, olası aktörlerin sayısı sonsuzdur; Son olarak, daha önce de vurgulandığı gibi, işleyen bir küresel bilgi altyapısını sürdürmek herkesin çıkarınadır.

Mevcut uluslararası yasal standartlar ve araçlar, ortaya çıkan siber güvenlik zorluklarıyla başa çıkmak için ideal olarak uygun olmadığından, bugün küresel tartışmalara ve işbirliğine ihtiyaç vardır. Ulusal yetki alanları, BİT'ler, kaynaklar ve çevrimiçi sistemler arasındaki artan örtüşmeyle birlikte teknolojinin evrimi, siber uzayda barışın sürdürülmesini garanti altına almak için yeni bir dizi stratejinin benimsenmesini ve uluslararası işbirliğinin uygulanmasını daha da önemli hale getirmektedir.

Siber saldırılar dünyanın herhangi bir yerinde başlatılabilir ve herhangi bir ülkeyi vurabilir; Bu nedenle bu tehditler, doğaları gereği uluslararası bir boyuta sahiptir ve uluslararası işbirliği, soruşturmada yardım ve bunlarla başa çıkmak için ortak maddi ve usul düzenlemelerinin benimsenmesini gerektirmektedir. Dahası, uluslararası işbirliğinin küresel siber güvenlik için temel koşullardan biri olduğu yaygın olarak kabul edilmektedir. Bu uluslararası işbirliğini sadece karşılıklı barış arzusu değil, aynı zamanda her ülkenin iyi anlaşılmış çıkarları izlemelidir. Günümüzde ticaret, finansal operasyonlar, sağlık hizmetleri, acil servisler, gıda dağıtımı için teknolojiye her zamankinden daha fazla bel bağlayan her ülkede, hayati ağların kaybı herkesi çabucak sakatlayacak ve hiç kimse bir siber saldırıya karşı güvende olmayacaktır. BİT'in üstünlüğü ve yeni teknolojilerin birbirine bağlanabilirliği, istikrarı sağlamak için bu yeni konularda işbirliğini haklı çıkaran yeni bir dünya düzeninin habercisidir.

Bir Devlet, kendi topraklarında bulunan bilgi sistemleri üzerinde egemenliğini kullanır ve bu egemenliği korumak için gerekli araçları uygular. Sistemlerine yönelik bir dizi güvenlik ve savunma önlemine ek olarak, mağduru olduğu herhangi bir siber saldırıya yanıt verme hakkını saklı tutar. Bu tanımlama, egemen ayrıcalıklarının kullanılmasında bir fırsat olarak karar verilen bir kamu atfına neden olabilmektedir. Devlet ortakları veya uluslararası kuruluşlarla bağlantılı olarak toplu bir atıfta bulunup bulunmayacağına karar vermek, Devletin kendi egemenliğine kalmıştır. Müdahale kararı siyasaldır ve uluslararası hukuka uygun olarak yürütülmektedir. Bu yanıt, siber saldırının ciddiyetine bağlı olarak güç kullanımına kadar gidebilmektedir. Devlet kökeninin devlet sistemlerine izinsiz girmesi veya bir dijital vektör tarafından bir devlet toprakları üzerinde herhangi bir etkinin üretilmesi, asgari olarak, egemenlik ihlali teşkil edebilmektedir. Buna, Birleşmiş Milletler Şartı'nın 2. maddesinin 4. fıkrasının anlamı dâhilinde silahlı güce başvurmayı oluşturan etkiler eşlik ediyorsa, bir devlet karşı önlemler alabilir veya konuyu Güvenlik Konseyi'ne sunabilecektir. Dahası, bir siber saldırının, Birleşmiş Milletler Şartı'nın 51. Maddesi uyarınca devletin meşru müdafaa yoluyla yanıt verebileceği silahlı saldırı eşiğine ulaşabileceği de göz ardı edilmemelidir. Yukarıda da bahsedildiği gibi, ihlal eşiğinin niteliği, uluslararası hukuk tarafından belirlenen kriterler ışığında, vaka bazında formüle edilen siyasi bir karardan kaynaklanmaktadır. Cumhurbaşkanı, Başbakan, silahlı kuvvetlerin başı veya yetkili herhangi bir devlet görevlisi; nihayetinde, uluslararası hukuk tarafından yetkilendirilenler yelpazesi içinde, özellikle de izinsiz girişe ve elebaşı niteliğine bağlı olarak, en uygun tepkiyi belirleyecektir.[344]

344 Örneğin, Fransa'da, saldırının ciddiyetine bağlı olarak Cumhurbaşkanı veya Silahlı Kuvvetler Başkanı silahlı bir müdahaleye izin verebilir. (4 Ekim 1958 Anayasasının 15. Maddesi). Türkiye ise, bu karar Türkiye Büyük Millet Meclisi alabılır (Anayasa, md. 92).

Siber uzayın gözenekliliği ve ona kuvvet uygulama kolaylığı, bazı aktörlerin siber savunma stratejileri benimsemeye başlamasına neden olmuştur. Bu stratejiler özellikle siber uzaydaki devleti, askeri ve sivil ağları korumayı amaçlamaktadır; bu durum, güvenlik açıklarını sınırlamak ve bu alanda gerçekleşen faaliyetlerin kesintiye uğramasına karşı korunmakla ilgilidir. Gözlemlenmesi ve analiz edilmesi en kolay siber savunma stratejileri, çoğunlukla kamuya açık oldukları için Devletler tarafından öne sürülen stratejilerdir. Özel şirketler veya uluslararası kuruluşlar gibi diğer aktörler de e-stratejiler uygulamıştır. Bununla birlikte, bu stratejileri değerlendirmek daha zordur, çünkü genellikle kamuya açık değildirler ve bu aktörler kurban oldukları saldırılarla ilgili nadiren bilgi yayınlarlar; bunun nedeni siber savunma stratejilerini benimsememeleri veya gizli kalması gereken unsurlar olduğunu düşünmeleri olabilir.

Büyük siber saldırıların neden olabileceği zararın boyutunu gerçekten ölçmek için siber savaşa bakmak gerekir. Siber savaş, gerçekten de siber saldırıların en gelişmiş ve tehlikeli biçimidir ve tüm insan faaliyetlerinin önemli ölçüde kesintiye uğramasına ve altyapının ve BT sistemlerinin büyük ölçüde yıkılmasına yol açabilmektedir. Bu nedenle, biz, bu konuyla ilgili daha fazla ayrıntıya yer verilecek olan bu tezin üçüncü bölümünde siber uzay ve uluslararası insancıl hukuk arasındaki sinerjiye odaklanmayı tercih etmiş bulunmaktayız.

ÜÇÜNCÜ BÖLÜM

ULUSLARARASI İNSANCIL HUKUKU SİBER UZAYA UYGULAMANIN ZORLUĞU

"Savaş hukuku" veya "Silahlı Çatışmalar Hukuku" olarak da adlandırılan Uluslararası İnsancıl Hukuk, ister ulusal ister uluslararası olsun, silahlı çatışmaların etkilerini sınırlandırmayı mümkün kılan bir kurallar bütünüdür. Bu uluslararası kurallar dizisi, geleneksel veya göreneksel bir kökene sahiptir. 1949 tarihli dört Cenevre Sözleşmesi ve bunların 1977 tarihli Ek Protokolleri, bu silahlı çatışmalara uygulanabilecek başlıca anlaşmalardır. Uluslararası insancıl hukuk, yalnızca, doğal olarak kara, deniz, uzay veya bu üçünü de içeren bir savaş alanı tarafından coğrafi olarak sınırlandırılmış silahlı çatışma durumlarında geçerlidir. Savaşanların düşmanlıklarını yönetmekle beraber, aynı zamanda düşmanın eline geçenlerin korunmasını ve bakımını da yönetmektedir. Bu hukuk, savaşa hiç katılmamış veya artık katılmayan kişileri korumakta ve savaş araç ve yöntemlerini kısıtlamaktadır.

Siber savaş kavramı uluslararası hukukta açıkça tanımlanmamıştır. Şu anda, Şangay İşbirliği Örgütü tarafından kurulan geleneksel düzenin yalnızca bir tanımı vardır.

Şanghay İşbirliği Örgütü, *"bilgi sistemlerine, süreçlere ve kaynaklara, kritik ve diğer yapılara zarar vermeyi, siyasi, ekonomik ve sosyal sistemleri baltalamayı, toplumu ve devleti istikrarsızlaştırmanın yanı sıra devleti karşı tarafın çıkarına kararlar almaya zorlamak için psikolojik beyin yıkamayı amaçlayan bilgi alanında iki veya daha fazla Devlet arasında bir çatışma*" [345]olarak tanımlanan daha geniş bir bilgi savaşı kavramı oluşturmuştur.

Bununla birlikte, "bilgi savaşı" terimleri çeşitli şekillerde kullanılmaktadır. Deniz Harp Okulu Uluslararası Hukuk Bölümü Dekanı Prof. Michael Schmitt'e göre, "*bilgi savaşı*

345 Uluslararası Bilgi Güvenliğinin Sağlanması Alanında İşbirliğine İlişkin ŞİÖ Üye Devletleri Hükümetleri Arasındaki Anlaşma (Yekaterinburg, 16 Haziran 2009) NATO CCDCOE tarafından resmi olmayan tercümesi, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf E.T 25 Nisan 2021.

yalnızca silahlı çatışma zamanlarında gerçekleştirilen bilgisayar operasyonlarıyla ilgilidir ve barış zamanında gerçekleştirilenlerin tümünü hariç tutmaktadır".[346]

ICRC'ye göre, "hukuki açıdan, uluslararası olmayan bir silahlı çatışma, uluslararası bir silahlı çatışmaya dönüşebilmekte, hatta bunun tam tersi de olabilmektedir. Başka bir silahlı çatışma türü bulunmamaktadır.[347]

Sonuç olarak, burada siber savaş olarak incelenecek olan bilgi savaşı kavramı, uluslararası insancıl hukuk anlamındaki silahlı çatışmalara ayrılmıştır. Dolayısıyla silahlı çatışma oluşturmayan siber saldırıların oluşturduğu güvenlik tehditleri, sadece siber suçları oluşturmaktadır.

I. ULUSLARARASI İNSANCİL HUKUKUN SİBER UZAYA UYGULANABİLİRLİĞİ

İki veya daha fazla Devlet arasında düşmanlık oluşturan siber operasyonlar, uluslararası bir silahlı çatışmanın (IAC) varlığını karakterize edebilmektedir. Aynı şekilde, bir devletin silahlı kuvvetlerini bir veya daha fazla silahlı grubun kuvvetlerine veya kendi aralarında birkaç silahlı gruba karşı çıkan uzun süreli siber operasyonlar, bu grupların asgari bir örgütlenme sergilemesi ve etkilerinin yeterli şiddet derecesine ulaşması koşuluyla uluslararası olmayan bir silahlı çatışma (NIAC) oluşturabilir.

Bunlar genellikle konvansiyonel askeri operasyonlarla eş zamanlı olan askeri operasyonlardır, dolayısıyla durumu silahlı çatışma olarak nitelendirmekte herhangi bir sakınca bulunmamaktadır. Yalnızca dijital faaliyetlerden oluşan bir silahlı çatışma hipotezi ilke olarak göz ardı edilemezken, yine de bu hipotez, özerk siber operasyonların böyle bir nitelik için gereken şiddet eşiğine ulaşma yeteneğine dayanmaktadır.

346 Schmitt, Michael N., 'Classification of cyber conflict', in *Journal of Conflict and Security Law*, Vol. 17, Issue 2, Summer 2012, s. 252
347 ICRC, "How is the term armed conflict defined in IHL?", Position paper 2008, s.1

Kaydileştirilmiş olmasına rağmen, siber operasyonlar, etkilerinin IAC'ye Taraf Devletlerin topraklarında ve NIAC'ta düşmanlıkların gerçekleştiği bölgede meydana gelmesi gerektiği sürece, IHL'nin coğrafi kapsamına tabi kalmaktadır.

Silahlı çatışma bağlamında silahlı kuvvetlerin angajmanına yönelik siber operasyonlar IHL'ye tabidir. Devletlerarasında bir çatışma oluşturan bir siber operasyon, bir IAC'nin varlığını karakterize edebilmektedir. Teknolojinin durumu şu anda siber operasyonların tek başına bir NIAC durumunu karakterize etmek için gereken şiddet eşiğine ulaşmasını engelliyor gibi görünmektedir.

A. ULUSLARARASI SİLAHLI ÇATIŞMA DURUMU

911, uluslararası gündemde siber yetenekler için çok az yer bıraktıysa da, artan kullanımları tartışmayı yeniden canlandırdı ve 2013'te Birleşmiş Milletler'de, ICRC'de, NATO tarafından düzenlenen ve 2017'de yeniden yayınlanan Tallinn El Kitabında veya ABD, Rus, Çin, Fransız ve İngiliz ulusal politika belgelerinde olduğu gibi birçok düşüncenin kaynağında yer almaktadır. Bununla birlikte, yansımalar, yasal bir kavrama tekabül etmeyen heterojen fenomenlere atıfta bulunan tanımlar sağlamaktadır. Bu nedenle, H. Lin'in terminolojisini kullanacak olursak, “siber saldırılar” ile “siber sömürü” arasında ayrım yapmamız gerekecektir. İlki, sistemi yeniden programlamak, kullanılamaz hale getirmek veya yok etmek için sistemin bütünlüğünü hedeflemekte, ikincisi ise uluslararası hukukta yasaklanmayan casusluğa benzemektedir.[348]

348 Herbert S. Lin, Offensive Cyber Operations and the Use of Force, JOURNAL OF NATIONAL SECURITY LAW & POLICY [Sayı. 4:63], s.63-86, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf E.T 8 Mayıs 2021

Bu ikilikten, yalnızca "siber saldırılar" potansiyel olarak insancıl hukukun ilgisini çekebilir ve ona meydan okuyabilir. Ancak, bu kategori jus in bello'nun yasal çerçevesini yansıtmayacak ve bu nedenle hepsi onun kapsamına giremeyecektir. Bu uygulama zorluğu, ana düşünce organları tarafından seçilen benzetme yoluyla yorumlama kuralından kaynaklanmaktadır (1). Ancak nadir durumlarda uygulanabilmeleri başlı başına bir son değildir. Gerçekten de, insancıl hukuk ilkeleri çağdaş gerçekleri yansıtmalıdır. Ancak analoji mantığı onları sibernetik araçların özgüllükleri karşısında yetersizlik durumuna sokmaktadır (2).

1. Uluslararası İnsancıl Hukukun Analoji Yoluyla Zor Uygulanması

Uluslararası güvenlik bağlamında telekomünikasyonun ilerlemesini incelemekle görevli Birleşmiş Milletler Hükümetler Arası Uzmanlar Grubu, 2015 yılında yeniden teyit edilen ilgili konu hakkında, 2013 yılında şu sonuca varmıştır: *"Uluslararası hukuk ve özellikle Birleşmiş Milletler Şartı,"*[349] *uygulanabilir olduğu durumlarda insanlık, gereklilik, orantılılık ve ayrım ilkeleri*[350] *dâhil olmak üzere uluslararası hukukun tanınmış ilkelerinin yanı sıra siber uzaya da uygulanabilmektedir."* Bunlar, insancıl hukukun temel ilkelerine tekabül etmektedir ve bu sonuç, "geleceğin […]dir.[351]

Ancak M.N. Schmitt'e göre, uluslararası kamu hukuku ve bileşenlerinin siber uzaya uygulanabilirliği konusunda çok az şüphe vardı, ancak bu grup, jus in bello yasasının ne zaman ve nasıl siber uzaya ve siber saldırılara uygulanacağı sorusuna cevap

349 Uluslararası Güvenlik Bağlamında Telekomünikasyonun İlerlemesini İncelemek için Hükümet Uzmanları Grubu Raporu, A / 68/98, 24 Haziran 2013, paragraf 19.
350 Uluslararası Güvenlik Bağlamında Telekomünikasyonun Gelişimini Gözden Geçirecek Hükümet Uzmanları Grubu Raporu, A / 70/174, 22 Temmuz 2015, para. 28.
351 M. N. SCHMITT, "The Law of Cyber Warfare: *Quo Vadis?*" in *Stanford Law & Policy Review*, vol. 5, no. 2, 2014, s. 271.

vermemektedir.[352]Bu yanıt eksikliği, ister devletler isterse özel gruplar tarafından saldırgan siber yeteneklerin kullanımı arttıkça belirsizlikler bırakmaktadır. Cevaplar, geçmişte insancıl hukukun uyarlanabilirlik gösterdiği yeni savaş araçlarına ve yöntemlerine uyum sağlamak için kullanılan analojiye dayanmaktadır.[353] Bununla birlikte, çerçevelenen fenomen önceki zorluklarla doğası gereği çelişkili olduğunda, analoji kolay değildir.

Bu nedenle, insancıl hukukun siber uzaya ve sibernetik araçlara uyarlanabilirliği ile ilgili soruları cevaplamak için önce uygulanabilirliği göz önünde bulundurulmalıdır. *Jus in bello,* silahlı çatışmalar için geçerlidir. Peki, siber uzayda saldırgan sibernetik araçların kullanılması bir siber savaşa yol açabilir mi (a)? Kısacası bu durum, yeni bir savaş alanında yeni bir tür silahlı çatışma mıdır?

İnsancıl hukuk, silahlı çatışmalarda aktörlerine ve kullanılan araç ve yöntemlere uygulanır. Ancak sibernetik araçların kullanımını düzenlemeye gelebilmek için bunun bir "saldırı" olarak nitelendirilmesi gerekmektedir. Ancak bu kavramı benzetme yoluyla siber saldırılara uygulamak yetersizdir ve bu durum, insancıl hukukun özüyle çelişmektedir (b).

a. Yeni Bir Savaş Alanında Yeni Bir Silahlı Çatışma Olarak "Siber Savaş"

Birbirine bağlı bir dünyanın yeni bir boyutu olan bu alan, devletlere meydan okumakta ve özellikle geleneksel güç ilişkilerinin ötesine geçen bir tehlikeler yeri olduğu için kolayca düzenlenememektedir. Siber uzay beşinci savaş alanı haline gelmekte ve örneğin Amerika Birleşik Devletleri, siber uzayda bazı altyapılarına karşı gerçekleştirilen eylemlerin askeri güç kullanımına yol açacağı konusunda, karşısındakini uyarmaktan

352 Ibid.
353 Ibid, s.289

çekinmemektedir.[354] Konvansiyonel savaş kadar önemli olan "siber savaş", doktrinlerinde özümsenen devletlerin güvenlik gündeminde yerini almaktadır. Bununla birlikte, Rusya ve Çin gibi bazı devletlerin savaş ve barış kavramları arasındaki çizgiyi bulanıklaştırmak istemesiyle, tanımlar ve yaklaşımlar kasıtlı olarak birbirinden ayrılmaktadır.[355]

Bu müdahale, siber uzayın doğasından ve orada gerçekleşen operasyonlardan kaynaklanmaktadır. Anlık bir iletişim yeri olan değiş tokuşlar, basit bilgilerden fidye virüslerine ve devlet altyapısını felç eden siber saldırılara kadar uzanmaktadır. Siber uzay herkes için erişilebilir olduğundan, bu sürekli iletişim akışını kavramak ve kimin sorumlu olduğunu belirlemek zordur. Ancak silahlı çatışmalar belirli bir alandaki nesnel durumlardır. Siber operasyonlar saldırgan olabilse de, insancıl hukuk anlamında silahlı bir çatışmanın bu yeni siber uzay alanında gerçekleşebileceğini düşünmek yine de kolay mıdır?

Teknoloji, savaşanların yeni alanlara savaşı getirmelerini sağlamıştır. Bu durum, başlangıçta kara ile sınırlıyken, şimdi ise, deniz, hava, uzay ve şimdi de siber uzaya yayılmıştır.[356] *Jus in bello*, geleneksel gelişimi içinde, deniz savaş alanı gibi belirli savaş alanlarına kendini özel olarak uyarlamıştır.[357] Stratejik sayılan bir konu, örneğin Amerika Birleşik Devletleri ve NATO tarafından bir savaş alanı olarak yoğun bir şekilde yansıtılmaktadır.[358]

---

354 U.S. Department of Defense, *International Strategy for Cyberspace*, 2011, s. 14.
355 L. KELLO, *Les cyber armés : dilemmes et futurs possibles*, in ***Politique étrangère***, no. 4, 2014, s. 149.
356 D. KUEHL, "From Cyberspace to Cyberpower: Defining the Problem", in F. KRAMER, S. STARR and L. WENTZ (ed.), *Cyberpower and National Security*, Washington D.C., National Defense University Press, 2009, s. 24.
357 Bununla birlikte, hava savaşı özel olarak çerçevelenmemiştir, ancak insancıl hukuk ilkelerine saygı gösterilmesine tabidir.
358 U.S. Department of Defense, *National Strategy to Secure Cyberspace*, 2003; U.S. Department of Defense, *National Military Strategy for Cyberspace Operations*, 2006.

Bununla birlikte, siber uzay insanlar tarafından yaratılmıştır ve bilgi ve iletişim yaratma, paylaşma ve etkileşim kurma şeklimizi değiştirmektedir. Dahası, değiş tokuşlar çoktur, kinetik dünyada hız hâkimdir ve gizlilik bu alanı karakterize eder ve bu da çeşitli türlerde gizli "çatışmalarına" yol açabilir. Siyasal söylem, siber uzayda gerçekleşen "ekonomik savaşlar", "bilgi savaşları" gibi isimlerle doludur. Bununla birlikte, bu nitelikler, "silahlı çatışma" yasal kategorisine girmedikleri için uluslararası insancıl hukukun uygulanmasını ve hatta Brezilya'nın Birleşmiş Milletler Şartı tasarıyı hazırlarken iradesinin aksine, ekonomik eylemler korunmadığı için güç kullanımını bile gerektirmemektedir.[359]

Ayrıca siber uzay diğer alanlardan bağımsız değildir, aksine onları etkileyebilse de onlara bağlıdır.[360] Bu nedenle araştırmacılar, "siber savaş" kavramını, sadece değiş tokuşların geçtiği yer olan ve etkilerin yeri olmayan siber uzayla sınırlandırmamaktadırlar.[361] Bu nedenle, siber uzayın niteliği, genel uluslararası hukuktan farklı olarak insancıl hukuk için çok da önemli değildir. Gerçekten de, silahlı çatışma insancıl hukuk belgelerinde belirtildiği gibi bir bölgede meydana gelirse, bu kriter Devletin sözleşmeye rızasını ilgilendirir ve jus in bello'nun maddi kapsamına değil, ICTY tarafından verilen silahlı çatışma tanımında tutulmaz.[362] Ancak, hedeflenen altyapılar fiziksel olarak hedeflenen Devletin topraklarında mevcut olduğundan, bu unsur çoğu durumda yerine getirilmektedir. Burada önemli olan ise, siber uzay değil, orada bulunan maddi olmayan varlıkların niteliğidir.

---

359 I. KILOVATY, "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", in *National Security Law Journal*, vol. 5, no. 1, 2014, s. 101.

360 M. CEPIK, D. CANABARRO ve T. FERREIRA, "Cyberwar: Clausewitzian Encounters", in *Space & Defense*, vol. 8, no. 1, 2015, s. 24.

361 N. LUBELL, "Cyber warfare as armed conflict", In: Proceedings of the 11th Bruges Colloquium: *Technological Challenges for the Humanitarian Legal Framework*, 2011, p. 43.

362 ICTY, Savcı / Duško Tadić, dava no. IT-94-AR72, Temyiz Dairesi, 2 Ekim 1995, para.70.

Bir savaş alanı olarak nitelendirilmesi hukuku etkilemiyorsa ve yalnızca devletlerin anlambilimine bağlıysa, ilgili silahlı kuvvetlerin özellikle bu alanda hareket etmek için bireyleri işe aldığı gerçeği kalacaktır. Bu, her askeri operasyonun silahlı çatışma veya saldırı olduğu anlamına gelmemektedir. Bu nedenle, ICRC'nin pozisyonunun hatırlattığı gibi, siber savaşın insancıl hukukun silahlı bir çatışma olarak uygulanmasına yol açıp açmadığını belirlemek için bir çatışmanın ve taraflarının yoğunluğunu temel almak gerekmektedir.[363]

b. Silahlı Çatışma Kavramının Siber Savaş İçin Yetersizliği

Terörizme gelince, savaş kelimesinin sözlük anlamı, durumun gerçekliğine bağlı olan insancıl hukukun uygulanmasını, "d*evletlerarasında silahlı kuvvete başvurulduğunda veya [...] hükümet yetkilileri ve organize silahlı gruplar arasında veya bir Devlet içindeki bu tür gruplar arasında yer alır*" şeklinde ifade etmektedir.[364] Bu kavram iki kritere dayanmaktadır: Silahlı kuvvet ve çatışmanın taraflarının niteliği.

Bu nedenle, siber savaşın silahlı çatışma olarak nitelendirilebilmesi için ilk kriteri karşılayacak bir yoğunluk göstermesi gerekmektedir. Devletlerin silahlı kuvvetleri siber bölünmeler ve siber operatörlerden oluşsa da, tüm askeri faaliyetler silahlı kuvvetlerin angajmanını oluşturmamaktadır.[365] Bu nedenle, Birleşmiş Milletler Şartı'nın 2 (4). Maddesini ve UAD'nin kuvvet kullanımına ilişkin Nikaragua içtihatlarının ayrıntılarını

---

363 ICRC, International Humanitarian Law and the challenges posed by contemporary armed conflicts, report presented at the 32nd International Conference of the Red Cross and Red Crescent, 32IC / 15/11, 2015, s. 50.

364 ICTY, Savcı / Duško Tadić, dava no. IT-94-AR72, Temyiz Dairesi, 2 Ekim 1995, para.70.

365 2011 yılında, misyonu Amerika Birleşik Devletleri'nin siber uzaydaki çıkarlarını ve altyapısını savunmak ve aynı zamanda askeri operasyonlar yürütmek olan ABD Siber Komutanlığı, askeri personele entegre edilmiş 90.000 kişiden oluşuyordu. N. LUBELL, "Cyber warfare as armed conflict", In: Proceedings of the 11th Bruges Colloquium: *Technological Challenges for the Humanitarian Legal Framework*, 2010, Bruges, 2011, s.4

dikkate almak gereklidir. Bununla birlikte, güç kullanımı, silahlı kuvvetlerin silahlandırılması ve eğitilmesi[366] gibi bir "silahlı saldırı"dan daha az yoğunluğa sahip eylemleri içerebileceğinden, jus ad bellum'un ihlali, otomatik olarak jus in bello'nun uygulanmasını gerektirmemektedir.[367] Bu nedenle, saldırgan siber araçların kullanımı, silahlı saldırı ile bağlantılı, ancak gerekli bir yoğunluk kriteri ile birleştirilmiş silahlı çatışma kavramının kurucu etkilerine benzetme yoluyla yanıt vermelidir. Prof. Schmitt'in Tallinn Kılavuzunda ele alınan yaklaşımı, kuralları iç tartışma konusu olmasına rağmen, saldırının insan zayiatına veya hasara ve mülkün tahribatına neden olması gerektiği gibi, etkisine ve bu etkiden doğan sonuçlara odaklanmaktadır.[368] Bununla birlikte, mevcut siber saldırılar, fiziksel hasara neden olmadıklarını, sadece Stuxnet'in neden olduğunu veya hatta bir çatışmanın gerekli yoğunluğunun bir parçası olduklarını göstermektedir, örneğin Estonya'daki kesintilerin bir saatten iki güne kadar değişken bir süresi bulunmaktaydı. Bu nedenle, siber saldırıların silahlı bir siber çatışma oluşturması için fiziksel veya maddi hasara yol açması gerekir, ancak aynı zamanda tekrar tekrar ve ara sıra değildir.[369]

Siber saldırıların silahlı çatışma tanımında belirtilen taraflardan gelmesi de gereklidir: Devlet(ler) ve/veya örgütlü silahlı gruplar. IAC'nin yeterliliği, teorik olarak, siber saldırılar hasara veya yıkıma neden olursa, iki devlet arasında bir zorluk savaşıyla sonuçlanmayacaktır. Ancak, siber operasyonlar genellikle anonimlik koşuluyla, bu tür etkilere neden olmadan yürütülmektedir. Böylece, Stuxnet, silahlı bir saldırı olarak görülmemiş ve yıkıcı bir şekilde İran ile ABD ve İsrail arasında silahlı çatışmaya yol açacak şekilde yayılmamıştır. Bu bağlamda, virüsün ancak belirli bir süre sonra, devreye

366 ICJ, Case of Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, Haziran 27, 1986, Rec. 1986, para. 228.
367 N. LUBELL, 2011, s. 44.
368 M. N. Schmitt, 2013, s. 47-51
369 M. N. SCHMITT, The Law of Cyber Warfare: *Quo Vadis?*-2014, s.292

alınmasının ardından keşfedildiğini ve yazarlığının (*authorship*) resmi olarak reddedildiğini belirtmek gerekir. NIAC olarak kalifiye olmak, özellikle sorumlu komuta, organizasyon ve kontrol kriterlerini karşılamayan bilgisayar korsanları grupları açısından daha zordur. Bununla birlikte, bireysel bir siber operasyon veya "örgütlenmemiş" bir grup tarafından gerçekleştirilen bir siber operasyon, ciddi sonuçlara yol açsa bile, geleneksel kriterlere göre silahlı çatışma oluşturamamaktadır.[370]Bu nedenle, Prof. Schmitt için, organizasyonun derecesi, yoğunluğun aksine, siber operasyonların özelliklerine uyarlanmalıdır.[371]

Bu nedenle, uygulama ve benzetme, siber savaşı silahlı çatışma olarak nitelendirmek için çok az yer bırakmaktadır. Bu kavram, benzetme yoluyla uyarlama eksik olduğundan, bu olgu için yetersiz görünmektedir. Bununla birlikte, siber savaş kavramı, siyaset bilimciler için gerçekten yeni bir savaş türü değildir. Daha ziyade, bazı eski savaş yöntemlerinin sofistike olmasına izin veren yeni araçların kullanımıyla ilgilidir.[372] Bu nedenle, siber saldırıların kullanımı şu ana kadar silahlı bir çatışmaya yol açmamış, aksine Rus-Gürcü örneğinin gösterdiği gibi silahlı bir çatışmayı desteklemek için gerçekleştirilmektedir. İnsancıl hukukun "*geleceğin silahları da dâhil olmak üzere tüm silahlara"*[373] uygulandığı için çerçevelemesi gereken gerçek budur. Ancak yine de bu siber operasyonların insancıl hukuk anlamında "*saldırı"* olarak nitelendirilmesi gerekmektedir. Ancak benzetme, kimilerine göre *jus in bello*'nun sibernetik araçlara uyarlanması ise de, bu yöntem aslında yetersizdir çünkü uygulama açısından IHL'nun özüne aykırıdır.

2. "Saldırı" Kavramının Yetersizliği ile Uluslararası İnsancil Hukukun Çelişkisi

370 Ibid.
371 Ibid
372 J. ARQUILLA ve D. RONFELDT, *In Athena's Camp: Preparing for Conflict in the Information Age*, 1997, s. 37.
373 ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 Temmuz 1996, Rec. 1996, para 86.

"Siber savaş", bazen casusluk ve fikir manipülasyonunu içeren daha geniş bir "bilgi savaşı" kavramıyla eşitlenen farklı doktrinel tanımlara tabidir.[374] Ancak bu kavramsal farklılıklar, siber saldırılara ilişkin farklı vizyon ve tepkilere sahip Devletlerin uygulamalarına yansımaktadır. Sibernetik operasyonların stratejik doktrinlerdeki etkileri bu nedenle hedeflerinden daha az önemli olmaktadır. ABD, dokunulmaz olan ve hatta casusluğun teoride bir saldırı teşkil edebileceği stratejik altyapıyı tanımlarken,[375] Çin ve Rusya hükümet sistemlerine herhangi bir sızmayı bu şekilde görmektedir.[376]

Uluslararası hukuk, uluslararası toplumun ihtiyaçlarına uyum sağlamak zorundayken, insancıl hukuk nesnel durumları çerçevelemeye dayanmaktadır. Sonuç olarak, kategorizasyonu devlet çıkarlarına bağlı olarak siyasi niteliklere bağlı olamaz. Bu nedenle, jus in bello'nun bu tür operasyonlara uygulanabilmesi için, araçları tarafından tanımlanan siber "saldırılar" kapsamına girmesi gerekir. Ancak bu kavram, insancıl hukuk gibi, bir eylemin doğasından çok fiziksel etkilerine odaklanmaktadır. Gerçekleri yansıtmak ve onu atlatmaktan kaçınmak söz konusuysa, siber kapasitelerin mevcut kullanımı göz önüne alındığında bu nitelik zordur ve bu özellikleri hesaba katmak için yetersizdir, bu da şu paradoksla sonuçlanır: Analoji, Uluslararası İnsancıl Hukuka saygı göstermek için haklıdır, ancak gerçekte özündeki çelişkiyi içermektedir.

B. ULUSLARARASI OLMAYAN SİLAHLI ÇATIŞMA DURUMU

374 K. J. KNAPP ve W. R. BOULTON, "Ten Information Warfare Trends", In L. J. JANCZEWSKI (ed.), *Cyber Warfare and Cyber Terrorism*, London, IGI Global, 2008, ss. 17-26

375 J. S. NYE, Cyber Power, *Belfer Center for Science and International Affairs*, Harvard Kennedy School, 2010, s. 16.

376 Lucas Kello, The Virtual Weapon: Dilemmas and Future Scenarios, In *Politique étrangère*, no 4, 2014, s.149

Uluslararası olmayan silahlı çatışma durumlarında uygulanabilir Uluslararası İnsancıl Hukukun maddi kuralları, esas olarak 1949 Cenevre Sözleşmelerinin[377] Ortak 3. Maddesinde ve 1977 Ek Protokol II'de (AP II)[378] bulunmaktadır. Ortak Madde 3, çatışmalarda aktif olarak yer almayan kişilere yönelik muamele için temel asgari standartları belirlerken, AP II, bu tür kişilere insani muameleye ilişkin[379]; yaralıların, hastaların ve kazazedelerin korunması için[380]; ve sivil nüfusun korunması için[381]; çok daha kapsamlı ve ayrıntılı hükümler içermektedir. Her iki araç da, belirli silah türlerinin kullanımı da dâhil olmak üzere, düşmanlıkların yürütülmesi veya savaş yöntemleri ve araçları hakkında hiçbir şey söylememektedir. Bununla birlikte, bu konular, uluslararası silahlı çatışmalar (IAC) ile ilgili yasada kapsamlı bir şekilde ele alınarak ICRC, aynı kuralların çoğunun NIAC'ta eşit olarak uygulanabilir olduğunu tartışmasız olarak önermemiştir.[382] Tallinn Kılavuzu, özellikle siber alandaki NIAC bağlamında bu kuralların çoğunu içermektedir.[383]

---

377 Savaş Alanındaki Silahlı Kuvvetlerde Yaralı ve Hastaların Durumunun İyileştirilmesine İlişkin Cenevre Sözleşmeleri, 12 Ağustos 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Denizdeki Silahlı Kuvvetlerin Yaralı, Hasta ve Gemi Enkazı Üyelerinin Durumlarının İyileştirilmesine İlişkin Cenevre Sözleşmesi, 12 Ağustos 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Savaş Esirlerine Uygulanacak Muameleye İlişkin Cenevre Sözleşmesi, 12 Ağustos 1949, 6 U.S.T. 3316, 75 U.N.T.S. 287; Savaş Zamanında Sivillerin Korunmasına İlişkin Cenevre Sözleşmesi, 12 Ağustos 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

378 12 Ağustos 1949 tarihli Cenevre Sözleşmelerine Ek Protokol ve Uluslararası Olmayan Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin Protokol (Protokol II), imzaya açıldı 12 Aralık 1977, 1125 U.N.T.S. 609, 16 I.L.M. 1442 [bundan sonra AP II olarak anılacaktır].

379 AP II, md. 4-6

380 AP II, md. 7-12

381 AP II, md. 13-18

382 Jean-Marie Henckaerts & Louise Doswald-Beck, Customary International Humanitarian Law – Volume I: Rules (2005).

383 Örneğin, Tallinn Kılavuzu, supra not 5, r. 31 (ayrım kuralı), 32 (sivillere saldırma yasağı), 35 (düşmanlığa doğrudan katılan siviller), 36 (terör saldırıları yasağı), 37 (sivil nesnelere saldırma yasağı), 42 (gereksiz yaralama veya gereksiz yere yaralama yasağı) acı çekme), 43 (ayrım gözetmeyen savaş araç ve yöntemlerinin yasaklanması), 44 (siber bubi

Tamamen çevrimiçi olarak organize olan bir grup tarafından gerçekleştirilen siber saldırıların sınıflandırılması daha zordur. Sanal organizasyonların üyeleri asla tanışmayabilir ve hatta birbirlerinin gerçek kimliğini bile bilmeyebilir. Bununla birlikte, bu tür gruplar hükümete (veya organize bir silahlı gruba) karşı koordineli bir şekilde hareket edebilir, sanal bir liderlikten emir alabilir ve oldukça organize olabilir. Örneğin, grubun bir üyesi hedef sistemlerdeki güvenlik açıklarını belirlemekle görevlendirilebilir, bir ikincisi bu güvenlik açıklarından yararlanmak için kötü amaçlı yazılım geliştirebilir, üçüncü, bir öğe operasyonları yürütebilir ve dördüncüsü karşı saldırılara karşı siber savunmayı koruyabilir.

Grubun örgütlü olarak nitelendirilmesinin önündeki en büyük engel, uluslararası insancıl hukuka uygunluğun sağlanamamaması olacaktır. Ek Protokol II, belgenin kapsadığı uluslararası olmayan bir silahlı çatışma ortaya çıkmadan önce bir grubun "sorumlu komuta altında"[384] olmasını şart koşmaktadır. Bu gereklilik çok katı yorumlanmamalıdır. ICRC'nin Madde Yorumunda belirtildiği gibi, 'terimi, isyancı silahlı grubun veya muhalif silahlı kuvvetlerin bir dereceye kadar örgütlenmesini ifade etse de, bu, düzenli silahlı kuvvetlerinkine benzer hiyerarşik bir askeri örgütlenme sistemi olduğu anlamına gelmemektedir; bir yandan sürekli ve uyumlu askeri operasyonları planlama ve yürütme, diğer yandan fiili bir otorite adına disiplin dayatma yeteneğine sahip bir örgüt anlamına gelmektedir.[385] Sanal olarak örgütlenmiş bir grupta, sürekli ve uyumlu askeri operasyonlar yürütme yeteneği gereksinimi, siber operasyonların askeri operasyonlarla eşit olduğu ve tartışıldığı gibi, olması gerektiği ölçüde karşılanabilir. Bununla birlikte, grup üyeleri üzerinde, fiziksel kontrolden yoksun olduğu için, bir disiplin dayatmak zor olacaktır.

---

tuzaklarının yasaklanması), 49 (ayrım gözetmeksizin saldırı yasağı), 51 (orantılılık kuralı), 52-57 (saldırıda önlemler), 60 (ihanet yasağı), 61 (hileler), 66(a) (siber casusluk).

384 AP II, md. 1(1).

385 AP II Yorumu, paragraf 4663

AP II'nin, grubun "bu Protokolü uygulayabilmesi" şartı, meseleleri karmaşık hale getirmektedir.[386] İfade, genellikle uluslararası insancıl hukuka uyma ve bunları uygulama yeteneği olarak anlaşılmaktadır. Şiddetin bir Protokol II çatışması olarak nitelendirilebilmesinden önce, 'tarafların gereken minimum altyapıya sahip olduklarından dolayı, makul olarak, Protokol'de geliştirilen kuralları uygulamaları beklenebilir.[387]Yasanın fiilen uygulanması için bir gereklilik bulunmamakla birlikte, grubun icrayı mümkün kılacak şekilde örgütlenmesi gerekmektedir. Neredeyse organize bir grupta, üyeler arasında fiziksel bir bağlantı olmadığı için böyle bir organizasyon eksiktir.

Bu antlaşma, yasası gereği Ek Protokol II'den kaynaklandığından, yalnızca bu belgenin geçerli olduğu çatışmalara kendi başına uygulanabilir olduğu konusunda uyarılmalıdır. Ortak 3. Madde eşdeğer bir koşul içermemekte, bu nedenle, Ek Protokol II'nin uluslararası olmayan silahlı çatışmalar dışında benzer bir örf ve adet hukuku normunun uygulanıp uygulanmadığı sorusunu gündeme getirmektedir. Bu bağlamda, 3. Maddenin Yorumu, 1949 Cenevre Sözleşmelerinin taslağını hazırlayan Diplomatik Konferansın bu tür çatışmalar için açık ön koşullar koymayı değerlendirdiğini kaydetmektedir. Öneri reddedilmiş olsa da, yorum, bunların 'uygun kriterler oluşturduğunu' iddia etmektedir.[388]İlk koşul, "De jure hükümete isyan eden tarafın, örgütlü bir askeri güce, eylemlerinden sorumlu, belirli bir bölge içinde hareket eden ve Sözleşmeye saygı gösterme ve Sözleşmeye saygıyı sağlama araçlarına sahip bir otoriteye sahip olması"dır.[389] Bu nedenle, sorumlu komuta (disiplinin uygulanmasına karşı) ve uluslararası insancıl hukuku uygulama becerisine ilişkin Ek Protokol II'nin gerekliliklerini uluslararası olmayan tüm

386 AP II, md. 1(1).
387 AP II Yorumu, paragraf 4470
388 J Pictet (ed), *Commentary: I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field* (ICRC 1952) 49.
389 İbid.

silahlı çatışmalara genişletmek makul görünmektedir. ICTY, Boskoski[390]'de bu yaklaşımı benimsemiştir ve uluslararası olmayan silahlı çatışmalarda komuta sorumluluğu ilkesiyle uyumludur.[391] Geçerli olması halinde, uluslararası olmayan tüm silahlı çatışmaların genişletilmesi, fiilen örgütlü grupların, bir çatışmayı uluslararası olmayan olarak sınıflandırmak amacıyla örgütlü silahlı gruplar olarak nitelendirilmesini engellemektedir.

Örgütlü olmanın yanı sıra, söz konusu grup silahlı olmalıdır. Uluslararası olmayan silahlı çatışma bağlamında silahlının anlamı, uluslararası silahlı çatışmalara katılmakla paraleldir. Tartışıldığı gibi, genellikle "saldırıların" gerçekleştirildiğini varsaymaktadır. Ancak, uluslararası olmayan silahlı çatışma, bir Devletten farklı olarak bir grubun faaliyetlerine dayandırıldığından, bireysel bir üyenin davranışının bir bütün olarak gruba atfedilmesi sorunu ortaya çıkmaktadır. Silahlandırılması gereken bir grup olduğundan, grubun kendisinin silahlı faaliyetlerde bulunma amacı olmalıdır. Örgütlü bir grubun bireysel üyeleri, kendi istekleriyle, yani grup adına değil, siber saldırılar gerçekleştiriyorsa, grup silahlı kriteri karşılamamaktadır.

Uluslararası silahlı çatışmalardan farklı olarak, uluslararası olmayan silahlı çatışmalar belirli bir yoğunluk derecesine sahiptir. Ayaklanmaların, sivil kargaşaların veya münferit ve düzensiz şiddet eylemlerinin yeterli olmadığını hatırlayın; düşmanlıklar da uzatılmalıdır. Konuyu yoğunluk eşiğinin karşılanıp karşılanmadığına bağlı olarak ele almak

390 *Prosecutor v Boskoski* (Judgment) ICTY-04-82-T (10 Temmuz 2008) para 205.
391 Sorumlu komuta ve komuta sorumluluğu ayrı hukuki kavramlar olmasına rağmen, sorumlu komuta altında olmayan bir grubun üyesi olan bireylerin eylemleri için bir bireye komuta sorumluluğu yüklemek mantıksız olacaktır; kavramlar bu nedenle farklıdır, ancak birbiriyle ilişkilidir. Konuyla ilgili olarak, bkz. Savcı - Hadzihazanoviç (Komuta Sorumluluğuna İlişkin Yargı Yetkisine Karşı Temyiz Kurulu Kararı) ICTY-01-47-AR72 (16 Temmuz 2003) paragraf 16–22.

için ICTY'nin kararları[392], saldırıların ağırlığı, düşmanlıkların kolektif karakteri, durumla başa çıkmak için güç artırma ihtiyacı, düşmanlıkların gerçekleştiği zaman ve Birleşmiş Milletler Güvenlik Konseyi'nin karar verip vermediği gibi faktörlere atıfta bulunmuştur. Bununla birlikte, net bir yoğunluk testi bulunmamaktadır ve "uzun süreli" çatışma için net bir standart yoktur. [393]Siber kampanyaların düzenleniş şeklinin ışığında, siber saldırıların ilgili olarak kabul edilebilecek kadar sık olması gerekse de, açıkça sürekli olması gerekmediği belirtilmelidir.

Bu, birçok siber operasyonun uluslararası olmayan bir silahlı çatışmayı bulmak için yeterli olmasına engel olacak yüksek bir eşiktir. Son derece yıkıcı siber saldırılar bile, zaman içinde düzenli olarak meydana gelmedikçe hak kazanamayacaktır. Bunun yerine ceza hukuku paradigması içinde ele alınacak ve uluslararası olarak insancıl hukuk tarafından değil, insan hakları tarafından yönetilecektir.

Biraz bulanık olan bir konu, iki Devlet arasındaki uluslararası silahlı çatışma sırasında organize bir silahlı grup tarafından gerçekleştirilen siber saldırıların sınıflandırma durumudur. Açıktır ki, bir grup, çatışmanın bir tarafına "aitse", çatışmanın karakteri tamamen uluslararası kalacaktır. III. Cenevre Sözleşmesi'nin 4. Maddesinden kaynaklanan aidiyet kavramı, grup ile taraf olan bir Devlet arasında en azından bir miktar fiili ilişkiyi ima etmektedir.[394] Maddenin yorumu, grubun hangi taraf için savaştığı açık olduğu sürece zımni anlaşmanın bile yeterli olduğunu öne sürmektedir.[395]

---

392 *Prosecutor v Haradinaj* (Judgment) ICTY-04-84-T (3 Nisan 2008) paragraf 49 (çeşitli gösterge faktörlerinin özetlenmesi).
393 Abella'da, Amerika Ülkeleri İnsan Hakları Komisyonu, muhalif silahlı kuvvetler ile Arjantin ordusu arasında 30 saatlik bir çatışmayı uluslararası olmayan silahlı çatışma olarak nitelendirdi. *Abella v Argentina*, Inter-American Commission HR Case 11.137 (1998) Doc OEA\ser.L\V\II.98 doc 6 rev.
394 Cenevre Sözlesmesi III, md. 4A (2).
395 Cenevre Sözlesmesi III Yorumu, 57

Bir grubun uluslararası silahlı çatışmanın taraflarından biri adına siber saldırılara giriştiği durum çok daha karmaşıktır. Bu uzak bir varsayım değildir. Örneğin, Irak'taki çatışma hâlâ uluslararası nitelikteyken, Baas rejimiyle hiçbir bağlantısı olmayan örgütlü silahlı gruplar koalisyon güçlerine saldırmıştır.[396] Şii milisler gibi gruplar, bu çatışma sırasında her iki tarafa da karşı çıkmıştır.[397] Bir grubun kendiliğinden bir partiye karşı siber saldırılar düzenlediği benzer bir durum kolaylıkla ortaya çıkabilmektedir.

ICRC'nin Düşmanlıklara Doğrudan Katılım Kavramına İlişkin Yorumlayıcı Rehberi bu tür durumları ele almaktadır. "Uluslararası bir silahlı çatışmanın daha geniş bağlamında faaliyet gösteren örgütlü silahlı grupların, bu çatışmanın bir tarafına ait olmaksızın, yine de uluslararası olmayan ayrı bir silahlı çatışmanın tarafları olarak kabul edilebileceğini" ileri sürmektedir.[398] Rehberlik ile sonuçlanan bilirkişilik sürecindeki bazı katılımcılar, aynı muharebe sahasında hem uluslararası hem de uluslararası olmayan silahlı çatışma hukukunun uygulanmasını gerektirdiğinden, uygulamada sorunlu olacağı gerekçesiyle ICRC'nin pozisyonunu reddetmiştir.[399] Onlara göre, herhangi bir taraf yerine, söz konusu grubun eylemleri ile uluslararası silahlı çatışma arasında açık bir bağlantı olup olmadığını sormak daha uygundur. Örneğin, organize bir silahlı grup, işgalcilere dini veya siyasi muhalefet nedeniyle işgalci bir güce karşı siber saldırılar düzenleyebilir, onları hükümet adına sınır dışı etmek için değil. Grup ile çatışma arasındaki zorunlu bağ, onların işgale

396 The Iraq war, https://www.cfr.org/timeline/iraq-war E.T 21 Aralık 2021
397 İd.
398 N Melzer, *Interpretive Guidance on the Notion of Direct Participation under International Humanitarian Law* (ICRC 2009) 24.
399 N. Melzer, Yazarın katılımına dayalı.

karşı muhalefeti olacaktır. Böyle bir durumda, grup ile işgal altındaki Devlet arasında bir ilişki olmamasına bakılmaksızın, çatışma tamamen uluslararası kalacaktır.[400]

Son olarak, Ek Protokol II'nin yalnızca organize silahlı gruplar bölgeyi kontrol ettiğinde geçerli olduğunu hatırlamak önemlidir. Bir grup, fiziksel mevcudiyet olmadan bölgeyi kontrol edemediği için, aracın genellikle yalnızca siber çatışmalara uygulanamayacağı düşünülmektedir. Buna göre, yalnızca bölgeyi kontrol eden ve bu tür operasyonları yürüten organize bir silahlı grubu içeren Ek Protokol II çatışmalarındaki siber operasyonlar için geçerli olacaktır.

II. SİBERNETİK ARAÇLARIN KULLANILDIĞI DUŞMANLIKLARIN DAVRANIŞ İLKELERİ

Bir savaş aracı ve yöntemi olarak "siber savaş", "*geleceğin silahları*"[401] da dâhil olmak üzere "*tüm savaş biçimlerine ve tüm silahlara*" uygulanabilen insancıl hukukun temel ilkelerinden kaçmamakta ve bu, açıkça belirlenmiş kuralların yokluğunda bile, Martens kaydının modern versiyonunda bahsedildiği gibi "*Buradaki beyan, savaş hukuku kuralları tam olarak tedvin edilene kadar, sivil ve muhariplerin yerleşmiş uygulamalar, insaniyet ilkeleri ve kamu vicdanın emirlerinden çıkartılabilecek uluslararası hukuk prensiplerinin koruması altında kalacağını ifade etmektedir*".[402]

400 Michael Schmitt, Classification of Cyber Conflict, *Journal of Conflict and Security Law*, Volume 17, Issue 2, Summer 2012, s. 245–260, https://doi.org/10.1093/jcsl/krs018 E.T 10 Hazıran 2021.
401 ICJ, Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 8 Temmuz 1996, Rec. 1996, § 86.
402 1949 Cenevre Sözleşmelerine Ek Protokol I'in I (2) Maddesi.

Ancak, sibernetik yollarla bir "saldırı" durumunda uluslararası insancıl hukukun uygulanabilirliği "geniş bir mutabakat" konusu ise[403]; bu hipotez, siber kapasitelerin özellikleri açısından sınırlı olsa da, aynı şey, bu tür siber saldırıların düşmanlıkların davranış ilkelerine saygı gösterme olasılıkları için doğru değildir. Nitekim silahlı çatışma ve saldırı kavramıyla aynı mantığı izleyen bu kuralların siber yeteneklerin kullanımıyla ilgili gerçekleri yansıtmada yetersiz kaldığı görülmektedir. Dolayısıyla, bu ilkeler, uluslararası insancıl hukuk olan karmaşık koruma sisteminin "bel kemiğini" oluştursalar da, işlemez hale getirilmektedir.[404]

Nitekim "saldırılar" sadece askeri hedefleri hedef alıp sivilleri, kişileri veya malları korumak zorundayken[405], ayrım ilkesi siber uzaya hâkim olan anonimlik veya onun bölgesel olmayışı ve analojinin getirdiği kısıtlayıcı fiziki mülahazalarla karşı karşıyadır. Sonuç olarak, ayrım ilkesi, ne kadar önemli ve insancıl hukukun temelinde olursa olsun, siber operasyonları çerçevelemek için yetersiz bulunmuştur.[406] Analojinin sınırları, sibernetik silahların kullanımının gerçeklerini yansıtma ve çerçeveleme konusundaki yetersizliği nedeniyle, nihayetinde, mantık ve yorumlarının bu tür operasyonların özgüllükleri ile çelişmesi nedeniyle, düşmanlıkların yürütülmesinin diğer ilkeleri üzerinde yankı uyandırmakta ve yetersizliklerine yol açmaktadır.

---

403 K. BANNELIER-CHRISTAKIS, *Enjeux de la cyberguerre pour la protection des personnes et des biens civils. Du principe de distinction au Manuel de Tallinn*, in SFDI, *Colloque de Rouen. Internet et le droit international*, Paris, Pedone, 2014, s. 277.

404 Meurant, Jacques. "Inter Arma Caritas: Evolution and Nature of International Humanitarian Law." ***Journal of Peace Research*** 24, no. 3 (Eylül 1987), s.237 https://doi.org/10.1177/002234338702400304 E.T 11 Haziran 2021

405 1949 Cenevre Sözleşmelerinin 1977 tarihli I. Ek Protokolünün 51 ve 52. maddeleri.

406 ICJ, Legality of the Threat or Use of nuclear weapons, Advisory Opinion, 8 Temmuz 1996, Rec. 1996, § 78

A. SİBERNETİK ARAÇLARLA AYRIM İLKESİ

Silahlı çatışmaların sadece askerleri ilgilendirdiğini ve sivilleri etkilemediğini iddia etmek inandırıcı olmasa da, insancıl hukuk yine de ikinci kategorideki kişileri ve malları onlara karşı saldırıları yasaklayarak korumak iddiasına dayanmaktadır. Bu ilke, sivil ve askeri ayırt etme yeteneğine, siber uzayın birbirine bağlılığı ve anonimliği tarafından zorlaştırılan bir kapasiteye dayanmaktadır. Ancak, devletler "*asla... Sivil ve askeri hedefleri ayırt edemeyecek silahları kullanmamalıdır*."[407]

İnsancıl hukukun temel bir ilkesi olarak, siviller ve savaşçılar arasındaki ayrımın önemi, tüm sistemin "temel taşını" oluşturacak şekildedir.[408] Bu nedenle, ayrım ilkesi bir durumu yönetmek için yetersiz olsaydı, insancıl hukuk bir bütün olarak artık tutarlı olmayacak ve hükümleriyle ve ilkeleriyle çelişecekti. Bununla birlikte, benzetme uygulanabilirliğini zayıflatırken ve çelişkiyle tehdit ederken, sibernetik araçların özgüllüklerine uyum sağlamasına da izin vermemekteydi.

Gerçekte, siber uzayın anonimliği, savaşçının tanımlanmasına ve onun analog kriterlerine meydan okurken, meşru askeri hedefin belirlenmesi siber uzayda hüküm süren karşılıklı bağlantı tarafından karmaşık hale gelmektedir. Bununla birlikte, ayrım ilkesi belirli bir uyarlanabilirliğe sahipse, sınırlarını tamamen farklı mantık ve nitelikteki durumlar karşısında sunacaktır.

1. Savaşçının Kimliği ve Siber Uzayın Anonimliği

Siber uzayı kullanmaya yönelik teknolojiler hazır ve ucuz olduğu için siber uzayda anonimlik hâkimdir; dahası, karmaşık olmayan sibernetik araçlar bile önemli zararlara neden olabilmektedir. J. Nye için, bu erişilebilirlik sayesinde, tek bir kişi siber uzayda

407 A.g.e
408 A.g.e

"daha düşük bir maliyetle önemli bir rol oynayabilmektedir".[409] Bununla birlikte, belirli siber yeteneklerin geleneksel operasyon desteği dışında kullanılmasına ilişkin ilkelerden biri, siber silahların etkilerinin anonimliği ve gecikmesine dayanmaktadır. Sonuç olarak, I. Ek Protokol'ün 37. Maddesinde yasaklanan ve "savaşçıların" kendilerini bu şekilde tanımlamayı reddetmekten daha fazlasını yaptıkları, ancak kasıtlı olarak rakibi aldatmak için sivil gibi davrandıkları ihanet uygulamasıyla bir paralellik kurulmaktadır. Bu durumlarda, S. Shackelford için bu uygulamalar kınanmalı ve yargılanmalıdır.[410]

Bununla birlikte, sınırlar zor olmaya devam etmektedir, çünkü bu tür ihlalleri önlemek için sibernetik operatörler kendilerini I. Protokolün 44. maddesine göre silahlı kuvvet olarak tanımlamalıdır. Bu kişilerin, devlet dışı grupların ve hatta tetikleyici Devletin operatörleri için sıklıkla paylaşılan bir özellik olan operasyonla aynı bölgede olmaları gerekmediği çok açık değildir. Bununla birlikte, "savaşçılar", düzenli silahlı kuvvetlere entegre olduklarında veya asimile olduklarında ve Devletler bu anlamda, silahlı kuvvetler içinde siber bölünmeler oluşturduklarında, kendilerini geleneksel kurallara göre tanımlayabileceklerdir.[411]

Bununla birlikte, bireyselliklere ek olarak, siber kapasiteler, kendilerini gizlemek isteyebilecek devlet dışı gruplar tarafından ve daha da fazlası bir devletle bağları olduğunda ve siber kapasiteler kullanıldığında yeni bir boyut kazanmaktadır. Örneğin, Rusya'nın Doğu Avrupa'daki Rus yanlısı gruplarla güçlü bağları vardır.[412] Bu durumda, bu zorluklar aynı zamanda uluslararası sorumluluk rejimine meydan okumakta ve kontrol kriteri konusunda

409 J. S. NYE, *The Future of Power*, New York, Public Affairs, 2011, s. 124.
410 S. J. SHACKELFORD, "From Nuclear War to Net War : Analogizing Cyber Attacks in International Law", in *Berkeley Journal of International Law*, vol. 27, no. 1, 2009, s. 241.
411 V. M. PADMANABHAN, "Cyber Warriors and the Jus in Bello", in *International Law Studies*, vol. 89, no. 1, 2013, s. 295.
412 T. RID ve J. ARQUILLA, "Think Again: Cyberwar", *Foreign Policy*, Mart/Nisan 2012, s. 83.

insancıl hukuk ile farklılıkları vurgulamaktadır. Gerçekten de, insancıl hukuk, çatışma niteliği bakımından "küresel kontrol" gerektirirken, üçüncü şahısların eylemlerine karşı devlet sorumluluğu rejimi "etkili kontrol" gerektirmektedir. Bu farklılık, siber uzayın kendine has özellikleri ve ona dahil olan gruplar karşısında bir kez daha sorgulanmaktadır.[413]

Bu özdeşleşme güçlükleri ve geleneksel olanları sorgulayan uygulamalarla karşı karşıya kalan S. Shackelford, bu gibi durumlarda; "Siber savaşçılar", örgütsel kriteri yerine getirmediklerinde, aslında "düşmanlığa doğrudan katılan siviller" kategorisine girerler, ancak başka bir bölgedeyse, hedeflemeleri jus ad bellum kurallarına bağlı olmalıdır.[414] Savaşan ve sivil arasındaki çizgi çağdaş silahlı çatışmalarda zaten bulanıksa, savaşçıyı ve statüsünü belirlemenin zor olduğu siber uzayda daha da bulanıktır. Bu uyumsuzluk aynı zamanda askeri hedeflerin belirlenmesinde ve siber uzayın karşılıklı bağımlılık ve ikili statü üreten bir karşılıklı bağlantı sistemi olması nedeniyle bunların sivillerden ayrılmasında da yankı bulmaktadır.

2. Sistemin Bağlantılılığı İçerisinde Meşru Askeri Hedefin Belirlenmesi

"Saldırı" kavramının tanımı göz önüne alındığında, yalnızca fiziksel etkilere ve ayrım yapamama ile sonuçlanan siber operasyonlar analoji ile yasaklanmıştır. Bu nedenle, "saldırılar" belirli bir askeri hedefe yönelik olmalıdır.[415] Mallar söz konusu olduğunda askeri hedefler, "*doğaları, konumları, amaçları ya da kullanımları gereği askeri eylemlere etkin bir katkıda bulunan ve tamamen ya da kısmen yok edilmesi, ele geçirilmesi ya da*

413 V. M. PADMANABHAN, 2013, s. 295.
414 S. J. SHACKELFORD, 2009, s.241
415 1949 Cenevre Sözleşmelerine Ek 1977 tarihli I. Protokolün 51 (4) (a) ve 52 (2) maddeleri

etkisiz hale getirilmesi durumunda, mevcut koşullar altında, kesin bir askeri avantaj sağlayan objelerle sınırlıdır".[416]

Bununla birlikte, hizmet reddi kullanımları, Estonya'da olduğu gibi, ayrım gözetmeyen etkilere sahiptir, ancak jus in bello anlamında saldırılar olarak kabul edilmediğinden, sivillere ulaşıp hedef alsalar da jus in bello tarafından ele alınmamaktadır. Bu katı çerçeve, siber saldırıların yıkıcı potansiyeline karşı bir koruma görevi görmektedir, ancak uygulamanın gerçeklerini yansıtmamaktadır. Gerçekten de Stuxnet, fiziksel etkilere neden olan ve virüs yayılmış olmasına rağmen ayrımcılık yapabilen tek siber saldırıdır.[417]

Siber uzay, bir "saldırı" bağlamında bile, değiş tokuşlarının hızı, potansiyel anonimliği ve ayrımcılık yapılmaması ile karakterize edilen soyut bir alan olduğu için "mülkiyet" tanımına meydan okumaktadır. Aslında, sivil veya askeri, bu kategoriler önemsizdir, çünkü askeri kullanım verileri sivil kanallardan geçer ve tersine sivil verilerin iletişimi, GPS sistemlerinde olduğu gibi askeri altyapılardan geçebilir.[418] Mariarosaria Taddeo'nun "Biyosfer"ine benzer bir "Infosphere" olarak tanımlanan bu sistem, birbirinden ayırt edilmesi zor ve her ihlali domino etkisi yaratacak bir dizi ara bağlantıdır.[419]

"Mülkiyetin" zor tanımına ve doğasının tanımlanmasına ek olarak, sivil hedefleri hedef alma yasağının hangi altyapının ikili kullanım olarak nitelendirildiği konusunda bir

---

416 1949 Cenevre Sözleşmelerine Ek I. Protokolün 52 (2) Maddesi

417 Stuxnet virüsü, 15.000'i Almanya, Fransa, Hindistan, Çin ve Endonezya'da olmak üzere 45.000 bilgisayar sistemine yayılmıştır. Ancak virüs, Natanz tesisindeki model santrifüjü sabote etmek için özel olarak tasarlanmış ve bu nedenle daha fazla hasara neden olmamıştır. Le Monde, *Plusieurs millions d'ordinateurs infectés par Stuxnet en Chine*, 30 Eylül, 2010. https://www.lemonde.fr/technologies/article/2010/09/30/plusieurs-millions-d-ordinateurs-infectes-par-stuxnet-en-chine_1418382_651865.html E.T 12 Haziran 2021.

418 J. KELSEY, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", in *Michigan Law Review*, vol. 106, no. 7, 2008, s. 1432.

419 M. TADDEO, "An Analysis for A Just Cyber Warfare", in C. CZOSSECK, R. OTTIS ve Z. ZIOLKOWSKI (ed.), *Warfare. Fourth International Conference of Cyber Conflict*, Tallinn, NATO CCD COE Publications, 2012, s. 214.

boyut sınırı vardır. Bunlar siber uzayın biriktirdiği hem askeri hem de sivil yönlere hizmet eden altyapılardır.[420] Uluslararası insancıl hukuk bu tür bir yapıya ilişkin özel bir hüküm içermiyorsa, askeri mülahazalar, askeri bir hedefin sivil işlevleri ona bu niteliğini kaybettirmeyeceğinden, onlara saldırma olasılığına yol açacaktır.[421] Bununla birlikte, ikilem, siber uzay sistemlerinin çoğunluğunun, doğası gereği çift kullanımlı olması ve İnternet'in kendisinin hala askeri köklerine dayanması bakımından önemlidir.[422]

Bu nedenle ayrım ilkesi, siber operasyonların kullanımını düzenlemek için yetersizdir. Her şeyden önce bu durum, siber kapasiteler fiziksel etkilere neden olmadığı sürece sivil halka yönelik saldırıları engellemeyen ve çok kısıtlayıcı olan "saldırı" tanımına bağlıdır; ikincisi, ilke siber uzayın doğasına, operasyonlarına, aktörlerine ve çift kullanımlı altyapılarına uygun olmadığı içindir. Bu yapılara yönelik saldırılara izin verilmesiyle siviller her zaman etkilenecektir. Ancak, benzetme yoluyla uluslararası insancıl hukukun uygulanmasını destekleyenler için, sivillerin korunması orantılılık ve ihtiyat ilkelerine bağlıdır.[423] Ancak tıpkı ayrım ilkesi gibi analoji mantığına bağlı olduklarından yetersizdirler.

B. SİBERNETİK ARAÇLARLA HASMANE İŞLEM YAPILMASINA İLİŞKİN DİĞER İLKELER

Prof. Schmitt'e göre, ihtiyat ve orantılılık ilkeleri, uluslararası insancıl hukukun eksikliklerine, benzetme yoluyla siber uzayın özelliklerine uyum sağlamak için cevap vermek zorundayken, bu ilkeler, uluslararası insancıl hukukun uygulamasını önemli ölçüde kısıtlaması yanı sıra uluslararası insancıl hukuku da yetersiz kılan bu yorumlama yöntemiyle eşit derecede yetersiz kalmaktadır.

---

420 N. LUBELL, “Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?”, in *International Law Studies*, vol. 89, no. 1, 2013, s. 272.
421 M. N. SCHMITT, 2013, s.113-114
422 M. N. SCHMITT, 2014, s.298
423 M. N. SCHMITT, 2014, s.297

Aslında, orantılılık ve ihtiyati tedbir ilkeleri, siber uzaydaki sistemlerin birbirine bağlılığı ve siber yeteneklerin yayılma kabiliyetinin belirsizliği ile ilgilenmelidir. İnsancıl hukuka saygı göstermek, savaşın araçları ve yöntemleri olsa da, siber saldırıların yalnızca küçük bir bölümünü düzenlemektedir. Bu nedenle, daha yıkıcı siber saldırılar, bu kurallara uymamaları nedeniyle hariç tutulacak olsa da, diğer siber kapasite kullanım biçimlerinin çoğu, sivil nüfusu önemli ölçüde etkileyebilmelerine rağmen, insancıl hukuk kapsamına girmeyecektir. O zaman, sivillerin korunmasını sağlamak için genişletilmesi gerektiğinde, analojinin kısıtlayıcı vizyonu nedeniyle orantılılık dengesinin hesaplanması zorlaşacaktır.

Bu nedenle jus in bello, ilkeleriyle çelişen bir yetersizlik durumunda, herhangi bir siber saldırıyı yasaklamanın pek gerçekçi olmayacağı göz önünde bulundurularak, harfine ve ruhuna saygının sağlanması için evrim geçirmeli[424]; gerçekten de, insanlık ilkeleri ile zorunluluk arasında bir denge kurmalıdır. Bu nedenle, ne çok kısıtlayıcı ne de çok izin verici olabilmektedir. Ancak, mevcut yetersizliğini düzeltmek için uluslararası insancıl hukuku gözden geçirmek mi yoksa uluslararası insancıl hukuku geliştirmek mi gereklidir?

1. Analojinin Kısıtlayıcı Görüşü Karşısında Orantılılık İlkesi

Bazıları için orantılılık ilkesi, askeri gereklilik lehine verilen tavizlerden kaynaklanırken, "öldürme veya yok etme izni" anlamına gelmemektedir.[425] Gerçekten de, sivil kayıplar kabul edilecekse eğer, bu durum tesadüfi olmalı ve beklenen askeri avantajla orantısız olmamalıdır[426] ve operasyonlar, geniş anlamda, ihtiyati tedbirleri içermelidir.[427] Bir taviz olarak değil, bir güvence olarak görülen Prof. Schmitt, bu ilkenin sivilleri siber

424 K. EICHENSEHR, “Cyberwar & International Law Step Zero”, in *Texas International Law Journal*, vol. 50, no. 2, 2015, s. 376.
425 J. D’ASPREMONT and J. DE HEMPTINNE, 2010, s.269
426 1949 Cenevre Sözleşmelerine Ek 1977 tarihli I. Protokolün 54. Maddesi
427 1949 Cenevre Sözleşmelerine Ek 1977 tarihli I. Protokolün 57. Maddesi

saldırıların tesadüfi etkilerine, özellikle de çift kullanımlı altyapılara karşı korumanın bir yolu olduğunu düşünmektedir.[428]

Tartışmalı olmakla birlikte, Ek Protokol I'den bu yana bu ilke, sivil nüfusun korunmasına ilişkin karmaşık sistemin temel düğümlerinden biri olmuştur.[429] Sonucun amacı, askeri gereklilik ve insanlık ilkesini temsil eden sorgulamaksızın çelişkili çıkarların dengelenmesini gerektirmektedir.[430] Görüldüğü gibi, bu hesaplama, çatışmaların evrimine ve kullanılan araç ve yöntemlere uyarlanabilir ise de, uluslararası insancıl hukukun siber operasyonlara uygulanmasında bir araç olarak analojinin yetersizliği nedeniyle bu durum gittikçe zorlaşmaktadır.

Gerçekten de benzetme, uluslararası insancıl hukuku fiziksel bir mantıkta dondururken, siber uzay soyut olan tarafından işaretlenmektedir. Saldırının katı vizyonunun sonuçları, bu hesaplamanın yalnızca bir siber saldırının fiziksel etkilerini içerebileceği şeklinde hissedilmektedir, ancak bu inceleme, genellikle siber yeteneklerin kullanılması durumunda en önemlisi düşünülen dolaylı etkileri göz önünde bulundurarak geniş bir şekilde takdir edilmektedir.[431] Bununla birlikte, pratikte gösterildiği gibi siber saldırıların gizli etkileri ve önemli bir yayılma kapasitesi bulunmaktadır. Dolayısıyla geç etkiler karşısında ihtiyata saygı gösterilmesi ve orantılılık garantisinin sağlanması ve bu yeteneğin sınırları aşarak diğer sistemlere yayılması kolay olmamaktadır.

Ayrıca, sadece etkilere değil, aynı zamanda etkilenen şeyin niteliğine de bağlı olduklarından, her tür dolaylı sonuç dikkate alınmamaktadır. Siber saldırılar öncelikle mülkiyeti etkiler, ancak ilgili şeyin bu şekilde nitelendirilmesi gerekir. Bu kategorinin

428 M. N. SCHMITT, 2014, s. 297.
429 M. A. NEWTON, "Proportionality and Precautions in Cyber Attacks", in D. SAXON (ed.), *International Humanitarian Law and the Changing Technology of War*, 2013, s. 241.
430 J. D'ASPREMONT ve J. DE HEMPTINNE, 2010, ss.258-259
431 M. A. NEWTON, 2013, s.246

sınırları, fiziksel özellikler kadar önemli olan ve zararları bireyler için gerçek sonuçlar doğuran somut olmayan bir veri kümesini korumakta yetersiz kaldığı için sorgulanmaktadır.[432]

Bu nedenle, benzetme çok kısıtlayıcıysa ve düşmanlıkların yürütülmesi ilkelerinin sağladığı koruma sistemini yetersiz kılıyorsa, yıkıcı siber silahların gerçekte uluslararası insancıl hukuka saygı duyma yeteneğine sahip olduğunu düşünmek zordur. Bir yanda, yine de sivil nüfusu etkileyen ve uluslararası insancıl hukuk tarafından çerçevelenmeyen, öldürücü olmayan siber kapasiteler ve diğer yanda buna a priori olarak saygı duymaktan aciz olan yıkıcı siber kapasiteler vardır. Uluslararası insancıl hukuk, bu yetersizlik durumunda, gerçekçi olamamakla kendini bir felç halinde bulmaktadır. Bu nedenle de Uluslararası insancıl hukukun evrim geçirmesi gerekmektedir, ancak bu, bir düzeltme ihtiyacından mı kaynaklanmaktadır yoksa geliştirme ihtiyacından mı?

2. Hukukun Revizyon İhtiyacı mı yoksa Geliştirme İhtiyacı mı?

Uluslararası insancıl hukuk, fiziki harekâtların aksine kinetik harekâtların talep ettiği esneklik ihtiyacından dolayı, kavramlarının tanımlanmasında katı bir tutum benimsemesine neden olan analoji nedeniyle devletlerin siber harekâtlarını düzenlemekte yetersiz kalmaktadır. Bununla birlikte, silahlı bir çatışmada yıkıcı siber saldırılara karşı bir koruma olarak uygulanabiliyorsa, saldırının tanımı ve düşmanlıkların davranış kurallarının bu gerçekleri yansıtmasına izin vermeyen ayrım ilkesi tarafından şartlandırılmalıdır.[433]

Gerçekten de, ihtiyat ve orantılılık ilkesi, operasyonların, hatta yıkıcı olmayanların bile ekonomik hedefler üzerindeki potansiyel etkilerini göz önünde bulundurarak, sivil ve askeri mülkün kesinliği ile siber saldırıları daha iyi yönetebilmektedir. Savaş gelişmiş ve

---

432 R. GEIß, "The legal regulation of cyber-attacks in times of armed conflict", in Technological challenges to the humanitarian legal framework, 2011, s. 52.
433 J. KELSEY, 2008, s. 1447.

devletler askeri stratejilerinde düşmanı zayıflatmak[434] için başka yöntemlere yönelmişlerdir. Örneğin, ABD'nin Irak ekonomisini çökertme planı vardı.[435] Ancak, özel gruplar bu tür bir hasara yol açabileceğinden uluslararası sahnede yalnız değillerdi: "Suriye Elektronik Ordusu" grubu, 2013 yılında, hacklenen Associated Press hesabı aracılığıyla Wall Street'te basit bir Tweetle 136 milyar dolarlık zarara neden olmuştur.[436] Ancak, silahlı bir saldırı bu etkiyi paylaşabilirdi.

Sibernetik operasyonların oluşturduğu tehditler ve ölümcül olmayan kinetik etkileri karşısında fiziksel olmayan etkilerin dikkate alınması gerekiyorsa da, ekonomik hedefler için meselenin genel olarak, meydan okumanın uluslararası hukuk algısı olduğunun yanı sıra jus ad bellum gerçeği devam etmektedir. Bu nedenle, bu kavramlar jus ad bellum ile karşılaştırılacağından, bu tür gelişmeler sadece jus in bello açısından gerçekleşemez. Bu nedenle, B. Louis-Sidney gibi bazı yazarlar, jus ad bellum'un ışığında, siber saldırı ve siber meşru savunma kavramlarını tanımlamak amacıyla siber operasyonları yönetecek bir anlaşmanın kabul edilmesi gerektiğini savunmaktadırlar.[437]Bu kavramların tanımında seçilen yaklaşım, bazılarını kritik olarak değerlendiren devlet uygulamalarına yanıt vermek için savaşçıların, mülklerin ve altyapıların nasıl tanımlandığını belirtmeden önce insancıl hukuktaki saldırı kavramı için aynı olmalıdır. Ayrıca, zararlarının siviller için önemli bir zarar olduğu ve onları tehlikeye atacağı düşünülen belirli çift kullanımlı mülklere yönelik saldırıların ve siber operasyonlar durumunda sorumluluk kurallarının özel olarak

---

434 M. C. Libicki, Conquest in Cyberspace: National Security and Information Warfare, Cambridge University Press, 2007, s. 291-292

435 N. LUBELL, 2011, s. 42
436 I. KILOVATY, 2014, s. 124
437 B. LOUIS-SIDNEY, "La dimension juridique du cyberespace", in *La Revue Internationale et Stratégique*, no. 87, 2012, s. 77.

yasaklanması da gerekmektedir.[438] Devletlerin ihtiyaçlarını karşılayan, gerçekçi ve herkese uygulanabilir bir hukuk elde etmek için savunulan amaç, açıklıktır[439], çünkü M. Sassoli'nin bize hatırlattığı gibi, hukuk sadece tek bir tarafa uygulanabilirse anlamını kaybedecektir.[440]

Bununla birlikte, artan uygulamaya ve kesin düzenleme ihtiyacına rağmen, 1997 Ottawa Sözleşmesi gibi katı uluslararası insancıl hukukun ötesine geçen bir antlaşma hipotezi böyle bir bağlamda zor olmaya devam etmektedir. Bazıları için bu geleneksel olasılık, silahları mevcut uygulamaya kıyasla düşüntülü etkilerle sınırlayacağı için de gereksizdir.[441] Bu nedenle, bu, J. Kelsey için, bir kodlamaya varmadan önce standartları revize etmek ya da belirli bir açıdan geliştirmek yerine, standartları onların yorumlarıyla evrimleştirmek meselesidir.[442]Bununla birlikte, bu yöntem, uluslararası insancıl hukukun bükülme olasılığı ile uyarlanabilirliğin sınırlarını sunmaktadır ve tersine, benzetme durumunu dondurur ve bunun sonucunda insancıl hukuk ilkelerinin yetersiz kalması, söz konusu Devletlerin yararına olabilir ki bunlar sivillere daha az ciddi zarar verme potansiyeline sahipken, denetlenmektedir.

Ancak insancıl hukuk, yeterli ve fiziksel durumlara uyum sağlama yeteneğine sahip olduğundan düzeltme gerektirmemektedir. Siber uzayın özellikleri, onun temelini ve kurallarını değil, benzetme yoluyla ele alınmasını sorgular. Bu nedenle, Birleşmiş Milletler ve Devletler içindeki mevcut tartışmaların sonucu olacak siber operasyonlara uygulanabilir

438 S. J. SHACKELFORD, 2009, ss. 250-251
439 Stephen Moore, Cyber Attacks and the Beginnings of an International Cyber Treaty, 39 N.C. J. Int'l L. & Com. Reg. 223, 2013, s.231. http://scholarship.law.unc.edu/ncilj/vol39/iss1/7 E.T 10 Temmuz 2021
440 M. SASSOLI, "How will technological development challenge IHL in the 21st century?", In Technological challenges to the humanitarian legal framework, 2011, s. 101.
441 J. KELSEY, 2008, ss. 1449-1450.
442 J. KELSEY, 2008, s.1450.

uluslararası insancıl hukukun evrimi yoluyla gelişme gereklidir, hepsi bu yeni silahların potansiyel tehlikelerinin ve bunların iki yönlü etkilerinin farkındadır.

C. GENEL DEĞERLENDİRME

Uluslararası insancıl hukuk, devletlerin karşılaştığı tüm zorluklara ve onların "savaş" olarak nitelendirilmesine uyum sağlamayı amaçlamasa da, uyarlanabilirliği başka bir sınırla karşı karşıyadır. Gerçekten de jus in bello, yazarları tarafından öngörülemeyen durumlara uyum sağlayacak araçlara sahipken, mantığı tek bir sabite dayanmaktadır: Çatışmaların ve saldırıların fiziksel boyutu. Bununla birlikte, bilgi ve iletişim teknolojilerinin gelişimi, başka bir alanın yaratılmasına yol açmaktadır: Sanallığın hâkim olduğu siber uzay ve olası fiziksel sonuçların yokluğu.

Devletler bu alanda ifade edilen tehditlere tepki gösterme ihtiyaçlarını ifade ederken, uluslararası hukuk hala onu düzenlemek için mücadele etmekte ve paradoksal olarak, bükülme yapmamak için uluslararası insancıl hukukun analojik yorumu benimsenirken, onunla çelişmektedir çünkü fiziksel etkiler için kısıtlayıcı olmaya devam etmektedir. Siber uzay tüm bunlara karşı bir "hukuki boşluk"[443] yaşamamakla birlikte, kendine özgü özellikleri, sibernetik konusunda gelişmeye çağrılan uluslararası insancıl hukuk ilkeleriyle çelişmekte ve yetersiz kalmaktadır.

Sonuç olarak, uluslararası insancıl hukukun uyarlanabilirliği, ya onları yönetmeyi amaçlamadığı için ya da geleneksel yöntemleriyle kendi paradoksal çelişkisine varmadan uygulanamadığı için durumları yönetme yetersizliği karşısında sınırlarını ortaya koymaktadır. Huluk, netlik ve sabitlik ile eş anlamlı olsa da, kesin olarak belirlenmiş

443 R. GEIß, "Cyber Warfare: Implications for Non-international Armed Conflicts", in *International Law Studies*, vol. 89, no. 1, 2013, s. 645.

değildir ve şu an için jus in bello'nun yetersiz olduğu bu durumlara uyum sağlamak için evrimleşmesi gerekebilir. Bununla birlikte, uyarlanabilirliğinin sınırlarının gösterdiği gibi, kendi başına getirilecek bir cevap değildir. Gerçekten de uluslararası hukuk, bazen paralel uygulamalarla birlikte var olan birkaç daldan oluşan karmaşık bir rejimdir ve yalnızca bunların tutarlı evrimi, uluslararası toplumun karşı karşıya olduğu zorlukların gerçeklerini yansıtmak için yeterli bir yanıt sağlayabilecektir.

SONUÇ

Bu tez, merkezi noktaları jus ad bellum ve jus in bello olmak üzere uluslararası hukukun siber uzaya genel olarak uygulanabilirliğini tartıştı. İlk bölüm siber uzayı çevreleyen farklı terimleri tartıştı. Burada siber uzay, siber güvenlik, siber saldırılar gibi terimler tanımlanmış ve tartışılmıştır. Ayrıca, uluslararası hukukun siber uzaya uygulanabilirliği ve internetin yönetimini çevreleyen sorunlar hakkında genel bir görüş tartışıldı. İkinci bölümde, siber operasyonun hangi aşamada olduğuna bağlı olarak bir siber operasyonun düşmanca bir eylem veya niyet olarak değerlendirilip değerlendirilemeyeceğini belirleme kriterleri incelenmiştir. Bunu belirlemek için, siber operasyonlara uygulayarak herhangi bir eylemi düşmanca olarak nitelendirmek için askeri dünyada kullanılan farklı yaklaşımları ziyaret ettik. Buradaki en önemli konu siber atıftı çünkü bir eylem bir aktöre atfedildiğinde uygun bir yanıt oluşturulabilir. Bu olası tepkiler arasında karşı önlemler ve güç kullanımı merkezi bir yer tutar. Son bölüm, uluslararası insancıl hukukun, uygulamalarının önündeki farklı engellerin incelendiği siber uzaya uygulanabilirliğini incelemiştir.

"Ebedi güncellik"[444] konusu, yalnızca uluslararası hukukun nasıl uyum sağladığı değil, aynı zamanda uluslararası hukukun, uluslararası sahnedeki gelişmelere uyum sağlayıp sağlayamayacağı sorusudur. Hukuk her zaman bunların gerisinde mi kalmaktadır? Her yeni durum için yeni yasal rejimler mi geliştirilmelidir? Bir yasal rejim için, kendi gerçeklerini yansıtmak adına uluslararası toplumun ihtiyaçlarına uyum sağlama yeteneğinin sorgulanması, uluslararası insancıl hukuk açısından belirli bir önem kazanır, kuralları *"buna saygının yıkıntıları... Silahlı kuvvet kullanımının yasaklanması olan jus cogens kurallarıdır*".[445] Uluslararası insancıl hukuk, silahlı çatışmalardan etkilenen herkese nihai koruma sağlamayı amaçlamaktadır. Çoğu zaman olayların üstesinden geldiği, savaşın dehşeti karşısında inşa edilmiş bir tepki hakkı olarak düşünülen bu hak, gerçekte "gerçekleştirilen deneyimler ile dikkatle değerlendirilen beklentiler arasında makul bir uzlaşma"dır.[446] İlan edilmiş bir savaş kanunundan, doğası gereği tüm silahlı çatışmaların evrensel kanunu haline gelmiştir.

Ancak yine de silahlı çatışmalar ve bileşenlerindeki gelişmelere uyum sağlayabilmesi gerekmektedir. Hukukun işlevi ihtiyaçları karşılamaksa, durumlara açıklık getirmek için tutarlılıkla da eş anlamlı olmalıdır. Yanıtın ilk unsuru, uluslararası insancıl hukukun uyarlanabilirliğinin, çağdaş çatışmaların evrimlerini ve aynı zamanda aktörleri ve kullanılan araçlar ve yöntemler açısından fizyonomisi açısından çerçevelemesine izin vermesidir. Tek uyarlama aracı olarak geleneksel hukuk kaynakları teorisi, uluslararası

---

444 Pellet, Alain, "*L'adaptation du droit international aux besoins changeants de la société internationale Conférence inaugurale, session de droit international public*, 2007 (Volume 329)", p.14 in : Collected Courses of the Hague Academy of International Law. http://dx.doi.org/10.1163/1875-8096_pplrdc_A9789004166196_01 E.T 21 Temmuz 2021

445 E. DAVID, *Principes de droit des conflits armés*, Bruxelles, Bruylant, 3rd Ed., 2002, s.100

446 J. PICTET, *La formation du droit international humanitaire*, IRRC-June 2002, Vol. 84 No 846, s.331

toplumda, uluslararası hukukta ve daha ziyade uluslararası insancıl hukuktaki hızlı değişimler karşısında yavaş görünüyorsa, hâkimler ve uluslararası kuruluşlar gibi etkili ve hızlı bağdaştırıcıların müdahalesi tıkanıklıklarla karşı karşıyadır.[447] S. Darcy, Tadić içtihatının "uluslararası insancıl hukukun adli gelişiminin zirvesi"[448] olduğunu düşünürken, T. Meron ise bu yasanın 1994'ten Nürnberg davalarından sonraki yarım yüzyıldan bu yana çok daha gelişmiş olduğunu düşünmektedir.[449]

Bununla birlikte, uluslararası insancıl hukukun uyarlanabilirliğinin temellerini zenginleştiren bu bağdaştırıcılar, özellikle gelenekleri değiştirerek geleneksel kurallardan kurtulmak için özelliklerini tartışmışlardır.[450] Bununla birlikte, bu esnemeler, sonuç olarak devlet direnişi yaratan bir meşruiyet kaybına yol açmaktadır. Devletlerin tekeli aşınıyor olsa da, uluslararası toplum ademi merkeziyetçi ve egemenlik kavramı üzerine kurulu olmaya devam etmektedir. Bu nedenle, devletler, birbirine bağlı bu dünyada, artan güvenlik sorunları karşısında kendilerine daha fazla özgürlük tanımak için gerçek bir yüksek otoritenin yokluğunun da yardımıyla uluslararası insancıl hukuku yeniden benimsemişlerdir.

Dolayısıyla terörle mücadele örneği, uluslararası insancıl hukukun uyarlanabilirliğinin sınırlarını göstermektedir. Nitekim bu yasal rejim, bu gerçekleri yansıtmada yetersiz kalırken, Devletlerin onu uygulamak için yaptıkları çarpıtmalar, çarpıtma yoluyla kendi çelişkisine yol açarak ihlale yol açmıştır. Bu sınıra, daha sonra bir soru eklenmektedir: Hukuk, uyarlanabilirliğinin sınırları göz önüne alındığında, istendiğinde esnek olamıyorsa, yine de ona saygı gösterilmelidir.

---

447 Pellet, Alain, 2007, s.21

448 S. DARCY, *Judges, Law and War : The Judicial Development of International Humanitarian Law*, Cambridge, Cambridge University Press, 2014, s. 334.

449 T. MERON, The Hague Tribunal: Working to Clarify International Humanitarian Law, in: American University International Law Review, vol. 13, no. 6, 1998, s.1154

450 J. D'ASPREMONT ve J. DE HEMPTINNE, 2012, s.482

Bununla birlikte, uluslararası insan hakları hukukunun genel rejiminin aksine, şu anda uluslararası insancıl hukuk, teröre karşı küresel mücadeleyi çerçevelemek için yetersizse de, bu kesin değildir. Aksine, bu durum, Devletler tarafından yeterli hale getirilmek üzere uyarlanacak olan jus in bello'yu değiştirmeyecektir. Bununla birlikte, bu uyarlama, geleneksel uluslararası insancıl hukukun gözden geçirilmesi yoluyla değil, yalnızca terörizmi düzenlemeyi amaçlayan uluslararası hukukun çok sektörlü bir gelişiminden geçebilmektedir. Mevcut bağlam kesin olarak belirlenmemiştir ve insancıl hukuk sürekli olarak uyarlanabilirliğinin ötesinde gelişmeye çağrılmaktadır.

Gerçekten de, değişime uyum sağlama becerisine sahip olsa da, siber uzayın ve sanallığının getirdiği yeni bir dizi zorluğu yönetmek için yetersiz kalmaktadır. Ancak bu yeni alanda yasal bir boşluk yoksa analoji, uluslararası hukukun farklı dallarını siber uzayın gerçeklerini yansıtmak için yeterli kılmayacaktır. Özellikle, sivil nüfusu büyük ölçüde etkileyen operasyonları denetlemeyi mümkün kılmadığı için bu yorumlama yöntemiyle kendisiyle çelişen, uluslararası insancıl hukuk olmaktadır. Bununla birlikte bu uygulama, siber operasyonların zararlı potansiyellerinde ihtiyatlı bir şekilde kullanıldığını göstermektedir.

Sonuç olarak, uyarlanabilirliği çağdaş silahlı çatışmalardaki gelişmelere yanıt vermesine izin verdiği için uluslararası insancıl hukukun gözden geçirilmesi gerekli değildir. Bununla birlikte, özellikle terör bağlamında, aynı zamanda Devletleri ve uluslararası örgütleri aşan yansımaları ile siber uzay ve onun zorlukları karşısında, geleneksel, çok sektörlü bir yaklaşım mümkün olmaya devam etmektedir. Uluslararası insancıl hukukun uyarlanabilirliğinin bir sınırı olarak yetersizlik, uluslararası kamu hukukunun yanıt verme kapasitesini etkilemez, çünkü ikincisi, bu durumlarda birbirini tamamlamaya çağrılan birkaç paralel daldan oluşan karmaşık bir rejimdir.

Bununla birlikte, hem siber teknolojinin hem de kullanımına ilişkin ulusal yasal çerçevelerin gelişmekte olduğu göz önüne alındığında, uluslararası konferansların, çalıştayların ve uzman toplantılarının olağan sürecinin, sınıflandırılmış ulusal anlayışlar ile bir yanda uygulayıcılar, diğer yanda kamusal bilimsel yorumlar ve onların savunucuların arasındaki uçurumu daraltmada verimli olması pek olası değildir. İhtiyaç duyulan şey, komutanlar, operatörler ve hukukçular dâhil olmak üzere ulusal siber güvenlik personelinin siber durum eğitim tatbikatlarında akademisyenler ve uluslararası ve sivil toplum kuruluşlarının temsilcileri ile birlikte çalışacağı ortak bir deneyimsel yaklaşımdır. Bu senaryoların amacı, belirli siber strateji ve taktiklerin başarılı olup olmayacağını test etmek olmayacak olup, daha ziyade, belirli yasal yorumların savunucularını, bu yorumları gelişen simülasyonlara uygulamak zorunda kalacakları bir konuma yerleştirecektir. Simülasyonlar aracılığıyla çalışan farklı grupların sonuçları daha sonra katılımcılar tarafından analiz edilebilir ve toplu olarak karşılaştırılabilir ve bu, siber operasyonlara yasal girdilerin gerçekte nasıl sonuçlanabileceği konusunda herkesin daha çok takdirine yol açabilir. Aksi takdirde, IHL'nin siber çatışmalardaki uygulamasına ilişkin sınıflandırılmış anlayışlar ile bunların kamu alanındaki muadilleri arasındaki farklılık, muhtemelen yalnızca siber uzay müşterekleri kavramının doğasında bulunan demokratik değerleri savunmanın zararına olacak şekilde genişleyecektir.

Bugün, ülkeler arasında düzenli olarak siber saldırılar gerçekleştirilmektedir, ancak ilgili ülkeler bu tür eylemlerin uluslararası hukuka göre yasallığını mutlaka netleştirmiş olmayabilir. Böyle bir durumun arka planında, silahlı saldırı teşkil etmeyen siber operasyonlarla ilgili uluslararası yasaları açıkça ortaya koyan Tallinn Kılavuzu 2.0'ın belirli bir ölçüde fayda sağladığı kabul edilmektedir. Öte yandan hem Tallinn Kılavuzu hem de Tallinn El Kılavuzu 2.0'ın yasa yapıcı açıklamalar ve çözülmemiş çekişme noktaları

içerdiğini belirtmek önemlidir. Ayrıca, uzmanlar tarafından çoğunluk görüşü olarak sunulan içerikler için bile Kılavuzların mekanik uygulamasından dikkatle kaçınılmaktadır. Bununla birlikte, tartıştığımız gibi bu kılavuz sadece analoji altında oluşturulmuş bir çalışmadır ve analojinin siber operasyonların tüm zor yönlerini kapsamakta nasıl başarısız olduğunu gösterdik. Siber uzayı düzenleyen hukuk her zaman dinamik olmalı ve yeni teknolojileri yakalamak için tekrar gözden geçirilmelidir.

KAYNAKÇA

KİTAPLAR

CHANG, Amy, **Warring State China's Cybersecurity Strategy**, Center For A New American Security, 2014.

CHONG, Alan, "China and Southeast Asia: Offline Information Penetration and Suspicions of Online Hacking – Strategic Implications from a Singaporean Perspective", In VENTRE, Daniel (ed.), **Chinese Cybersecurity and Defence,** Wiley, 2014

Davies, Simon (ed.), "A Crisis of Accountability", **A global analysis of the impact of the Snowden revelations**, The Privacy Surgeon, June 2014.

DELACROIX, Sylvie, **Legal norms and normativity: an essay in genealogy**, Bloomsbury Publishing, London, 2006.

DODGE, Martin & KITCHIN, Rob, **Atlas of Cyberspace**, Pearson Education, London, 2001

DUBUISSON, François, "Vers un renforcement des obligations de diligence en matière de lutte contre le terrorisme ?", In BANNELIER, Karine et al. (eds), **Le droit international face au terrorisme**, Paris, Pedone, 2002

FAIRCLOTH, Jeremy(ed.), (2014), **Enterprise Applications Administration**, Morgan Kaufmann,.

FELLMETH, Aaron. X. & HORWITZ, Maurice, **Guide to Latin in International Law**, Oxford University Press, 2009

GARNETT, Richard & CLARKE, Paul, "Cyberterrorism: a new challenge for international law", in Andrea Bianchi (ed), **Enforcing International Law Norms against Terrorism**, Hart Oxford, 2004.

Goldsmith, Jack & Wu, Tim, **Who Controls the Internet?: Illusions of a Borderless World**, Oxford University Press, 2006

KAPLAN, J. M. Et al. (ed.), (2015), **Beyond Cybersecurity: Protecting your Digital Business**, Hoboken, NJ: Wiley.

KATSH, Ethan, **The Electronic Media and the Transformation of Law**, Oxford University Press, New York, 1989

KEMPF, Olivier, **Introduction à la cyberstratégie,** Economica, Paris, 2012

KRAMER, F. D., STARR, S. H. & WENTZ, L. K. (Ed.)., (2009), **Cyberpower and national Security**, 1st ed. Washington, D.C: National Defense University Press: Potomac Books.

KURLANTZICK, Joshua, Charm **Offensive: How China's Soft Power Is Transforming the World**, Yale University Press, Connecticut, 2007.

LACOSTE, Yves, ***De la* géopolitique aux paysages**, *Dictionnaire de la géographie*, Armand Colin. Paris, 2003

LENOBLE, Jacques & OST, François, Droit**, mythe et raison : essai sur la dérive mythologique de la rationalité juridique**, Saint-Louis Üniversitesi Yayınları, Brüksel, 1980

Libicki, Martin C., **Conquest in Cyberspace: National Security and Information Warfare**, Cambridge University Press, 2007

LING, Yin, "Human Interactions in Physical and Virtual Spaces: A Gis-Based Time-Geographic Exploratory Approach. " **Doktora Tezi**, University of Tennessee, 2011.

LIPPERT, Barbara & PERTHES, Volker (eds.)., **Strategic Rivalry between United States and China: Causes, Trajectories, and Implications for Europe**, SWP Research Paper 2020/RP, 2020.

LIU, Lu & PAN, Yu, "Review of 20 Years of Internet Development in China", In XIE, Yungeng (eds), **New Media and China's Social Development**, Research Series on the Chinese Dream and China's Development Path, Springer, Singapore, 2017

McNeilly, Marc, **Sun Tzu and the Art of Modern Warfare**, Oxford University Press, 2001

MESSIER, Ric, **Collaboration with Cloud Computing: Security, Social Media, and Unified Communication**, Syngress Publication, Massachusetts, 2014

MURRAY, Andrew, **The Regulation of Cyberspace: Control in the Online Environment**, Routledge-Cavendish, 2007

Pufeng, Wang, "The Challenge of Information Warfare", in PILLSBURY, Michael (ed)., **Chinese View of Future Warfare**, National Defense University Press, Washington DC, 1998.

SCHMITT, Michael N. (ed.)., (2013), **Tallinn Manual on the International Law Applicable to Cyber Warfare,** Cambridge: Cambridge University Press.

Thompson, Mueller, M. D., "ICANN and INTELSAT: Global Communication Technologies and their Incorporation into International Regimes", In: Braman, S. (eds) **The Emergent Global Information Policy Regime. International Political Economy Series**, Palgrave Macmillan, London. 2004

TURNER, Fred, **From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism**, University of Chicago Press, Chicago, 2010

WEBER, Max, The ***Protestant Ethic and the Spirit of Capitalism***, Dover Publications, 2003

YOSHIHARA, Toshi, Chinese **Information Warfare: A Phantom Menace or Emerging Threat?,** The Strategic Studies Institute, 2001.

MAKALELER

BAYLIS, John, ‘’Uluslararası İlişkilerde Güvenlik Kavramı’’, **Uluslararası İlişkiler**, Cilt 5, Sayı 18, Yaz 2008, s. 69 - 85 Makalenin ingilizceden Türkçeye tercümesi Burcu Yavuz tarafından yapılmıştır. Orijinal metin için bkz. Brauch et. al., Globalization and Environmental Challanges, s. 495-502

BENVENISTI, Eyal, “Substituting International Law?”, **American Society of International Law**, cilt. 100, 2006, s. 289-290.

CHEN, Wenji, LIU, Yang ve GUAN, Yong, "Cardinality change-based early detection of large-scale cyber-attacks," 2013 **Proceedings IEEE INFOCOM**, Turin, 2013, ss. 1788-1796.

COLARIK, Andrew. M & JANCZEWSKI, Lench, “Establishing Cyber Warfare Doctrine”, Journal **of Strategic Security,** Cilt.5, no. 1 (2012), s.31-48

DÖNMEZ, Suat., “Kuvvet Kullanma Kapsamında Ön alıcı ve Önleyici Saldırı kavramları”,

Balkan and Near Eastern Journal of Social Sciences, 8-15, 2017: 03 (03)

FARHAT, Vince Et al., “Cyber Attacks: Prevention and Proactive Responses”, **Practical Law Publishing Limited and Practical law Company**, 2011, s. 1-12.

FRAVEL, M. Taylor, China’s New Military Strategy: “Winning Informationized Local Wars”, **China Brief**, cilt 15 sayı: 13, 2 Temmuz 2015, s.3-7

FURNELL, Steven & WARREN, Matthew John, “Computer hacking and cyber terrorism: the real threats in the new millennium?”, **Computers & Security**, Volume 18, Issue 1, 1999, s. 28-34.

GEERS, Kenneth, “The Cyber Threat to National Critical Infrastructures: Beyond Theory,” **Information Security Journal: A Global Perspective**, sayı. 18, 2009, s.1–7,

GEISS, Robin & LAHMANN, Henning, “Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention”, in Ziolkowski, Katharina (ed.), **Peacetime Regime for State Activities in Cyberspace**, International Law, International Relations and Diplomacy, Tallinn 2013, s.625-657.

GUILLAUME, Gilbert, “Terrorism and international law”, **International and Comparative Law Quarterly**, 2004, 53(3), s.537-548

Güntay, Vahit, "SİBER UZAY VE GÜVENLİK POLİTİKASI ÜZERİNE TEORİK BİR YAKLAŞIM", ***Cyberpolitik Journal***, vol. 2, no. 4, ss. 9-21, Jan. 2018

HALATÇI ULUSOY, Ülkü, "Uluslararası Hukuk Açısından Libya ve Suriye Örneğinde, Koruma Sorumluluğu", **TAAD**, Yıl 4, Sayı 14, Temmuz 2013, ss. 269-297

HEBERT, Robert, "Christian Atias, Savoir des juges et savoir des juristes. Mes premiers regards sur la culture juridique québécoise, Montréal, Centre de recherche en droit privé et comparé du Québec, 1990". **Philosophiques,** sayı: 19, no.1, 1992, s. 123-129.

HARDY, I. Trotter, "The Proper Legal Regime for "Cyberspace", **University of Pittsburgh Law Review**, no.55, 1994, s. 993-1055

HOFMANN, Jeannette; KATZENBACH, Christian ve GOLLATZ, Kristen "Between coordination and regulation: Finding the governance in Internet governance", **New media & society**, ISSN 1461-7315, Sage, Thousand Oaks, CA, Vol. 19, Iss. 9, 2017, s. 1406-1423.

HOLLIS, Duncan. B., "Why states need an international law for information operations", **Lewis & Clark Law Review**, cilt. 11, 2007, s. 1023-1061

Hunter, Dan, "Cyberspace as Place and the Tragedy of the Digital Anticommons", 91 **California Law Review**, No. 2, 2003, s.439-519

KASTNER, Scott. L. "The Global Implications of China's Rise**", International Studies Review**, cilt. 10, sayı. 4 (Aralık., 2008), s. 786-794.

KEMPF, Olivier, "Le cyberterrorisme : un discours plus qu'une réalité " **Hérodote**, cilt. 152-153, no 1, 2014, s. 82-97

KENDALL, Joel; BARRON, Pamela & ALLENBAUGH, Mark H., "The diligence due in the era of globalized terrorism", **The International Lawyer**, 2002, vol. 36, s. 49-66.

Korhan, Sevda, "SİBER UZAYDA AKTÖR- GÜÇ İLİŞKİSİ", ***Cyberpolitik Journal***, vol. 2, no. 4, pp. 75-104, Ocak. 2018

KOVALEVA, Natalya, "Russian Information Space, Russian Scholarship, and Kremlin Controls", **Defence Strategic Communications**, sayı:4, 2018, s.133-172

KOZLOWSKI, Andrzej, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan", **European Scientific Journal**, 3. sayı, 2014, s. 237-245

LOPEZ- JACOISTE, Eugenia, 'The UN Collective Security System and its Relationship with Economic Sanctions and Human Rights' (2010), 14 **Max Planck UNYB,** s. 302

LYSENKO**, Volodymyr** & BROOKS, **Catherine** **"**Russian information troops, disinformation", and democracy, **First Monday**, cilt 23, sayı 5 Mayıs 2018

MANNERS, Ian, "Normative Power Europe: A Contradiction in Terms?", **Journal of Common Market Studies** 70, no. 2, 2002, s.235-258

MAZZESCHI, Ricardo Pisillo, "The Due Diligence Rule and the Nature of the International Responsibility of States", **35. The German Yearbook of International Law**, 9 (1992), ss. 31- 36.

METAXAS, Panagiotis Takis, "Network Manipulation (with application to Political issues)", **Wellesley College,** 2011, p.1-3.

NELSON, Nell, "The Impact of Dragonfly Malware on Industrial Control Systems", **SANS Institute**, 2016, p.1-27.

NEWHOUSE, W. Et al., (2017), ***NICE Cybersecurity Workforce Framework***, NIST Special Publication 800-181.

NÚÑEZ, Jorge Emilio, "About the Impossibility of Absolute State Sovereignty", **International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique,** Springer Netherlands, 1 Aralık 2014, Cilt. 27, Sayı 4, s. 645-664.

OTTIS, Rain, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", **Cooperative Cyber Defence Centre of Excellence**, Tallin, Estonia, 2008, p.1-6

RENARD, Thomas, "EU Cyber Partnerships: Assessing the EU cyber strategic partnership with third countries in cyber domain", **European Politic and Society**, 2018, s. 1-19

SHAKARIAN, Paulo; SHAKARIAN, Jana & RUEF, Andrew "Cyber Attacks and Public Embarrassment: A Survey of Some Notable Hacks" **Introduction to Cyber Warfare:** ***A Multidisciplinary Approach,*** Syngress; 1. baskı, *2013*, s.1-28.

SCHMITT, Michael N & WATTS, Sean, "Beyond State-Centrism: International Law and Non-State Actors in Cyberspace", **Journal of Conflict & Security Law**, cilt. 21, no 3, 2016, s. 595-611.

SOLAN, M. Laurence & GALES, Tammy, "Finding Ordinary Meaning in Law: The Judge, the Dictionary or the Corpus?", **The International Journal of Legal Discourse**, Forthcoming Brooklyn Law School, Legal Studies Paper No. 474, 10 Ekim 2016, p. 2-19.

STADNIK, Ilona, "Internet Governance in Russia – Sovereign Basics for Independent Runet", **TPRC47 Working Paper**, 2019https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421984 (02.07.2020).

TIKK-RINGAS, Eneken, "International Cyber Norms Dialogue as an Exercise of Normative Power", **Upcoming in Georgetown Journal of International Affairs**, 2017

TOURNIER, Jacques, "Les Deux Phases De La Cyberguerre*",* **Annuaire Français de Relations Internationales** Vol. XVII, Université Panthéon-Assas Centre Thucydide, 2016, s.643-644.

TRUDEL, Pierre, "Les effets juridiques de l'autoréglementation", **Revue de droit de l'université de Sherbrooke**, no 19, (1989), s. 251-286

WINNER, Langdon. "Do Artifacts Have Politics?" ***Daedalus,*** **Sayı:**109, no. 1 (1980), s.121-36.

WINNEFELD JR, A. James; KIRCHHOFF, Christopher & UPTON, M. David, "Cybersecurity's Human Factor: Lessons from the Pentagon", **Harvard Business Review**, The Magazine, Eylül 2015

YAYLA, Mehmet, "Uluslararasi Hukukta Siber Saldirilara Karşi Kuvvet Kullanma" **TBB Dergisi** 2013 (107), s.199-220

YELI, Hao, "A Three-Perspective Theory of Cyber Sovereignty", **PRISM**, Sayı- 7, NO. 2, 2017, p.109-115

RAPORLAR VE DİĞER BELGELER

Armed Activities on the Territory of the Congo, , (**the Democratic Republic of the Congo v Uganda)**, Judgment, Merits, ICJ GL No 116, [2005] ICJ Rep 168, ICGJ 31 (ICJ 2005), 19th December 2005, International Court of Justice [ICJ]

Avrupa Konseyi, Siber Suçlar Hakkindaki Sözleşmesi, ETS 185 – Cybercrime (Convention), 23.XI.2001, Budapest 2001, European Treaty series no 185.

Birleşmiş Milletler Genel Kurulu Kararı 3314, https://undocs.org/en/A/RES/3314(XXIX) (12.07.2020).

Birleşmiş Milletler Genel Kurulu Kararı 73/226. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266 (10.11.2020)
Cabinet Office, "The National Security Strategy of the United Kingdom", **Security in an interdependent world**, Mart 2008.

Cabinet Office, **The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world**, Londra, 2011.

Center for Strategic and International Studies (CSIS), **Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR)**, Haziran 2012.

CHAN, Cherry, "Cybergeddon, Fiscal Crises and Natural Catastrophes", **Global Risks,** 31 Temmuz 2014.

Corfu Strait Case, **Judgment of April 9, 1949**, I.C.J. Reports 1949

CORNISH, Paul Et al., "On Cyber Warfare", **A Chatham House Report,** Kasım 2010.

Council on Foreign Relations, **Operation Aurora**, Ocak 2010'deki Raporu. https://www.cfr.org/cyber-operations/operation-aurora (20.05.2020)

Department of Defense, "Cyberspace Policy Report", **A Report to Congress Pursuant to the National Defense Authorization Act for fiscal Year 2011**, Section 934, Kasım 2011.

Department of Defense, **Strategy for Operating in Cyberspace**, Temmuz 2011

Department of States, **Quadrennial Defense Review Report**, Şubat 2010

F-Secure "Malwares analysis Report", **Regin**, 2014. https://www.f-secure.com/en/web/labs_global/whitepapers (22.05.2020)

Federal Ministry of the Interior, **Cyber-Sicherheitsstrategie für Deutschland**, Berlin, Şubat 2011

Federal Ministry of the Interior, **Cyber-Sicherheitsstrategie für Deutschland**, 9 Kasım 2016

Foreign & Commonwealth Office and The Rt Hon William Hague, **London Conference on Cyberspace: Chair's statement**, 2 Kasım 2011

General Keith B. Alexander, "Hearing to Receive Testimony on The Future of Warfare," **Alderson Reporting Company**, 2015 s. 75, https://www.armed-services.senate.gov/imo/media/doc/15-83%20-%2011-3-15.pdf (12.09.2020)

Genel Sekreter'in notu, A / 70/174, 22 Temmuz 2015 (GGE 2015).

Güvenlik Konseyi, **28 Eylül 2001 tarihli 1373 (2001) sayılı kararı**

HM Government, "Securing Britain in an Age of Uncertainty", **The Strategic Defence and Security Review,** Ekim 2010.

HM Government, **The National Cybersecurity Strategy 2016-2020**, Londra, 1 Kasım 2016.

Metin: "Obama's Remarks on Cyber-Security**",** 29 Mayıs 2009, **The New York Times** https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html E.T 29 Mayıs 2020

Organisation for Economic Co-operation and Development, **OECD internet economy outlook**, *Paris, 2012*

Organisation for Economic Co-operation and Development, ***The Seoul Declaration for the Future of the Internet Economy****, OECD* Digital Economy Papers, 2008

Public Safety Canada, **Canada's Vision for Security and Prosperity in the Digital Age**, National Cyber Security Strategy, 2018.

Public Safety Canada, **Department Performance Report 2012-2013**, Ministry of Public Safety and Emergency Preparedness, 2012.

Pulp Mills on the River Uruguay, **(Argentina v. Uruguay) Judgment**, I.C.J. Reports 2010

RAPOLD, Nicolas, "We are Legion: The Story of the Hacktivists", Brian Knappenberger tarafından yönetilen belgesel, **New York Time-Movie Review**, 18 Ekim 2012. https://www.nytimes.com/2012/10/19/movies/we-are-legion-on-computer-hacker-activists.html (20.05.2020)

The 13th Five-Year Plan for Economic and Social Development of The People's Republic of China (2016–2020).

The United-Kingdom Government-Cabinet Office, **The UK Cyber Security Strategy, Protecting and promo ting the UK in a digital world**, Londra, 2011

The White House, "Cybersecurity Funding", **Analytical Perspectives**, 2019

The White House, **International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World**, Washington, Mayıs 2011 Raporu.

The White House, **National Security Presidential Directive/Nspd-54-Homeland Security Presidential Directive/Hspd-23: Cybersecurity Policy (U),** 8 Ocak 2008.

The White House, **Presidential Decision Directive/ NSC-63: Critical Infrastructure Protection**, Washington, 22 Mayıs 1998.

UN GGE Report 2015 (A/70/174)

VERIZON - 2014 **Data breach investigations report**, 2014.

İNTERNET KAYNAKLARI

Annalee Newitz, The Bizarre Evolution of the Word "Cyber", Gizmodo, 2013,

https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487

E.T 30.06.2022

AVEY, Chester, "Historic Hacking: A Brief History of Cybersecurity", **Secure World Expo** 18 Ağustos 2019. URL: https://www.secureworldexpo.com/industry-news/historic-hacking-brief-history-cybersecurity E.T 19 Mayıs 2020.

BARLOW, John Perry**, A Declaration of the Independence of Cyberspace**, Davos, İsviçre
Şubat 8, 1996, https://www.eff.org/cyberspace-independence (25.02. 2020)

BBC News, **Ministry of Defence foiled 1,000 cyber-attacks says Fox**, 7 Haziran 2011. URL: https://www.bbc.com/news/uk-politics-13691375 (01.06.2020)

BENILLOUCHE, Jacques, **Israël a lancé une attaque électronique contre l'Iran**, 26 Eylül 2010. http://www.slate.fr/story/27763/israel-attaque-electronique-iran (03.05. 2020)

Broad, William J.; Markoff, John; ve David, E. Sanger, Haber makalesi, "**Israeli Test on Worm Called Crucial in Iran Nuclear Delay**", 15-Jan-2011, The New York Times, http://nyti.ms/esygjV (04.05.2020)

CHANDLER, Nathan, "How Anonymous Works", **HowStuffWorks,** 12 Mart 2013. https://computer.howstuffworks.com/anonymous.htm (20.05.2020)

Check Point, **What Is the Purpose of Malware**?, URL: https://www.checkpoint.com/definitions/what-is-malware/ (11.05.2020)

China to deepen international cooperation on cyber security, CCTV.com, 10 Şubat 2015, http://english.cntv.cn/2015/02/10/VIDE1423536244824155.shtml (09.06.2020)

CISCO, **Critical Infrastructure Cyberattacks a Greater Concern than Enterprise Data Breaches**, 26 March 2020, https://www.securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-concern-than-enterprise-data-breaches e.t 5 Mayıs 2020.

CLABURN, Thomas, ***Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting with Google And Elsewhere,*** Information Week, 12 Ağustos 2008, https://www.darkreading.com/attacks-and-breaches/under-cyberattack-georgia-finds-bullet-proof-hosting-with-google-and-elsewhere/d/d-id/1070892? (09.03.2020)

CLOUDFLARE, **what is DDoS attack?** https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (11 Mayıs 2020)

Cyberattack definition, "*what does cyberattack mean*?" **Techopedia.** http://www.techopedia.com/definition/24748/cyberattack , (05.05. 2020)

DATE, Jack et al., **Hackers Launch Cyberattack on Federal Labs**, ABC News, 7 Aralık 2007, http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1 (09.03.2020)

DAVIS, Joshua, **Hackers Take Down the Most Wired Country in Europe**, 21 Ağustos 2007, https://www.wired.com/2007/08/ff-estonia/ (04.11.2020)
ECPI University, **How Cyber Attacks Affect Individuals and How You can Help Keep them Safe**, *T.Y.* https://www.ecpi.edu/blog/how-cyber-attacks-affect-individuals-and-how-you-can-help-keep-them-safe erişim tarih 4 Mayıs 2020.

Editor's note, "Evolution of the Internet in China", **China Daily**, 2016 http://www.chinadaily.com.cn/china/2016even/index.html (15.09.2020)
Electronic Frontier Foundation, **State-Sponsored Malware.** URL: https://www.eff.org/issues/state-sponsored-malware (11.05.2020).
ELGIN, Ben & RILEY, Michael, **Now at the Sands Casino: An Iranian Hacker in Every Server,** Bloomberg, 12 Aralık 2014. https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas (05.05.2020)

ELLIOT, Steven, **Analysis on Defense and Cyberwarfare**, Infosec Island, 8 Temmuz 2010. http://www.infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-arfare.html (07.03.2020)

Fox News, **Hackers Declare War on Scientology,** 25 Ocak 2008. URL: http://www.foxnews.com/story/0,2933,325586,00.html (20.05.2020)

FRUHLINGER, Josh, **what is a cyber-attack? Recent examples show disturbing trends**, 27 February 2020. https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html (05.05.2020)

GILES, Martin, **Triton is the world's most murderous malware and it's spreading,** 5 Mart 2019. https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/ (05.05. 2020)
GHAHRAI, Amir, "*Confidentiality, Integrity and Availability*", **DevQA** 24 Haziran 2019. https://devqa.io/confidentiality-integrity-availability/ (05.05.2020)

Google, **A New Aprroach to China,** 12 Ocak 2010, https://googleblog.blogspot.com/2010/01/new-approach-to-china.html (20.05.2020)

GREENBERG, Andy, **The Untold Story of NotPetya, the Most Devastating Cyberattack in History,** 22 Ağustos 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, (03.05. 2020)

Hackernoon, **Are We Ever Going to Solve Cybersecurity?** 5 Şubat 2020. https://connexion3.gr/are-we-ever-going-to-solve-cyber-security/ (18.05.2020).

HATTON, Matt, "The IoT in 2030: 24 billion connected things generating $1.5 trillion", **IOT Business News**, 20 Mayıs 2020. URL:https://iotbusinessnews.com/2020/05/20/03177-the-iot-in-2030-24-billion-connected-things-generating-1-5-trillion/ (22.05.2020)

IBM, **How much would a data breach cost your business**, 2019 Cost of a Data Breach Report https://www.ibm.com/security/data-breach (20.05.2020)

ICCAN Policy, https://www.icann.org/policy#what_is_policy (6.03.2020)

IoT vs M2M, **what is the Difference?** 16 Ocak 2019. URL: https://www.avsystem.com/blog/iot-and-m2m-what-is-the-difference/ (22.05.2020)

KULIKOVA, Alexandra, "China-Russia cyber-security pact: should the U.S. be concerned?", **Russia Direct**, 21 Mayıs 2015, https://www.pircenter.org/media/content/files/13/14358794770.pdf? (09.06.2020)

LAKE, Josh, "what is a drive-by download and how can it infect your computer?", **COMPARITECH,** 13 Aralık 2019. URL: https://www.comparitech.com/blog/information-security/drive-by-download/ (11.05. 2020).

LORD, Nate, "what is an Advanced Persistent Threat? APT Definition*"*, **Data Insider**, 11 Eylül 2018. https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition (20.05.2020)

LYNN III, J. William, "Defending a New Domain the Pentagon's Cyberstrategy", **Foreign Affairs,** September/ October 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (29.05.2020)

MACASKILL, Ewen, **British army creates team of Facebook warriors**, The Guardian*, 2015.* http://www.theguardian.com/uk-news/2015/jan/31/britisharmy-facebook-warriors-77th-brigade (27.02.2020)

MARKOFF, John, "cyberattack on Google Said to Hit Password System*"*, 19 Nisan 2010, **The New York Times**. URL: https://www.nytimes.com/2010/04/20/technology/20google.html E.T. (20.05.2020)

MARKOFF, John & BARBOSA, David, "2 *China Schools Said to Be Tied to Online Attacks"*, 18 Şubat 2010, **The New York Times**. URL: https://www.nytimes.com/2010/02/19/technology/19china.html?_r=1&hp (20.05.2020)

MATTHEW, Tim, "A Brief History of Cybersecurity", **Cybersecurity Insider**, 2019. https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/ (19.05.2020)

MCGUINNESS, Damien, **How a Cyber-attack Transformed Estonia**, 27 Nisan 2017. https://www.bbc.com/news/39655415 (03.05.2020)

MESSMER, Ellen, **Cyberattack Seen as Top Threat to Zap U.S. Power Grid**, Network World, 2 Temmuz 2010. https://www.networkworld.com/article/2210851/cyberattacks-seen-as-top-threat-to-zap-u-s--power-grid.html (08.03.2020)

MINDCORE, **Types of Cybersecurity Threats and How they Will Impact your Business**, 1 Mayıs 2019, https://mind-core.com/types-of-cyber-security-threats-and-how-they-will-impact-your-business/ (10.05.2020)

MYLREA, Michael "*Brazil's Next Battlefield: Cyberspace*," **Foreign Policy Journal**, 15 Kasım 2009, https://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/ (10.03.2020)

PAMELA, Fox, "Computer malware and attacks", **Khan Academy-Online Course**, URL https://www.khanacademy.org/computing/ap-computer-science-principles/the-internet/cybercrime-and-prevention/a/computer-vulnerabilities (11.05.2020)

PAMELA, Fox, "From electricity to bits", **Khan Academy**. URL: https://www.khanacademy.org/computing/ap-computer-science-principles/computers-101/digital-data-representation/a/from-electricity-to-bits (26.05.2020)

PERLROTH, Nicole, ***In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back***, New York Times, 23 Ekim 2012, https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (03.05.2020)

PETERSON, Andrea, **The Post just got hacked by the Syrian Electronic Army. Here's who they are,** The Washington Post, 15 Ağustos 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/08/15/the-post-just-got-hacked-by-the-syrian-electronic-army-heres-who-they-are/?arc404=true (28.02. 2020)

Penta Security, **DDoS Top 6: Why Hackers Attack,** 22 July 2016. Available at https://www.pentasecurity.com/blog/ddos-top-6-hackers-attack/ (11.05.2020).

PUTMAN, Patrick, "Script Kiddie: Unskilled Amateur or Dangerous Hackers?", **United States Cybersecurity Magazine**, https://www.uscybersecurity.net/script-kiddie/ (05.05. 2020).

RADU, Sintia, "China, Russia Biggest Cyber Offenders", A new study attributes more than 200 cyberattacks to the two countries over the past 12 years, **US. News**, 1 Şubat 2019. URL: https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows (03.07.2020)

RAWLINSON, Kevin & PEACHEY, Paul, "Hackers step up war on security services", **The Independent**, 13 Nisan 2012. URL: https://archive.vn/20130629103235/http://www.highbeam.com/doc/1P2-31126850.html (20.05.2020)

Robert S. Mueller III, Director of Federal Bureau of Investigation, **RSA Cyber Security Conference, San Francisco**, CA 1 Mart 2012. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (05.05.2020)

ROLLAND, Nadege, "A fibre-optic Silk Road", The **Diplomat**, 2 Nisan 2015. https://thediplomat.com/2015/04/a-fiber-optic-silk-road/ (30.06.2020)

ROSENZWEIG, Paul, "Significant Cyber Attacks on Federal Systems -- 2004-present", **Lawfare**, 7 Mayıs 2012. URL: https://www.lawfareblog.com/significant-cyber-attacks-federal-systems-2004-present (29.05.2020)

ROUSE, Margaret, "Acceptable use policy (AUP)", **TechTarget Network,** Temmuz 2014. https://whatis.techtarget.com/definition/acceptable-use-policy-AUP (26.05.2020)

ROUSE, Margaret "RSA Algorithm", **TechTarget Network**, Kasım 2018. https://searchsecurity.techtarget.com/definition/RSA (18.05.2020)

SALTONSTALL, David, "The Creeper and The First Anti-Virus Program", **Ezine Articles**, 15 Nisan 2009. URL: https://ezinearticles.com/?The-Creeper-and-The-First-Anti-virus-Program&id=2224501 (18.05.2020)

SANG-HUN, Chloe & MARKOFF, John, **Cyber-attacks Jam Government and Commercial Web Sites in U.S. and South Korea,** The New York Times, 8 Temmuz 2009, https://www.nytimes.com/2009/07/09/technology/09cyber.html (09.03.2020)

SANGER, David. E., **Obama Order Sped Up Wave of Cyberattacks Against Iran**, 1 Hazıran 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (03.05.2020)

Scientific America, **when did the term 'computer virus' arise?** 19 Ekim 2001. URL: https://www.scientificamerican.com/article/when-did-the-term-compute/ E.T. 18 Mayıs 2020

SCOFIELD, Jack, "Google, Yahoo, Adobe and who?", 14 Ocak 2010, **The Guardian**. URL: https://www.theguardian.com/technology/2010/jan/14/google-yahoo-china-cyber-attack (20.05.2020)

SECURI, **what is a DDoS Attack**, 9 Ağustos 2019. https://sucuri.net/guides/what-is-a-ddos-attack/ E.T 11 Mayıs 2020.

SHULER, Rus, **How does the Internet Work?,** Pomeroy IT Solution 2002. https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm (6.03.2020)

SNOW, John, "Top 5 most notorious cyberattacks", **Kaspersky Daily** 6 Kasım 2018. https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/ (11.05.2020).

STEPHENS, Sarah, "Why companies underestimate the physical damage of cyber-attacks", **JLT**, *1 Mart 2016.* https://www.airmic.com/news-story/why-companies-underestimate-physical-damage-cyber-attacks e.t 5 Mayıs 2020.

Stratégie de cybersécurité du gouvernement du Canada 2010, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf (27.02. 2020)

SWINHOE, Dan, **what is a man-in-the-middle attack? How MitM attacks work and how to prevent them**, CSO 13 February 2019. https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html (11.05.2020)

The Coming Storm, **Google Hacked, says it Will Stop Censoring Chinese Search Results**, 12 Ocak 2010. URL: https://krebsonsecurity.com/2010/01/hack-against-google-prompts-search-giant-to-stop-censoring-chinese-search-results/ (27.02. 2020)

TURNER, Lauren, "Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and PayPal", **Independent** 24 Ocak 2013. https://www.independent.co.uk/news/uk/crime/anonymous-hackers-jailed-for-ddos-attacks-on-visa-mastercard-and-paypal-8465791.html (20.05.2020).

Types of Cyber-attackers, https://www.javatpoint.com/types-of-cyber-attackers (05.05.2020)

UNTERSINGER, Martin, ***Les Etats-Unis inculpent un Nord-Coréen d'opérations de piratage « sans précédent »***, Le Monde, 6 Eylül 2018, https://www.lemonde.fr/pixels/article/2018/09/06/les-etats-unis-accusent-un-nord-coreen-d-etre-derriere-le-piratage-de-sony-pictures-et-wannacry_5351390_4408996.html (04.11.2020)

UNTERSINGER, Martin, **L'Ukraine, cible préférée des hackeurs russes**, Le Monde, 4 Nisan 2019, https://www.lemonde.fr/international/article/2019/04/04/l-ukraine-cible-preferee-des-hackeurs-russes_5445462_3210.html (05.05.2020)

VIGLIAROLO, Brandon, "Brute force and dictionary attacks: A cheat sheet", **TechRepublic**, 17 Aralık 2018. URL: https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/ (11.05.2020)

WINDREM, Robert, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations", **NBC News,** 18 Aralık 2016.https://www.nbcnews.com/storyline/hacking-in-america/timeline-ten-years-russian-cyber-attacks-other-nations-n697111 (03.07.2020)

WOODHAMS, Samuel, "The Rise of Internet Sovereignty and the End of the World Wide Web?", **Opinion** 23 Nisan 2019. URL: https://theglobepost.com/2019/04/23/internet-sovereignty/ (26.05.2020)

WOODS, Ben, "Viruses, trojans, malware, worms - what's the difference", **WIRED**, 9 Mayıs 2017. URL: https://www.wired.co.uk/article/ransomware-viruses-trojans-worms (11.05.2020)

YI, Shen, "Cyber security depends on US cooperation", **China Daily**, 16 Aralık 2015. URL: http://europe.chinadaily.com.cn/opinion/2015-12/16/content_22724400_2.htm E.T 5 Haziran 2020.

ÖZET

Bu tez üç önemli konuyu tartışmıştır. İlk konu, uluslararası hukukun siber uzaya genel uygulaması hakkındaydı. Bu bölüm, uluslararası hukukun farklı yönlerini ve devletin egemenliğini içeren bir sorun olduğunda siber uzayda nasıl uygulanabileceklerini tartışmıştır. İkinci konu, siber uzayda düşmanca niyet ve düşmanca eylemi tanımlamak için gerekli kriterler hakkındaydı. Bu bölümde siber uzayda güç kullanımına ilişkin konular ele alınmıştır. Güç kullanımına söz konusu siber saldırının yoğunluğuna göre izin verilebilir ancak bu araştırmanın da gösterdiği gibi bugüne kadar farklı iddialara bakılmaksızın hiçbir ülke şüphesiz siber saldırıların kaynağı olarak etiketlenmemiştir ve sadece iddialar üzerine bir ülkeye yaptırım uygulamak zordur.[451] Son önemli tartışma, Uluslararası İnsancıl Hukukun siber uzaya uygulanabilirliği ile ilgiliydi. Bulgularımıza göre, silahlı çatışmalara uygulanabilir kurallar bütünü olarak uluslararası insancıl hukuk, bu kuralların askeri hedeflerin ayrımı ve orantılılık gibi birçok önemli ilkesinin siber uzayda kolayca uygulanamaması nedeniyle siber savaşa uygulanma kategorisine girememektedir. Yıkıcı siber silahların uluslararası insancıl hukuka saygı duyma yeteneğine sahip olduğunu düşünmek de çok zordur.

[451] Eugenia Lopez- Jacoiste, 'The UN Collective Security System and its Relationship with Economic Sanctions and Human Rights' (2010), 14 Max Planck UNYB, s. 302.

SUMMARY

This thesis discussed three important issues. The first issue was about the general application of international law to cyberspace. This topic discussed different aspects of international law and how they can apply in the cyberspace when there is an issue involving state's sovereignty. The second issue was about the necessary criteria for defining hostile intent and hostile act in the cyberspace. In this part, issues relating to the use of force in the cyberspace have been discussed. The use of force can be authorized depending on the intensity of the cyber attack in question but as this research has demonstrated until now regardless of different allegations no country has ever been doubtlessly labelled as the origin of cyber attacks and it is difficult to sanction a country on just allegations. The last important discussion was the issue relating to the applicability of International Humanitarian Law to cyberspace. As for our findings, international humanitarian law as a body of rules applicable to armed conflicts fails category to apply to cyber warfare since many important principles of these rules such as the dicrimination of military targets and proportionality do not easily apply in the cyberspace and it is very difficult to consider that destructive cyber weapons are capable of respecting international humanitarian law.