T.C.

ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER UZAYDAKİ YENİ DEVLET DIŞI AKTÖRLERİN ULUSLARARASI HUKUK BAKIMINDAN SORUMLULUKLARI

Doktora Tezi

Mammad ISMAYILOV

Kamu Hukuku Anabilim Dalı

Kamu Hukuku Doktora Programı

Ağustos 2025

T.C.

ANKARA SOSYAL BİLİMLER ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER UZAYDAKİ YENİ DEVLET DIŞI AKTÖRLERİN ULUSLARARASI HUKUK BAKIMINDAN SORUMLULUKLARI

Doktora Tezi

Mammad ISMAYILOV

Kamu Hukuku Anabilim Dalı

Doktora Programı

Dr. Öğr. Üyesi Fethullah BAYRAKTAR

Ağustos 2025

TEŞEKKÜRLER

Bu tez çalışmam boyunca değerli bilgi ve desteklerini esirgemeyen danışman hocama, akademik rehberliği ve yol göstericiliği için içten teşekkürlerimi sunarım. Ayrıca, siber uzayın gittikçe karmaşıklaşan yapısı ve devlet dışı aktörlerin rolü üzerine yapılmış olan kapsamlı literatür ve kaynakları bizlerle paylaşan tüm akademisyenlere minnettarım. Siber alanda egemenlik, sorumluluk ve uluslararası hukuk bağlamındaki güncel tartışmaların anlaşılmasında onların çalışmaları yol gösterici olmuştur.

Tez sürecim boyunca sabrı, anlayışı ve sarsılmaz desteğiyle her an yanımda olan eşim Habibe Aydemir'e duyduğum şükran kelimelerle ifade edilemez. Onun varlığı, yolculuğumun her anına güç ve umut kattı. Bu çalışmayı, hayatıma anlam ve ışık katan sevgili eşime gönülden ithaf ediyorum.

İÇİNDEKİLER

ÖZET

Günümüzde, devletlerin hem klasik sınırları içerisinde hem de bu sınırların ötesinde yer alan ve çoğunlukla "gri alan" olarak tanımlanan siber uzayda faaliyet gösteren yeni devlet dışı aktörler, uluslararası hukukun geleneksel devlet merkezli yapısına meydan okuyan güçlü özneler olarak ortaya çıkmaktadır. Bu çalışma, söz konusu yeni devlet dışı aktörlerin fiillerinden kaynaklanan durumlarda devletin uluslararası sorumluluğunu incelemektedir. "Yeni devlet dışı aktörler" ifadesinin tercih edilmesinin temel nedeni, bu aktörlerin siber uzay gibi sınır ötesi ve sınırsız bir alanda eş zamanlı olarak faaliyet gösterebilme kapasitesine sahip olmaları; klasik devlet dışı aktörlerden farklı olarak esasen özel sektörün ürünü olmaları; ve siyasi ile jeopolitik alanlarda giderek devletlerden daha fazla etki gücüne ulaşmalarıdır.

Dijital teknolojinin hızla gelişmesi ve siber uzayın siyasi, ekonomik ve güvenlik faaliyetlerinin merkezi bir alan haline gelmesiyle birlikte, büyük teknoloji şirketleri, bilgisayar korsanları ve diğer özel aktörler, klasik devlet dışı aktörlerin ötesinde siber uzayın etkin unsurları olarak varlık göstermiştir. Bu dönüşüm, siber uzaydaki yeni devlet dışı aktörlerin faaliyetleri nedeniyle devletin uluslararası sorumluluğu başta olmak üzere uluslararası hukukun diğer kurallarının da sorgulanmasına yol açmaktadır.

Çalışmada, öncelikle siber uzay, yeni devlet dışı aktörler ve siber saldırı kavramları tanımlanarak kavramsal bir çerçeve oluşturulmuştur. Devamında, bu aktörlerin fiillerinden kaynaklanan durumlarda devletin uluslararası sorumluluğu ele alınmıştır. Ardından, uluslararası hukukun temel prensipleri olan devletlerin egemen eşitliği, iç işlerine müdahale yasağı, kuvvet kullanma yasağı ve insan hakları ihlalleri, siber uzaydaki yeni devlet dışı aktörler bağlamında detaylı biçimde incelenmiştir. Mevcut uluslararası hukuk düzeni, esasen yalnızca devletlerin sorumluluğunu öngördüğünden, yeni devlet dışı aktörlerin fiilleri sebebiyle devletlerin uluslararası hukuk çerçevesinde sorumlu tutulup tutulamayacağı meselesi; mevcut teoriler, içtihat niteliğindeki mahkeme kararları, kurgusal senaryolar ve somut vakalar ışığında kapsamlı biçimde değerlendirilmiştir.

Çalışmada, yeni bir olgu niteliğindeki siber uzaya mevcut uluslararası hukuk kurallarının uygulanması suretiyle devletin uluslararası sorumluluğunun tespit edilmesi amaçlanmıştır. Bu kapsamda, 2001 tarihli *Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu Taslak Maddeleri* ile özen yükümlülüğü ilkesi gibi hukuki

araçlardan yararlanılmıştır. Sonuç olarak, çalışma, mevcut uluslararası hukuk kurallarını esas alarak, devletle doğrudan bağı bulunsun ya da bulunmasın, yeni devlet dışı aktörlerin fiillerinden kaynaklanan durumlarda hem devletin hem de bu aktörlerin uluslararası hukuk bağlamındaki sorumluluğunu kapsamlı biçimde incelemiştir.

Anahtar Kelimeler: Siber Uzay, Siber Saldırı, Yeni Devlet Dışı Aktörler, Devlet Sorumluluğu

ABSTRACT

In the contemporary era, new non-state actors operating in cyberspace—an area that lies both within and beyond the traditional boundaries of states and is often described as a "grey zone"—are emerging as powerful entities challenging the traditional state-centric structure of international law. This study examines the international responsibility of states in situations arising from the conduct of these new non-state actors. The term "new non-state actors" is preferred primarily because these actors possess the capacity to operate simultaneously in a borderless and transnational domain such as cyberspace; unlike traditional non-state actors, they are essentially products of the private sector; and they increasingly wield greater political and geopolitical influence than many states.

With the rapid advancement of digital technology and the transformation of cyberspace into a central arena for political, economic, and security activities, big tech companies, hackers, and other private actors have emerged as influential components of cyberspace, surpassing the traditional scope of non-state actors. This transformation has prompted renewed scrutiny of not only the international responsibility of states for the activities of new non-state actors in cyberspace, but also other established rules of international law.

The study first defines the concepts of cyberspace, new non-state actors, and cyberattacks to establish a conceptual framework. It then addresses the issue of state responsibility under international law for acts committed by these actors. Subsequently, the fundamental principles of international law—namely, the sovereign equality of states, the prohibition of intervention in internal affairs, the prohibition on the use of force, and the protection against human rights violations—are examined in detail within the context of new non-state actors in cyberspace. As the current framework of international law essentially envisages responsibility only for states, the question of whether states can be held responsible under international law for acts committed by new non-state actors is assessed through existing theories, precedent-setting judicial decisions, hypothetical scenarios, and concrete case studies.

The study aims to determine the international responsibility of states by applying existing rules of international law to the relatively new phenomenon of cyberspace. To this end, it makes use of instruments such as the *2001 Articles on Responsibility of States for Internationally Wrongful Acts* and the principle of due diligence. Ultimately, building upon the

current body of international law, the study comprehensively examines the responsibility—both of states and of non-state actors themselves—for acts committed by new non-state actors in cyberspace, regardless of whether they have a direct link to a state.

Keywords: Cyberspace, Cyberattack, New Non-State Actors, State Responsibility

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AHİS	: Avrupa İnsan Hakları Sözleşmesi
AİHM	: Avrupa İnsan Hakları Mahkemesi
ANSSI	: Fransa Ulusal Siber Güvenlik Ajansı
APT	: Gelişmiş Sürekli Tehdit
ARPA	: İleri Araştırma Projeleri Ajansı
BM	: Birleşmiş Milletler
BMGK	: Birlemiş Milletler Güvenlik Konseyi
BMGenK	: Birleşmiş Milletler Genel Kurulu
BMHAUG	: Birleşmiş Milletler Hükümetler Arası Uzmanlar Grubunu
DDoS	: Dağınık Hizmet Engelleme Saldırısı
DHC	: Demokratik Ulusal Komite
EYUCM	: Eski Yugoslavya Uluslararası Ceza Mahkemesi
GCHQ	: Birleşik Krallık Hükümet İletişim Merkezi
GRU	: Rusya'nın Askeri İstihbarat Teşkilatı
İHEB	: İnsan Hakları Evrensel Beyannamesi
NATO	: Kuzey Atlantik Antlaşması Örgütü
NSA	: ABD Ulusal Güvenlik Ajansı
PDoS	: Kalıcı Hizmet Engelleme
SSCB	: Sovyet Sosyalist Cumhuriyetler Birliği
UAD	: Uluslararası Adalet Divanı
UCM	: Uluslararası Ceza Mahkemesi
UHK	: Uluslararası Hukuk Komisyonu
UNGPs	: BM İş Dünyası ve İnsan Hakları Rehber İlkeler

GİRİŞ

Siber uzayı, bilgisayar ve internet bağlantısına sahip herkesin erişimine açık küresel bir alan olarak tanımlamak abartılı olmayacaktır. Bu alanı eşsiz kılan en önemli özelliği düşük giriş engellerine ve yüksek derecede anonimliğe sahip olmasıdır; bu da bu alanı devletler ve devlet dışı aktörler için dostane olmayan fiiller, saldırganlık ve savaş fiillerini neredeyse herhangi bir cezaya maruz kalmadan gerçekleştirebilecekleri bir alan haline getirmiştir. İçinde bulunduğumuz dijital çağ ise, bu alanı, devlet egemenliği, güvenlik ve uluslararası hukukun benzersiz bir karmaşıklıkla kesiştiği kritik bir alan haline getirmiştir.

Uluslararası hukuku siber uzay bağlamında değerlendirirken, siber uzayın kendine has özelliklerini dikkate almak gerekecektir. Bu bağlamda, siber uzayın tamamen insan yapımı bir alan olması bu alanın en önemli özelliklerden biridir. Siber uzay, dünya genelindeki kamu ve özel sektör paydaşları tarafından kolektif bir şekilde oluşturulmakta, sürdürülmekte, sahiplenilmekte ve işletilmekte; aynı zamanda teknolojik yeniliklere hızla adapte olarak sürekli değişmektedir.

Siber uzayı eşsiz kılan bir diğer özelliği herhangi bir fiziksel sınırının olmaması ve izlenebilir rotalara sahip olmamasıdır. Jeopolitik veya doğal sınırlara tabi olmayan siber uzayda, bilgi ve elektronik yükler, elektromanyetik spektrum aracılığıyla herhangi bir çıkış noktasından herhangi bir varış noktasına anlık olarak dağılır. Bu yükler, önceden tahmin edilemeyen rotalarda seyahat eder ve varış noktalarında yeniden oluşturulmadan önce çeşitli dijital parçalara ayrılır.

Siber uzayı benzersiz kılan bir diğer özelliği, kara, hava, deniz ve uzay gibi diğer dört alanın aksine, insanları ve insan faaliyetlerini fiziksel olarak yerleştiremediğimiz bir alan olmasıdır. Daha açık bir ifadeyle, siber uzay fiziksel olarak insanların gidemediği ve yerleşemediği bir alandır. Diğer bir ifadeyle insanlar ve insan faaliyetleri diğer dört alanda gerçekleştirilebilir ve bu alanlar arasında seyahat mümkündür. Örneğin, denizaltına veya uzaya gitmek özel bir hazırlık ve uygun ekipman gerektirse de bu fiziksel olarak mümkündür ve gerçekleştirilebilir. Deniz altında bulunan bir denizaltı, karada, denizde, havada veya uzayda bulunan nesneleri hedef alabilecek bir füze fırlatabilir. Ancak, siber uzayda bulunan bir nesneyi hedef almak için bu füzeyi doğrudan siber uzaya fırlatmak mümkün değildir. Tek etkileşim yöntemi, siber nesnenin depolandığı bilgisayarı hedef almak olacaktır; ancak bu tür bir

davranışın siber uzayla doğrudan bir ilgisi yoktur. Bu kapsamda, siber uzayın diğer dört alandan ayrı bir alan olmadığını, diğer alanlardaki objeleri etkilemek için kullanılan bir araç olduğunu söyleyebiliriz. Dolayısıyla, siber uzay karada, havada, denizde ve uzayda insan faaliyetlerinin yürütülmesi ve savaş yapılabilmesi için kullanılan bir araç olarak hizmet vermektedir. Örneğin, açık denizlerde bulunan bir tekneden başlatılan bir siber saldırı, büyük olasılıkla uydu telekomünikasyonu aracılığıyla iletilir ve bu sayede uzay ve hava gibi diğer alanlardan geçer, dört alandaki nesneleri hedef alabilir. Bu nedenle, siber uzayı diğer dört alandan farklı bir beşinci alan olarak tanımlamak yerine, siber uzayın, diğer alanlardaki faaliyetleri destekleyen ve etkileyen bir araç olduğunu vurgulamak daha doğru olacaktır.

Dolayısıyla siber uzay, internet, internete bağlı olan veya olmayan bilgisayarlar ve telekomünikasyon ağlarından oluşan "teorik bir ortam" (*theoretical enviroment*) olarak tanımlanabilir; bu, yalnızca "kavramsal bir alan" (*notional environment*) ya da "etki alanı" (notional domain) olarak da ifade edilebilir. Buraya kadar aktarılanlardan hareketle siber uzayın, hava sahası ve dış uzaydan ayrı "kurgusal bir alan" olduğunu söyleyebiliriz.

Siber uzay, yukarıda belirtildiği üzere, uluslararası hukuk açısından yeni bir alan veya bölge oluşturmamaktadır. Bu nedenle, bu alandaki faaliyetler, yeni uluslararası hukuk kurallarına gerek duyulmadan, mevcut uluslararası hukuk kuralları çerçevesinde düzenlenebilir. Dolayısıyla, uluslararası hukukun siber uzaya uygulanabilirliğini tartışmak gereksizdir.

Bu çalışmada ele alınan araştırma sorusu iki aşamalı olarak oluşturulmuştur. İlk aşama aşağıdaki şekilde ifade edilebilir: 1) Mevcut uluslararası hukuk kuralları çerçevesinde, siber uzaydaki yeni devlet dışı aktörlerin fiillerinden kaynaklanan ve devlete atfedilemeyen siber eylemler bağlamında devletin uluslararası sorumluluğu mümkün müdür? Araştırma sorusunun ikinci aşaması ise şu şekilde formüle edilebilir: 2) Herhangi bir şekilde devlete atfedilemeyen fiillerden ötürü, yeni devlet dışı aktörlerin doğrudan sorumluluğu söz konusu olabilir mi?

Araştırma problematiği, doğrudan araştırma sorusuyla ilişkilidir. Bu çerçevede, mevcut uluslararası hukuk kuralları arasında, siber uzaydaki yeni devlet dışı aktörler tarafından gerçekleştirilen hukuka aykırı eylemler bakımından açık ve bağlayıcı bir sorumluluk düzenlemesi bulunmamaktadır. Daha açık bir ifadeyle, devletin uluslararası sorumluluğuna ilişkin 2001 tarihli Taslak Maddeler ile mevcut yargı içtihatları, yalnızca devlete atfedilebilen fiilleri kapsam altına almaktadır. Diğer bir deyişle, fiilin faili olan aktörün eyleminin herhangi bir devlete hiçbir şekilde atfedilemediği durumlarda, uluslararası sorumluluğun nasıl tesis edileceğine ilişkin açık bir hüküm mevcut değildir.

Araştırmanın amacı da mevcut uluslararası hukuk kuralları çerçevesinde, yeni devlet dışı aktörlerin fiillerinden dolayı hem devleti hem de ilgili devlet dışı aktörleri doğrudan sorumlu tutma imkânını değerlendirmektir.

Bu araştırmada kullanılan yöntem, mevcut uluslararası hukuk kurallarının, yeni ve özgün bir alan olan siber uzaya uygulanmasına dayanmaktadır. Daha açık bir ifadeyle, çalışmada mevcut uluslararası hukuk kuralları siber uzay bağlamında değerlendirilerek, hem devletin hem de devlet dışı aktörlerin doğrudan sorumluluğunun tespiti amaçlanmıştır. Bu amacı gerçekleştirebilmek için normatif analiz yöntemi tercih edilmiştir. Bu çerçevede; egemenlik, müdahale yasağı, kuvvet kullanma yasağı, insan haklarının ihlali, uluslararası sorumluluk ve özen yükümlülüğü gibi temel ilke ve normlara başvurulmuştur.

Araştırmada incelenen doktrinsel yaklaşımlar çeşitlilik arz etmektedir. Bu çerçevede, *göz yumma teorisi, suç ortaklığı teorisi* ve *kolektif sorumluluk teorisi* gibi yaklaşımlar detaylı şekilde ele alınmıştır. İncelenen başlıca belgeler arasında 2001 tarihli Taslak Maddeler, Tallinn Manual 2.0 ve diğer uluslararası belgeler yer almaktadır. Çalışmada ayrıca çok sayıda uluslararası yargı kararına da yer verilmiştir. Bu bağlamda, Uluslararası Adalet Divanı (UAD) tarafından verilen *Tahran Rehineler Davası, Nikaragua Davası* ile Eski Yugoslavya Uluslararası Ceza Mahkemesi (bundan böyle EYUCM kısaltması kullanılacaktır) tarafından verilen *Tadić Kararı* örnek olarak gösterilebilir. Yeni devlet dışı aktörlerin fiillerinden dolayı bir devletin sorumlu tutulabilmesine ilişkin tartışmalar bağlamında, Google'ın 2011 yılında Mısır'daki halk ayaklanmaları üzerindeki etkisi de çalışmada ele alınmıştır.

Bu çalışmanın literatüre en önemli katkısı, 2001 tarihli Taslak Maddeler'in ötesine geçerek, hem devletin hem de devlet dışı aktörlerin doğrudan sorumluluğunu ortaya koymaya çalışmasıdır. Daha açık bir ifadeyle, mevcut literatürdeki çalışmaların büyük çoğunluğu, yalnızca 2001 tarihli Taslak Maddeler çerçevesinde kalarak, devlet dışı aktörlerin fiillerinden ötürü devleti sorumlu tutmaya odaklanmıştır. Bu bağlamda, şimdiye kadar yapılan araştırmaların önemli bir kısmı, devlet dışı aktörlerin eylemlerinden kaynaklanan sorumluluğu yalnızca devletin yükümlülüğü üzerinden açıklamaya çalışmış; özellikle Taslak Maddeler'in 4., 5., 8. ve 11. maddeleri kapsamında devlete atfı esas alarak bir sorumluluk analizi yapmıştır.

Bu çalışma, kapsam itibarıyla uluslararası hukukla sınırlıdır. Bu nedenle, iç hukuk sistemleri, ulusal siber güvenlik mevzuatı ve cezai sorumluluk rejimleri bu çalışmanın kapsamı dışında bırakılmıştır.

Çalışmada, yapay zekânın fiillerinden dolayı devletin sorumluluğu konusu ele alınmamıştır. Zira devlete, gerçek kişilere ve şirketler gibi tüzel kişilere atfın sınırları dahi uluslararası hukuk bakımından açık şekilde belirlenmemişken, bir makine ya da uygulamaya

atfı ifade edecek şekilde yapay zekâyı sorumlu tutmak oldukça güçtür. Siber uzaydaki aktörlerin fiillerinde dahi anonimlik nedeniyle ispat yükümlülüğü bağlamında atfın gerçekleştirilmesi zorken, yapay zekâ açısından bu neredeyse imkânsız hâle gelmektedir. Bu nedenle, çalışmanın kapsamı dışında bırakılan bir diğer konu da yapay zekânın sorumluluğu olmuştur.

Tez çalışmasının birinci bölümünde, kavramsal bir tartışma çerçevesinde öncelikle siber uzay, siber uzayın sınırları, uluslararası hukukun bu alana uygulanabilirliği ve siber saldırı kavramı ele alınmıştır. Ardından, siber uzaydaki yeni devlet dışı aktörlerin kimlikleri incelenmiştir. Son olarak, uluslararası hukukun özneleri tartışması bağlamında, siber uzaydaki yeni devlet dışı aktörlerin uluslararası hukukun özneleri olarak kabul edilip edilemeyeceği sorusu tartışılmıştır. Dolayısıyla bu tez çalışmasının en önemli odak noktalarından biri de yeni devlet dışı aktörler kavramıdır.

Yeni devlet dışı aktörlerden kasıt ise siber uzaydaki devlet destekli gruplar, siber paralı askerler, bağımsız bilgisayar korsanları ve hayati dijital altyapıyı kontrol eden büyük teknoloji şirketleridir. Bu çalışma bağlamında en önemli tartışma konularından biri de bu aktörlerin uluslararası hukuk bağlamındaki hukuki statüsü ve gerçekleştirdiklerin fiillerin devletlere atfedilebilmesi sorunudur.

Bu kapsamda çalışmanın ikinci bölümünde, bir devlet dışı aktör tarafından gerçekleştirilen siber saldırının bir devlete atfedilebilmesi için izlenmesi gereken yöntemler ele alınmıştır. Bu çerçevede, yeni devlet dışı aktörlerin fiillerinden dolayı devletin sorumluluğunu doğurabilecek isnat kurallarına ilişkin teorik tartışmalar incelenmiş, 2001 tarihli Taslak Maddeler'in ilgili hükümleri değerlendirilmiş ve bu konuda içtihat teşkil eden mahkeme kararları ayrıntılı bir şekilde analiz edilmiştir.

Çalışmanın son bölümünde, siber uzaydan kaynaklanan saldırıların uluslararası hukukun temel ilkeleri olan devlet egemenliğinin ihlali, iç işlerine müdahale yasağı, kuvvet kullanma yasağı ve insan haklarının korunması yükümlülüğü üzerindeki etkileri kapsamlı bir şekilde ele alınmıştır. Bu bağlamda, 2001 tarihli Taslak Maddeleri ile mahkeme kararlarında geliştirilen içtihatların yetersiz kaldığı durumlarda, doğrudan devlete atfedilemeyen fiiller dolayısıyla devletin uluslararası sorumluluğunu tespit etmek amacıyla "özen yükümlülüğü" (*due diligence*) ilkesi incelenmiştir. Doğrudan devletle bağ kurulması mümkün olmayan bu fiiller nedeniyle, özen yükümlülüğü çerçevesinde devletin uluslararası hukuk açısından sorumlu tutulabileceği durumlar, hem teorik kurgusal senaryolar hem de somut vakalar ışığında değerlendirilmiştir. Sonuç itibarıyla, siber uzaydaki yeni devlet dışı aktörlerin fiillerinden dolayı devletin uluslararası hukuk kapsamında sorumlu tutulabilmesi için, Taslak Maddeler ve

mevcut mahkeme içtihatlarının yetersiz kaldığı hallerde, özen yükümlülüğü ilkesinin uygulanabilirliği detaylı biçimde analiz edilmiş ve çalışmada bu temel sorunun çözümüne yönelik önemli bir katkı sağlanmıştır.

BİRİNCİ BÖLÜM

SİBER UZAY VE YENİ DEVLET DIŞI AKTÖRLER

Siber uzay doğası gereği asimetriktir.[1] Bu özelliğinden dolayı siber uzay, internet bağlantısı olan bir bilgisayara, akıllı telefona ya da başka türde bir multimedya cihazına erişimi olan hemen herkes tarafından kullanılabilmektedir. Bu alanda farklı ihtiyaçları, hedefleri ve niyetleri olan çeşitli aktörler paralel olarak var olabilmektedir. Bu aktörlerden bazıları tek başına hareket ederken, diğerleri daha esnek bağlantılı ağlar ya da daha resmi yapılar içinde hareket etmektedir. Roller de duruma göre değişebilir ve çakışabilir. Bu özelliklerinden dolayı siber uzay silah çatışmaların vazgeçilmez unsuru olarak kabul edilmektedir.[2]

Devletin kara, deniz, hava ve uzay sınırları arasında bir araç olarak faaliyet gösteren siber uzay, kurgusal bir alan niteliğindedir. Bu alanda yürütülen faaliyetlerin tespit edilebilirliği oldukça güçtür. Bu nedenle siber uzay, devlet faaliyetlerinin yürütüldüğü bir "gri alan" olarak da nitelendirilmektedir. Devletler bu alanı çoğu zaman uluslararası sorumluluktan kaçınmak amacıyla kullanmaktadır. Ancak siber uzay yalnızca devletlerin değil, aynı zamanda devletlerden daha büyük jeopolitik etkiye sahip olan bilgisayar korsanları ve büyük teknoloji şirketleri gibi aktörlerin de faaliyet gösterdiği bir alandır.

Bu çalışmada, anılan aktörler "yeni devlet dışı aktörler" olarak tanımlanmıştır. Zira bu aktörler, klasik devlet dışı aktörlerden farklı olarak, doğrudan devlet adına değil, özel sektör mantığıyla hareket etmektedir. Buna rağmen, faaliyetleri itibarıyla devletlere yönelik son derece ciddi tehditler oluşturabilmektedirler.

Bu bölümde öncelikle, siber uzayın kendine özgü nitelikleri ele alınarak, siber uzaya ilişkin çeşitli tanımlar incelenmiştir. Ardından, uluslararası hukukun bu alana uygulanabilir olup olmadığı tartışılmıştır. Takiben, siber saldırı türlerine yer verilmiş ve siber saldırılar ile siber savaş arasındaki farklar analiz edilmiştir. Son olarak ise, klasik devlet dışı aktörlerle siber uzaydaki yeni devlet dışı aktörler arasında karşılaştırmalı bir tasnif yapılmıştır.

[1] Ralph Martins, "Anonymous" Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts", *The Cyber Defense Review* 2/3 (2017), 95.
[2] James A. Lewis- Erica D. Lonergan - Julia Voo - Melanie Garson - Amy Ertan, "Evolving Cyber Operations and Capabilities", (*Center for Strategic and International Studies (CSIS)* 2023) 5.

1. SİBER UZAY VE ULUSLARARASI HUKUK

Siber uzayın tarihi olarak telekomünikasyon, yani uzaktan iletişim sistemi gösterilebilir. Telekomünikasyon yoluyla iletişim ise yeni bir olgu değildir. Telekomünikasyon, 19. yüzyılın ortalarında telgraf, posta ve semafor gibi mevcut olan diğer uzun mesafe sistemlerinin yerini alarak ya da onları tamamlayıcı bir unsur olarak Britanya İmparatorluğu genelinde hayati bir iletişim ağı olarak varlık göstermiştir. 19. yüzyılın ortalarında döşenen Atlantik telgraf kabloları sayesinde transatlantik iletişim uzun bir süre boyunca mümkün olmuştu.[3] 19. yüzyılın sonunda ise telefon icat edilmiştir. Ancak 1960'lara kadar Batı'da bile telefonlar oldukça az, son derece pahalıydı ve daha da önemlisi yerel aramalar dışında bağlantıların hala elle yapılması gerekiyordu.

Siber uzayın ortaya çıkışı ise, Soğuk Savaş döneminde Amerika Birleşik Devletleri (ABD) ile Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) arasında başlayan rekabetle yakından ilişkilidir. Soğuk Savaş döneminde Amerikalılar, savaşın çıkması halinde ordunun nasıl iletişim kuracağına dair araştırmalar yapmışlardır. Çünkü merkezi bir sistem, Sovyetler Birliği tarafından kolaylıkla yok edilebilirdi. Bu nedenle, geleneksel teknolojiler iletişim için yeterli değildi. ABD'nin içinde bulunduğu bu durum, ülkeyi farklı bir adım atmaya ve iletişim için tamamen yeni yöntemler geliştirmeye sevk etmiştir. Bu amaçla, ABD Savunma Bakanlığı bünyesindeki bilim insanları, ağı dağıtık bir yapıya kavuşturmayı hedeflemişlerdir; böylece iletişim merkezlerinden birine veya daha fazlasına saldırı düzenlense bile ağın varlığını sürdürebilmesi mümkün olacaktı. Bilim insanlarının aklındaki temel fikir, savaş zamanında "savunma ile ilgili sırların saklanacağı merkezi olmayan bir depo" oluşturmaktı.[4] Bu gelişme, günümüzde kullandığımız internetin, dünyanın dört bir yanındaki insanlar arasında etkin ve düşük maliyetli iletişim sağlamasına olanak tanıyarak, Soğuk Savaş paranoyasının az sayıdaki olumlu miraslarından biri olarak ortaya çıkmasına yol açmıştır.[5]

Yukarıda aktarılanlardan da anlaşılacağı üzere, internetin diğer bir ifadeyle siber uzayın kökenleri, ABD ile SSCB arasındaki rekabete dayanmaktadır. Bu bağlamda, ABD Savunma Bakanlığı, SSCB'ye karşı üstünlük sağlamak amacıyla 1958 yılında İleri Araştırma Projeleri Ajansı (*Advanced Research Projects Agency - ARPA*) kurmuştur.[6] ARPA'nın misyonu yenilikçi

[3] Jason Whittaker, *The Cyberspace Handbook*, (Londra-Newyork: Routledge, 2004), 23-24.
[4] Raphael Cohen-Almagor, "Internet History", 47.
[5] Scott Ruthfield, "The Internet's History and Development: From Wartime Tool To Fish-Cam" *The ACM Magazine for Students* 2/1 (Eylül 1995), 1.
[6] Raphael Cohen-Almagor, "Internet History", *International Journal of Technoethics* 2/2 (Nisan-Haziran 2011), 48.

araştırma fikirleri üretmek, geleneksel gelişim yaklaşımlarının çok ötesine geçen anlamlı teknolojik etki sağlamak ve prototip sistemler geliştirerek bu fikirler üzerinde harekete geçmekti. Bu amaçla kurulan ARPA ofislerinden biri olan Bilgi İşleme Teknikleri Ofisi, Amerikan üniversiteleri ve araştırma laboratuvarlarını devlete komuta ve kontrol bağlamında mesajlaşma yetenekleri sağlayacak stratejik bir iletişim ağı oluşturmak üzere harekete geçirmek amacıyla bilgisayar bilimi araştırmalarını finanse etmek üzere tasarlanmıştır.[7] Eylül 1969'da ARPA'nın ARPANET adlı bir departmanından çıkan küçük bir bilgisayar ağı projesi icat edildi. Amacı, "ajans için çalışan çeşitli bilgisayar merkezleri ve araştırma grupları arasında on-line bilgi işlem zamanını paylaşmanın bir yolunu" kolaylaştırmaktı.[8]

ARPA Ağı projesinin öncüleri, ARPANET'in nükleer savaşa dayanıklı bir ağ inşa etmek amacıyla geliştirildiği yönündeki görüşü reddetmektedir. ARPANET'in kurulmasına katkıda bulunan dijital ağ iletişiminin öncülerinden ve "Modern Veri Ağının" (Modern Data Networking) babası olarak kabul edilen Leonard Kleinrock, ARPA'nın ağ kurma amacının araştırmacıların birbirlerinin özel kaynaklarını (donanım, yazılım, hizmetler ve uygulamalar) paylaşmalarını sağlamak olduğunu belirtmiştir. Diğer bir ifadeyle, Kleinrock'a göre, amaç askeri bir saldırıya karşı koruma sağlamak değildir.[9]

Bununla birlikte, 1990'lı yıllara kadar internet, ABD'de öncelikle akademisyenler ve araştırmacılar tarafından e-posta ve dosya transferi amaçlı kullanılmış ve ortak bilimsel araştırmaların yürütülmesi için bir araç olarak tanımlanmıştır. Ancak, 1990'dan sonra internetin ticari amaçlarla kullanılmaya başlanması, akademik amaçlı kullanımın önüne geçmiştir. Ayrıca, grafiksel ve hipermetinsel bir arayüz olan World Wide Web'in (*WWW*) internet sitelerinde gezinmek için temel araç haline gelmesi, siber uzay kavramının olgunlaşmasına zemin hazırlamıştı.[10]

1.1.Siber Uzay Kavramı

Siber uzay kavramı, bilgisayar bilimcileri ya da mühendisleri tarafından oluşturulmuş teknik bir terim değildir. Bu kavram ilk olarak bilim kurgu edebiyatında, özellikle de William Gibson'ın yazılarında ortaya çıkmış ve daha sonra zamanla ve aşamalı olarak bilim kurgu

[7] James Curran - Jean Seaton, *Power Without Responsibility Press, Broadcasting and the Internet in Britain* (London: Routledge, 2009), 88.
[8] Manuel Castells, *The Internet Galaxy. Reflections on the Internet, Business, and Society*, (New York: Oxford University Press, 2001), 10.
[9] Raphael Cohen-Almagor, "Internet History", 47.
[10] David Holmes, *Virtual Globalization: Virtual Spaces/Tourists Spaces*, (London: Routledge, 2001), 57.

alanından çıkarak başka alanlarda önemli bir yer edinmiştir.[11] Bu bağlamda William Gibson, siber uzay kavramını kullanan ve popülerleştiren ilk yazarlardan biri olarak bilinmektedir.[12] Gibson, bu kavramı ilk kez Temmuz 1982'de Omni dergisinde yayınlanan kısa öyküsü "Burning Chrome"da kullanmıştır.[13] 1984 tarihli *Neuromancer* adlı romanında Gibson, siber uzay kavramını şu şekilde tasvir etmiştir:

"Her gün milyarlarca yetkili operatör tarafından, her ulusta matematiksel kavramlar öğrenen çocuklar tarafından deneyimlenen, rızaya dayalı bir halüsinasyon... İnsan sistemindeki her bilgisayarın veri tabanından soyutlanmış grafiksel bir temsil. Akıl almaz bir karmaşıklık. Zihnin uzay boşluğunda sıralanan ışık çizgileri, veri kümeleri ve takımyıldızları. Uzaklaşan şehir ışıkları gibi."[14]

İlk başlarda siber uzayın açıkça tanımlanmış bilimsel bir anlamı yoktu. Ancak bu kavram, yavaş yavaş ve aşamalı olarak bilim kurgu alanından göç ederek başka alanlarda da önemli bir yer edinmeye başladı. Örneğin, François Delerue'ye göre siber uzay, internete bağlı olsun ya da olmasın, internet ve diğer bilgisayar ile telekomünikasyon ağlarından oluşan kavramsal bir ortamı ifade eder.[15]

ABD Savunma Bakanlığı tarafından 2006 yılında yayınlanan *The National Military Strategy for Cyber Operations* adlı memorandum belgesinde siber uzay, "ağa bağlı sistemler ve ilgili fiziksel altyapılar aracılığıyla veri depolamak, düzenlemek ve değiştirmek için elektronik ve elektromanyetik spektrumun kullanılmasıyla karakterize edilen bir alan" [16] olarak tanımlanmıştır.

ABD Savunma Bakanlığı, 2008 tarihli memorandumunda siber uzayı, "bilgi teknolojisi altyapılarının birbirine bağlı ağından oluşan ve internet, telekomünikasyon ağları, bilgisayar sistemleri ile gömülü işlemciler ve denetleyicileri içeren bilgi ortamındaki küresel bir alan" olarak tanımlamaktadır.[17]

---

[11] Jeff Prucher (ed.), *"The Oxford Dictionary of Science Fiction",* (Oxford: Oxford University Press, 2006).

[12] Scott Thill, "March 17, 1948: William Gibson, Father of Cyberspace*"* *WIRED*, https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/ (Erişim 8 Haziran 2023)

[13] William Gibson, "Burning Chrome", (Omni Publications International Ltd. 1982) 72

[14] William Gibson, "Neuromancer", (Londra: Gollancz, 2016), 69.

[15] François Delerue, *"Cyber Operations and International Law",* (Cambridge: Cambridge University Press, 2020), 29.

[16] The Depertman of Defense (DoD), Chairman of the Joint Chiefs of Staff Washington, D.C. 20318, "The National Military Strategy for Cyber Operations", Bağlantı adresi: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (Erişim 7 Haziran 2023)

[17] U.S. Deputy Secretary of Defense Gordon England, "The Definition of 'Cyberspace'," Memorandum for Secretaries of the Military Departments, Washington, DC, May 12, 2008, available from integrator.hanscom.af.mil/2008/ May/05292008/05292008-24.htm.

2009 tarihli *Siber Uzay Politikası İncelemesi* adlı raporda ise, "siber uzay teriminin yaygın kullanımı aynı zamanda bilginin ve insanlar arasındaki etkileşimlerin sanal ortamını da ifade etmektedir" ifadelerine yer verilmiştir.[18]

Siber uzayın mevcut kara, deniz, hava ve uzay alanlarının yanı sıra askeri faaliyetler için beşinci bir alan teşkil edip etmediği konusunda bir tartışma ortaya çıkmış ve bugün de bu tartışma devam etmektedir.[19] Aynı şekilde, herhangi bir devletin egemenliği dışında kalan ve Antarktika, açık denizler veya uzay gibi insanlığın ortak mirası gibi muamele görmesi gereken bir alan veya bölge olarak bir "küresel alan" teşkil edip etmediği de tartışılmaktadır.[20]

Yukarıda anlatılanlardan hareketle, siber uzayın kendine özgü özelliklere sahip karmaşık bir alan olduğu sonucuna varabiliriz. Siber uzaydaki bu karmaşık yapı; bilgisayarlar, fiber optik kablolar, telekomünikasyon bileşenleri, kritik altyapılar, siber kişilikler, dijitalleştirilmiş veriler ve daha fazlasından oluşmaktadır.[21]

1.2.Bilgisayar Ağı ve İnternet

Bir bilgisayar ağı, veri alışverişine izin veren en az iki cihazın birbirine bağlanmasıyla oluşur. Bu ağ, fiziksel bileşenler (*physical components*) ve yazılım bileşenleri (*software components*) olmak üzere ikiye ayrılır.[22]

Donanım bileşeni olarak da adlandırılan fiziksel bileşen; bir yandan, birbirine bağlı cihazlar da dahil olmak üzere ağın üzerinde çalıştığı donanımı (*hardware*), diğer yandan ise bu cihazların birbirine bağlanma şeklini ifade etmektedir. Çok çeşitli cihazlar (örneğin bilgisayarlar, sunucular, çıkarılabilir aygıtlar (*removable devices*), akıllı telefonlar ve hatta diğer ağlar) bir ağ içinde birbirine bağlanabilir ve bu ağ daha sonra internet gibi bir "ağlar ağı"na bağlanabilir. Örneğin, bir USB bellek bir bilgisayara takıldığında bir ağ oluşur. Benzer şekilde, bir fare, klavye veya yazıcıya bağlı bir kişisel bilgisayar da bir ağ kurabilir. Nesnelerin interneti (*The Development of the Internet of Things* – IoT) gelişimi, arabalar, buzdolapları, akıllı saatler ve hatta tıbbi cihazlar gibi yeni nesne türlerinin de birbirine bağlanmasına olanak sağlamaktadır. Ara bağlantı (*interconnection*), kablolar (örneğin bakır kablo veya fiber optik

[18] Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington, DC: The White House, May 2009, 1

[19] *The Economist*, "Cyberwar: War in the Fifth Domain", (1 Temmuz 2010), 1; Christy Marx, "*Battlefield Command Systems of the Future"*, (Rosen Young Adult, 2006), 14; Yaroslav Radziwill, *"Cyber-Attacks and the Exploitable Imperfections of International Law",* (Boston: Brill-Martinus Nijhoff Publishers, 2015), 13.

[20] *UNT Libraries*, "Assured Access to the Global Commons: Maritime, Air, Space, and Cyber", (8 Mart 2013), 1.

[21] Can Kasapoglu, "Cyber Security: Understanding the Fifth Domain", *Centre for Economics and Foreign Policy Studies* (EDAM Cyber Policy Paper Series 2017/1), 1.

[22] Delerue, *"Cyber Operations and International Law",* 29-30.

kablo) aracılığıyla ya da kablosuz olarak (örneğin mikrodalgalar, kızılötesi, Wi-Fi ve hatta uydu iletişimi) gerçekleştirilebilir.[23]

Bir cihaz aynı anda birden fazla ağa bağlı olabilir. Örneğin, bir dizüstü bilgisayar hem Bluetooth ile bağlı bir kablosuz fare aracılığıyla bir bilgisayar ağının parçası olabilir hem de Wi-Fi bağlantısı veya Ethernet kablosu ile internete erişebilir. Ayrıca, bir bilgisayar farklı zamanlarda hareket ederek değişik bilgisayar ağlarına bağlanabilir. Örneğin, bir dizüstü bilgisayar geceleri sahibinin ev ağına, diğer zamanlarda ise iş yerinin ağına bağlı olabilir. Bu durum siber güvenlik açısından önemlidir; zira birbirine doğrudan bağlı olmasalar bile, verilerin bir ağdan diğerine geçmesine imkân tanımaktadır.[24]

Bilgisayar ağları birbirine bağlanabilir, başka bir ağ oluşturabilir veya izole edilebilir. Genel olarak izole edilmiş ağlar, diğer ağlarla aralarında herhangi bir iletişim bulunmadığını göstermek için "hava boşluklu" olarak kabul edilir. Ancak veriler, hava boşluklu bir ağ ya da sistem ile diğer cihazlar arasında siber uzay üzerinden değil, fiziksel bir bağlantı kurulması yoluyla da aktarılabilir.[25]

Hava boşluğunun varlığı, siber saldırılara karşı etkili bir koruma sağlasa da kusursuz değildir. [26] Örneğin, nüfusun yalnızca küçük bir kısmının internet erişimine izin verildiği ve çoğu kişinin yalnızca "Kwangmyong" adı verilen ulusal intranete erişebildiği Kuzey Kore'de, Kwangmyong internetten fiziksel olarak hava boşluğu ile ayrılmıştır. Bu nedenle iki ağ arasında doğrudan veri alışverişi yapılamamaktadır. Ancak 2013 yılında, hacktivist grup Anonymous'a bağlı olduğunu iddia eden bir grup bilgisayar korsanı, Kwangmyong'u internete bağlamak amacıyla ülkenin Twitter ve Flickr hesaplarını hackledikleri "Kuzey Kore Operasyonu"nu (*Operation North Korea*) gerçekleştirmiştir. Grup, bir Pastebin (metin depolama platformu) hesabında yöntemlerini şu şekilde açıklamıştır:

"Sahada, özel frekanslara sahip uzun mesafeli Wi-Fi tekrarlayıcılar zinciri kullanarak gerçek interneti ülkeye getirmeyi başaran birkaç adamımız var, bu yüzden (henüz) tespit edilmediler. Ayrıca çevirmeli bağlantılar aracılığıyla Kwangmyong'a bağlanan bazı Birleşik Krallık telefon sabit hatlarına da erişimimiz var. Yapbozun son eksik parçası iki ağı birbirine bağlamaktı ve bu adamlar sonunda bunu başardılar."

Amaçlarının ise, "bağlantılar stabilize ve optimize edilir edilmez, Kuzey Kore vatandaşlarına gerçek, özgür ve sansürsüz interneti sağlamak" olduğunu belirten grup, bunun

[23] Delerue, *"Cyber Operations and International Law",* 30.
[24] Delerue, *"Cyber Operations and International Law",* 30.
[25] Delerue, *Cyber Operations and International Law,* 30-31.
[26] Delerue, *Cyber Operations and International Law,* 30-31.

ilk adımı olarak "kedi yavrularını ve cinsel içerikli materyali ağlara enjekte etmeyi" planladıklarını ifade etmiştir. Bu olay, hava boşluğuna sahip bir ağın dahi internet ile veri paylaşma potansiyeline sahip olabileceğini göstermektedir.[27]

Benzer şekilde, 25 Ocak 2003 tarihinde Slammer solucanı, on beş dakikadan kısa bir sürede dünya çapında binlerce sunucuya bulaşmıştır. [28] Bu solucan, teorik olarak solucana karşı bağışıklık sağlayan bir güvenlik duvarı ile korunan ABD'deki Davis-Besse nükleer santralinin bilgisayar sistemine de sızmayı başarmıştır. Solucanın güvenlik duvarını aşabilmesinin nedeni, santralde görevli bir danışmanın, güvenlik duvarının arkasında nükleer santral ağı ile daha az güvenli olan kendi ofis ağını birbirine bağlamasıydı. Sistem hava boşluklu değildi, ancak Slammer'a karşı savunmasızdı.

Aynı şekilde, aşağıda siber saldırı vakası olarak ayrıntılı şekilde ele alınacak olan Stuxnet, İran'ın hava boşluklu olduğu bilinen bir nükleer santralinin bilgisayar sistemine bulaşmıştır. Verilerin aktarımı, önce internete bağlı virüslü bir sisteme, ardından da nükleer santralin hava boşluklu sistemine bağlanan taşınabilir bir cihaz aracılığıyla gerçekleşmiş ve bu durum Stuxnet'in sistem içinde kendini kopyalamasına olanak sağlamıştır.[29]

Yazılım bileşeni (*software component*), verilerin ağ içerisinde nasıl iletileceğini belirler. Bu bağlamda iletişim ağları iki kategoriye ayrılabilir: yayın ağları (*broadcast networks*) ve anahtarlamalı ağlar (*switched networks*). Yayın ağlarında, ağa bağlı bir cihaz verileri diğer tüm cihazlara iletir. Buna karşılık, anahtarlamalı ağlarda veriler ağdaki tüm düğümlere gönderilmez; yalnızca kaynak ağdan hedeflenen ağa, çeşitli ara düğümler üzerinden iletilir. Başta internet olmak üzere, günümüzdeki bilgisayar ağlarının çoğu anahtarlamalı ağ yapısına sahiptir.[30]

Anahtarlamalı bir ağda (*switched network*) veri iletimi için farklı yöntemler kullanılmaktadır. Bunlardan en yaygın ikisi devre anahtarlama (*circuit switching*) ve paket anahtarlamadır (*packet switching*). Devre anahtarlama yönteminde, ilk adım iki düğüm arasında iletişime izin verecek bir bağlantı kurmaktır. "Devre" (*circuit*) olarak adlandırılan bu iletişim kanalı, yalnızca ilgili iletişim süresi boyunca var olur ve iletişim sona erdiğinde sonlandırılır. Devre, iki cihaz arasında noktadan noktaya iletişime adanmıştır ve başka herhangi bir iletişim için kullanılamaz.

---

[27] Delerue, *Cyber Operations and International Law,* 31.
[28] Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack", *Strategic Insights* 10/1, (2011), 19–20.
[29] Delerue, *"Cyber Operations and International Law",* 31.
[30] Hossein Bidgoli (ed.), *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications* (New Jersey-Canada: John Wiley and Sons, 2008), 146.

Devre anahtarlamanın temel dezavantajı, kaynakların belirli bir devreye tahsis edilmesi gerekliliğidir. Bu nedenle, devrede veri akışı olmasa bile, devre var olduğu sürece tahsis edilen kaynaklar başka iletişimler için kullanılamaz. Bu durum, bağlantı kapasitesinin boşa harcanmasına yol açar.[31]

Paket anahtarlama yöntemi (*packet-switching method*), 1960'larda devre anahtarlama yöntemine (*circuit-switching method*) alternatif olarak geliştirilmiştir. Bir paket anahtarlama ağında, veriler sabit bir maksimum boyuta sahip paketlere bölünür. Bu paketler, belirli kaynaklar tahsis edilmeksizin ağ üzerinden iletilir; devre anahtarlamanın aksine, veri paketlerinin iletimi için özel bir devre oluşturulmaz. Böylece farklı iletişimlerden gelen paketlerin aynı bağlantıyı paylaşmasına olanak tanınır.

Aynı veri akışına ait paketler, ağ üzerinde farklı bağlantı yollarını izleyebilir. Bu sayede bir ağ düğümü aynı anda farklı düğümlere veri gönderebilir ve onlardan veri alabilir. Bir paketin maksimum boyutunu aşan her mesaj, ağ üzerinde bağımsız olarak seyahat eden birden fazla pakete bölünür. Her paket; kaynak ve hedef adresleri, veri türü, doğrulama bilgileri gibi çeşitli başlık bilgilerini içerir.

Paketler ağ düğümleri arasında "sakla ve ilet" (*store and forward*) yöntemiyle aktarılır. Farklı paketler, son alıcı düğüm tarafından yeniden birleştirilerek orijinal mesaj oluşturulur. İnternetin öncüsü olan ARPANET, paket anahtarlama kullanan ilk ağlardan biridir. Günümüzde paket anahtarlama, veri iletişimi için baskın yöntem olup en yaygın olarak internet tarafından kullanılmaktadır[32]

Ara bağlantı (*interconnection*), küresel internetin yükselişinin önünü açan önemli bir gelişme olarak değerlendirilebilir. Bu duruma örnek olarak, birbirine bağlı farklı cihazlarda bulunan kaynakların Tekdüzen Kaynak Konum Belirleyicileri (*Uniform Resource Locators* – URL) ile tanımlandığı ve hiper metin bağlantıları aracılığıyla birbirine bağlandığı dağıtılmış bilgi hizmeti World Wide Web (WWW) gösterilebilir.

World Wide Web, 1989 yılında Avrupa Nükleer Araştırma Örgütü'nde (*European Organization for Nuclear Research* – CERN) Tim Berners-Lee ve Robert Cailliau tarafından geliştirilmiştir. Günümüzde World Wide Web, hemen herkesin aşina olduğu ve günlük yaşamda rutin olarak kullandığı internet hizmetidir.[33]

İnternette "adresler" bulunmasına rağmen, ".it", ".uk" veya ".tr" gibi menşe ülke alan adı göstergeleri her zaman doğru konumu yansıtmayabilir. İnternet adresleri keyfi olup,

[31] Delerue, *Cyber Operations and International Law",* 31.
[32] Delerue, *Cyber Operations and International Law",* 32-33.
[33] François Delerue, *Cyber Operations and International Law,* 34-35.

sunucular fiziksel ve coğrafi olarak farklı konumlara taşınırken site adresleri sabit kalabilir. Bu nedenle, siber uzay adresleri ile gerçek uzaydaki konumlar arasında kesin bir bağlantı bulunmamaktadır.[34]

Bu teknik açıklamalardan da anlaşılacağı üzere, internet maddi olmayan bir boyutta faaliyet göstermektedir. Bununla birlikte, internet hem fiziksel hem de fiziksel olmayan gerçeklik arasında gidip gelmektedir. Bu durum, internetin merkezi kontrolü olmayan bir varlık olarak mevcut olduğunu göstermektedir. Her birey ve bu bireylere ait bilgisayarlar, internet kullanımını yönetecek merkezi bir otorite olmaksızın özerk şekilde hareket etmektedir. Bu da internetin kimsenin mülkiyetinde olmadığını ortaya koymaktadır. Dolayısıyla, internet ağı coğrafi sınır kavramlarını aşmaktadır.[35]

1.3.Siber Uzayın Sınırları ve Uluslararası Tanım Sorunları

Sınır, dış tehditlerin iç gerçekliğe dönüştüğü noktadır. Devletin hak ve yükümlülüğü, ülkeyi ve halkını dış tehditlerden korumak amacıyla sınırlarından kimin ve neyin geçtiğini kontrol etmektir. Gümrük ve sınır koruma memurları, sınır devriye ajanları ve sahil güvenlik botları, ülkeye giren ve bazı durumlarda ülkeden çıkan kişi ve malzemelerin hareketlerini denetlemek için kullanılan fiziksel önlemlerdir. Bu önlemler, sınırı kimin ve neyin geçmesine izin verileceğini belirlemek ve kontrol etmek amacıyla ülke sınırlarında kurulan fiziksel caydırıcılar ve denetim mekanizmalarıdır. Ancak, siber tehditlerin ortaya çıkması sınır güvenliği alanında köklü değişikliklere yol açmıştır.[36]

İnternet ve siber teknikler, geleneksel sınır güvenliği önlemlerini aşarak suç işleme ve ülkeye, eskiden yalnızca büyük ölçekli askeri operasyonlarla mümkün olan düzeyde zarar verme imkânı sunmaktadır. Teröristler, suçlular ve ulus devletler, siber yöntemlerin asimetrik doğasından faydalanarak devleti ve halkını tehdit edebilir ve zarar verebilirler.[37]

Siber uzayın sınırlarının olup olmadığına dair verilen cevapların çoğu, bu alanın fiziksel sınırlarının bulunmadığını ve dolayısıyla sınırsız olduğunu, bu yüzden fiziksel dünyada geçerli olan hukuka tabi olamayacağını savunmaktadır. Ancak bu görüş doğru değildir. Çünkü veri

[34] Michael P. Fischerkeller, "Current International Law Is Not an Adequate Regime for Cyberspace", *Lawfare* (22 Nisan 2021).
[35] Erin L. Anzelmo, "Cyberspace In Internatıonal Law: Does The Internet Negate The Relevance Of Terrıtorıalıty In Internatıonal Law?", *Egmont Institute* 58/4 (Erişim 9 Şubat 2023), 155-156.
[36] Phillip Osborn, "Cyber Border Security – Defining and Defending a National Cyber Border*", Homeland Security Affairs* 13/ 5 (6 Şubat 2024), 3.
[37] Osborn, "Cyber Border Security – Defining and Defending a National Cyber Border*",* 4.

iletim hatlarının geçtiği fiziksel sınırlar ile verilerin doğrudan yabancı ülkelerden geldiği sınırların işlevsel muadilleri bulunmaktadır.

Siber uzayda sınır kavramı, bilgisayar ağları terminolojisine dahi nüfuz etmiştir; ağlar arasındaki sınırları ifade etmek için "sınır yönlendiricileri" (*border routers*) ve "sınır çizgileri" (demarcation lines) gibi terimler kullanılmaktadır. Bu durum, siber uzayda sınırların varlığını göstermektedir.

"Siber uzayın sınırları var mıdır?" sorusu, uluslararası hukuk kuralları çerçevesinde de ele alınabilir. Bu bağlamda, uluslararası hukukun en temel ilkelerinden olan toprak bütünlüğü ve devlet egemenliği ilkelerinin bu alana uygulanıp uygulanamayacağı test edilmelidir. Kuehl'ün[38] siber uzaya ilişkin tanımı bu konuda yol gösterici olabilir:

"Bilgi-iletişim teknolojilerini kullanarak birbirine bağımlı ve bağlı ağlar aracılığıyla bilgi oluşturmak, depolamak, düzenlemek, değiş tokuş etmek ve kullanmak için elektronik ve elektromanyetik spektrumun kullanılmasıyla ayırt edici ve benzersiz bir karaktere sahip bilgi ortamında küresel bir alan."

Bu tanımdan hareketle, siber uzayın bilgisayarlar, entegre devreler, kablolar, iletişim altyapısı ve benzerlerinden oluşan fiziksel bir katmana (*physical layer*); yazılım, mantık, veri paketleri ve elektronikten oluşan mantıksal bir katmana (*logical layer*); ve insan unsurlarını içeren sosyal bir katmana (*social layer*) sahip olduğu ortaya çıkmaktadır. Bu durum, bir devletin egemenliğini fiziksel katman üzerinde, yani kendi topraklarında bulunan altyapı üzerinde genişletebileceğini göstermektedir. Aynı şekilde, devlet sosyal katman üzerinde, yani kendi topraklarında bulunan kişiler üzerinde de egemenlik yetkisini kullanabilir.

Buna ek olarak, devlet kaynağı ne olursa olsun, kendi topraklarında hissedilen siber faaliyetlerin etkileri üzerinde de egemenliğini ileri sürebilir. Ayrıca devlet, kendi altyapısından geçen veya kendi topraklarında başlayan ya da sona eren bilgi üzerinde de egemenlik iddia edebilir. Yukarıda belirtilenler, toprak bütünlüğü ve devlet egemenliği gibi mevcut uluslararası hukuk normlarının siber faaliyetleri de kapsayabileceğini ve düzenleyebileceğini göstermektedir.[39]

Uluslararası hukuk kurallarının devletin kara, deniz ve hava sınırlarının yanı sıra siber uzayda da geçerli olduğuna dair en önemli çalışma, Birleşmiş Milletler Hükümet Uzmanlar Grubu (*The United Nations Group of Governmental Experts* – GGE)'nun uluslararası güvenlik

[38] Daniel T Kuehl, "From cyberspace to cyberpower: Defining the problem", *Cyberpower and National Security,* mlf. Franklin D. Kramer - Stuart H. Starr - Larry K Wentz, (Amerika: National Defense University Press, 2009), 28.

[39] Nicholas Tsagourias, "The Legal Status of Cyberspace", *Research Handbook on International Law and Cyberspace,* Nicholas Tsagourias - Russell Buchan, (Amerika: Edward Elgar Publishing, 2021), 15-18.

bağlamında bilgi ve telekomünikasyon alanındaki gelişmelere ilişkin 2013 tarihli raporudur. Bu rapor, uluslararası hukukun, özellikle de Birleşmiş Milletler Şartı'nın siber uzay için de geçerli olduğunu ve devlet egemenliği ile egemenlikten kaynaklanan uluslararası norm ve ilkelerin, devletlerin bilgi ve iletişim teknolojileri (BİT) ile ilgili faaliyetlerini yürütmesi ve bir devletin ülkesindeki BİT altyapısı üzerindeki yargı yetkisi için bağlayıcı olduğunu teyit etmiştir.

BM Genel Sekreteri'ne göre, raporda yer alan tavsiyeler "BİT güvenliğinin mevcut uluslararası hukuk çerçevesine ve devlet ilişkilerini yöneten, uluslararası barış ve güvenliğin temelini oluşturan kavramlara sabitlenmesi için ileriye dönük bir yol göstermektedir."[40]

Siber uzayda sınır olgusunu anlamak açısından, Rusya'nın 2016 ABD seçimlerine müdahale ettiği iddiası örnek olarak gösterilebilir.[41] Somut olay, Demokratik Ulusal Komite'nin e-postalarının hacklenmesini ve Demokrat aday Hillary Clinton'ın kampanyasını zayıflatacak bilgiler içeren e-postaların WikiLeaks tarafından yayınlanmasını kapsamaktadır.

ABD İç Güvenlik Bakanlığı (*Department of Homeland Security* – DHS) ile Ulusal İstihbarat Direktörlüğü Ofisi (*Office of the Director of National Intelligence* – ODNI), ortak bir açıklama yaparak Rus hükümetini, ABD seçim sürecine müdahale amacıyla söz konusu materyallerin hacklenmesi ve yayınlanmasından sorumlu tutmuştur.[42]

O dönemde basında yer alan haberlere göre, ABD Başkanı Barack Obama, Rusya Federasyonu Devlet Başkanı Vladimir Putin'e "silahlı çatışmalar hukuku da dahil olmak üzere uluslararası hukukun siber uzaydaki eylemler için de geçerli olduğunu" belirtmiş ve ABD'nin bu olaya vereceği tepkileri değerlendirdiğini ifade etmiştir.[43]

Bilgisayar korsanlığından Rusya'nın sorumlu olduğu varsayımı temelinde, bu olay Birleşmiş Milletler Hükümet Uzmanlar Grubu (*Group of Governmental Experts* – GGE) tarafından siber uzaya uygulanabilir olarak tanımlanan iki uluslararası hukuk ilkesini ilgilendirmektedir: bunlardan biri egemenlik ilkesi, diğeri ise iç işlerine müdahale yasağı ilkesidir. Bu iki ilke, uluslararası hukukun ülkesel sınırlar yaklaşımının merkezinde yer almakta ve bu yaklaşımın temel tezahürleridir.

---

[40] UNGA, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 24 June 2013, UN Doc A/68/98, paras. 19-20.

[41] Jens David Ohlin, "Did Russian Cyber interference in the 2016 Election Violate International Law?" *Texas Law Review* 95 (Erişim 7 Şubat 2024),

[42] Director of National Intelligence, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security" (7 October 2016), available at: https://www.dhs.gov/news/2016/10/07/jointstatement-department-homeland-security-and-office-director-national. (Erişim 7 Şubat 2024).

[43] Nicholas Tsaugourias, "Law, Borders And The Territorialisation Of Cyberspaces*", Indonesian Journal of International Law* 15 /4 (Erişim 8 Mart 2024) 540-541.

GGE, belirli norm ve ilkelerin siber uzaya nasıl uygulanacağı konusunda fikir birliğine varılamaması nedeniyle 2017 yılında bir rapor hazırlayamamıştır. Ancak buna rağmen, önceki raporlar fiziksel dünya için geliştirilen ve uygulanabilir olan, bölgesel olarak sınırlandırılmış alanlarla bağlantılı ilke ve normların siber uzaya da uygulanabileceği görüşünü teyit etmektedir. Bu durum, siber uzayın "ülkeselleştirilmesi" olarak nitelendirilebilir; yani ülkeselci yaklaşımın ve bunun sonucu olarak egemen otorite ve hukuk kavramlarının siber uzaya uygulanmasıdır.

1.4.Kritik Altyapı

Yeni devlet dışı aktörler tarafından siber uzayda gerçekleştirilen faaliyetlerin uluslararası hukukun ihlali olarak değerlendirilebilmesi için, hedef alınan unsurların kritik altyapı niteliğinde olması gerekmektedir. Bu tespitin yapılabilmesi için öncelikle kritik altyapı (*critical infrastructure*) [44] ve kritik enformasyon altyapısı (*critical information infrastructure*)[45] kavramlarının ne anlama geldiğinin incelenmesi gerekmektedir.

Genel olarak "kritik altyapı", devletin toplumsal işlevlerin sürdürülmesi için gerekli gördüğü veya nüfus açısından potansiyel ciddi risk teşkil eden altyapı, varlık ya da sistemleri ifade etmektedir. Bu altyapılar zarar gördüğünde, tahrip edildiğinde veya kesintiye uğradığında, ülke nüfusu için ciddi bir risk oluşturabilir ve devletin güvenliğini olumsuz yönde etkileyebilir.

Kritik altyapıya ilişkin yapılan tanımların çoğu, güvenlik, gıda, su, ulaşım, enerji, sağlık, finans ve bankacılık gibi devlet ve kamu hizmetlerine ait sektörleri kritik altyapı olarak kabul etmektedir. [46] Ancak kritik altyapının neyi kapsadığına dair evrensel olarak kabul edilmiş bir tanım bulunmamaktadır.

Devletlerin çoğu, kritik sektörler ve kritik altyapıların ne olduğunu belirlemek üzere kendi tanımlarını benimsemiştir. Örneğin, Türkiye kritik altyapıları; "içinde işlenen verilerin gizliliğinin, bütünlüğünün veya kullanılabilirliğinin bozulmasının can kaybına, geniş çaplı ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninde bozulmaya yol açabileceği bilgi ve iletişim sistemlerini içeren altyapılar" olarak tanımlamaktadır.[47] Kanada ise kritik

[44] C Gallais - E Filiol, "Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure", *Journal of Information Warfare* 16/1 (2017), 64.
[45] Eugene Nickolov, "Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations", *Informatıon & Securıty: An International Journal* 17 (Ocak 2005), 107.
[46] James A. Lewis, "Cyber Threats to Our Nation's Critical Infrastructure", *Center for Strategic and International Studies (CSIS)* (Ağustos 2018), 2.
[47] Republic of Turkey Ministry of Transport and Infrastructure, "National Cyber Security Strategy and Action Plan (2020-2023)" 23.

altyapılar arasında enerji ve kamu hizmetleri, iletişim ve bilgi teknolojileri, finans, sağlık hizmetleri, gıda, su, ulaşım, hükümet ve imalat sektörlerini saymaktadır.[48]

1996 yılında ABD Başkanı Bill Clinton, kritik altyapıları şu şekilde tanımlamıştır:

"Bazı ulusal altyapılar o kadar hayati öneme sahiptir ki, bunların yetersiz kalması ya da yok olması, Birleşik Devletler'in savunması veya ekonomik güvenliği üzerinde zayıflatıcı bir etki yaratacaktır. Bu kritik altyapılar arasında telekomünikasyon, elektrik güç sistemleri, gaz ve petrol depolama ve nakliyesi, bankacılık ve finans, ulaşım, su tedarik sistemleri, acil durum hizmetleri (tıbbi, polis, yangın ve kurtarma dahil) ve hükümetin sürekliliği yer almaktadır."[49] ABD zamanla kritik altyapılara ilişkin farklı yaklaşımlar benimsemiş ve günümüzde on altı alanı kritik altyapı olarak kabul etmektedir. Bunlar şunlardır: kimyasal alanlar; ticari tesisler; iletişim; hassas imalat; barajlar; savunma sanayi üsleri; acil durum hizmetleri; enerji; finansal hizmetler; gıda ve tarım; devlet tesisleri; sağlık hizmetleri ve halk sağlığı; bilgi teknolojisi; nükleer reaktörler, malzemeler ve atıklar; ulaşım sistemleri; su ve atık su sistemleri.[50]

Uluslararası düzeyde, Birleşmiş Milletler Genel Kurulu 2003 yılında "Küresel Bir Siber Güvenlik Kültürünün Oluşturulması ve Kritik Bilgi Altyapılarının Korunması" hakkında bir karar kabul etmiş ve genel olarak kritik altyapıların enerji üretimi, iletimi ve dağıtımı, hava ve deniz taşımacılığı, bankacılık ve finansal hizmetler, e-ticaret, su temini, gıda dağıtımı ve kamu sağlığı ile ilgili olduğunu belirtmiştir. Bununla birlikte, kararda her ülkenin kendi kritik bilişim altyapılarını belirleme yetkisine sahip olduğu kabul edilmektedir.[51]

Bölgesel düzeyde ise Avrupa Komisyonu, kritik altyapıyı; kesintiye uğraması veya yok olması halinde vatandaşların sağlığı, emniyeti, güvenliği, ekonomik refahı ya da hükümetlerin etkin işleyişi üzerinde ciddi etkilere yol açabilecek bilişim teknolojisi tesisleri, ağları, hizmetleri ve varlıkları olarak tanımlamaktadır.

Komisyon'a göre kritik altyapı şu unsurları içermektedir: enerji tesisleri ve ağları; iletişim ve bilişim teknolojisi; finans sektörü (bankacılık, menkul kıymetler ve yatırım); sağlık hizmetleri; gıda sektörü; su altyapısı (barajlar, depolama, arıtma ve dağıtım ağları); ulaşım sistemleri (havaalanları, limanlar, intermodal tesisler, demiryolu ve toplu taşıma ağları ile trafik kontrol sistemleri); tehlikeli maddelerin (örneğin kimyasal, biyolojik, radyolojik ve nükleer

[48] Marco Roscini, *"Cyber Operations and the Use of Force in International Law",* (London: Oxford University Press, 2014) 57.
[49] Eric Talbot Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", *BYU Law Digital Commons* (Aralık 2002), 226.
[50] François Delerue, *"Cyber Operations and International Law",* 301.
[51] United Nations General Assembly, "Creation of A Global Culture Of Cybersecurity and the Protection of Critical İnformation İnfrastructures," Karar No: A/RES/58/199 (30 Ocak 2004).

malzemeler) üretimi, depolanması ve taşınması; ve devlet yapıları (kritik hizmetler, tesisler, bilgi ağları, varlıklar ile kilit ulusal alanlar ve anıtlar).[52]

Kritik altyapı kavramıyla yakından bağlantılı bir diğer kavram ise kritik bilişim altyapılarıdır (*Critical Information Infrastructure*). Bu kavram ilk kez 2001 yılında G8 ve Ekonomik İşbirliği ve Kalkınma Örgütü (*Organisation for Economic Co-operation and Development* – OECD) tarafından kullanılmaya başlanmıştır. Ancak, bu kavrama ilişkin geniş çapta kabul görmüş ortak bir tanım henüz mevcut değildir.[53]

Kritik bilişim altyapıları kavramı, kritik altyapılar kavramının bir alt kategorisidir ve özellikle bilgisayar ağları ile sistemleri kapsamaktadır. OECD'ye göre kritik bilişim altyapıları, "kesintiye uğraması ya da yok olması durumunda vatandaşların sağlığı, güvenliği, emniyeti veya ekonomik refahını ya da hükümetin ve ekonominin etkin işleyişini ciddi şekilde etkileyebilecek bilgisayar ağları ve sistemleri" olarak tanımlanmaktadır.[54]

Küreselleşen dünya ile birlikte günümüz toplumları ve ekonomileri tamamen bilgi ve iletişim teknolojilerine bağımlı hale gelmiştir. Bu durum, önemli sayıda bilgisayar sistemi ve ağının kritik bilişim altyapısı kategorisinde değerlendirilmesini gerektirmektedir. Bu nedenle, kritik bilişim altyapısına bağımlı devletler, siber saldırılar karşısında oldukça savunmasız konuma gelmektedir.[55] Örnek olarak, 2007 yılında Estonya'ya yönelik gerçekleştirilen siber operasyonlar gösterilebilir. Estonya'ya düzenlenen dağıtılmış hizmet engelleme (*Distributed Denial of Service* – DDoS) saldırıları, ülkenin kritik bilgisayar sistemleri ve ağlarını kesintiye uğratarak devletin işlevselliği üzerinde dramatik sonuçlara yol açmıştır.[56]

1.5.Uluslararası Hukukun Siber Uzaya Uygulanabilirliği

Siber uzay, devletin kara, deniz ve hava ülkelerinden oldukça farklıdır. Siber uzayı diğer alanlardan ayıran en önemli özellik, insan yapımı tek alan olmasıdır. Bu alan, dünyadaki kamu

[52] Commission of the European Communities, "Critical Infrastructure Protection in the Fight against Terrorism", COM(2004) 702 final (Bürüksel: 20 Ekim 2004).
[53] Eric Luiijf, "The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers", *Global Forum on Cyber Expertise* (GFCE), 6.
[54] OECD Recommendation of the Council on the Protection of Critical Information Infrastructures' (2008) C(2008)35; European Union, COM(2009) 149 final (n 133).
[55] Myriam Dunn - Victor Mauer - Isabelle Abele-Wigert , "Understanding Critical Information Infrastructures: An Elusive Quest", The International CIIP Handbook (Mart 2011), 29-32.
[56] European Union (EU), "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009) 149 final, (Bürüksel: 30 Mart 2009).

ve özel sektör paydaşları tarafından kolektif şekilde oluşturulmakta ve teknolojik yeniliklere yanıt olarak sürekli değişmektedir.[57]

Siber uzay, insan yapımı bir alan[58] olduğu için devletin kara, deniz ve hava alanlarının aksine jeopolitik ya da doğal sınırlara tabi değildir. Bu alandaki bilgi ve elektronik yükler, elektromanyetik spektrum aracılığıyla herhangi bir çıkış noktasından herhangi bir varış noktasına anlık olarak iletilmektedir. Bu yükler, varış noktalarına ulaşmadan önce, yeniden oluşturulmadan, öngörülemeyen rotalar boyunca çoklu dijitalleştirilmiş parçalar halinde seyahat ederler.[59]

Bu özelliklerinden dolayı siber uzay devletler, devlet dışı örgütler, özel teşebbüsler ve bireyler tarafından kolayca erişilebilen bir alan olarak görülmektedir. Ancak "IP sahteciliği" (*IP spoofing*)[60] ve botnet kullanımı[61] gibi siber yöntemler bir operasyonun kaynağını gizlemeyi kolaylaştırmaktadır. Bu da siber faaliyetlerin kolaylıkla tespit edilmesini ve ilişkilendirmesini son derece zorlaştırmaktadır.[62]

Siber uzayın kendine özgü özellikleri, bu alanın çatışmaların "beşinci alanı" olup olmadığı tartışmasını gündeme getirmiştir.[63] Kanaatimizce, bu tartışma isabetli değildir. Daha açık bir ifadeyle, siber uzay çatışmaların beşinci alanı olma özelliğine sahip değildir.

Bu sonuca varmak için, diğer dört alan olan kara, deniz, hava ve uzayın özelliklerine bakmak yeterlidir. Her şeyden önce, siber uzay bu alanların aksine insanları ve insan faaliyetlerini "yükleyebileceğimiz" bir alan değildir; çünkü diğer dört alanın aksine siber uzaya "gidemeyiz." Örneğin, insan ve insan faaliyetleri diğer dört alanda konuşlandırılarak gerçekleştirilebilir ve insan bu dört alan arasında seyahat edebilir. Özel hazırlık veya doğru ekipman olmadan denizaltına ya da uzaya gitmek ölümcül sonuçlar doğurabilse de, yine de mümkündür.

---

[57] Uche Mbanaso - E.S. Dandaura, "The Cyberspace: Redefining A New World", *IOSR Journal of Computer Engineering (IOSR-JCE)* 17/3 (Haziran 2015), 17.

[58] Nils Melzer, "Cyberwarfare and International Law", *UNIDIR RESOURCES* (2011), 5.

[59] R. A. Lukman Adewale Quadri - Monsuru Olaitan Rasaq, "Cyber Theatre a Fifth Domain of International Politics: Africa and the rest of the world in the Cyberspace", *AHBV Akdeniz Havzası ve Afrika Medeniyetleri Dergisi* 2/2, (Aralık 2020), 99-100.

[60] "IP sahtekarlığı", gönderenin kimliğini gizlemek veya başka bir bilgisayar sistemini taklit etmek amacıyla sahte bir kaynak adresiyle İnternet Protokolü (IP) paketlerinin oluşturulması anlamına gelmektedir.

[61] "Botnet", kötü niyetli amaçlar için kullanılan, güvenliği ihlal edilmiş bilgisayarların birbirine bağlı bir serisidir. Bir bilgisayar, içine bot yazılımı yerleştirilmiş bir dosyayı çalıştırdığında bir "bot" haline gelmektedir.

[62] Nils Melzer, "Cyberwarfare and International Law", 5.

[63] Thomas Rid, "Cyber War Will Not Take Place", Journal of Strategic Studies 35/1 (Ekim 2011), 165–166. Patrick D Allen and Denis P Gilbert, Jr, "The Information Sphere Domain – Increasing Understanding and Cooperation" in Christian Czosseck and Kenneth Geers (eds), The Virtual Battlefield: Perspectives on Cyber Warfare (IOS Press 2009) 132–142.

Başka bir örnek olarak, denizin altında bulunan bir denizaltı, karada, denizde, havada veya uzayda bulunan nesneleri hedef alabilecek bir füze fırlatabilir. Buna karşılık, siber uzayda bulunan bir nesneyi hedef almak için bu füzeyi denizaltıdan doğrudan fırlatmak mümkün değildir. Mümkün olan tek etkileşim, siber nesnenin depolandığı bilgisayarı hedef almak olacaktır; ancak bu tür bir davranışın kendisi siber uzay ile ilgili değildir.[64]

Siber uzayı diğer alanlardan farklı kılan bir diğer özellik, bu alanın ayrı bir alan olmaktan ziyade, diğer dört alanda bulunan nesneleri etkilemek için kullanılan bir araç olmasıdır. Kara, deniz, hava ve uzay alanları birbirinden farklıdır. Örneğin, hava ile uzay arasındaki sınır açık bir şekilde tespit edilemese de aralarındaki sınır bir şekilde belirlenebilmektedir. Buna karşılık, siber uzay bir alan değildir; ancak dört alanda da konuşlandırılmıştır.

Dolayısıyla siber uzay, karada, havada, denizde ve uzayda insan faaliyetlerini yürütmek ve savaşmak için kullanılan bir araçtır. Örneğin, açık denizlerde bulunan bir tekneden başlatılan bir siber operasyon büyük olasılıkla uydu telekomünikasyonu yoluyla iletilecek, böylece uzay ve havadan geçerek dört alandan herhangi birinde bulunan bir nesneyi hedef alabilecektir.

Bu nedenlerle, siber uzay bir alan (*domain*) ya da bir ortam (*environment*) teşkil etmemekte ve daha da önemlisi beşinci bir savaş alanı olarak değerlendirilmemelidir. Bununla birlikte, siber uzaya yeni bir alan olarak atıfta bulunmanın, teknik doğruluktan yoksun olmasına rağmen, özellikle orduların siber faaliyetlerini tanımlamak için diğer bağlamlarda yararlı olabileceği kabul edilebilir.[65]

Sonuç olarak, uluslararası hukuk çerçevesinde siber uzay, insan faaliyetleri için yeni bir alan (*a new domain*) veya bölge (*area*) değildir. Bu nedenle, siber uzayın hava sahası ve dış uzaydan ayrılması gerekmektedir. Gerçekten de, siber faaliyetler kara, deniz, hava ve dış uzay olmak üzere dört alanda gerçekleşmekte ve dolayısıyla bu alanlara ilişkin uluslararası hukuk normları tarafından düzenlenmektedir. Kanaatimizce, sadece kurgusal bir alan (*a fictional domain*) olması sebebiyle, uluslararası hukukun siber uzaya uygulanabilirliğini sorgulamak gereksiz görünmektedir.[66]

Siber uzay hakkında süregelen tartışmalardan bir diğeri, bu alanın hukuki bir alan olmadığı yönündedir. John Barlow'un *A Declaration of the Independence of Cyberspace* adlı

[64] Christian Czosseck - Kenneth Geers, *The Virtual Battlefield: Perspectives On Cyber Warfare*, (Amsterdam: Ios Press, 2009) 132–142.

[65] Delerue, *Cyber Operations and International Law",* 11-12

[66] Delerue, *Cyber Operations and International Law",* 12-13.

eserinde, "hukuki kavramların siber uzay için geçerli olmadığı" ifade edilmiştir.[67] Siber uzayın hukuki bir alan olmadığı görüşü, bir dizi varsayıma dayanmaktadır. İlk varsayım, siber uzayın diğer dört alandan farklı olduğu düşüncesidir. Çünkü siber uzay, ülkesel olmayan, sınırsız ve her yerde varlık gösteren bir karaktere sahiptir. Bu durum, siber uzayı hukuki düzenlemeye tabi olan fiziksel ve sınırlı alanlardan ayırmaktadır.

İkinci varsayım ise, siber uzayın orijinal kavramsallaştırma ve tasarımına, ayrıca çoklu paydaşların katılımına sadık kalarak, hukuki düzenlemeler tarafından engellenmeyen ya da en azından yalnızca devlet öncülüğündeki düzenlemelere tabi olmayan, açık, merkezi olmayan ve katılımcı bir alan olarak kalması gerektiği düşüncesidir.[68] Ancak, kanaatimizce bu varsayımlar doğru değildir. Aşağıda bu hususlaki görüşlerimize detaylı bir şekilde yer vereceğiz.

Yukarıda da belirttiğimiz üzere, siber uzay uluslararası hukuk açısından yeni bir alan veya bölge teşkil etmemektedir. Bu durum, siber uzayda gerçekleşen faaliyetlerin kara, deniz, hava ve uzay olmak üzere dört farklı alanda meydana gelen ve dijital boyutu bulunan faaliyetler olduğunu göstermektedir. Bu sonuç, uluslararası hukukun siber uzaya uygulanabilirliğine işaret edebilir. Ancak, siber uzaya ilişkin yeni uluslararası hukuk kuralları henüz mevcut değildir. Bu bağlamda, mevcut uluslararası hukuk kurallarının bu alana uygulanabilirliğinin tartışılması gerekmektedir. Çünkü ister antlaşma hukuku ister uluslararası teamül hukuku olsun, uluslararası hukuk kurallarının büyük çoğunluğu siber uzay olgusundan önce geliştirilmiştir.

Bu bakımından günümüzde siber uzayla ilgili uluslararası hukuka konu olan hususların çoğu, 1945 tarihli Birleşmiş Milletler Antlaşması (BM Antlaşması),[69]1949 tarihli *Cenevre* Sözleşmeleri ve Ek Protokolleri[70] ile en önemlisi BM Uluslararası Hukuk Komisyonu tarafından 2001 yılında kodifiye edilen "Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu"na[71] ilişkin taslak maddelere dayanmaktadır. Bu normların siber uzayın icadından önce var olması, siber uzaya uygulanabilirliği açısından engel teşkil etmemelidir. Çünkü yukarıda da ifade edildiği gibi siber uzay, yeni bir alan olmayıp, diğer dört alandaki nesneleri etkilemek için kullanılan bir araçtır. Ayrıca bu normlar, sadece kabul

---

[67] John Perry Barlow, "A Declaration of the Independence of Cyberspace", Electronic Frontier Foundation (EFF), (8 Şubat 1996).

[68] Nicholas Tsagourias, "The legal status of cyberspace: sovereignty redux?". *Research Handbook on International Law and Cyberspace.* ed. Nicholas Tsagourias-Russell Buchan (Massachusetts: Edward Elgar, 2021), 9.

[69] Charter Of The United Natıons, (San Francısco: 1945) Bağlantı Adresi: https://treaties.un.org/doc/publication/ctc/uncharter.pdf

[70] International Committee of the Red Cross, "The Geneva Conventions and their Commentaries", (12 Ağustos 1949).

[71] Responsibility of States for Internationally Wrongful Acts, International Law Commission, General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4.

edildikleri veya kodifiye edildikleri tarihte var olan devlet faaliyetlerine değil, genel olarak devlet faaliyetlerine uygulanmaktadır.

Bu açıklamalardan hareketle, mevcut uluslararası hukuk kurallarının siber uzayda gerçekleşen faaliyetler için uygulanabilir olduğunu söyleyebiliriz. Ancak, mevcut uluslararası hukuk kurallarının siber uzaya uygulanabilirliği hususunda bazı temel sorunlarla karşılaşılmaktadır.

Bu kapsamda Birleşmiş Milletler Uluslararası Uzman Gruplar (BMUUG) tarafından hazırlanan 2013 tarihli "Tallinn Manual On The International Law Applicable To Cyber Warfare" [72] ve 2017 tarihli "Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations"[73] el kitaplarının uluslararası hukuka uygulanabilirliğine ilişkin başarısızlığı örnek olarak gösterilebilir. Ayrıca, devlet dışı aktörlerin kanun yapma sürecindeki artan rollerinin de bu süreci başarısızlığa sürükleyen bir diğer etken olduğu değerlendirilebilir. Bir diğer faktör ise, devletlerin bağlayıcı uluslararası hukuk kuralları yerine, davranış normları ve güven artırıcı önlemler içeren yumuşak hukuk (*soft law*) yaklaşımını benimsemeleridir. Dördüncü olarak ise, siber operasyonlara ilişkin uluslararası hukukun uygulanabilirliğine yönelik yeni bir antlaşma hazırlanmasına dair süregelen tartışmalar bu konudaki karmaşayı artırmaktadır.[74]

Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler, 1998 yılından itibaren Birleşmiş Milletler (BM) Genel Kurulu tarafından tartışılmaya başlanmış ve 4 Ocak 1999 tarihinde 53/70 sayılı kararın kabulüyle sonuçlanmıştır. O tarihten itibaren BM Genel Kurulu, bu konuyla ilgili çok sayıda karar almıştır. Bu kararların en önemli başarılarından biri, 2004, 2009, 2012, 2014 ve 2016 yıllarında uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler üzerine ardışık olarak toplanan beş Birleşmiş Milletler Hükümetler Arası Uzmanlar Grubu'nun (BMHAUG) oluşturulmasıdır. 2004'teki ilk BMHAUG'na katılan uzmanlar bir uzlaşmaya varamamış ve herhangi bir rapor kabul edilmemiştir. Bunu takip eden üç BMHAUG ise 2010 (UN Doc A/65/201),[75] 2013 (UN Doc A/68/98)[76] ve 2015 (UN Doc A/70/174)[77] yıllarında somut sonuçlar elde etmiş ve BM Genel

[72] Michael N. Schmitt (ed.), *"Tallinn Manual On The International Law Applicable To Cyber Warfare",* (Cambridge: Cambridge University Press, 2013).
[73] Michael N. Schmitt (ed.), *"*Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*",* (Cambridge: Cambridge University Press, 2017).
[74] Delerue, *Cyber Operations and International Law,* 13-14.
[75] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *United Nations General Assembly* A/65/201, (30 Temmuz 2010).
[76] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *United Nations General Assembly* A/68/98, (24 Haziran 2023).
[77] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *United Nations General Assembly* A/70/174, (22 Temmuz 2015).

Kurulu tarafından kabul edilen uzlaşı raporlarını kabul etmişlerdir. Üçüncü BMHAUG'nin 2013 raporu, uluslararası hukukun, özellikle de BM Şartı'nın siber uzaya uygulanabilirliğini teyit ettiği için bir dönüm noktası olmuştur ve bu husus daha sonra 2015 raporunda da teyit edilmiştir.[78]

Haziran 2017'de beşinci BM Hükümetler Arası Uzmanlar Grubu (BMHAUG) zirvesi gerçekleştirilmiştir. Ancak katılımcı hükümetlerarası uzmanlar, uluslararası hukukun devletler tarafından bilgi ve iletişim teknolojilerinin kullanımına nasıl uygulanacağını detaylı şekilde ele alan nihai raporun taslak 34. paragrafı üzerinde anlaşmaya varamadıkları için beşinci BMHAUG başarısızlıkla sonuçlanmıştır. Sonuç olarak, herhangi bir rapor kabul edilmemiş ve BMHAUG süreci tıkanmıştır.[79]

2017'deki müzakerelerin başarısız olmasının sebebi, karşı tedbirler, meşru müdafaa ve uluslararası insancıl hukuk gibi uluslararası hukukla ilgili konularda uzlaşı sağlanamamasıdır. Çin, Küba ve Rusya'nın 34. paragrafa karşı çıktığı bildirilmiştir.

Uluslararası hukukun siber uzaya uygulanabilirliğine ilişkin olarak, 2018 sonbaharında Birleşmiş Milletler Güvenlik Konseyi'nin (BMGK) yetmiş üçüncü oturumunda iki karar kabul edilmiştir. Bunlardan ilki, "Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler" (Developments in the field of information and telecommunications in the context of international security) (A/RES/73/27) başlıklı karar olup, Çin ve Rusya'nın da aralarında bulunduğu 31 devlet tarafından önerilmiş ve 119 lehte, 46 aleyhte ve 14 çekimser oyla kabul edilmiştir.[80] İkincisi, "Uluslararası Güvenlik Bağlamında Siber Uzayda Sorumlu Devlet Davranışının Geliştirilmesi" (Advancing Responsible State Behaviour in Cyberspace in the Context of International Security) (A/RES/73/266) adlı karardır. Bu karar, ABD ve Avrupa devletleri de dahil olmak üzere 36 devlet tarafından önerilmiş ve 138 lehte, 12 aleyhte ve 16 çekimser oyla kabul edilmiştir.

Her iki proje de önceki BM Hükümetler Arası Uzmanlar Grubu (BMHAUG) sonuçlarına dayanmakta olup, özellikle 2013 ve 2015 tarihli BMHAUG raporlarını referans göstererek uluslararası hukukun ve özellikle BM Antlaşması'nın siber uzaya uygulanabilirliğini kabul etmektedir. A/RES/73/266 sayılı karar uluslararası hukuk alanında daha ileri bir adım atmazken, A/RES/73/27 sayılı karar ise bazı gelişmeler ekleyerek geçerli uluslararası hukuk ilkelerinin detaylandırılmasını sağlamaktadır.

[78] Delerue, *Cyber Operations and International Law,* 14-15.
[79] Delerue, *Cyber Operations and International Law,* 14.
[80] Developments in the field of information and telecommunications in the context of international security, *United Nations General Assembly* A/RES/73/27 (11 Aralık 2018).

Uluslararası hukukun siber uzaya uygulanabilirliğine ilişkin 2013 tarihli Tallinn el Kitabı'nda [81] uluslararası hukukun ve BM Antlaşması'nın yanı sıra devlet egemenliği ilkesi ve egemenlikten kaynaklanan uluslararası norm ve ilkelerin siber uzay için de geçerli olduğuna açıkça yer verilmiştir.[82] BM Genel Sekreteri'nin de raporun önsözünde belirttiği gibi, "tavsiyeler, Bilgi ve İletişim Teknolojileri (BİT) güvenliğinin mevcut uluslararası hukuk çerçevesine ve devlet ilişkilerini yöneten ve uluslararası barış ve güvenliğin temelini oluşturan anlayışlara sabitlenmesi için ileriye dönük bir yol göstermektedir." [83]

2015 tarihli BM Hükümetler Arası Uzmanlar Grubu (BMHAUG) Raporu, siber uzay için geçerli olan veya olması gereken belirli uluslararası norm ve ilkeleri daha da ileri götürmüştür. Raporda, açık, güvenli, istikrarlı, erişilebilir ve barışçıl bir siber ortamı teşvik etmek amacıyla on bir "bağlayıcı olmayan norm, kural veya devletlerin sorumlu oldukları davranış ilkesi" sıralanmıştır.[84] Ayrıca bu raporda siber uzay ve siber faaliyetler için geçerli olan ve 2021 tarihli 2021 BMHAUG Raporunda[85] da teyit edilen egelenlik ilkesine yer verilmiştir.

Devlet dışı aktörler, uluslararası hukukun siber uzaya uygulanması ve siber normların geliştirilmesinde önemli roller üstlenmektedir. Bu bağlamda, örneğin "Siber Uzayın İstikrarı Küresel Komisyonu" (*The Global Commission on the Stability of Cyberspace* – GCSC) ile çok uluslu şirketlerden Microsoft gibi aktörler aktif biçimde katkıda bulunmuşlardır. Ancak, bu devlet dışı aktörler tarafından geliştirilen düzenlemelerin devletler tarafından henüz resmi olarak onaylanmadığı ve genellikle yumuşak hukuk (*soft law*) kapsamında değerlendirildiği belirtilmelidir.[86]

Devlet dışı aktörler tarafından siber uzaya ilişkin yapılan bu düzenlemelerin devletler tarafından onaylanmaması ve yumuşak hukuk olarak değerlendirilmesinin temel nedeni, devletlerin hukuken bağlayıcı yeni uluslararası hukuk normlarının geliştirilmesine karşı isteksiz olmaları ve bir ölçüde mevcut normlara itiraz etmeleridir.

---

[81] Michael N. Schmitt (ed.), *"Tallinn Manual On The International Law Applicable To Cyber Warfare",* (Cambridge: Cambridge University Press, 2013).
[82] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/68/98 (24 June 2013) paras 19–20.
[83] UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/68/98 (24 June 2013) paras 19–20.
[84] UNGA, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (22 July 2015) para 13.
[85] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security *United Nations General Assembly* A/76/135 (14 Temmuz 2021)
[86] François Delerue, *Cyber Operations and International Law,* 22.

Siber saldırıların düzenlenmesine ilişkin devlet uygulamaları, devletlerin hukuki olarak bağlayıcı normlardan çok, bağlayıcı olmayan normları tartışmaya daha yatkın olduklarını göstermektedir. Bu durum Birleşmiş Milletler (BM) düzeyinde de geçerlidir. Çünkü birbirini takip eden BM Hükümetler Arası Uzmanlar Grubu (BMHAUG) çalışmalarında, uluslararası hukukun ve BM Antlaşması'nın uygulanabilirliği kabul edilmiş; ancak süreç sonunda sadece davranış normları ve güven artırıcı önlemler benimsenmiştir. Bu durum, BMHAUG'un esasen yumuşak hukuk (*soft law*) ürettiğini göstermektedir. Hukuki bağlayıcılığı bulunmayan bu normların bazıları, uluslararası hukuktaki mevcut bağlayıcı normların yansıması olup, nasıl yorumlanmaları gerektiği konusunda ipuçları sunmaktadır. Ancak normların çoğu tamamen yenidir ve mevcut bağlayıcı normlardan bağımsızdır. Sonuç olarak, bu normlar uluslararası hukukun mevcut kurallarının siber uzay ve siber operasyonlara uygulanması konusunda doğrudan bir etkiye sahip değildir.

Uluslararası hukukun siber operasyonlara uygulanmasına ilişkin dünya devletlerinin tutumu açısından, Rusya genel olarak yeni bir uluslararası antlaşmanın kabul edilmesini desteklemektedir. Buna karşılık, ABD ve Avrupa devletleri mevcut uluslararası hukuk kurallarının siber uzay bağlamında yorumlanması gerektiğini savunmaktadır. Devlet dışı bir aktör olan Microsoft ise, sivilleri devlet destekli siber saldırılardan korumayı amaçlayan uluslararası bir antlaşmanın kabul edilmesi gerektiğini ileri sürmektedir. Microsoft'un bu önerisi genel olarak "Dijital Cenevre Sözleşmesi" olarak adlandırılmaktadır.[87]

Kanaatimizce, uluslararası hukukun siber uzaya uygulanmasına yönelik yaklaşımda daha çok mevcut uluslararası hukuk normlarının yorumlanmasına odaklanılmalı; buradan hareketle, uluslararası hukukun mevcut kapsamı dikkate alınarak, yeni normların kabulünü haklı çıkaracak potansiyel uluslararası hukuk boşlukları tespit edilmelidir.

1.6.Uluslararası Hukuk Kişisi Olarak Gerçek Kişiler ve Şirketler

Klasik uluslararası hukuk anlayışında kişilik yalnızca devletlere atfedilmiştir. Bu yaklaşım, Montevideo Sözleşmesi gibi temel belgelerde tanımlanan egemenlik ve toprak unsurlarına dayanan bir sistemin ürünüdür. Ancak uluslararası toplumun normatif, yapısal ve işlevsel anlamda dönüşüme uğradığı günümüzde, bu sınırlı kişilik tanımı yetersiz kalmaktadır. Uluslararası hukukta kişilik mutlak ve durağan bir kategori olmaktan ziyade, toplumsal ihtiyaçlara ve uluslararası ilişkilerin dönüşümüne bağlı olarak evrilen dinamik bir yapıdır. Bu

[87] Brad Smith, "The need for a Digital Geneva Convention", *Microsoft* (17 Şubat 2017), 1.

görüş, Uluslararası Adalet Divanı'nın (UAD) 1949 tarihli "Birleşmiş Milletler Hizmetinde Uğranılan Zararların Tazmini" konulu danışma görüşünde açıkça dile getirilmiştir.[88] UAD'ye göre, bir varlığın uluslararası kişilik kazanması yalnızca kurucu belgelerde açıkça belirtilmiş olmasına değil, aynı zamanda uluslararası toplumun işlevsel ihtiyaçlarına da dayanır. Bu esnek ve işlevsel yaklaşım, bireyler ve şirketler gibi yeni aktörlerin uluslararası hukuk öznesi olabilmesi için teorik ve pratik zemini oluşturmaktadır.

Bu bağlamda bireylerin uluslararası hukukta hem hak sahibi hem de sorumlu fail olarak konumlanmaları, kişilik kazandıklarını ortaya koymaktadır. II. Dünya Savaşı sonrası dönemde gelişen uluslararası insan hakları hukuku, bireylere doğrudan haklar tanımaya başlamış ve bu hakların devletlere karşı bireysel düzeyde ileri sürülebilmesini mümkün kılmıştır. Avrupa İnsan Hakları Sözleşmesi kapsamında bireysel başvuru hakkı, bireyin yalnızca ulusal hukuk sisteminde değil, uluslararası alanda da aktif bir hukuk süjesi olduğunu göstermektedir. Bu durum, bireyin sadece devlet aracılığıyla hak arayabileceği yönündeki klasik anlayışla açık bir tezat oluşturmaktadır. Öte yandan, Uluslararası Ceza Mahkemesi (UCM) Statüsü ve Eski Yugoslavya ile Ruanda Uluslararası Ceza Mahkemelerinin statüleri, bireyleri doğrudan uluslararası yükümlülük altına sokmuş; bireylerin soykırım, savaş suçları ve insanlığa karşı suçlar gibi eylemler nedeniyle bireysel olarak cezai sorumluluk taşımalarını öngörmüştür. Bu gelişmeler ışığında, bireylere hem hak hem de yükümlülük yükleniyor olması, onları uluslararası hukuk kişisi olarak kabul etmenin doğal bir sonucudur.

Benzer şekilde, çok uluslu şirketler de uluslararası hukukta giderek artan bir rol oynamaktadır. Her ne kadar bu şirketler devletler gibi tam yetkili özne olmasalar da, günümüz koşullarında doğrudan hak ve yükümlülük sahibi olmaktadırlar. Bu durum, hem devletlerle yapılan uluslararası yatırım anlaşmaları hem de Birleşmiş Milletler İş Dünyası ve İnsan Hakları Rehber İlkeleri (UNGPs) gibi normatif belgeler aracılığıyla somutlaşmaktadır.[89] Çok uluslu şirketler, yalnızca devletlerle değil, aynı zamanda uluslararası örgütlerle ve diğer şirketlerle uluslararası düzeyde ilişki kurabilme kapasitesine sahiptir. Montevideo Sözleşmesi'nde yer alan "diğer devletlerle ilişkiye girme kabiliyeti" kriteri, günümüzde tüm uluslararası hukuk kişilerine uygulanabilecek genel bir kriter halini almıştır.[90] Bu kapsamda şirketler, sadece ulusal düzeyde değil, uluslararası düzeyde de yükümlülük üstlenmekte ve uluslararası toplumun parçası olarak kabul edilmektedir. Örneğin çevre hukukunda ve iş dünyasına yönelik insan

[88] Uluslararası Adalet Divanı (UAD), *Birleşmiş Milletler Hizmetinde Uğranılan Zararların Tazmini Danışma Görüşü* (1949), ICJ Reports 1949, 174.
[89] United Nations Human Rights Council (UNHRC), *Guiding Principles on Business and Human Rights* (New York – Geneva: United Nations, 2011), HR/PUB/11/04.
[90] Montevideo Devletlerin Hak ve Yükümlülükleri Sözleşmesi (Montevideo Sözleşmesi), 26 Aralık 1933, md. 1.

hakları standartlarında, çok uluslu şirketlerin doğrudan yükümlülük altına alınması bu eğilimin bir tezahürüdür.

Bu çerçevede, uluslararası hukuk kişiliğinin belirlenmesinde yeni bir kriter olarak "uluslararası toplumla etkileşime girme kabiliyeti" önerilmektedir. Artık uluslararası kişilik yalnızca devlet egemenliğine ya da kurumsal yapıların tanınmasına dayanmamakta; bir varlığın uluslararası aktörlerle hukukî ilişki kurabilme kapasitesi, kişilik değerlendirmesinde belirleyici unsur hâline gelmektedir. Bireyler, uluslararası mahkemelere bireysel başvuru yaparak; şirketler ise devletlerle bağlayıcı sözleşmeler akdederek ve uluslararası normlara tabi olarak bu etkileşimi gerçekleştirmektedirler. Bu türden bir etkileşim, söz konusu aktörlerin sadece pasif hukuk nesneleri değil, aktif hukuk süjeleri olduklarını göstermektedir.

Sonuç olarak, uluslararası hukukun kişileri yalnızca statik devlet yapıları değil, günümüzün değişen dünya düzeninde ortaya çıkan yeni aktörlerdir. Bireyler ve çok uluslu şirketler, artık uluslararası hukukun marjinal unsurları değil; sınırlı da olsa gerçek ve etkin öznesi konumundadırlar. Bu aktörlerin sahip oldukları haklar ve yükümlülükler, onların uluslararası hukuki statülerinin tanınmasını zorunlu kılmaktadır. Dolayısıyla, uluslararası hukuk kişiliği kavramı, "tam" ve "kısmi" ayrımı çerçevesinde yeniden yorumlanmalı; uluslararası toplumla doğrudan ilişkiye girme kapasitesine sahip her aktör, belirli düzeyde bir uluslararası hukuk öznesi olarak değerlendirilmelidir.

Bu dönüşüm, uluslararası hukukun yalnızca devletlerin sistemi olmaktan çıktığını ve çok aktörlü, çok katmanlı bir yapıya evrildiğini göstermektedir. Günümüz itibarıyla gerçek kişiler ve çok uluslu şirketler, uluslararası hukukun pasif nesneleri değil, aktif ve sorumluluk taşıyan hukuk aktörleridir.

2. SİBER TEHDİTLER VE HUKUKİ DEĞERLENDİRİLMESİ

21. yüzyılın başından itibaren dijital teknolojilerdeki hızlı gelişmeler, devletlerin, özel sektörün ve bireylerin faaliyetlerini köklü bir biçimde dönüştürmüş; bu dönüşüm beraberinde yeni tehdit alanlarını da getirmiştir. Özellikle devletler arası ilişkilerde, geleneksel güvenlik anlayışının ötesine geçen siber uzay, günümüzde hem egemenlik hem de uluslararası barış ve güvenlik açısından stratejik bir alan hâline gelmiştir. Kritik altyapılara yönelik siber saldırılar, kamu hizmetlerinin durmasına, ekonomik kayıplara ve hatta ulusal güvenliğin zafiyete uğramasına yol açabilecek boyutlara ulaşmıştır. Bununla birlikte, devlet dışı aktörlerin gelişmiş siber yeteneklere sahip olmaları, tehdit spektrumunu daha da karmaşıklaştırmaktadır. Bu bağlamda, siber tehditlerin tespiti, sınıflandırılması ve bunlara karşı alınacak önlemlerin hukuki

çerçevesinin belirlenmesi, gerek ulusal gerekse uluslararası hukuk açısından ciddi bir ihtiyaç hâline gelmiştir. Ancak siber tehditlerin sınır aşan, aktör çeşitliliği içeren ve teknik olarak dinamik yapısı, mevcut hukuki düzenlemelerin yetersizliklerini de ortaya koymaktadır. Aşağıda, siber tehditlerin uluslararası düzeyde nasıl tanımlandığını, hangi hukuki araçlarla değerlendirildiğini ve mevcut normatif boşlukların nasıl doldurulabileceği incelenmiştir.

2.1.Kötü Amaçlı Yazılımlar

Kötü amaçlı yazılım (*malware*), bilgisayar güvenliği bağlamında her türlü kötü amaçlı yazılım için kullanılan genel bir terimdir.[91] Kötü amaçlı yazılım, kötü niyetli yazılım (*malicious software*) anlamına da gelmektedir. Bu kapsamda yazılım (*software*) üzerinde bulunduğu bilgisayara ya da başka bir bilgisayara zarar vermek için kullanılabiliyorsa potansiyel olarak kötü niyetlidir. Yazılım ayrıca, bilgisayar sahibinin izni olmadan kendisini bir bilgisayara yüklemek üzere tasarlanmışsa, özellikle de bunu bilgisayarın güvenliğini tehlikeye atabilecek şekilde yapıyorsa, kötü amaçlı olarak kabul edilebilir. Görüldüğü üzere kötü niyetli (*malicious*) ve yazılım (*software*) terimleri biraz esnek yorumlanabilmektedir. Örneğin bir yazılım parçası, tartışılabilir bir fayda sağlamak amacıyla başlatılmış olsa bile kötü niyetli olarak nitelendirilebilir. Kötü amaçlı yazılımlar, hedef sisteme sokulma şekline ve neden olması amaçlanan kural ihlalinin türüne bağlı olarak genellikle birkaç sınıfa ayrılmaktadır. Bunlara aşağıda detaylı olarak yer verilecektir.

2.1.1. Virüs

Kötü amaçlı yazılım türlerinden biri olan bilgisayar virüsleri, bir program içinde var olabilen, mevcut sistemde çoğalabilen, bir dosya veya programdan diğerine yayılabilen, dosyalar kopyalanıp paylaşıldığında başka bilgisayarlara bulaşabilen ve dosyalara zarar verebilen yazılımlardır.

Virüs kavramı, zamanla, bir bilgisayarın kötü amaçlı yazılımlar tarafından saldırıya uğrayabileceği tüm farklı yolları ifade eden genel bir terim hâline gelmiştir. Bir virüs; bilgisayarı izlemek, şifreleri çalmak, reklam görüntülemek veya sistemi çökertmek gibi amaçlarla kullanılabilir.

[91] Robin Sharp, "An Introduction to Malware", *DTU Library* (2007), 1.

Virüslerin en belirgin özelliği yayılma biçimleridir. Örneğin, taşınabilir bir USB bellekteki bir dosyaya virüs bulaşırsa, bu bellek bir bilgisayara takılıp çalıştırıldığında virüs o bilgisayardaki dosyalara bulaşarak yayılır. Ardından, aynı bellek başka bir cihaza takıldığında o cihaz da virüsle enfekte olur ve bulaşma zinciri devam eder.[92]

2.1.2. Solucanlar

Solucanlar, virüslere benzemekle birlikte farklı bir yayılma stratejisine sahiptir. Virüslerin aksine, bir dosyaya bulaşarak insan etkileşimi yoluyla yayılmak yerine, solucanlar kendi başlarına hareket edebilir ve ağ bağlantılarını kullanarak yayılır.

Virüsler gibi, solucanlar da bir sisteme bulaştıktan sonra çeşitli zararlara neden olabilir. Hızlı ve yaygın şekilde çoğalabilen solucanlar, e-posta ekleri, dosya paylaşımı veya güvenlik açıklarından yararlanma gibi yöntemlerle diğer bilgisayarlara bulaşabilir. Bu durum, hedef sistemlerin çökmesine ve internet bağlantılarının ciddi ölçüde yavaşlamasına yol açabilir.[93]

2010 yılında İran'da gerçekleşen Stuxnet Saldırısı, virüsler ve solucanlar bağlamında önemli bir örnek teşkil etmektedir. İran'ın nükleer tesislerini hedef alan bu saldırının, ABD'li ve İsrailli uzmanlar tarafından geliştirildiğine inanılan sofistike bir kodla gerçekleştirildiği iddia edilmektedir.

Stuxnet, bulaştığı sistemlere "ortadaki adam" yazılımı yerleştirerek makine ile kontrol bilgisayarı arasındaki bağlantıyı kesmiş, ayrıca ana bilgisayara herhangi bir sorun bildirmeyerek sistemdeki hataları gizlemiştir. Bu sayede saldırı uzun süre fark edilmemiştir. Sonuç olarak İran'ın nükleer çalışmaları ciddi şekilde sekteye uğramış ve yaklaşık 30 bin bilgisayar etkilenmiştir. Hatta Stuxnet'in, Çernobil'e benzer bir nükleer felakete yol açabilecek kapasitede olduğu öne sürülmüştür. Bu olay, virüsler ve solucanlar aracılığıyla gerçekleştirilen sofistike siber saldırıların ne denli etkili ve tehlikeli olabileceğini açıkça göstermektedir.[94]

[92] Erdi Şafak, "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 28/1 (Şubat 2020), 138.
[93] Şafak, "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", 138.
[94] Şafak, "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar", 139.

2.1.3. Truva Atı

Truva atları, genellikle kötü amaçlı yazılım (*malware*) olarak adlandırılan kötü amaçlı kod (*malicious code*) veya kötü amaçlı yazılımların (*malicious software*) bir alt türüdür.[95] Bu tür yazılımlar, faydalı veya zararsız bir amaca hizmet ediyormuş gibi görünen, ancak gerçekte gizli ve kötü niyetli işlevler barındıran programlardır. Truva atlarının barındırdığı kötü amaçlı işlevler; izinsiz dosya indirme, veri hırsızlığı veya diğer bilgisayarlara saldırı düzenleme gibi çok çeşitli zararlı faaliyetleri kapsayabilmektedir.[96]

Truva atı, bir bilgisayara veya mobil cihaza indirilebilmek için yasal bir programı ya da uygulamayı taklit eden bir tür kötü amaçlı yazılımdır. Truva atı saldırılarında, sosyal mühendislik teknikleri kullanılarak yasal yazılımın içine gizlenmiş kötü amaçlı kod, dağıtım mekanizması olarak işlev görür. Kurbanın bu yazılımı çalıştırması, saldırgana kendi zararlı yazılımını devreye sokma ve hedef sistem üzerinde yetkisiz erişim sağlama imkânı tanır.[97]

Truva atı saldırıları farklı şekillerde gerçekleştirilebilir. Örneğin, kullanıcının cihazına e-posta yoluyla gönderilen bir ek veya genellikle bu ekin içine gizlenmiş kötü amaçlı yazılım içeren ücretsiz indirilebilir bir dosya, "Truva atı nedir?" sorusuna verilebilecek basit bir örnek olacaktır. Saldırganın tasarladığı görevin yerine getirilmesi için kötü amaçlı kod, dosya eki indirildiği anda çalışmaya başlar. Bu kod, hassas verileri çalmak, işletim sistemine arka kapı erişimi sağlamak, kullanıcıların çevrimiçi faaliyetlerini izlemek veya sistem düzeyinde kalıcı bir erişim elde etmek amacıyla kullanılabilir.

Çoğu bilgisayar ve mobil virüsün aksine, Truva atı kendiliğinden yayılmaz. Bir Truva atının ortaya çıkması için kullanıcının, saldırgan tarafından hazırlanan yazılım veya uygulamayı indirmesi gerekir. Başka bir ifadeyle, bir Truva atı saldırısının kullanıcının cihazında veya sisteminde çalışabilmesi için yürütülebilir dosyanın —örneğin bir Excel dosyasının, Android paketinin (APK) veya iOS uygulama paketinin— cihaza yüklenmiş olması şarttır.[98]

Truva atı virüsünü daha geniş bir kitleye yaymak için genellikle yasal görünümlü e-posta ekleri, uygulamalar ve yazılımlar kullanılır. E-posta açılıp kötü amaçlı ek indirildiğinde, Truva atı sunucusu yüklenir ve virüslü cihaz her açıldığında otomatik olarak etkinleşir. Ayrıca

[95] Dan Tang - Xiao-Hong Kuang, "A Generic Model for Trojan Horse Attacks Prevention and Handling" *Atlantis Press* (Ekim 2015), 189.
[96] Susan W. Brenner-Brian Carrier - Jef Henninger, "The Trojan Horse Defense In Cybercrime Cases", *The Santa Clara High Technology Law Journal* 21/1 (2004), 5.
[97] Senesh N. Wijayarathne, "Trojan Horse Malware-Case Study", *Sri Lanka Institute of Information Technology (SLIIT)* (Temmuz 2022), 1.
[98] Wijayarathne, "Trojan Horse Malware-Case Study", 2.

afiş reklamları, web sitelerindeki bağlantılar, çevrim içi reklamlar ve açılır pencereler de Truva atı saldırısına yol açabilecek gizli kötü amaçlı dosyalar barındırabilir.

Truva atı kötü amaçlı yazılımının bulaştığı tüm cihazlar, bu yazılımı diğer cihazlara da yayabilir. Bu durumda siber saldırgan, cihazı bir "zombi" cihaza dönüştürerek, kullanıcının haberi olmadan cihazın uzaktan kontrolünü ele geçirir. Siber saldırgan, zombi cihazı kullanarak Truva atı kötü amaçlı yazılımını veya diğer kötü amaçlı yazılımları ve virüsleri ağdaki bağlı cihazlar arasında yaymaya devam edebilir; bu tür bir ağ yapısı "botnet" olarak adlandırılmaktadır.[99]

Truva atı virüsünü daha iyi anlamak için aşağıdaki kurgusal örneğe bakalım. Bir kullanıcı, yakın etkileşimde olduğu bir kişiden meşru görünen bir dosya eki içeren bir e-posta alır. Ancak, e-posta yoluyla gönderilen bu ek, kullanıcının cihazına bir Truva Atı yükleyecek kötü niyetli bir kod uygulaması içermektedir. Truva Atı cihaza yüklendiğinde, kullanıcı cihazına kötü amaçlı bir yazılım bulaştığını fark etmeyebilir çünkü cihaz, Truva Atı'ndan kaynaklanan herhangi bir belirti veya müdahale olmaksızın normal şekilde çalışmaya devam edecektir. Kullanıcı belirli bir web sitesini ziyaret edene, bankacılık uygulamasını kullanana ya da belirli eylemleri gerçekleştirmeye başlayana kadar kötü niyetli kod gizli kalacaktır. Kullanıcının bu eylemi gerçekleştirmesiyle kötü amaçlı kod aktif hale gelecek ve siber saldırganın istediği işlemleri yerine getirecektir. Truva Atı çalıştırıldıktan sonra işlevlerini devre dışı bırakabilir, normale dönebilir ya da aktif kalarak kurbanın cihazında çalışmaya devam edebilir.[100]

2.1.4. Yazılım Bombası

Yazılım bombası, yazılıma gömülü olan ve belirli koşullar sağlanana kadar hareketsiz kalan bir tür kötü amaçlı koddur. Bir yazılım bombası saldırısı gerçekleştiğinde, dosyaların silinmesi veya kritik sistemlerin zarar görmesi gibi yıkıcı sonuçlar ortaya çıkabilir. Geleneksel kötü amaçlı yazılımların aksine, yazılım bombası aktif olarak yayılmaz; bunun yerine önceden tanımlanmış bir tetikleyici olayı bekler.

[99] Wijayarathne, "Trojan Horse Malware-Case Study", 3.
[100] Wijayarathne, "Trojan Horse Malware-Case Study", 3.

Yazılım bombası diğer uygulamalarda çoğalmaz. Daha açık bir ifadeyle yalnızca tasarlandığı yazılım için çalışır. Yazılım bombasının sistemde bulunması, sistemin güvenliği ve bütünlüğü için büyük riskler oluşturmaktadır.[101]

Altyapısının bilgisayar ağlarına bağlı olduğu devletler yazılım bombası saldırılarına karşı oldukça savunmasız durumdadırlar. Yazılım bombası saldırısının en bilinen örneklerinden biri 1982 yılında meydana gelmiş olup Trans-Sibirya Boru Hattı olayı olarak bilinmektedir. 1982 yılında Sibirya'dan geçen önemli bir boru hattında meydana gelen büyük bir patlama doğal gaz akışını kesintiye uğrattı. Yıllar boyunca bunun bir CIA sabotajı olduğu söylentisi devam etti. ABD istihbarat ajanları Sovyet meslektaşlarının boru hattını otomatik hale getirmek için gerekli bilgisayar kodunu Batı'dan çalmaya çalıştıklarını keşfetmişlerdi, çünkü yerli Sovyet yazılım endüstrisi bu işe uygun değildi; bu nedenle Amerikalılar Sovyetlerin içine yazılım bombası saklanmış bir kodla kaçmalarına izin verdiler ve bu da boru hattının tahrip olmasına neden oldu. Bu olay bilinen ilk siber saldırı vakası olarak kaydedildi.[102]

2.2.Teknik Saldırı Yöntemleri

Siber uzaydan kaynaklanan tehditlerin etkili bir şekilde anlaşılabilmesi ve bu tehditlere karşı hukuki ve teknik önlemlerin geliştirilmesi için, öncelikle kullanılan saldırı yöntemlerinin teknik yapısının detaylı biçimde incelenmesi gerekmektedir. "Teknik saldırı yöntemleri" ifadesi, bilgi sistemlerine izinsiz erişim sağlama, verileri bozma, çalma, manipüle etme veya sistemleri çalışamaz hâle getirme amacıyla geliştirilen çeşitli dijital araç ve yöntemleri kapsamaktadır. Bu yöntemler arasında IP spoofing, dijital manifülasyon, hizmet dışı bırakma saldırıları (*DDoS*), oltalama (*phishing*), kalıcı hizmet engelleme (*PDoS*) ve sürekli gelişmiş tehdit (*APT*) gibi teknikler öne çıkmaktadır. Söz konusu saldırılar, yalnızca bireysel düzeyde değil; aynı zamanda devletlerin kritik altyapılarına, kamu hizmetlerine, seçim sistemlerine ve uluslararası finansal ağlara yöneltilerek geniş çaplı zararlar doğurabilmektedir. Dolayısıyla aşağıda, siber saldırganlar tarafından yaygın olarak kullanılan teknik yöntemler kategorik biçimde ele alınacak; işleyiş mekanizmaları, tespit zorlukları ve mevcut teknik savunma kapasitesiyle birlikte değerlendirilecektir.

[101] Palash Sandip Dusane - Yallamandhala Pavithra, "Logic Bomb: An Insider Attack", *International Journal of Advanced Trends in Computer Science and Engineering* 9/3 (Mayıs-Haziran 2020), 3662.
[102] Josh Fruhlinger, "Logic bomb attacks: 4 famous examples", *CSO* (1 Haziran 2022), 2.

2.2.1. IP Spoofing

IP Spoofing, göndericinin kimliğini gizlemek veya başka bir bilgisayar sistemini taklit etmek amacıyla, spoofing adı verilen sahte bir kaynak IP adresi ile İnternet Protokolü (IP) paketlerinin oluşturulması anlamına gelmektedir. IP spoofing, diğer bağlantıları taklit etmek ve bilgi gönderirken kimliğini gizlemek amacıyla sahte IP adresleri içeren IP paketleri oluşturarak IP adresini gizlemektedir. Bu yöntem, spam gönderenler ve dolandırıcı kişiler tarafından başkalarını gönderdikleri bilgilerin kaynağı konusunda yanıltmak için kullanılan yaygın bir tekniktir.[103]

IP Spoofing bilgisayarlara yetkisiz erişim sağlamak için kullanılan bir tekniktir. Bu teknikte saldırgan, mesajın güvenilir bir ana bilgisayardan geldiğini gösteren IP adresine sahip bir bilgisayara mesaj göndermektedir. IP sahtekarlığı tekniğini kullanmak için bir bilgisayar korsanının öncelikle güvenilir bir ana bilgisayarın IP adresini bulmak amacıyla çeşitli teknikler kullanması ve ardından paket başlıklarını değiştirerek paketlerin bu ana bilgisayardan geliyormuş gibi görünmesini sağlaması gerekmektedir.[104]

IP sahteciliğinin bir başka yaygın kullanımı da IP adresine veya bölgeye dayalı kullanıcı kimlik doğrulamasının atlatılabilmesidir. Örneğin, birçok şirket bir intranet sistemi kullanmaktadır. Bu intranetteki tüm içeriğe erişmek için, erişim talep eden makinelerin, güvenilir bir makine olarak algılandığını veya makineye güvenilir bir konumdan erişildiğini gösteren belirli bir geçerli aralık dahilinde bir IP adresine sahip olması gerekmektedir. Güvenilir bir makineden sahte bir bağlantı kurarak, kişiler bu kimlik doğrulama yöntemini atlayabilir ve ağa yasadışı olarak erişebilirler.[105]

IP sahteciliği genellikle iki amaç için kullanılır: İnternet tabanlı saldırılar başlatmak ve bir bilgisayar sistemine yetkisiz erişim sağlamak.

IP sahteciliği, çevrimiçi suç faaliyetlerinde bulunmak ve ağ güvenliğini ihlal etmek için kullanılmaktadır. Bilgisayar korsanları IP sahteciliğini spam gönderirken yakalanmamak ve hizmet reddi saldırıları gerçekleştirmek için kullanmaktadır. Bu saldırılar, tüm ağı çökertmek amacıyla bir ağ üzerinden bilgisayarlara büyük miktarda bilgi gönderilmesini içermektedir. Saldırılarda sahte IP adresinden dolayı mesajların kaynağı tespit edilemediği için bilgisayar korsanı yakalanmamaktadır.

---

[103] Ritika Arora -Sunny Behal, "Ip Spoofing", *Shaheed Bhagat Singh College of Engineering* (Ocak 2010), 2.
[104] Arora - Behal, "Ip Spoofing", 2.
[105] Asma Basharat - Rabia Sirhindi - Ahmad Raza Cheema -Imtiaz Khokhar, "A Novel Solution for IP Spoofing Attacks*", 6th WSEAS International Conference on Information Security and Privacy*, Tenerife, Spain, (Aralık 2007), 108-109.

IP sahteciliği ayrıca bilgisayar korsanları tarafından ağdaki adreslerden birini yansıtan sahte bir IP adresi kullanarak ağ güvenlik önlemlerini ihlal etmek için de kullanılmaktadır. Bu, bilgisayar korsanının ağda oturum açmak için bir kullanıcı adı ve parola sağlama ihtiyacını ortadan kaldırmaktadır.[106]

2.2.2. Dijital Manipülasyon

Siber uzayda gerçekleştirilen faaliyetlerden biri de bilgisayar programları ve yazılımları kullanarak yeni bir anlam yansıtan sahte bir görüntünün üretilmesidir. Bu teknik dijital manipülasyon olarak adlandırılmaktadır. Dijital manipülasyon, medya içeriği görüntülerinin veya videolarının daha benzersiz, aşırı ve farklı görünmesini sağlamak için değiştirilmesi, saptırılması veya başkalaştırılmasıdır.[107]

Bu teknikte manipülasyona uğrayan görüntüleri tespit etmek oldukça zordur. Bu da fotoğrafta yer alan kişi veya nesnelerin fotoğrafın çekildiği zaman gerçekten de orada olup olmadıklarının tespitini neredeyse imkânsız hale getirmektedir.

Dijital manipülasyon sadece kişiler üzerinde değil devletler üzerinde de olumsuz etkilere neden olabilir. Örneğin bu yöntemde bir devlet, diğer devletlerin internetinde yer alan görüntülerin değiştirilmesinden dolayı kolaylıkla fotoğraf manipülasyonuna maruz kalabilir. Bir başka örnek olarak silah çatışmalar zamanı çekilen video kayıtlar üzerinde yapılan dijital manipülasyonlardan bahsedebiliriz. Savaşan taraflardan birine ait bir video üzerinde ön planda hareket eden herhangi bir kişi ya da nesne değiştirilebilir, çıkarılabilir ve videoda yer almayan nesneler videoya eklenerek gerçekmiş gibi gösterilebilir.[108]

2.2.3. Oltalama

Oltalama (*phishing*) saldırıları, kullanıcılara gönderilen sahte e-postalar, kısa mesajlar, telefon aramaları veya web siteleri aracılığıyla gerçekleştirilmektedir. Kullanıcılar, bu platformlar üzerinden gelen içeriklere tıklayarak kötü amaçlı yazılımları indirir, hassas

[106] Arora - Behal, "Ip Spoofing", 2.
[107] Asmita Parajuli, "Digital Manipulation On Social Media", *Social Media and Online Journalism* (Şubat 2022), 6.
[108] Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", 1189.

bilgilerini ve kişisel verilerini paylaşır ve farkında olmadan kendilerini ve kuruluşlarını siber suçlara maruz bırakan diğer eylemleri gerçekleştirirler.[109]

Bu yöntemde saldırgan, cazip bir taleple saygın bir kaynak gibi görünerek, bir balıkçının balık yakalamak için yem kullanmasına benzer şekilde, kurbanı kandırmak için cezbetmektedir. Örneğin, popüler sosyal medya sitelerinden, açık artırma platformlarından, çevrimiçi ödeme işlemlerinden ya da BT yöneticisinden geldiğini iddia eden iletiler, genellikle masum insanları tuzağa düşürmek için kullanılmaktadır.[110]

Oltalama yöntemi çoğunlukla e-posta korsanlığında kullanılmaktadır. Bu yöntemde, bilgisayar korsanı örneğin bazı banka bilgileri veya diğer kişisel bilgiler için kullanıcıya e-posta yoluyla sahte bir bağlantı göndermektedir. Kullanıcı bu bağlantıya tıkladığında, açılan sayfadaki tüm bilgileri doldurmakta ve böylece bilgisayar korsanı kullanıcının tüm bilgilerine erişim sağlamaktadır.[111]

2.2.4. Hizmet Reddi ve Dağınık Hizmet Reddi Saldırısı (DDoS))

Hizmet reddi (*DoS*) saldırısı, bir ağın veya bilgisayarın yetkili kullanıcılara hizmet vermesini engelleyen bir saldırı olarak tanımlanmaktadır.[112] Bir başka tanıma göre ise hizmet reddi saldırısı, bilgi işlem veya iletişim hizmetini bozmak veya durma noktasına getirmek, böylece yetkili kullanıcıların erişimini engellemek için tasarlanmış kasıtlı bir eylemdir.[113] Bununla birlikte hizmet reddi, yazılımdaki hatalar ve kötü kodlama gibi kasıtsız eylemlerin yanı sıra kasıtlı istismar eylemlerinden de kaynaklanabilmektedir. Bu saldırı türü siber saldırılar arasında en yaygın olanıdır.

Hizmet reddi saldırıları, bir sunucuyu yavaşlatmak amacıyla sunucuya milyonlarca istek göndermekten, sunucuyu geçersiz verilerden oluşan büyük paketlerle doldurmaya, geçersiz veya sahte IP adresiyle istek göndermeye kadar uzanmaktadır.[114] Hizmet reddi saldırısının

---

[109] Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", *International Journal of Multidisciplinary Studies and Innovative Technologies* 1/1 (2017), 26.
[110] Vaishnavi Bhavsar- Aditya Kadlak- Shabnam Sharma, "Study on Phishing Attacks", *International Journal of Computer Applications* 182/33 (Aralık 2018), 27.
[111] Bhavsar- Kadlak- Sharma, "Study on Phishing Attacks", 27.
[112] Nirwan Ansari- Amey Shevtekar, *"On the New Breed of Denial of Service (Dos) Attacks In The Internet"*, Strategic Studies Institute, US Army War College, 2011), 281.
[113] H. L. Armstrong, "Denial of Service and Protection of Critical Infrastructure", *Journal of Information Warfare* 1/2 (2001), 24.
[114] Khaled M. Elleithy- Drazen Blagovic -Wang Cheng- Paul Sideleau, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", *Journal of Systemics Cybernetics and Informatics* 3/1 (Ocak 2006), 66.

avantajı, daha büyük ve ileri teknolojiye sahip bilgisayar veya ağı hızlı bir şekilde etkisizleştirebilmesidir.[115]

Hizmet reddi (Denial of Service - DoS) saldırılarına aşağıdaki örnekler verilebilir:

- Bir ağı "flood" ederek meşru ağ trafiğinin önüne geçmek;
- İki makine arasındaki bağlantıları bozarak bir hizmete erişimi engellemek;
- Belirli bir kişinin bir hizmete erişimini engellemeye çalışmak;
- Belirli bir sisteme veya kullanıcıya sunulan hizmeti kesintiye uğratmak.[116]

Eğer bir saldırı dünya çapında birçok noktadan gerçekleştirilirse, buna dağıtık hizmet reddi saldırısı (*Distributed Denial of Service* - DDoS) denir. DDoS saldırısı sırasında, dünya genelindeki çok sayıda sistem mağdur olan sisteme eş zamanlı olarak saldırabilir. DoS ve DDoS saldırılarını tamamen önlemek neredeyse imkânsızdır.[117]

DoS ve DDoS saldırıları, kullanılan protokollerin yanı sıra saldırının dağılımına göre çeşitli şekillerde sınıflandırılabilmektedir. DDoS saldırılarını üç ana sınıfa ayırmak mümkündür: TCP Tabanlı Saldırılar, TCP/UDP Tabanlı Saldırılar ve UDP Tabanlı Saldırılar.

Her sınıfta, kullanılan protokol türü ve saldırıların amacı farklılık göstermektedir. *Email Flooding, SYN Flooding, Ping of Death* ve *Reflection* saldırısı, DDoS saldırılarının en bilinen türlerindendir. SYN Flooding saldırısında, saldırgan sahte (taklit) bir kaynak adresi kullanarak birkaç paket gönderir; hedef ise SYN/ACK ile yanıt verir, ancak yanıt hiçbir yere ulaşmaz. Belirli bir süre sonra hedef sistem daha fazla isteği karşılayamaz hale gelir ve kullanılamaz duruma düşer. Ping of Death saldırısında ise, saldırgan ping komutunu kullanarak büyük boyutlu paketler göndererek hedef sistemin çökmesine neden olmaya çalışır.[118]

2007 baharında, Rusya yanlısı olduğu düşünülen kişi ve grupların gerçekleştirdiği üç haftalık küresel Dağıtık Hizmet Engelleme (DDoS) saldırıları, Estonya'nın resmi, siyasi, mali ve diğer web siteleri ile e-hizmetlerini hedef almıştır. Bu olay, dünya çapında ilk büyük siber savaş eylemi olarak yaygın bir şekilde kabul edilmektedir.

Bu saldırılar sırasında, Rus (ya da Rusça konuşan) bilgisayar korsanları tarafından forumlarda paylaşılan değiştirilmiş saldırı araçları ve daha sonra "kiralanmış" botnetler, Estonya'nın internete erişimini neredeyse tamamen engelledi. İki saldırı dalgası yaşandı ve bunlardan ikincisi, birincisinden çok daha ileri düzeydeydi. Saldırılar, Estonya hükümetinin

[115] Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", 1188.
[116] Felix Lau- Stuart H. Rubin- Michael H. Smith- Ljiljana Trajkovic, "Distributed Denial of Service Attacks", *Advancing Technology for Humanity* (Aralık 2024), 2275.
[117] Ömer Aslan, "A Methodology to Detect Distributed Denial of Service Attacks", *Bilişim Teknolojileri Dergisi* 15/2 (Nisan 2022), 150.
[118] Aslan, "A Methodology to Detect Distributed Denial of Service Attacks", 150.

Sovyet döneminden kalma bir savaş anıtı olan Bronz Asker ile Tallinn'in mezar yerini değiştirme niyetine karşı açık bir tepkiydi. Rusya, herhangi bir bağlantısı olduğunu reddetti ve kendisinin de hedef olduğunun kanıtı olarak uğradığı nispeten küçük bir saldırıyı gösterdi.[119]

2.2.5. Kalıcı Hizmet Engelleme (PDoS)

Günümüzün dinamik siber tehdit ortamında, kalıcı hizmet engelleme (*PDoS*) saldırıları özellikle yıkıcı siber tehditler olarak kabul edilmektedir. Geçici kesintilere neden olan geçici hizmet reddi (*DoS*) saldırılarının aksine, *PDoS* saldırıları geri dönüşü olmayan donanım hasarlarına, önemli ekonomik zararlara, sağlık hizmetleri ve kritik altyapı gibi alanlarda insan hayatına yönelik tehditlere neden olabilmektedir.

PDoS saldırılarına örnek olarak *2017 NotPetya* saldırısı gösterilebilir. *NotPetya* saldırısında binlerce bilgisayar kalıcı olarak tehlikeye atılarak küresel çapta milyarlarca dolarlık zarara yol açmıştır. [120]

Çok çeşitli sofistike stratejiler kullanan geçici hizmet reddi (*DoS*) saldırılarından farklı olarak, *PDoS* saldırıları hem yazılımı (*software*) hem de donanımı (*hardware*) hedef almaktadır. *PDoS* stratejileri sadece kesinti oluşturmanın ötesine geçerek kalıcı zarar vermeyi amaçlamaktadır.

Siber suç araçlarının giderek yaygınlaşması, daha az nitelikli saldırganların bile güçlü *PDoS* saldırıları başlatabilmesine neden olmaktadır. Örneğin, kullanıma hazır *DDoS* araçları ve DoS kötü amaçlı yazılımlarına artık dark web üzerinden kolayca erişilebilmekte ve bu da potansiyel saldırganlar için giriş bariyerini düşürmektedir. 2017'deki *NotPetya* salgını ve Ukrayna kamu hizmetlerine yönelik *2015 BlackEnergy* saldırısı gibi yüksek profilli olaylar, *PDoS* saldırılarının gelişen ve tehlikeli doğasını vurgulamaktadır.[121]

PDoS saldırılarını tespit etmek, kalıcı ve genellikle geri döndürülemez hasar verme eğilimleri nedeniyle doğası gereği oldukça karmaşıktır. Modern *PDoS* saldırganları geleneksel saldırı tespit sistemlerini atlatmak için genellikle IP sahteciliği ve meşru trafiği taklit etme (*mimicking legitimate traffic*) gibi ince ve uzun vadeli taktikler kullanmaktadır.

---

[119] Andreas Schmidt, "The Estonian Cyberattacks", *Delft University of Technology* (Ocak 2013), 1-2.
[120] Stanislav Abaimov, "Understanding and Classifying Permanent Denial of Service Attacks", *Preprints.org*, (Şubat 2024), 2.
[121] Abaimov, "Understanding and Classifying Permanent Denial of Service Attacks", 2-3.

2.2.6. Sürekli Gelişmiş Tehdit (APT)

Advanced persistent threat (APT) en kapsamlı ve güçlü güvenlik tehdidi sınıfı olarak kabul edilmektedir. APT, bir davetsiz misafirin uzun süre boyunca hassas verileri çalmak için ağda tespit edilmeyen bir varlık oluşturduğu sofistike, sürekli bir siber saldırıdır. Bir APT saldırısı, belirli bir kuruluşa sızmak ve mevcut güvenlik önlemlerinden uzun süre kaçmak için dikkatlice planlanır ve tasarlanır.[122]

Görüldüğü üzere APT, sıradan bir bilgisayar korsanı tarafından yapılan bir saldırı değildir. APT'ler çoğunlukla bir kuruluş ya da devlet tarafından iyi finanse edilen bir grup gelişmiş saldırgan tarafından hedef aldıkları kuruluş ya da devlet hakkında önemli bilgiler elde etmek amacıyla gerçekleştirilmektedir.[123]

APT, devletler tarafından gerçekleştirilen saldırıları ifade eden ve bilgi güvenliği bağlamına uyarlanmış askeri bir terimdir. APT üç kelimenin birleşimiyle tanımlanır, bunlar:

Advanced: APT saldırısı gerçekleştirenler genellikle iyi finanse edilmekte ve bir APT saldırısı gerçekleştirmek için gereken gelişmiş araç ve yöntemlere erişebilmektedirler. Bu gelişmiş yöntemler, saldırıyı başlatmak ve devam ettirmek için birden fazla saldırı vektörünün kullanılmasını içermektedir.

Persistent: APT saldırganları oldukça kararlı ve ısrarcıdırlar. Bir kez sisteme girdiklerinde, sistemde kalabildikleri kadar uzun süre kalmaya çalışmaktadırlar. Takip ettikleri hedefin saldırı tespit sistemleri tarafından fark edilmemesi için çeşitli kaçamak teknikler kullanırlar. Başarı oranlarını artırmak için "düşük ve yavaş" (*low and slow*) yaklaşımını izlerler.[124]

Threat (Tehdit): APT saldırılarındaki tehdit çoğunlukla hassas veri kaybı ya da kritik bileşenlerin veya görevlerin işlevsiz hale gelmesidir. Bunlar, görevlerini ve/veya verilerini koruyan gelişmiş koruma sistemlerine sahip birçok ulusal kurum ve kuruluş için artan tehditlerdir.[125]

---

[122] Atif Ahmad - Jeb Webb - Kevin C. Desouza - James Boorman, "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack", *Computers & Security* 86/5 (2019), 402.

[123] Adel Alshamrani -Sowmya Myneni - Ankur Chowdhary- Dijiang Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities", *IEEE Communıcations Surveys & Tutorials* 21/2 (2019), 2.

[124] Alshamrani - Myneni - Chowdhary- Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities", 2.

[125] Alshamrani - Myneni - Chowdhary- Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities", 2.

Ulusal Standartlar ve Teknoloji Enstitüsü'ne (*National Institute of Standards and Technology* - NIST) göre, bir APT saldırganı: (i) hedeflerini uzun bir süre boyunca takip eder; (ii) savunma tarafının kendisine karşı koyma çabalarına uyum sağlar; ve (iii) hedeflerini gerçekleştirmek için gereken etkileşim düzeyini sürdürmeye kararlıdır. Bu hedefler bilgi sızdırma ya da çoklu saldırı vektörleri aracılığıyla bir görev ya da programın kritik yönlerini zayıflatma ya da engellemedir.[126]

2.3.Siber Saldırı, Siber Savaş ve Siber Suç Arasındaki Farklılıklar

Siber uzay kavramında olduğu gibi, "siber saldırı" kavramı için de genel kabul görmüş bir tanım bulunmamaktadır.[127] Bu durumun temel nedeni, siber uzaydaki farklı nitelikteki faaliyetleri aynılaştırma çabasıdır. Başka bir deyişle, "siber savaş", "siber saldırı" ve "siber suç" gibi kavramların çoğu zaman aynı statüde değerlendirilerek tanımlanmaya çalışılması, ortak bir tanımın ortaya çıkmasını güçleştirmektedir. Oysa bu kavramlar, uygulanacak hukuk bakımından birbirinden farklı niteliklere sahiptir. Bu nedenle, siber uzaydaki aktörler tarafından gerçekleştirilen tüm fiilleri yalnızca "siber saldırı" (*cyber attack*) olarak nitelendirmek doğru olmayacaktır. Daha açık bir ifadeyle, "siber saldırı", "siber savaş" ve "siber suç" terimleri, içerikleri yeterince dikkate alınmadan sıklıkla birbirinin yerine kullanılmakta ve bu durum anlamlı bir hukuki yanıt oluşturmayı güçleştirmektedir. Dolayısıyla, aşağıda siber saldırı türlerine geçmeden önce, "siber saldırı" kavramının ne olduğunun açıklığa kavuşturulması gerekmektedir. Bu husus, siber uzaya uluslararası hukukun uygulanabilirliğinin belirlenmesi açısından da önem taşımaktadır.

Siber saldırı, "siyasi veya ulusal güvenlik amacıyla bir bilgisayar ağının işlevlerini zayıflatmaya yönelik herhangi bir eylem" olarak tanımlanabilir. Bu tanım, "siber saldırı" kavramının üç yaygın biçimini ortaya koymak suretiyle, onu "siber savaş" (*cyber warfare*) ve "siber suçlar" (*cyber crime*) kavramlarından ayırmaktadır. Bu bağlamda, siber saldırılar; dağıtılmış hizmet reddi saldırıları (*distributed denial of service – DDoS attacks*), yanlış bilgi yerleştirme (*planting inaccurate information*) ve güvenli bir bilgisayar ağına sızma (*infiltration of a secure computer network*) şeklinde gerçekleşebilmektedir.[128]

---

[126] Alshamrani - Myneni - Chowdhary- Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities", 2.

[127] Şeyda Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", *İstanbul Hukuk Mecmuası* LXXI/1 (Ağustos 2013) 1179.

[128] Oona A. Hathaway- Rebecca Crootof - Philip Levitz - Haley Nix - Aileen Nowlan - William Perdue - Julia Spiegel, "The Law of Cyber-Attack", *California Law Review* 100/4 (Ağustos 2012) 821.

On yılı aşkın bir süredir analistler, bir siber saldırının olası sonuçlarına ilişkin çeşitli senaryolar üzerinde spekülasyon yapmaktadır. Bu senaryolar; finansal kayıtların tahrif edilmesi, borsanın işlevsiz hale getirilmesi, bir nükleer reaktörün devre dışı bırakılması, bir barajın açılmasına yol açacak yanlış bir mesajın iletilmesi veya hava trafik kontrol sisteminin devre dışı bırakılması sonucu uçak kazalarının meydana gelmesi gibi örnekleri kapsamaktadır.[129] Tüm bu öngörüler, siber saldırıların ciddi ve yaygın ekonomik ya da fiziksel zararlara yol açabileceğini göstermektedir. Her ne kadar bu senaryoların hiçbiri bugüne kadar gerçekleşmemiş olsa da çok sayıda siber olay düzenli olarak meydana gelmektedir. Ancak bu olayları "siber savaş" olarak nitelendirmek bir yana, "siber saldırı" olarak tanımlamak için dahi genel kabul görmüş bir tanım mevcut değildir. Bu tanımsal belirsizlik, siber uzaya uygulanacak hukuki rejimin belirlenmesini de güçleştirmektedir. Bu nedenle, öncelikle "siber saldırı" kavramına ilişkin teknik bir çerçevenin ortaya konulması gerekmektedir.

Siber saldırı terimine ilişkin tanımlar arasında en yaygın kabul görenlerden biri, güvenlik uzmanı Richard A. Clarke'a aittir. Clarke, siber savaşı "bir devletin, başka bir devletin bilgisayarlarına veya ağlarına zarar vermek ya da onları bozmak amacıyla gerçekleştirdiği sızma eylemleri" olarak tanımlamaktadır. Benzer şekilde, eski ABD Ulusal Güvenlik Ajansı (*National Security Agency* – NSA) ve Merkezi İstihbarat Teşkilatı (*Central Intelligence Agency* – CIA) direktörü Michael Hayden, siber savaşı "başka bir ülkenin bilgisayar ağlarını devre dışı bırakmaya veya yok etmeye yönelik kasıtlı girişim" şeklinde tanımlamaktadır. Ancak bu tanımlar, "siber suç", "siber saldırı" ve "siber savaş" kavramları arasında net bir ayrım yapmamaktadır. Bu nedenle, söz konusu tanımlar savaş kavramının siber bağlamda tehlikeli derecede geniş yorumlanmasına imkân tanımaktadır. Ayrıca, Clarke'ın tanımı bir açıdan dar kapsamlıdır; zira siber saldırıları yalnızca devletler tarafından gerçekleştirilen fiillerle sınırlamakta ve böylelikle devlet dışı aktörler tarafından gerçekleştirilebilecek tamamen makul senaryoları kapsam dışında bırakmaktadır.[130]

ABD Genelkurmay Başkanlığı, 2011 yılında siber operasyonlarda askeri kullanım amacıyla, "siber saldırı" kavramının ilk resmi askeri tanımını içeren bir sözlük yayımlamıştır. Bu tanıma göre siber saldırı, "bilgisayar veya ilgili ağlar ya da sistemler kullanılarak gerçekleştirilen ve karşı tarafın kritik siber sistemlerini, varlıklarını veya fonksiyonlarını bozmayı ve/veya yok etmeyi amaçlayan düşmanca bir eylemdir." Tanımda ayrıca, siber saldırının istenen etkilerinin yalnızca hedef alınan bilgisayar sistemleri veya verilerin kendileriyle sınırlı olmadığı belirtilmektedir. Örneğin, altyapıyı veya komuta-kontrol

[129] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 822.
[130] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 823-824.

(*Command and Control* – C2) kapasitesini bozmayı ya da yok etmeyi hedefleyen bilgisayar sistemlerine yönelik saldırılar da bu kapsamda değerlendirilmektedir. Buna ek olarak, bir siber saldırı; çevresel cihazlar, elektronik vericiler, gömülü kod veya insan operatörler gibi ara dağıtım araçlarını kullanabilir. Tanıma göre bir siber saldırının etkileri veya aktivasyonu, geçici nitelikte olabileceği gibi coğrafi olarak saldırının gerçekleştirildiği yerden oldukça uzakta da ortaya çıkabilir.[131]

Bu yaklaşımın en önemli özelliği, "siber saldırı"yı kritik siber sistemlere zarar vermeyi amaçlayan düşmanca eylemlerle sınırlandırması ve tanımı saldırının amacına göre kısıtlamasıdır.[132] Buna karşılık, Şanghay İşbirliği Örgütü (ŞİÖ) siber saldırılara ilişkin olarak daha geniş kapsamlı, araç-temelli bir yaklaşım benimsemiştir. Örgüt, "yeni bilgi ve iletişim teknolojilerinin" hem sivil hem de askeri alanlarda, uluslararası güvenlik ve istikrarla bağdaşmayan amaçlar doğrultusunda kullanılma ihtimalinin yarattığı tehditlere dair endişelerini dile getirmiştir.[133] Bu çerçevede, ŞİÖ "enformasyon savaşı"nı, "toplumu ve devleti istikrarsızlaştırmak ve devleti karşı tarafın çıkarına olacak kararlar almaya zorlamak amacıyla kitlesel psikolojik beyin yıkama" olarak tanımlamaktadır. Ayrıca, örgüt "diğer devletlerin sosyal, siyasi, ekonomik, manevi, ahlaki ve kültürel sistemlerine zararlı bilgilerin yayılmasını" da bilgi güvenliğine yönelik başlıca tehditlerden biri olarak görmektedir.[134] Görüldüğü üzere, Şanghay İşbirliği Örgütü, siyasi istikrarı baltalamak amacıyla siber teknolojilerin kullanılmasını da siber saldırı kapsamında değerlendirmektedir.

Buradan hareketle, siber saldırıya ilişkin olarak çalışmamız açısından daha uygun görülen tanım şu şekildedir:

"Bir siber saldırı, siyasi veya ulusal güvenlik amacıyla bir bilgisayar ağının işlevlerini zayıflatmak için gerçekleştirilen herhangi bir eylemden oluşur."

Bu tanım, bir siber saldırının hangi unsurları içermesi gerektiğini anlamak bakımından önemlidir. Daha açık bir ifadeyle, bir fiilin siber saldırı olarak nitelendirilebilmesi için bazı temel unsurların bulunması gerekmektedir. Öncelikle, siber saldırı niteliğindeki fiil aktif bir davranış olmalıdır. Ayrıca, bu tür bir saldırı; hackleme, bombalama, iletişimi kesme, virüs bulaştırma gibi çeşitli yollarla gerçekleştirilebilir. Ancak, söz konusu eylemin "siber saldırı" sayılabilmesi için nihai amacının bir bilgisayar ağının işlevini zayıflatmak veya bozmak olması

[131] Memorandum For Chiefs of The Mılıtary Servıces Commanders Of The Combatant Commands Dırectors Of The Joınt Staff Directorates, "Joint Terminology for Cyberspace Operations", (Washington: D.C. 20318-9999, Kasım 2011).
[132] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 824.
[133] DoD, U.S. Department of Defense. "Joint Terminology for Cyberspace Operations." Kasım 2010. Erişim 13 Temmuz 2025. https://info.publicintelligence.net/DoD-JointCyberTerms.pdf.
[134] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 825.

gerekir. Bu yönüyle, tanım Şanghay İşbirliği Örgütü'nün araç-temelli yaklaşımından ziyade, Amerika Birleşik Devletleri'nin amaç-temelli yaklaşımını benimsemektedir.

Bir bilgisayar ağı farklı şekillerde tehlikeye atılabilir. Kod temelli saldırılar (*code-based attacks*), bir bilgisayarın işletim sistemini bozarak ağın arızalanmasına neden olur; bu tür saldırılara örnek olarak solucanlar (*worms*), virüsler (*viruses*) ve Truva atları (*Trojan horses*) verilebilir. Buna karşılık, semantik saldırılar (*semantic attacks*), işletim sistemini korumakla birlikte sistemin işlediği ve tepki verdiği bilgilerin doğruluğunu hedef alır. Bu tür saldırılarda, sistem ya normal şekilde çalışmaya devam eder ya da öyleymiş gibi görünür; ancak gerçekte yanlış veya yanıltıcı çıktılar üretir. Nitekim, aşağıda ayrıntılı olarak ele alınacak olan Stuxnet saldırısı kısmen semantik bir saldırı niteliği taşımaktadır; zira hedef alınan nükleer santral arızalı olmasına rağmen, sistem onu normal çalışıyormuş gibi göstermekteydi.

Buna karşılık, ne siber casusluk (*cyber espionage*) ne de siber sömürü (*cyber exploitation*) bir siber saldırı olarak nitelendirilebilir; zira bu eylemler, bilgisayar ağlarının mevcut veya gelecekteki işleyiş kabiliyetlerini etkileyecek şekilde değiştirilmesini içermemektedir. Örneğin, 2003 yılında birkaç ay boyunca devam eden bir güvenlik ihlali, Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı'na ait bilgisayarlardan çok sayıda hassas bilginin sızmasına yol açmıştır. Bakanlık, topluca "Titan Yağmuru" (*Titan Rain*) olarak adlandırılan bu tür olayların çoğunun, Çin tarafından bir siber casusluk yöntemi olarak gerçekleştirildiğini teyit etmiştir.[135]

Söz konusu siber casusluk olayı, her ne kadar askeri bir amacı gerçekleştirmek üzere bir bilgisayar ağının güvenliğini tehlikeye atmış olsa da, bir bilgisayar sisteminin "işlevini zayıflatmamış" ve dolayısıyla yukarıda belirtilen tanıma göre bir siber saldırı teşkil etmemiştir. Bir bilgisayar sisteminin işlevini zayıflatmak için, bir aktörün bilgisayar ağını gizli olsa dahi yalnızca pasif şekilde gözlemlemesi veya verileri kopyalaması yeterli değildir. Bunun ötesinde, aktörün ya işletim sistemine zarar vermesi ya da yanlış, yanıltıcı veya istenmeyen bilgiler ekleyerek sistemin işleyişini etkilemesi gerekmektedir. Bu tür faaliyetler, şirketler veya siyasi amaç güden aktörler tarafından gerçekleştirildiğinde siber casusluk kapsamında suç teşkil edebilir; ancak siber saldırı niteliğinde değildir. Bu bakımdan, yukarıda sunduğumuz tanım, casusluk ile daha geleneksel ortamlarda gerçekleştirilen saldırılar arasındaki yaygın ayrımı yansıtmaktadır.[136]

Siber saldırının hedefi mutlaka bir bilgisayar ağı olmalıdır. Burada bilgisayar ağı, iletişim kanalları aracılığıyla birbirine bağlı bilgisayarlar ve cihazlardan oluşan bir sistem

[135] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 825.
[136] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 830.

anlamına gelmektedir. Önemle belirtilmelidir ki, günümüzde "bilgisayar" kavramı artık yalnızca masaüstü veya dizüstü bilgisayarlardan ibaret değildir. Daha kapsamlı bir ifadeyle, bilgisayarlar asansörleri ve trafik ışıklarını kontrol eden sistemlerden, su şebekesindeki basıncı düzenleyen altyapılara; cep telefonları, televizyonlar ve hatta çamaşır makineleri gibi günlük hayatımızda yaygın şekilde kullanılan akıllı cihazlara kadar her yerde bulunmaktadır. Bu kapsamda, siber saldırıların geniş çaplı zarar verme potansiyeli, bilgisayarların insan faaliyetlerinin neredeyse tüm alanına yayılmasıyla birlikte önemli ölçüde artmaktadır.[137]

Bir fiilin siber saldırı olarak nitelendirilebilmesi için son ve en önemli unsur, söz konusu eylemin siyasi veya ulusal güvenlik amacıyla gerçekleştirilmiş olmasıdır. Bu unsur, siber saldırıları basit siber suçlardan ayıran temel kriterdir. Bir devlet aktörü tarafından siber alanda gerçekleştirilen herhangi bir saldırgan fiil, mutlaka ulusal güvenliği ilgilendirmekte olup, bu fiil siber savaş seviyesine yükselse de yükselmese de siber saldırı olarak kabul edilir. Bu bağlamda, devlet dışı bir aktör tarafından siyasi veya ulusal güvenliğe yönelik işlenen bir siber suç da siber saldırı kapsamında değerlendirilmektedir. Öte yandan, internet dolandırıcılığı, kimlik hırsızlığı veya fikri mülkiyet korsanlığı gibi siyasi veya ulusal güvenlik amacı taşımayan siber suçlar, bu tanımdaki son unsura uymadığından yalnızca siber suç olarak kalmaktadır.[138] Yukarıda açıklanan esaslar doğrultusunda, aşağıda siber saldırı, siber suç ve siber savaş arasındaki farklılıklar ortaya konacaktır:

Siber suç (*cyber-crime*), yalnızca devlet dışı aktörlerin taraf olduğu ve ceza hukuku kurallarını ihlal eden bir suç türüdür; bu suçlar bilgisayar sistemleri aracılığıyla işlenir. Buna karşılık, siber saldırı (*cyber-attack*), bir bilgisayar ağının işlevini zayıflatmayı ve siyasi veya ulusal güvenliğe yönelik tehdit oluşturacak bir amaca hizmet etmeyi amaçlayan eylemleri ifade eder. Bu unsurlar, siber savaş (*cyber-warfare*) kavramı için de geçerlidir. Ancak, siber uzayda gerçekleştirilen fiillerin siber savaş olarak kabul edilebilmesi için, söz konusu fiillerin etkilerinin "silahlı saldırı" ile eşdeğer olması veya silahlı çatışma kapsamında gerçekleştirilmiş olması gerekmektedir.

Siber suç, siber saldırıya kıyasla oldukça geniş kapsamlı bir kavramdır ve her iki terim için de genel kabul görmüş ortak bir tanım mevcut değildir. Bununla birlikte, siber suç, siber saldırının aksine bazı genel kabul görmüş özelliklere sahiptir. Genel anlamda siber suç, hukuk dışı bir fiilin işlenmesi amacıyla bilgisayar tabanlı bir aracın kullanılması olarak tanımlanmaktadır. Daha kapsamlı bir tanıma göre ise siber suç, "bir bilgisayar, ağ veya donanım

[137] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 830.
[138] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 830.

cihazı kullanılarak kolaylaştırılan veya işlenen herhangi bir suç" şeklinde ifade edilmektedir. Her iki tanımdan da anlaşılacağı üzere, siber suçlar siber saldırılardan farklı olarak, genellikle araçlarıyla yani bilgisayar sistemleri veya ağlarıyla tanımlanır ve çok geniş bir yelpazede hukuk dışı fiilleri kapsar. Bu kapsamda, internet dolandırıcılığı, çevrimiçi korsanlık, çocuk pornografisinin bilgisayarda depolanması ve paylaşılması ile bilgisayara izinsiz girişler gibi eylemler siber suç olarak kabul edilmektedir.

Siber suç ile siber saldırı arasındaki en temel farklardan biri, siber saldırıların aksine, siber suçlarda hedef bilgisayar ağına zarar verilmesinin zorunlu olmamasıdır. Diğer bir önemli fark ise, siber suçların siyasi veya ulusal güvenlik amacı taşımaması ve genellikle devlet dışı aktörler tarafından işlenmesidir; oysa siber saldırılar siyasi veya ulusal güvenlik amacı güder ve çoğunlukla devlet aktörleriyle ilişkilendirilir.[139]

Siber suçlar bakımından dikkat edilmesi gereken bir diğer önemli husus, birçok siber suçun aynı zamanda siber saldırı veya siber savaş unsuru da barındırabilmesidir. Ancak devlet dışı bir aktör tarafından işlenen bir fiil, yalnızca ulusal veya uluslararası hukuk tarafından suç sayılıyorsa siber suç teşkil eder. Aşağıda, her biri doğrudan bir siber saldırı fiili olmasa dahi, siber suç unsuru taşıyan üç farklı senaryo ele alınacaktır.

İlk senaryoda, devlet dışı bir aktör bir bilgisayar ağı aracılığıyla siyasi veya ulusal güvenliğe yönelik hukuka aykırı bir eylem gerçekleştirmekte ancak bu ağa doğrudan zarar vermemektedir. Örneğin, bir birey internet üzerinden iktidara karşı muhalif görüşlerini ifade ederek ilgili iç hukuk kapsamında siber suç işleyebilir; ancak bu eylem ağın işleyişine zarar vermez. Benzer şekilde, bir kişi ulusal güvenliğe karşı ya da siyasi amaçlarla büyük bir bankanın kayıtlarına izinsiz erişim sağlayarak siber suç işleyebilir, ancak bu süreçte bankanın sistemine zarar vermeyebilir.

İkinci senaryoda ise devlet dışı bir aktör, bir bilgisayar ağı aracılığıyla yasadışı bir fiil gerçekleştirmekte ve bu fiil sonucunda bilgisayar ağı zayıflatılmaktadır; ancak bu eylem siyasi veya ulusal güvenliğe yönelik değildir. Örneğin, bankanın çevrimiçi hesap sistemine zarar vererek ekonomik kazanç elde etmeyi amaçlayan bir veri korsanı, bu fiiliyle siber suç işlemiş olur; fakat bu durum ne siber saldırı ne de siber savaş kapsamına girer.

Üçüncü senaryoda, devlet dışı bir aktör bilgisayar veya ağ kullanarak yasadışı bir faaliyette bulunmaktadır; ancak bu faaliyet ne bir bilgisayar ağının işlevini zayıflatmakta ne de siyasi ya da ulusal güvenlik amacı taşımaktadır. Örneğin, çocuk pornografisi yayımlayan bir

[139] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 833-834.

kişinin fiilleri, bilgisayar ağının işlevine zarar vermemesi ve siyasi ya da ulusal güvenlik amacı taşımaması nedeniyle siber saldırı değil, yalnızca siber suç olarak değerlendirilir.[140]

Siber savaş, yukarıda bahsedilen üç kategoriden farklıdır. Çünkü siber savaş, aynı zamanda bir siber saldırı niteliği taşımalıdır. Siber savaş, devlet aktörleri tarafından gerçekleştirilen ve etkileri konvansiyonel bir silahlı saldırıya eşdeğer olan eylemleri kapsamaktadır. Bu kuvvet kullanımı hukuka uygun veya hukuka aykırı olabilir; ancak aktör bir devlet olduğundan, hukuka aykırı fiiller her zaman "siber suç" teşkil etmeyebilir.[141]

Siber savaş, aynı zamanda hem siber saldırı hem de siber suç niteliği taşıyabilir. Bu kapsamda, devlet dışı aktörler tarafından gerçekleştirilen iki farklı saldırı türü ele alınabilir. İlk senaryoda, mevcut bir silahlı çatışma bağlamında gerçekleştirilen siber savaş eylemleri, siyasi veya ulusal güvenlik amacıyla bir bilgisayar ağının işlevini zayıflatabilir ve ceza hukuku açısından ihlal teşkil edebilir (örneğin, savaş suçları). Bu tür siber savaş fiilleri, bir bilgisayar sistemi veya ağı aracılığıyla işlenen saldırıları içermektedir.

İkinci senaryoda ise, siber uzayda gerçekleştirilen bir eylem, konvansiyonel bir silahlı saldırıya eşdeğer etkiler yaratabilir, siyasi veya ulusal güvenlik amacıyla bir bilgisayar ağının işlevini zayıflatabilir ve aynı zamanda bilgisayar sistemi veya ağı aracılığıyla işlenen ceza hukuku ihlalleri niteliğindeki saldırıları kapsayabilir.[142]

Yukarıda belirtilen hususlar doğrultusunda, bir siber saldırı hem devlet hem de devlet dışı aktörler tarafından gerçekleştirilebilir. Ancak bu saldırının aktif bir davranış olması, bir bilgisayar ağının işlevini zayıflatmayı amaçlaması ve siyasi veya ulusal güvenliğe yönelik bir tehdit oluşturma amacı taşıması gerekmektedir.

Yukarıda açıklananlardan hareketle, bazı siber saldırıların aynı zamanda siber suç teşkil ettiği, ancak tüm siber suçların siber saldırı kapsamında değerlendirilemeyeceği söylenebilir. Öte yandan, siber savaş her zaman siber saldırı koşullarını karşılamaktadır; ancak tüm siber saldırılar siber savaş değildir. Sadece, konvansiyonel bir "silahlı saldırı" ile eşdeğer etkilere sahip olan veya silahlı çatışma bağlamında gerçekleşen siber saldırılar siber savaş seviyesine yükselmektedir.

Bu nedenle, çalışmamız bağlamında en uygun kavram "siber saldırı"dır. Çünkü siber saldırının yukarıda belirtilen kendine özgü özellikleri, bu saldırı türünü siber suç kavramından ayırmakta ve kendisine uygulanacak hukukun esasen uluslararası hukuk olduğunu göstermektedir. Buna karşılık, siber savaşa atfedilen anlam ise uluslararası hukukun yalnızca

[140] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 835.
[141] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 836.
[142] Hathaway- Crootof - Levitz - Nix - Nowlan - Perdue - Spiegel, "The Law of Cyber-Attack", 836.

sınırlı durumlarda uygulanmasına imkân tanımaktadır. Ancak siber saldırı kavramı Clauswitz'in "Savaş Üzerine" adlı kitabında ifade ettiği üzere*;* "Savaş, düşmanımızı istediğimizi yaptırmaya mecbur etmek için kullanılan güçtür"[143] ve Sun Tzu'nun "en iyi savaş yolu düşmanının dövüşmeden ele geçirildiği yoldur"[144] ifadeleriyle uyuşmaktadır. Clauswitz ve Sun Tzu'nun tanımları, siber saldırı kavramı açısından uygundur. Çünkü siber saldırılarda, klasik savaş yöntemlerinin aksine, fiziksel şiddet ve tahribat ya uygulanmamakta ya da saldırıların şiddetine bağlı olarak fiziksel zararlar meydana gelmemektedir. Bu tür saldırılarda amaç, hedef devletin sahip olduğu gizli ve kritik güce siber yollarla erişmek; gerekli bilgi veya kaynakları ele geçirerek hedef devleti zor durumda bırakmak ve nihai hedef olarak yenilgiye zorlamaktır.[145] Çalışmamızın odak noktası olan siber uzaydaki devlet dışı aktörler ise kendilerine özgü özellikleri nedeniyle sadece savaş zamanlarında değil, barış dönemlerinde de faaliyet gösterebilmekte ve hedef devlet üzerinde fiziksel şiddet veya tahribat uygulamadan ağır sonuçlar doğurabilmektedirler.

2.4.Siber Casusluk

Siber casusluk, casusluk dünyasının yeni bir alanıdır. Siber casusluk, yetkisiz bir kullanıcının ekonomik kazanç, rekabet avantajı, siyasi amaçlar veya askeri avantaj için hassas veya gizli verilere, fikri mülkiyete erişmeye çalıştığı bir siber eylem türüdür.[146] Siber casusluk, bir hasım tarafından kullanılmakta olan bilgisayar sistemlerine veya ağlarına nüfuz ederek bu sistemlerde veya ağlarda bulunan veya bunlar üzerinden geçen bilgileri elde etmeye yönelik kasıtlı faaliyetleri içermektedir.[147]

Siber casusluk eylemleri maddi kazanç amaçlı olabileceği gibi, askeri operasyonlarla bağlantılı olarak veya siber terörizm ya da siber savaş eylemi olarak da gerçekleştirilebilir. Siber casusluğun etkisi, özellikle de daha geniş bir askeri veya siyasi kampanyanın parçası olduğunda, kamu hizmetlerinin ve altyapının aksamasına ve can kaybına yol açabilmektedir.[148]

---

[143] Carl von Clausewitz, *On War*, çev. Michael Howard-Peter Paret), (New Jersey: Princeton University Press, 1989), 583.
[144] Sun Tzu, *The Art of War*, çev. Samuel B. Griffith, (Oxford: Oxford University Press, 1963) 77.
[145] Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", 1181.
[146] Abdulla Civuli - Shkurte Luma-Osmani - Eip Rufati - Gjulie Arifi, "Cyber Espionage Consequences As A Growing Threat", *Journal of Natural Sciences and Mathematics of UT* 7 /13-14 (Ekim 2022), 13.
[147] William C. Banks, "Cyber Espionage And Electronic Surveillance: Beyond The Media Coverage", *Emory Law Journal* 66/513 (2017), 513.
[148] CrowdStrike, "What is Cyber Espionage?" (28 Şubat 2023).

Devlet istihbarat teşkilatları tarafından gerçekleştirilen ilk büyük siber casusluk eylemi, 1990'ların ortalarında "Moonlight Maze" kod adıyla gerçekleşmiştir. ABD'li yetkililer, saldırganların Rusya kökenli olduğuna kanaat getirmiş, ancak Rusya bu iddiaları reddetmiştir.[149]

Bir diğer önemli siber casusluk örneği ise 2000 ile 2003 yılları arasında Amerikan savunma altyapısını hedef alan "Titan Rain" kod adlı saldırı dizisidir. Bu saldırılar kapsamında NASA, Sandia ve Lockheed Martin gibi kritik kurumlar hedef alınmıştır. Siber saldırılar sonucunda hayati öneme sahip bilgiler ele geçirilmiş ve arka planda, saldırganların istedikleri zaman yeniden sisteme erişim sağlamalarına olanak veren, neredeyse tespit edilemeyen izler bırakılmıştır. Yetkililer, bu siber saldırıların Çin tarafından gerçekleştirilen devlet destekli siber casusluk faaliyetlerinin bir parçası olduğunu belirlemiştir.[150]

Siber casusluğun en yaygın hedefleri arasında büyük şirketler, devlet kurumları, askeri istihbarat birimleri, akademik kurumlar ve diğer stratejik kuruluşlar yer almaktadır. Siber casuslar, en çok siyasi stratejiler, siyasi bağlantılar ve siyasi iletişim gibi kritik bilgilere erişmeye çalışmaktadırlar. Bu tür siber casusluk faaliyetlerinin birçoğu, *Advanced Persistent Threat* (APT) yani gelişmiş sürekli tehdit olarak adlandırılmaktadır. [151]

2.5.Enformasyon Savaşı ve Siber Manipülasyon Teknikleri

İnsanlık tarihinin büyük bir bölümünde savaşlar toprak kazanmayı ve ilhak etmeyi amaçlamıştır.[152] Ancak 1970'lerin sonundan günümüze kadar yaşanan savaşlarda amaç, bilgi akışını kontrol etmekti.[153] 21. yüzyılda teknolojide yaşanan hızlı gelişmeler, bilginin etkin ve stratejik bir şekilde kullanılmasına imkân tanımıştır. Facebook, Twitter, Instagram gibi sosyal medya platformları, günlük yaşamın ayrılmaz bir parçası haline gelerek bireylerin algılarını, davranışlarını ve tercihlerini etkileyebilecek bir güce ulaşmıştır. Bu gelişmeleri yakından takip eden devletler, askeri stratejilerinde, savunma ve saldırı planlarında ile istihbarat faaliyetlerinde bilgiyi önemli bir etki aracı olarak kullanmaya başlamıştır.

[149] Harry Cylinder, "A Brief History of Cyber-Espionage", *The Baecon Group of Companies* (18 Ocak 2021).
[150] Abdulla Civuli - Shkurte Luma-Osmani - Eip Rufati - Gjulie Arifi, "Cyber Espionage Consequences As A Growing Threat", 13.
[151] Abdulla Civuli - Shkurte Luma-Osmani - Eip Rufati - Gjulie Arifi, "Cyber Espionage Consequences As A Growing Threat", 13.

[153] Kazım Babacan- Mehmet Sinan Tam, "The Information Warfare Role of Social Media: Fake News in the Russia - Ukraine War", *Erciyes İletişim Dergisi* 3 (Ekim 2022), 77.

Enformasyon operasyonlarının uluslararası düzeyde üzerinde uzlaşılmış tek bir tanımı bulunmamaktadır. Bu çalışmanın amaçları doğrultusunda enformasyon savaşları, hedef kitlenin tutum ve davranışlarını, failin çıkarlarıyla uyumlu olacak şekilde değiştirmek veya pekiştirmek amacıyla enformasyon kaynaklarının bilişsel hedeflerle kullanılması olarak tanımlanabilir.[154] Enformasyon savaşı; bilgisayar casusluğu ve sabotajı, istihbarat ve casusluk faaliyetleri, iletişim dinleme, algı yönetimi ve elektronik saldırı gibi farklı faaliyet gruplarını kapsayan geniş bir kavramdır. [155] Aynı zamanda, toplumların ve bireylerin zihinlerini etkileme ve yönlendirme amacıyla başlatılan bir mücadele türü olarak da tanımlanmaktadır.[156]

Günümüzdeki çatışma örneklerinden de görüldüğü üzere, enformasyon savaşının nihai amacı; bir ulusu veya o ulusun ortak inanç ve değerlerini istikrarsızlaştırmak, toplumsal birliktelik ve bir arada yaşama kapasitesini ortadan kaldırmak, savaş ve o topluma yönelik saldırıları meşrulaştırmak, güvenliği sağlayan kurumların işlevlerini zayıflatmak ya da etkinliklerini yönlendirmek amacıyla toplumsal örgütlenme biçimini dönüştürmektir.[157]

Genel olarak enformasyon savaşı, propaganda, dezenformasyon veya "yalan haber" gibi yöntemlerle rakibin itibarını zedeleyerek ona maddi olmayan zararlar vermeyi hedeflemekte ve bu amacını kitle iletişim araçları, sosyal medya veya benzeri platformlar aracılığıyla gerçekleştirmektedir. Çoğu zaman soyut nitelikte görünen enformasyon savaşı yöntemleri, somut zararlara da yol açabilmektedir. Örneğin, yazılım saldırı yöntemleri (*software intrusion methods*), bir düşmanın stratejik veya ekonomik açıdan kritik bilgisayar veri sistemlerine zarar vermek amacıyla kullanıldığında, başlangıçta soyut olan bu zarar somut nitelik kazanabilmektedir. Bu durum özellikle, düşmanın askeri komuta ve kontrol sistemlerine kötü amaçlı yazılım veya virüslerle müdahale edildiğinde ortaya çıkmaktadır. Böyle bir saldırı, savaş uçaklarının bilgisayar kontrol sistemleri ya da diğer yüksek maliyetli askeri araçlar gibi silah sistemlerine yöneltildiğinde, ağır maddi kayıplara yol açabilmekte; hatta silah sistemlerinin kontrolden çıkması halinde, örneğin jet uçaklarının düşmesi gibi ciddi can kayıpları da meydana gelebilmektedir.[158]

Enformasyon savaşı, yalnızca devletler tarafından değil, aynı zamanda devlet dışı aktörler tarafından da hasımlarına karşı rekabet avantajı elde etmek amacıyla kullanılan yöntemler bütünüdür. Bu yöntemler, kuvvet kullanılarak ya da kuvvet kullanılmaksızın

[154] Tsvetelina van Benthem - Talita Dias - Duncan B. Hollis, "Information Operations under International Law", *Vanderbilt Law Review* 55/5 (Kasım 2022), 1226-1227.
[155] Babacan- Tam, "The Information Warfare Role of Social Media: Fake News in the Russia - Ukraine War", 77.
[156] Babacan- Tam, "The Information Warfare Role of Social Media: Fake News in the Russia - Ukraine War", 78.
[157] Qureshi, "Information Warfare, International Law, And The Changing Battlefield", 905-906.
[158] Qureshi, "Information Warfare, International Law, And The Changing Battlefield", 905-906.

uygulanabilmekte; böylece hem barış hem de çatışma dönemlerinde etkili bir araç olarak işlev görmektedir.

Günümüzde enformasyon savaşının tercih edilmesinin başlıca nedenlerinden biri, enformasyon ortamına giriş engellerinin son derece zayıf ve kırılgan olmasıdır. Bu durum, hem devletlerin hem de devlet dışı aktörlerin söz konusu ortama kolaylıkla erişebilmesine ve burayı bir savaş alanına dönüştürmesine imkân tanımaktadır.[159] Diğer bir neden ise enformasyon savaşı için gereken kaynakların konvansiyonel askeri araçlardan çok daha düşük olmasıdır.[160]

Geçmişte tanık olunan geleneksel savaşların aksine, bilgi savaşı bir ülkenin tüm elektronik altyapısını hedef almakta; sivil ve devlet bilişim sistemleri üzerinde kontrol sağlamayı amaçlamaktadır. Kitle iletişim araçları arasında yer alan internet ise, enformasyon savaşının en önemli bileşenlerinden birini oluşturmaktadır.[161]

Başarılı bir enformasyon savaşında hedefin doğrudan tehdit edilmesine veya gözdağı verilmesine gerek yoktur. Zira fail, enformasyon savaşında açık ya da aldatıcı yöntemler kullanarak hedef kitlenin üyelerini etkilemekte, ikna etmekte, inandırmakta veya başka bir şekilde kendi amaç ve hedeflerinin kabul edilmesini sağlamaktadır.[162]

Yeni nesil enformasyon savaş tekniklerinin örneklerini, Gezi Olayları sırasında uluslararası medya kuruluşlarının Türkiye aleyhine gerçekleştirdiği canlı yayınlarda görmek mümkündür.[163] Enformasyon savaşına bir diğer örnek, Rusya merkezli propaganda aracı Sputnik News'tir. Sputnik News, yanıltıcı, manipülatif ve yönlendirici yayınlar yaparak Rus devletinin bir etki silahı olarak işlev görmektedir. Nitekim Kasım 2015'te Rus savaş uçaklarının Türkiye sınırını ihlal etmesi sonucunda bu uçaklar Türkiye tarafından düşürülmüş; akabinde Sputnik'e ait sosyal medya hesapları, bu olayı Türkiye'nin sözde IŞİD'e (Irak Şam İslam Devleti) yardım ettiği iddiasıyla manipülatif bir propaganda kampanyasına dönüştürmüştür.[164]

Enformasyon savaşı, kimi zaman ikna veya enformasyon operasyonu (*Information Operations* – IO) ve hatta psikolojik savaş operasyonları (*Psychological Warfare Operations* – PSYOP) olarak adlandırılmaktadır. Bu bağlamda, psikolojik savaş operasyonları (PSYOP),

---

[159] E. Anders Eriksson, "Information Warfare: Hype Or Reality?", *The Nonproliferation Review/Spring-Summer* 6/63 (1999), 60-61.
[160] Holger Mölder -Vladimir Sazonov- Archil Chochia-Tanel Kerikmäe (ed.), *"The Russian Federation in Global Knowledge Warfare Influence Operations in Europe and Its Neighbourhood"* (Almanya: Springer, 2021), 3.
[161] Iryna Sopilko - Andrii Svintsytskyi -Yevheniia Krasovska - Andrii Padalka - Andrii Lyseiuk, "Information wars as a threat to the information security of Ukraine", *Conflict Resolution Quarterly*, 39/3 (Kasım 2021), 77.
[162] Tsvetelina van Benthem - Talita Dias - Duncan B. Hollis, "Information Operations under International Law", *Vanderbilt Law Review* 55/5 (Kasım 2022), 1226-1227.
[163] Ali Burak Darıcılı -Barış Özdal, "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi" *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi* 4/1 (Şubat 2017) 28.
[164] Babacan- Tam, "The Information Warfare Role of Social Media: Fake News in the Russia - Ukraine War", 78.

siber uzay operasyonları (*Cyberspace Operations* – CO) ve elektronik savaş (*Electronic Warfare* – EW) unsurlarını, enformasyon savaşının (*Information Warfare* – IW) temel bileşenleri olarak değerlendirmek isabetli olacaktır.[165] Yukarıda bahsedilen unsurlar da dâhil olmak üzere birçok faaliyet alanını kapsayan enformasyon savaşının, teknik açıdan daha nötr ve kabul edilebilir bir ifade olan "enformasyon operasyonları" terimiyle anılması daha uygun olacaktır.

"Etki operasyonları" (*influence operations*) kavramı, "enformasyon operasyonları" (*information operations*) kavramından daha geniş bir kapsam taşımakta; propaganda gibi askeri nitelikte olmayan ve zorlama (*coercive*) unsurları içeren faaliyetleri de bünyesinde barındırmaktadır.[166] Enformasyon operasyonları kavramı ile savaş (warfare) kavramını bir araya getiren RAND Corporation, "rakibe karşı rekabet avantajı elde etmek amacıyla propaganda yayılmasını" içeren bir etki operasyonları tanımı ortaya koymuştur.[167]

Enformasyon savaşı bağlamında "etki operasyonları" terimi; ister bireysel bir lider, ister bir karar alma grubunun üyeleri, askeri örgütler ve personel, ister belirli nüfus alt grupları ya da geniş halk kitleleri olsun, hedef kitleyi etkilemeye yönelik tüm çabaları ifade etmektedir. Bu nedenle, etki operasyonları kavramı, yumuşak güç faaliyetleri de dâhil olmak üzere enformasyon alanındaki tüm operasyonları kapsayan şemsiye bir terim olarak değerlendirilmektedir.[168]

Yukarıda açıklananlardan hareketle, enformasyon savaşlarının oluşturabileceği bilişsel tehditler hem soyut hem de somut zararlara yol açabilmektedir. Örneğin, 2020 ABD başkanlık seçimleri sürecinde yayılan yalan haberler, seçim sonuçlarının istikrarını sarsıcı etkiler yaratmıştır. Bu bağlamda, Sputnik News tarafından yapılan dezenformasyon faaliyetleri örnek teşkil etmektedir. Sputnik, kritik seçim döneminde, Barack Obama ve Hillary Clinton'ın IŞİD'i kurduğu yönünde tamamen asılsız ve manipülatif haberler yayımlamış; bu dezenformasyonları manşetlere taşımıştır. Ayrıca sosyal medyada #CrookedHillary etiketiyle organize edilen kampanyalar aracılığıyla, Demokrat Parti'nin başkan adayı Hillary Clinton'u sistematik biçimde itibarsızlaştırmaya çalışmıştır. Sputnik tarafından üretilen bu içerikler, Cumhuriyetçi

---

[165] Bipin Bakshi, "Information Warfare: Concepts and Components", *International Journal of Research and Analytical Review*s 5/4 (Kasım 2022) 178–179.

[166] Sean Cordey, "Cyber Influence Operations: An Overview and Comparative Analysis" *Center for Security Studies (CSS)* (Ekim 2019), 4-10.

[167] Eric V. Larson -Richard E. Darilek - Daniel Gibran -Brian Nichiporuk - Amy Richardson, Lowell H. Schwartz - Cathryn Quantic Thurston, *"Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities"* (ABD: RAND Corporation, 2009) 2.

[168] Daniel Cohen -Ofir Bar'el, *"The Use of Cyberwarfare in Influence Operations"* (Tel Aviv: Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University), 7-15.

Parti'nin başkan adayı Donald Trump lehine yürütülen kapsamlı ve kasıtlı dezenformasyon stratejisinin temel unsurlarından biri olarak değerlendirilmiştir.[169]

Enformasyon savaşı aynı zamanda kamu sağlığı üzerinde de olumsuz etkiler yaratmaktadır. COVID-19 pandemisi sürecinde yayılan yanlış bilgiler, kamu sağlığına yönelik önemli bir bilişsel tehdit teşkil etmiştir. Ayrıca, enformasyon savaşı ayrımcılığı, şiddeti, soykırımı ve diğer zalimane eylemleri teşvik edebilmektedir. Bu duruma örnek olarak, 2017'den itibaren Facebook platformunda Myanmar'daki Rohingya halkına yönelik yayılan yanlış ve nefret dolu söylemler gösterilebilir.

Bununla birlikte, tüm enformasyon operasyonlarının zarara yol açtığı söylenemez; bu durum, enformasyon operasyonlarının farklı türlere sahip olduğunu göstermektedir. Aşağıda, failin niyetine göre yaygın olarak kabul edilen üç enformasyon operasyonu tipolojisi yer almaktadır:

i. Yanlış bilgilendirme (*misinformation*): Zarara yönelik herhangi bir kast olmaksızın yanlış bilginin paylaşılması;

ii. Dezenformasyon (*disinformation*): Zararlı amaçlarla kasıtlı olarak yanlış bilginin paylaşılması;

iii. Zararlı bilgi (*malinformation*): Mahrem kalması gereken bilgilerin kamusal alana taşınması da dâhil olmak üzere, doğrulanabilir gerçeklerin, kişisel görüşlerin veya fikirlerin zarar verme amacıyla paylaşılması.[170]

2.5.1. Sosyal Medya Aracılığıyla Yürütülen Operasyonlar

Çatışma ve geleneksel medya arasındaki ilişki, birçok araştırmanın odak noktası olmuştur. Geleneksel kitle iletişim araçları, belirli bakış açılarını ve ideolojileri güçlendirmek ve yaymak, ülke içindeki kitleleri ikna etmek ve çatışmalarda karşıt tarafları etkilemek amacıyla kullanılmıştır.

Enformasyon savaşı bağlamında manipülasyonun en etkin şekilde kullanıldığı alanlardan biri de sosyal medyadır. Sosyal medyada manipülasyon yöntemleri arasında, içeriğin kaynağını veya kimliklerini gizlemek, içeriğin bağlamını değiştirmek ve algoritmaları yanıltmak amacıyla spam türü araçların kullanılması yer almaktadır.[171]

---

[169] Jonathan Masters, "Russia, Trump, and the 2016 U.S. Election", *Council on Foreign Relations* (Erişim 13 Temmuz 2025). https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

[170] Tsvetelina van Benthem - Talita Dias - Duncan B. Hollis, "Information Operations under International Law", *Vanderbilt Law Review* 55/5 (Kasım 2022), 1226-1227.

[171] Teke - Lale, "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik", 52.

21. yüzyılda internetin çığır açan gelişimiyle birlikte, sosyal medya ile ilgili ilişkilerin araştırılması bağlamında "medya ve çatışma arasındaki karmaşık ilişkinin uzun süredir devam ettiği" ileri sürülmektedir.[172] Bu olağanüstü gelişmeler, Facebook, Twitter ve YouTube gibi yeni sosyal medya platformları ile popüler arama motoru Google'ın dünya çapında önemli ve büyük ölçüde kontrolsüz enformasyon kaynakları haline gelmesine yol açmıştır.[173]

2010 yılında Tunus'ta başlayan ve Mısır başta olmak üzere diğer Ortadoğu ülkelerine yayılan protesto ve ayaklanmalar, protestocular, aktivistler ve destekçileri tarafından Facebook ve Twitter gibi sosyal medya platformları üzerinden yayılan kullanıcı kaynaklı içeriklerin yaygın kullanımı nedeniyle "Twitter Devrimleri" ve "Facebook Devrimleri" olarak anılmıştır. Bu ayaklanmalarda başlıca çevrimiçi araçlar olarak Facebook ile mikro blog platformu Twitter gibi sosyal ağlar öne çıkmıştır.[174]

Twitter'ın devrim amacıyla kullanıldığı ülkeler arasında Moldova ve İran da bulunmaktadır. 2009 yılında bu ülkelerde meşru hükümetlere karşı gerçekleştirilen protestolarda Twitter etkin bir iletişim aracı olarak kullanılmış ve bu protestolar yorumcular tarafından "Twitter Devrimleri" olarak adlandırılmıştır.[175] Öte yandan, 2001 yılında Filipinler'de Devlet Başkanı Joseph Estrada'nın halk tarafından görevden uzaklaştırılması sürecinde, protestocuların bir araya gelmesini sağlayan kısa mesajların yaygın kullanımı nedeniyle bu olay "SMS Devrimi" olarak anılmıştır.[176]

Sosyal medyanın çeşitli yönlendirmelere, diğer bir ifadeyle manipülasyona açık bir araca dönüşmesi, "sosyal medyanın silahlandırılması" olarak tanımlanmıştır. [177] Bu durum, sosyal medyanın çatışmalarda devletler, devlet dışı örgütler ve hatta bireyler tarafından askeri nitelikli eylemler için kullanılmasına yol açmıştır. [178]

Sosyal medyanın çeşitli yönlendirmelere, yani manipülasyona açık bir araca dönüşmesi "sosyal medyanın silahlandırılması" olarak nitelendirilmiş; bu durum, sosyal medyanın

---

[172] Thorsten Hochwald, "How Do Social Media Affect Intra-State Conflicts other than War?", *Connections* 12/3 (2013), 18.
[173] Murat Mete- Filiz Balta Peltekoğlu, "Sosyal Medyada Enformasyon Savaşı: Kurumsal Güvenlik Bağlamında Bireysel Sosyal Medya Kullanımı" *International Social Sciences Studies Journal* 7/86 (Ağustos 2021), 3332.
[174] Alex Comninos, "Twitter revolutions and cyber crackdowns User-generated content and social networking in the Arab spring and beyond", *Association for Progressive Communications (APC)*, (Haziran 2011), 4.
[175] Evgeny Morozov, "Moldova's Twitter Revolution", *Foreign Policy* (7 Nisan 2009).
[176] Julius Court, *"People Power II in the Philippines: The First E-Revolution?"*, (Overseas Development Institute, Ocak 2001).
[177] Aynur Teke - Aybala Lale, "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik", *Akademik İncelemeler Dergisi* 16/2 (Ekim 2021) 49.
[178] Mete- Peltekoğlu, "Sosyal Medyada Enformasyon Savaşı: Kurumsal Güvenlik Bağlamında Bireysel Sosyal Medya Kullanımı" 3332.

çatışmalarda devletler, devlet dışı örgütler ve hatta bireyler tarafından askeri nitelikli eylemler için kullanılmasına zemin hazırlamıştır.

Sosyal medyayı tehlikeli kılan en önemli özellik, neredeyse herkes tarafından tüm etkileme faaliyetlerinin gerçekleştirilebileceği veya bu faaliyetleri desteklemek amacıyla kullanılabileceği bir alan olmasıdır. Bu ortam, sosyal mühendislik için aktörlere geniş olanaklar sunmakta ve açık ya da kapalı kaynaklar ile ağlar vasıtasıyla eş zamanlı olarak yürütülen etkileme faaliyetlerinin tespit edilmesini ve etkisiz hale getirilmesini neredeyse imkânsız kılmaktadır.[179] Başka bir ifadeyle, sosyal medya bireyleri etkileme gücünü temsil eden manipülasyonun destekleyicisi konumunda olup, manipülasyona uygun bir ortam yaratma işlevini üstlenmektedir.[180]

Çığır açan bu etkileme gücünün bir sonucu olarak, sosyal medyadan kaynaklanan tehditler klasik tehditler ve modern tehditler olmak üzere ikiye ayrılmaktadır. Klasik tehditler, belirli bir ağdaki tüm kullanıcıların saldırıya açık hale getirilmesini ifade ederken; modern tehditler ise yalnızca kullanıcı gizliliğini ve güvenliğini tehlikeye atabilecek çevrimiçi sosyal ağ altyapısı ve kullanıcılarını hedef almaktadır.

Klasik tehditler arasında en yaygın olanlar kötü amaçlı yazılımlar, kimlik avı saldırıları, hizmet engelleme saldırıları, solucanlar, virüsler ve gelişmiş kalıcı tehditlerdir. Modern tehditler ise kullanıcıların kişisel bilgilerini ele geçirme, kişisel verilerin gizliliğini tehdit etme, sahte profiller oluşturma ve anonimleştirme saldırıları, siber taciz, bilgi gizliliği sızıntısı, bilgi manipülasyonu ve dolandırıcılık gibi çeşitli biçimlerde ortaya çıkmaktadır.[181]

Sosyal medya aktörleri, çeşitli manipülasyon yöntemleri kullanabilmektedir. Örneğin, bu aktörler toplumda ön yargı ve kavram yanılgıları oluşturarak süreçlere, bireylere veya topluluklara olumlu ya da olumsuz etkilerde bulunabilirler. Siber uzayda hâkim olan gündem konusunu değiştirebilir, anonim kaynaklara atıfta bulunabilir ve verileri kötüye kullanabilirler. Bu bağlamda, çarpıcı bir örnek olarak 2016 ABD seçimleri gösterilebilir. Cambridge Analytica şirketi, bir uygulama aracılığıyla Facebook kullanıcılarının verilerini elde ederek seçimlere müdahale etmiştir. New York Times'a göre, 2014 yılında Amerikalı seçmenlerin psikolojik profillerini siyasi kampanyalara satmaya hevesli olan Cambridge Analytica, on milyonlarca kullanıcının özel Facebook verilerini ele geçirmiştir. Bu olay, Facebook tarihinin bilinen en

[179] Mete- Peltekoğlu, "Sosyal Medyada Enformasyon Savaşı: Kurumsal Güvenlik Bağlamında Bireysel Sosyal Medya Kullanımı" 3332.
[180] Teke - Lale, "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik", 48.
[181] Teke - Lale, "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik", 52.

büyük veri sızıntısı olarak kayıtlara geçmiştir.[182] İki eski Cambridge Analytica çalışanına göre, şirket verileri satmak amacıyla Kremlin bağlantılı petrol devi Lukoil ile temasa geçmiştir.[183] Ancak SCL ve Lukoil, görüşmelerin siyasi nitelikte olduğunu reddetmiştir.[184]

Bu yöntemin 2016 ABD başkanlık seçimlerinde Donald Trump lehine de kullanıldığı iddia edilmiştir. Seçimleri Trump'ın kazanmasının ardından ortaya çıkan hile iddialarının ardından Facebook, Rusya'nın seçimlere nüfuz operasyonunda etkisi olduğunu öne sürmüştür. Seçim kampanyası süresince Facebook, Twitter gibi sosyal medya platformlarında büyük ölçüde sahte hesaplar kullanılmıştır. Gündem oluşturulurken, duyguların ve inançların objektif gerçeklere tercih edildiği durumları ifade eden hakikat ötesi (*post-truth*) kavramı, bu sürecin önemli bir yansımasıdır. Çünkü günümüzde insanlar çoğunlukla doğru bilgi yerine bilgi yığınlarını sorgusuz kabul etme eğilimindedir.[185]

2.5.2. Siber Sızmalar ve Veri Hırsızlığı

Siber uzaya sızma, enformasyon savaşının önemli türlerinden biridir. Bu kavram, düşmanın stratejik öneme sahip bilgisayar sistemlerine bilgisayar korsanlığı yoluyla virüs veya kötü amaçlı yazılımlar aracılığıyla saldırması anlamına gelmektedir. ABD Savunma Bakanlığı verilerine göre, Pentagon bilgisayar ağ sistemlerini korumak amacıyla günlük yaklaşık 36 milyon e-posta ihlalini engellemek zorunda kalmaktadır. Bu durum, teknolojinin bir devletin güvenlik sistemlerine yönelik tehditlerinin ne denli ciddi olduğunu açıkça göstermektedir.[186]

Veri hırsızlığı, enformasyon saldırısı gerçekleştirenlerin başvurduğu temel yöntemlerden biridir. Bu yöntem genellikle rakibin gizli ve stratejik açıdan kritik bilgilerini veya banka hesaplarındaki fonları ele geçirmek amacıyla kullanılmaktadır. Stratejik öneme sahip bilgilerin çalınması, maddi olmayan zararların yanı sıra, etkilenen tarafın rakiplerine kıyasla dezavantajlı bir konuma düşmesine de yol açabilir.[187]

Bazı durumlarda veri hırsızlığı siyasi amaçlar taşımaktadır. Daha açık bir ifadeyle, bu yöntemle siyasi koşullar manipüle edilmeye çalışılmaktadır.

---

[182] Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", *The New York Times* (4 Nisan 2018) 1.
[183] Danny Hakım - Matthew Rosenberg, "Data Firm Tied to Trump Campaign Talked Business With Russians", *The New York Times* (18 Mart 2018) 1.
[184] Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", 1.
[185] Teke - Lale, "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik", 54.
[186] Qureshi, "Information Warfare, International Law, and The Changing Battlefield", 914.
[187] Qureshi, "Information Warfare, International Law, and The Changing Battlefield", 914.

Veri hırsızlığının yakın tarihli bir örneği, yukarıda kısaca değindiğimiz *Cambridge Analytica* skandalıdır. Bu skandalda, Cambridge Analytica firmasının yönetim kurulu üyelerinden biri aracılığıyla yaklaşık 87.000 Facebook kullanıcısının verilerine erişilmiştir. Elde edilen bu veriler, 2016 yılında Donald Trump'ın başkanlık seçim kampanyasında kullanılmıştır. Soruşturma raporlarına göre, verilere bağımsız araştırmacı ve Cambridge Üniversitesi öğretim görevlisi Alexandr Kogan tarafından geliştirilen *"This Is Your Digital Life"* adlı çevrimiçi kişilik testi uygulaması aracılığıyla erişilmiştir. Uygulama Facebook kullanıcıları arasında yaygın olarak kullanılmış ve kullanıcılar, kişilik testi amacıyla uygulamaya erişirken, farkında olmadan kendi ve arkadaşlarının Facebook verilerini Kogan'ın uygulamasına aktarmışlardır. Kogan ise bu verileri Cambridge Analytica ile paylaşmıştır. Verilerin çoğunluğu ABD ve Birleşik Krallık vatandaşlarına ait olup, bu olay Trump'ın siyasi ekibinin seçim kampanyasını yürüttüğü 2015 yılında gerçekleşmiştir. Trump'ın siyasi ekibinden Steve Bannon, Cambridge Analytica'nın yönetim kurulu üyesi olarak Kogan'ın topladığı verilerin Trump'ın seçim kampanyasında kullanılmasını sağlamıştır. Bu sayede, Trump'ın konuşmaları ve diğer kampanya materyalleri, veri erişimi sağlanan kişilerin ilgi ve tercihleri doğrultusunda şekillendirilmiştir. Bu olay, binlerce ABD vatandaşının kişisel verilerinin izinleri olmaksızın ele geçirilmesi yoluyla ABD başkanlık seçimlerinin sonucunu etkilemeye yönelik bir girişim olarak değerlendirilmektedir.[188] Her ne kadar Rusya'nın bu veri hırsızlığı operasyonunu desteklediği ve Trump'ın seçim kampanyasının Cambridge Analytica aracılığıyla çalınan verilere erişerek seçim başarısını sağladığı yönünde iddialar ortaya atılmış olsa da, Rus devletinin olaya doğrudan karıştığına dair kesin bir kanıt bulunmamaktadır.[189]

2.5.3. Söylem İnşası ve Devlet Kitleleri Üzerindeki Etkisi

Enformasyon savaşı, genellikle hedef kitlenin algılarını ve anlatılarını yönlendirmeyi temel amaç edinir. Bu amaç, hedef kitleye manipüle edilmiş bilgi yaymak suretiyle gerçekleştirilir. Bir devlet veya onun kurumları, bu işlevi medya hizmetlerini kullanarak ya da kullanmadan yerine getirebilir. Özellikle devletin kendi sınırları içinde medya, enformasyon savaşının bu amacı için etkin bir araç olarak kullanılabilmektedir.

Enformasyon savaşının hasım devlete yönelik kamuoyunda bir anlatı oluşturmak amacıyla kullanıldığı en önemli örneklerden biri, 2003 yılında ABD'nin Irak'ta uyguladığı

[188] Qureshi, "Information Warfare, International Law, and The Changing Battlefield", 914-915.
[189] Sean Illing, "Cambridge Analytica, the Shady Data Firm That Might Be A Key Trump-Russia Link, Explained", *Vox* (4 Nisan 2018), 1.

stratejidir. Bu tür enformasyon savaşının temel amacı, Irak güçlerinin ve halkının direnişini azaltarak kuvvet kullanımı için uygun koşulların hazırlanmasıydı. ABD, Irak'a saldırmadan önce manipüle edilmiş bilgileri broşürler ve el ilanları şeklinde yayımlayarak bunları Irak vatandaşlarına ve kilit ordu subaylarına dağıttı. Bazı broşürlerde, Iraklı subaylar Saddam Hüseyin'in emirlerine karşı çıkarak petrol kuyularını yok etmemeye çağrılıyordu. Bu broşürlerde, petrol kuyularının Irak halkının malı olduğu ve bu nedenle yok edilmemesi gerektiği vurgulanıyordu. Ayrıca, Saddam Hüseyin'in petrol kuyularını yok etme emri vermesi halinde ABD'nin bu kuyuları koruyacağı iddia ediliyordu. ABD, kendisinin Irak halkının çıkarları için, Saddam Hüseyin'in ise kendi çıkarları için hareket ettiği yönünde bir anlatı sunarak Irak halkını ve uluslararası toplumu bu şekilde yönlendirmeye çalıştı. Aynı anlatı, ABD hükümeti tarafından, Irak'a yapılacak saldırıya destek sağlamak amacıyla ABD vatandaşlarına da sunuldu. Manipüle edilmiş bu anlatının yaygınlaştırılması sonucunda, ABD Irak'ı işgal etti ve ülke topraklarının tamamını ele geçirirken önemli bir direnişle karşılaşmadı. Böylece ABD'nin Irak'ta kuvvet kullanımı öncesinde başlattığı enformasyon savaşı, askeri müdahaleye zemin hazırlamış oldu.[190]

2.5.4. Enformasyon Savaşı ve Siber Savaş Arasındaki Ayrım

Enformasyon savaşı ile siber savaş arasında bazı ortak noktalar bulunsa da, iki kavram arasında temel farklılıklar mevcuttur. Enformasyon savaşı, tarih boyunca konvansiyonel savaşların ayrılmaz bir parçası olarak var olmuş eski bir olgudur. Buna karşılık, siber savaş nispeten yeni bir kavramdır ve ancak internet ile bilgisayar teknolojilerinin gelişmesiyle ortaya çıkmıştır. Önceki enformasyon savaşı operasyonlarının aksine, siber savaş bu teknolojik ilerlemeler sayesinde mümkün hale gelmiştir.[191]

Enformasyon savaşı bağlamında, düşmana karşı kullanılan en temel araç enformasyondur. Bu alandaki faaliyetler oldukça geniş kapsamlıdır; medya ve sosyal medya üzerinden propaganda yapmak, "yalan haber" veya dezenformasyon yaymak enformasyon savaşının parçalarıdır. Ayrıca kötü amaçlı yazılımlar (*malware*) ve virüslerin yayılması ile düşmanın askeri komuta ve kontrol sistemlerine yönelik hizmet engelleme (*DDoS*) saldırıları da enformasyon savaşının unsurları arasında yer almaktadır. Öte yandan, siber savaş ise internet ve bilgisayar teknolojilerini kullanarak düşmana karşı stratejik rekabet avantajı sağlamaya

[190] Qureshi, "Information Warfare, International Law, and The Changing Battlefield", 917-918.
[191] Waseem Ahmad Qureshi, "Information Warfare, International Law, And The Changing Battlefield", *Fordham International Law Journal* 43/4 (2020), 908.

yönelik bir araçtır. Siber savaş; DDoS saldırıları, bilgisayar virüsleri, bilgisayar korsanlığı ve rakibin stratejik öneme sahip bilgisayar sistemlerine yapılan kötü amaçlı yazılım saldırılarını içermektedir.

Enformasyon savaşı, basılı ve elektronik medya, bilgisayarlar, yazılım, gözetleme ve casusluk gibi daha geniş bir alanı kapsarken; siber savaşın kapsamı ise yalnızca internet ve bilgisayarlarla sınırlıdır. Bu nedenle, siber savaş bilgi savaşının çok boyutlu alanında sadece bir boyut veya disiplin olarak değerlendirilebilir. [192] Çalışmamızın önemli unsurlarından biri olan "yeni devlet dışı aktörler" bağlamında, enformasyon savaşı özellikle büyük bir öneme sahiptir.

3. SİBER UZAYDAKİ DEVLET DIŞI AKTÖRLER

3.1. Klasik Devlet Dışı Aktörler

Devlet dışı aktörlerin uluslararası hukuktaki yerini anlama bakımından önce "aktör" kavramını ardından "devlet dışı aktör" kavramını açıklamak yerinde olacaktır. Bu iki kavramın uluslararası hukuk kapsamındaki konumunun belirlenmesi tezin üçüncü bölümünde ele alınacak olan uluslararası sorumluluk bakımından da son derece önemlidir.

Aktör "ispat yükünün üzerinde olduğu kişi" anlamına gelmektedir.[193] Hukuk bakımından "aktör" kelimesi "bir eylem veya süreci gerçekleştiren kişi" olarak tanımlanmaktadır.[194] Roma hukukunda ise "aktör" kavramı başkası için hareket eden kişi başkasının işine katılan kişi, bir yönetici veya temsilci anlamlarına gelmektedir. Roma hukukunda efendisinin işine veya işlerine katılan, işlem yapan veya denetleyen, para alan, ödeyen ve hesap tutan bir köle" olarak da tanımlanmıştır.[195]

Devlet dışı aktörler kavramı ise, uluslararası ilişkilerde devletler dışında kalan tüm aktörleri kapsayan bir üst kavramdır. Bu kavram, uluslararası hukuktaki bireylerin yanı sıra, küresel, bölgesel, alt-bölgesel ve yerel düzeyde çok çeşitli örgüt ve kurumları kapsayan varlıkları içine almaktadır. Daha açık bir ifadeyle bu kavram uluslararası örgütleri, şirketleri, sivil toplum örgütlerini, *de facto* rejimleri, ticari kuruluşları, ulusötesi şirketleri, terörist grupları ve ulusötesi suç örgütlerini kapsamaktadır. [196]

---

[192] Qureshi, "Information Warfare, International Law, and The Changing Battlefield", 909.
[193] The Law.Com Dictionary, "Actor", https://dictionary.thelaw.com/actor/ (Erişim 3 Mart 2024).
[194] World Law Dictionary, "Definitions of Actor", https://dictionary.translegal.com/en/actor/noun (Erişim 3 Mart 2024).
[195] Tenney Frank, "The Status of Actors at Rome", *The University of Chicago Press* 26/1 (3 Mart 2024) 12-16.
[196] Wijninga - Oosterveld - Galdiga - Marten, "State And Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies*, 142.

Devlet dışı aktörler, esnek ve merkeziyetten uzak bir niteliğe sahiptir. Geleneksel büyük ölçekli örgütlerin yanı sıra, yeni ortaya çıkan devlet dışı aktörlerin genel örgütsel yapısı son yıllarda oldukça gevşek bir hal almıştır.

Küçük ve gevşek örgütsel yapılarından dolayı, devlet dışı aktörler katı hiyerarşik sistemler ve yönetim modellerinden uzak durmaktadırlar. Bu durum devlet dışı aktörlerin bireysel üyelerinin esnek ve gönüllü bir şekilde faaliyet yürütmesinde önemli bir rol oynamaktadır. Bu gevşek ve merkeziyetten uzak örgütlenme biçimi, devlet dışı aktörlerin etki göstermesi için önemli bir kolaylık sağlar.[197]

Devlet dışı aktörlerin uluslararası hukuktaki konumunu daha iyi anlayabilmek için öncelikle devlet ile devlet dışı aktör arasındaki farklılıkları ortaya koyabilmek önemlidir. Örneğin, devlet dışı bir aktör belirli bir nüfus üzerinde veya onun adına resmi bir güç kullanmaz. Ancak bu, kendi tabanı olmadığı anlamına gelmez. Çünkü büyük şirketler ve STK'ler gibi çoğu devlet dışı aktörün resmi üyelik tabanları, çalışanları ve sempatizanları vardır. Ayrıca bazen devlet dışı aktörler bir ülkedeki belirlenmiş grupların resmi temsilcileri olarak hareket ederler. Etnik olarak tanımlanmış siyasi bir parti buna örnek olarak gösterilebilir. Devlet dışı bir aktörü devletten ayıran bir diğer özelliği ise resmi olarak kontrol ettiği topraklarının olmamasıdır. Bu kural olarak doğrudur, ancak ayrılıkçı hareketler, büyük şirketler veya Katolik Kilisesi gibi yapılar toprakların etkin kontrolüne de sahip olabilmektedirler. [198] Pakistan'ın aşiret bölgelerinde olduğu gibi, devletin kendisi de her zaman kendi yetki alanındaki tüm toprakların kontrolünü elinde bulundurmayabilir.[199]

Devlet dışı aktörler iki geniş kategoride sınıflandırılabilir; bunlardan ilki uluslararası örgütler, devlet oluşumları (*örneğin Sekizler Grubu -G8*) ve devlet altı aktörlerdir (*Federal Devletler*); bunlar devlet veya hükümet özelliklerini korurlar. Diğer grup ise sayısız tezahürü olan özel aktörlerden oluşur; bazıları hiyerarşik yapıları olsun veya olmasın devletler tarafından tanınan aktörler şeklini alırken, diğerleri bu tür bir sınıflandırmaya meydan okur, ulusal sınırlar içinde veya ötesinde gevşek bir şekilde örgütlenir. Bazen devlet dışı aktörler arasında, bazen de devlet dışı aktörler ile devletler arasında yakın bir karşılıklı bağımlılık da söz konusudur.[200]

Devlet ve devlet dışı aktörler arasındaki ilişkiyi anlama bakımından devletin kapsamı ve güvenliği sağlama kabiliyeti bir ölçü olarak dikkate alınabilir. Bu durum dünya genelinde önemli farklılıklar gösterebilir. Örneğin, gelişmiş ülkelerde devlet, güvenliği sağlamak için

[197] Yan, "The Role and Impact of Nonstate Actors from the Perspective of the Russia—Ukraine Crisis", 72.
[198] Wijninga - Oosterveld - Galdiga - Marten, "State and Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies*, 145.
[199] Tenney Frank, "The Status of Actors at Rome", *The University of Chicago Press* 26/1 (3 Mart 2024) 12-16.
[200] Wagner, "Non-State Actors", 1-2.

kuvvet kullanma tekelini tamamıyla eline alabilmiştir. Dünyanın diğer bölgelerinde ise durum bunun tam tersidir. [201] Somali, Mali, Lübnan, Pakistan, Kongo Demokratik Cumhuriyeti ve Ukrayna buna örnek gösterilebilir. Bu ülkeler etnik, aşiret ya da özel grupların bazen kendi emirlerini uygulamak için o kadar çok silah ve araç biriktirdikleri ülkelerdir ki, fiilen "devlet içinde devlet" oluşturmuşlardır. [202]

3.2.Yeni Devlet Dışı Aktörler

"Siber uzaydaki yeni devlet dışı aktörler" ifadesi ilk kez bu çalışmada kavramsallaştırılmıştır. Bu türden bir kavramsal ayrımın yapılmasının temel nedeni, siber uzaydaki devlet dışı aktörler ile klasik devlet dışı aktörler arasında belirgin farkların bulunmasıdır. Sivil toplum kuruluşları (STK'lar), silahlı gruplar ve çok uluslu şirketler gibi klasik devlet dışı aktörler genellikle devletle doğrudan veya dolaylı bir ilişki içerisindedir. Oysa siber uzay, farklı bir ortam, kontrol mekanizması ve etki düzlemi sunmaktadır. Bu alanda faaliyet gösteren aktörlerin büyük bir kısmı devlet kökenli değil, özel sektör kökenlidir. *Google, Apple, Facebook, Microsoft, Amazon* ve *SpaceX* gibi büyük teknoloji şirketleri artık yalnızca dijital altyapıyı sunan değil, aynı zamanda bu altyapıyı yöneten ve şekillendirme kapasitesine sahip küresel aktörler hâline gelmiştir. Örneğin, *Google* kullanıcıların tüm arama alışkanlıklarını detaylı biçimde kayıt altına almaktadır. *Apple*, hem bilgisayar hem de telefon aracılığıyla yalnızca cihaz kullanım bilgilerini değil, biyometrik veriler ve parmak izi gibi son derece hassas kişisel bilgileri de toplamaktadır. *Facebook*, kullanıcıların sosyal ilişkilerini, beğeni ve tercihlerinden beslenme alışkanlıklarına kadar geniş bir yelpazede takip edebilmektedir. Amazon, bireylerin alışveriş biçimlerini, izledikleri filmleri ve ilgi alanlarını sistematik olarak analiz etmektedir. *Microsoft* ise kullanıcıların yararlandığı tüm iletişim platformları üzerinden kapsamlı veri erişimine sahiptir.[203]

Bu bağlamda örneğin, *Google*'ın 2011 Arap Baharı sürecinde Mısır'daki hükümet karşıtı protestolarda aktivistlere destek sağlaması, şirketin yalnızca bir iletişim sağlayıcısı değil, aynı zamanda siyasi bir aktör olarak da hareket ettiğini göstermektedir. Benzer şekilde, Elon Musk'ın sahibi olduğu *SpaceX*'in sunduğu *Starlink* uydu hizmetleri, Ukrayna'nın iletişim altyapısını ayakta tutarak savaşın seyrini doğrudan etkilemiştir. Dolayısıyla siber uzayda ortaya

[201] Wijninga - Oosterveld - Galdiga - Marten, "State And Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies*, 144.
[202] Peter Wijninga - Willem Theo Oosterveld - Jan Hendrik Galdiga -Philipp Marten, "State And Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies* (Erişim Mart 2024), 141.
[203] Mehmet Çatlı, *Dijital Devlet Teorisi* (Ankara: Adalet Yayınevi, 2021), 127.

çıkan bu özel sektör temelli, ekonomik ve teknik güce sahip aktörler; devlet dışı olmalarına rağmen, kimi durumlarda devletlerden daha fazla jeopolitik etki kapasitesine sahip olabilmektedir. Bu nedenle "siber uzaydaki yeni devlet dışı aktörler" ifadesi hem kavramsal hem de olgusal açıdan yerinde bir tanımlamadır.

Devletler, siber çatışmanın var olduğu on yıllar boyunca çeşitli siber aktörlerle hem bilerek hem de bilmeyerek belirsiz makul bir inkâr edilebilirlik derecesinde ilişkiler kurmuşlardır. Bu aktörler farklı gelişmişlik seviyelerindeki siber suç örgütlerinden, vatansever bilgisayar korsanlarına, hacktivistlere,[204] medya kuruluşlarından, özel şirketlere, özel işletmelere, lobi gruplarına, özel askeri örgütlere ve hükümetlerle daha yakın ancak yine de makul bir şekilde inkâr edilebilir ilişkileri olan "gelişmiş kalıcı tehdit aktörleri" (*advanced persistent threat actors)* arasında değişmektedir.[205]

Devletler siber uzaydaki yeni devlet dışı aktörlerle çalışmayı çeşitli nedenlerle cazip bulmuşlardır. Bunun başlıca nedeni devletlerle devlet dışı aktörler arasındaki ilişkilerin muğlak ve gizli olmasıdır. Bu da devletlerin siber olaylardaki rollerini makul bir şekilde inkâr edebilmelerine ve düşmanlarının olası misillemelerinden veya kendi iç politikaları bağlamında siyasi bedeller ödemekten korunabilmelerine imkân vermektedir.[206]

Devletlerin siber uzaydaki yeni devlet dışı aktörleri kullanmalarının en önemli nedenlerinden biri, uluslararası hukuk bağlamında sorumluluktan kaçma isteğidir. Zira siber uzay, yüksek düzeyde anonimlik sağlayan bir alan olup, faillerin tespit edilmesini ve sorumluluğun belirlenmesini oldukça güçleştirmektedir. Uluslararası hukukta devletler, genellikle kendi organları ya da kamu gücünü kullanan kuruluşları tarafından işlenen fiillerden sorumlu tutulmaktadır. Ancak siber saldırıların bilgisayar korsanları veya büyük teknoloji şirketleri gibi yeni devlet dışı aktörler tarafından gerçekleştirilmesi halinde, bu fiillerin devlete atfedilebilmesi daha karmaşık ve dikkatli bir hukuki değerlendirme gerektirmektedir. Bu sayede devletler, bu tür aktörleri kullanarak yürüttükleri faaliyetleri inkâr edebilmekte ve doğrudan sorumluluktan kaçınabilmektedirler.

Yeni devlet dışı aktörlerin uluslararası bir çatışmada ilk kez yer almaları Kosova Savaşı'nda gerçekleşmiştir. Bu olay, aynı zamanda "internetteki ilk savaş" olarak da nitelendirilmektedir. Kosova Savaşı'nın siber uzay boyutu, hem devlet hem de devlet dışı aktörler tarafından bilgi yaymak, propaganda yapmak, muhalifleri şeytanlaştırmak ve kendi

[204] Vivi Cathrine Ringnes Wilhelmsen, *Soft War In Cyberspace: How Syrian non-state actors use hacking to influence the conflict's battle of narratives*, (University of Oslo, Yüksek Lisans Tezi, 2014), 6.
[205] Lewis - Lonergan - Voo - Garson - Ertan, "Evolving Cyber Operations and Capabilities", 7.
[206] Lewis - Lonergan - Voo - Garson - Ertan, "Evolving Cyber Operations and Capabilities", 7.

pozisyonlarına destek aramak amacıyla kullanılmıştır. Bilgisayar korsanları, kamuya ait bilgisayarlarda hizmet kesintilerine yol açarak ve çeşitli web sitelerini ele geçirerek, hem Yugoslavya'ya hem de NATO'ya yönelik saldırganlığa karşı tepkilerini dile getirmişlerdir. Sivil halk ise bu alanı, çatışma bölgesinde yaşadıkları olayları ve maruz kaldıkları korku ile dehşet anılarını dünyaya aktarmak için kullanmıştır.[207] Nisan 1999'da Los Angeles Times, Kosova'daki çatışmanın "siber uzayı; elektronik görüntüler, çevrimiçi tartışma grubu gönderileri ve bilgisayar korsanlığı saldırıları yoluyla, kalpler ve zihinler uğruna yürütülen savaşın uhrevi bir savaş alanına dönüştürdüğünü" yazmıştır.[208] Bu yönüyle Kosova Savaşı, siber uzaydaki farklı niteliklere sahip yeni devlet dışı aktörlerin ilk kez nasıl ortaya çıktıklarını gözler önüne sermiştir.[209]

Siber uzaydaki yeni devlet dışı aktörler, motivasyonları, örgütlenme biçimleri ve ev sahibi devletle ilişkilerine göre farklı şekillerde tasnif edilebilmektedirler.[210] Bu alandaki aktörler finansal motivasyonla hareket edebilir, kötü niyetli faaliyetlerinden elde ettikleri kârla bir hükümetin siber stratejisini destekleyebilir ya da operasyonlarını siyasi veya ideolojik nedenlerle gerçekleştirebilirler. Bu aktörlerden bazıları doğrudan ancak gayrı resmi olarak ev sahibi devletin istihbaratının ve askeri kurumlarının kontrolü altında faaliyet gösterebilirken, diğerleri devlet aktörlerine desteklerini para karşılığında veya herhangi bir menfaat karşılığında vermektedir.[211] Aşağıda yeni devlet dışı aktörler olarak ilk önce gerçek kişiler ardından büyük teknoloji şirketleri incelenecektir.

3.2.1. Yeni Devlet Dışı Aktörler Olarak Gerçek Kişiler

Siber uzaydaki gerçek kişileri oluşturan yeni devlet dışı aktörler arasında; sıradan yurttaşlar, script kiddie'ler, bilgisayar korsanları, aktivist aktörler ve siber organize suç örgütleri yer almaktadır.

---

[207] Dorothy E. Denning, "Activıism, Hacktivism, And Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy", *Networks and Netwars* ed. John Arquilla - David Ronfeldt (Santa Monica, Kaliforniya: RAND Corporation, 1999), 239-240.

[208] Ashley Dunn, "Crisis in Yugoslavia—Battle Spilling over onto the Internet," *Los Angeles Times*, (3 Nisan 1999).

[209] Sico van der Meer, "How states could respond to non-state cyber-attackers", *Clingendael Institute* (Haziran 2020), 14.

[210] Johan Sigholm, "Non-State Actors in Cyberspace Operations", *Journal of Military Studies* 4/1 (Aralık 2013) 9.

[211] Johan Sigholm, "Non-State Actors in Cyberspace Operations", *Journal of Military Studies* 4/1 (Aralık 2013) 9.

3.2.1.1.Sıradan Yurttaşlar

Siber uzaydaki en yaygın aktör, internette gezinmek ve çevrimiçi hizmetleri kullanmak gibi çeşitli yasal amaçlar için interneti kullanan sıradan yurttaşlardır. Bu aktör kategorisinde ev kullanıcılarının yanı sıra şirketlerin, kamu ve özel kuruluşların çalışanları da yer alır. Ortak özellikleri eylemlerinin ve güdülerinin tamamen bireysel ve çoğunlukla iyi niyetli olmasıdır.

Siber eylemler söz konusu olduğunda bu aktör kategorisi genellikle pasiftir ya da dolaylı olarak hareket etmektedir. Örneğin, bu kategorideki kişiler bir "botnet"in — güvenlik savunmaları ihlal edilmiş ve kontrolü kötü niyetli bir aktöre geçmiş internete bağlı bilgisayarlar topluluğunun — "zombileştirilmiş" kurbanları olabilir ya da daha bilinçli bir şekilde, kendi kaynaklarının bir siber eylemde başkaları tarafından kullanılmasına isteyerek izin verebilirler.[212]

3.2.1.2.Script Kiddies

Script kiddie, siber saldırılar gerçekleştirmek için mevcut komut dosyalarını ve yazılımları kullanan amatör bilgisayar korsanlarını tanımlamak için kullanılan küçümseyici bir terimdir.[213] Daha açık bir ifadeyle script kiddieler, bilgisayar sistemlerine veya ağlarına saldırılar başlatmak için önceden var olan otomatik araçları veya komut dosyalarını kullanan, teknik uzmanlığı çok az veya hiç olmayan kişileri ifade etmek için kullanılır. Kullandıkları araçları oluşturmak için başkalarına güvenirler, bu da onları kendi yöntemlerini geliştirme becerisine sahip olmayan amatör bilgisayar korsanları haline getirir.[214]

Script kiddie'lerin çoğu eğlenmek için bilgisayar korsanlığı yapan ve bunu bir oyun olarak gören gençlerden oluşmaktadır. Bununla birlikte script kiddie'ler maddi kazanç, siyasi veya ideolojik güdüler ve macera duygusuyla da hareket edebilmektedirler.[215]

Script kiddie'ler yetenekli bilgisayar korsanlarının teknik bilgisine sahip olmasalar da, saldırıları yine de önemli zararlara neden olabilir. Bu saldırılar itibar kaybına, mali kayıplara ve hatta hukuki sonuçlara da yol açabilir. [216]

[212] Sigholm, "Non-State Actors in Cyberspace Operations", 13.
[213] Clare Stouffer, "What is a script kiddie? Definition + examples", *Norton* (22 Haziran 2023).
[214] Sangfor Technologies (SANGFOR), "What Are Script Kiddies in Cybersecurtity" (Erişim 8 Nisan 2024).
[215] Techslang, "What is a Script Kiddie?" (Erişim 8 Nisan 2024).
[216] Techslang, "What is a Script Kiddie?" (Erişim 8 Nisan 2024).

Script kiddie'ler genellikle yüksek profilli hedeflere yönelirler. Saldırıları başlatmak için çoğunlukla hazır araçlar ve komut dosyaları kullanırlar, bu da hızlı bir şekilde yaygın hasara neden olmalarını kolaylaştırır. [217]

Script kiddie saldırılarıyla ilişkili en önemli risklerden biri, daha yetenekli saldırganlarla aynı yöntemleri kullanabilmeleridir. Bu, daha gelişmiş saldırganların yararlanabileceği güvenlik açıklarını yanlışlıkla keşfedebilecekleri ve daha da ciddi sonuçlara yol açabilecekleri anlamına gelir.[218]

3.2.1.3.Bilgisayar Korsanları

Siber uzaydaki yeni devlet dışı aktör olarak bilgisayar korsanları, tek başına faaliyet gösteren gerçek kişilerden organize ve sofistike kabiliyetlere sahip gruplara dönüşmüş, sıklıkla devletler tarafından vekil olarak kullanılarak siber casusluk, sabotaj ve dezenformasyon kampanyaları gibi saldırılar gerçekleştirmişlerdir. Bu bağlamda örneğin, Kuzey Kore ve İran gibi devletlerin, *Bureau 121* ve *MuddyWater* gibi bilgisayar korsanı gruplarını yabancı hedeflere yönelik siber saldırılar gerçekleştirmek için kullandıkları bildirilmektedir. Bu durum, doğrudan askeri müdahaleye başvurmaksızın stratejik etki alanlarını genişletmelerine imkan tanımaktadır.

Bilgisayar korsanlarının kim olduğu ve tam olarak ne yaptıkları konusundaki hararetli münakaşalar internetin ilk dönemlerine ve daha sonraki yıllara kadar devam etmiştir. Genel olarak bilgisayar korsanı, bilgisayar sistemleri ve ağlarındaki zayıflıkları bulmaya çalışan ve istismar eden kişi olarak tanımlanabilir. Bilgisayar korsanları benimsedikleri amaçlara göre farklı kategorilere ayrılabilir. Çünkü bazı bilgisayar korsanları şirketlere ya da hükümetlere destek olmak için güvenlik açıkları arar ve bu açıklardan istifade eder.

Bilgisayar korsanları çoğu zaman özgürlük, mahremiyet, liyakat ve erişim gibi bazı ortak ilkeleri paylaşan çeşitli bireylerden oluşmaktadır.[219] Bu ilkeler yalnızca bilgisayar korsanlarına mahsus olmamakla birlikte, bu etiketi benimseyenler süregelen siyasi kaygıları teknolojik araçlarla yeniden gündeme getirerek ahlaki ve hukuki meselelerin dijital çağla ilgisini ortaya koymuşlardır. Bununla birlikte, bilgisayar korsanları giderek teknolojinin

[217] SANGFOR, "What Are Script Kiddies in Cybersecurtity".
[218] SANGFOR, "What Are Script Kiddies in Cybersecurtity".
[219] Gabriella Coleman, "The Anthropology of Hackers," *The Atlantic* (21 Eylül 2010).

siyaseti ile meşgul olmak yerine, anarşist ve küreselleşme karşıtı hareketlerde aktif rol alarak siyasi süreçlerde iştirak etmeye başlamışlardır.[220]

Rusya Devlet Başkanı Vladimir Putin 1 Haziran 2017 tarihinde Petersburg Uluslararası Ekonomik Forumu kapsamında ulusal haber ajanslarıyla birlikte gerçekleştirdiği bir basın toplantısında Rusya'nın Almanya'ya ve 2016 ABD başkanlık seçimlerine olası müdahalesiyle ilgili bir soruyu yanıtlarken bilgisayar korsanları ile ilgili ilginç ifadelere yer vermişti. Putin'e göre; "*Bilgisayar korsanları özgür insanlardır, tıpkı sanatçılar gibi: iyi bir ruh hali içinde uyanırlar ve resim yapmaya başlarlar. Bilgisayar korsanları için de aynı şey geçerlidir; eğer uyandıklarında uluslararası ilişkilerde bir şeyler olduğunu okurlarsa ve vatanseverlik eğilimleri varsa, üzerlerine düşeni yaparlar*."[221]

Putin tarafından yapılan bu açıklama, bilgisayar korsanlarının jeopolitik olaylardaki rolüne vurgu yapmaktadır. Daha açık bir ifadeyle bu ifadeler devlet dışı aktörlerin seçimler, askeri çatışmalar ve sivil ayaklanmalar gibi durumlarda ulus devletlerle girdikleri muğlak ilişkilere dair süregelen daha geniş bir tartışmaya işaret etmektedir.[222] Aşağıda bilgisayar korsanları "siyah şapkalı bilgisayar korsanı", "beyaz şapkalı bilgisayar korsanı" ve "gri şapkalı bilgisayar korsanı" olarak tasnif edilmişlerdir.

3.2.1.4.Siyah Şapkalı Bilgisayar Korsanı

Siyah şapkalı bilgisayar korsanları, "kırıcı" *(cracker)* olarak adlandırılan kötü niyetli bilgisayar korsanlarıdır. Bunlar bilgisayar sistemlerini ve ağlarını kendi çıkarları için kullanan kişilerdir. Örneğin, bir çevrimiçi mağazanın bilgisayar sistemine girip kayıtlı kredi kartı numaralarını çalabilirler. Daha sonra çalınan bilgileri ürün, teknik ekipman satın almak veya kredi kartı numaralarını üçüncü bir tarafa satmak için kullanabilirler. Siyah şapkalı bilgisayar korsanları genellikle bilgisayar korsanlığı dünyasının en kötü niyetli aktörleri olarak görülmektedirler.[223]

[220] Jeffrey S. Juris, *Networking futures: the movements against corporate globalization* (Londan: 2008), 96.
[221] Tetyana Lokot, "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism", *Irish Studies in International Affairs*, 28 (2017), 99-100.
[222] Lokot, "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism", 100.
[223] Sigholm, "Non-State Actors in Cyberspace Operations", 14.

Yeni bir güvenlik açığı bulan siyah şapkalı bir bilgisayar korsanı, bu açığı kullanan bir yazılımı karaborsada suç örgütlerine satabilir ya da bilgisayar sistemlerini tehlikeye atmak için kullanabilir.[224]

3.2.1.5.Beyaz şapkalı Bilgisayar Korsanı

Beyaz şapkalı bilgisayar korsanı, güvenliklerini test etmek ve değerlendirmek amacıyla korunan sistemlere ve ağlara giren bir bilgisayar güvenliği uzmanıdır. Bu kişiler, güvenlik açıklarını siyah şapkalı korsanlar tarafından tespit edilmeden önce ortaya çıkararak güvenliği artırmayı hedeflemektedir. Kullandıkları yöntemler, kötü niyetli bilgisayar korsanlarının yöntemleriyle birebir aynı olmasa da benzerlik göstermektedir.[225]

Beyaz şapkalı bilgisayar korsanları, kamu ve özel kuruluşların güvenlik sisteminde tespit edilen güvenlik açığını ifşa eder, böylece kötü niyetli aktörler tarafından istismar edilmeden önce düzeltilebilir.[226] Beyaz şapkalı bilgisayar korsanları, bir sistemin güvenliğini arttırmak için çeşitli kurumlarla birlikte çalışan iyi adamlar olarak kabul edilirler. Bunlar "etik bilgisayar korsanları" olarak da adlandırılır. Bu bireyler, bir kuruluşun bilgi sistemlerini güvence altına almak için etik hack araçları, teknikleri ve metodolojileri konusunda uzmanlaşmıştır. Siyah şapkalı bilgisayar korsanlarının aksine, beyaz şapkalı bilgisayar korsanları güvenlik ağlarını istismar eder ve yasal olarak izin verildiğinde arka kapılar ararlar.

3.2.1.6.Gri Şapkalı Bilgisayar Korsanı

Gri şapkalı bilgisayar korsanları beyaz şapkalı ve siyah şapkalı bilgisayar korsanları arasında bir yerde yer alır. Onların hackleme türü, doğası gereği kötü niyetli olmasa da çoğu durumda hukuka aykırıdır. Koşullara bağlı olarak saldırgan veya korumacı olarak çalışabilirler.[227]

Genellikle kendi başlarına çalışırlar. Güvenlik ağlarındaki tehditleri ve zayıflıkları sahibinin izni olmadan araştırırlar. Bir kuruluşun ağına sahibinin izni olmadan girerler ve

[224] Sijbren de Jong - Willem Th. Oosterveld - Stephan De Spiegeleire - Frank Bekkers - Artur Usanov, Kamal Eldin Salah - Petra Vermeulen - Dana Polácková, *Better Together* (Hague Centre for Strategic Studies, 2016), 57.
[225] Sanchit Nanda, "World of White Hat Hackers", *International Journal of Scientific & Engineering Research* 10/ 5 (Mayıs 2019), 285.
[226] Nanda, "World of White Hat Hackers", 286.
[227] Prachi Arora - Mishita Poojary- Ishita Patel, "A Review Paper on White Hat Hackers", *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* 12/ 1(Aralık 2021), 283.

sistemdeki açıkları bulmaya çalışırlar. Bir ücret karşılığında yöneticiyi potansiyel tehditler hakkında bilgilendirirler.[228]

Bu kişiler genellikle buldukları güvenlik açığı hakkında sessiz kalmak için bir miktar talep ederler. Şirketin veya bireyin sistemine yetkisiz erişim sağlamak için yasaları çiğnerler, ancak her zaman kötü niyetli değildirler.[229]

3.2.1.7. Aktivist Aktörler

Siber uzayda faaliyet gösteren aktörler yalnızca devletler veya bilgisayar korsanlarıyla sınırlı değildir; bireylerden oluşan veya gevşek yapılarla örgütlenen siber aktivist gruplar da uluslararası sistemde giderek daha görünür hâle gelmektedir. Bu tür aktörler, genellikle siyasi, ideolojik ya da etik saiklerle hareket ederek hükümetlere, çok uluslu şirketlere ya da çeşitli kurumlara yönelik dijital protesto ve müdahalelerde bulunmaktadır. "*Hacktivist*" olarak da adlandırılan bu gruplar, DDoS saldırıları, web sitelerini tahrif etme, veri sızdırma veya sistemleri geçici olarak işlevsiz hâle getirme gibi yöntemler kullanmaktadır. *Anonymous, LulzSec* gibi kolektifler bu kategorideki aktörlere örnek teşkil etmektedir. Bu grupların eylemleri, çoğu zaman bir savaş ya da silahlı çatışma bağlamına oturmamakla birlikte, ulusal güvenliği tehdit eden sonuçlar doğurabilmekte ve iç hukuka veya uluslararası normlara aykırılık teşkil edebilmektedir.[230] Aşağıda bu aktörlerden "*hacktivistler*"e ve "vatansever bilgisayar korsanları"na yer verilmiştir.

3.2.1.7.1. Hacktivistler

Hacktivizm, bilgisayar korsanlığı ve aktivizmin birlikteliğini temsil eder.[231] Bir tanım yapacak olursak hacktivizm, siber uzay kaynaklarının yasal veya yasadışı yollarla, genel bir protesto aracı olarak veya ifade edilen bir ideolojiyi veya siyasi bir gündemi desteklemek için kullanılmasıdır.[232] Bu tanımdan da anlaşılacağı üzere hacktivizm aslında çevrimiçi aktivizmi ifade etmektedir.[233] Daha açık bir ifadeyle hacktivizm geniş bir siber faaliyet kategorisidir ve

[228] Arora - Poojary- Patel, "A Review Paper on White Hat Hackers", 283.
[229] Arora - Poojary- Patel, "A Review Paper on White Hat Hackers", 283.
[230] John Arquilla -David Ronfeldt (ed.) *Networks and Netwars* (Santa Monica, Kaliforniya: RAND Corporation, 1999), 241.
[231] Arquilla - Ronfeldt (ed.) *Networks and* Netwars, 241.
[232] Sigholm, Non-State Actors in Cyberspace Operations", 14.
[233] Paganini, "Non State Actors In Cyberspace: An Attempt To A Taxonomıc Classification, Role, Impact And Relations Wıth A State's Socio Economic Structure", 9.

ideolojik olarak motive olmuş yeraltı örgütlerin ve yaşanan bir adaletsizlikten dolayı mutsuz olan kişilerin faaliyet alanına tekabül eder.[234] Hacktivistler siyasi veya ideolojik motivasyona sahip bağımsız bilgisayar korsanlarıdır.[235]

Hacktivistler "yalnız kurt" olarak veya Anonymous[236] gibi merkezi olmayan, ulus ötesi kolektifler şeklinde faaliyet gösterirler. Bu bağlamda Anonymous, siber uzaydaki hedeflere saldıran; bilgi özgürlüğü ve insan hakları gibi çeşitli gerekçelerle hareket eden, gevşek bir biçimde birbirine bağlı bireyler, gruplar ve diğer oluşumlardan oluşan hacktivist bir kolektiftir.[237] Anonymous kendisini direktiflerden ziyade fikirlerle çalışan oldukça gevşek ve merkezi olmayan bir komuta yapısına sahip bir oluşum olarak tanımlamaktadır.[238]

Hacktivistler genellikle sosyal medya platformları ve bilgisayar korsanlığı forumları aracılığıyla başlatılan ve düzenlenen belirli operasyonlara bağlı olarak geçici kümelenmeler halinde faaliyet gösterebilen gruplardan oluşur. Hacktivistler tarafından kullanılan araçlar arasında web sitesi tahrifatları, internet kaynak yönlendirmeleri, hizmet reddi saldırıları, bilgi hırsızlığı, web sitesi parodileri, sanal oturma eylemleri ve çeşitli siber sabotaj biçimleri yer almaktadır.[239]

3.2.1.7.2. Vatansever Bilgisayar Korsanları

Vatansever bilgisayar korsanları, siber eylemler ve faaliyetler gerçekleştirerek milli ve siyasi hedeflere ulaşmak için siber saldırılar düzenleyen bireyler veya gruplardır.[240] Bununla birlikte vatansever bilgisayar korsanlarını ifade etmek için literatürde çeşitli tanımlar mevcuttur. Örneğin, Denning onları "devletten devlete siber çatışmaya giren vatandaşlar veya gurbetçiler" olarak tanımlamaktadır.[241] Borghard ve Lonergan vatansever bilgisayar korsanlarını siyasi hedefleri olan örgütlenmemiş gruplar ya da bireyler olarak ifade etmiştir.[242]

---

[234] Rachel A. Gabriel - Barnett S. Koven, *Malicious Non-state Actors and Contested Space Operations*, (Office of University Programs and DoD Strategic Multilayer Assessment Branch, 2018),23.
[235] Jong - Oosterveld - Spiegeleire - Bekkers - Usanov, Salah - Vermeulen - Polácková, *Better Together* 57.
[236] Nadiya Kostyuk- Scott Powell -Matt Skach, "Determinants of the Cyber Escalation Ladder", *The Cyber Defense Review* 3/1 (2018), 126.
[237] Ralph Martins, "Anonymous' Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts", *The Cyber Defense Review* 2/3 (2017), 96.
[238] Tim Jordan, Information *Politics* (Londra: Pluto Press, 2015), 178.
[239] Sigholm, "Non-State Actors in Cyberspace Operations", 14.
[240] Drioueche Asma Sarra Youssra, "Patriotic Hackers in Cyberspace Operations: Independent or Sponsored Cyber Actors?", *The Algerian Journal of Political Studies* 09/ 01 (Haziran 2022), 652.
[241]Dorothy E. Denning, "The Ethics of Cyber Conflict", *The Handbook of Information and Computer Ethics*, ed. Kenneth Einar Himma ve Herman T. Tavani (Hoboken, NJ: John Wiley & Sons, 2008), 17.
[242] Steven Wood, *Patriotic Hackers* (Manchester: Faculty of Business and Law Manchester Metropolitan University, Yüksek Lisans Tezi, 2017), 7.

Holt ve Schell vatansever bilgisayar korsanlarını anavatanlarını ya da etnik kökenlerinin bulunduğu ülkeyi savunmak için siber saldırılarda bulunan vatandaşlar ve gurbetçiler olarak tanımlamaktadır.[243] Dinniss ise vatansever bilgisayar korsanlarını ulusal ve siyasi amaçlar güden ve siber saldırılar düzenleyen bireyler ve gruplar olduğunu vurgulamıştır.[244] Steven Wood ise bunları "devletlerinin rızasıyla ya da rızası olmadan, ülkeleri adına kötü niyetli bilgi teknolojileri eylemleri gerçekleştiren kişiler" olarak belirtmiştir.[245]

Vatansever bilgisayar korsanları devletlerinin vatandaşlarıdır, bununla birlikte devletlerinin ihtiyaç duyduğu bilgileri sağlamak için siber casuslar gibi çalışabilirler. Bu kişiler yaptıkları işi ülkelerinin siyasi ve askeri meselelerine yardımcı olmak amacıyla yaptıklarını düşünmektedirler.[246]

1999'da ABD'nin yanlışlıkla Çin büyükelçiliğini bombalamasının ardından Çinliler tarafından gerçekleştirilen siber saldırılar, 2007'de Estonya'ya yapılan siber saldırılar, 2016'da ABD Demokrat Partisinin Ruslar tarafından siber saldırılara maruz kalması vatansever bilgisayar korsanı saldırı vakıalarıdır.

Vatansever bilgisayar korsanları ile hacktivistler çoğu zaman birbirleriyle karıştırılmaktadır. Her iki grup da siyasi motivasyonla hareket etse de, hacktivistler vatandaşı oldukları ya da ikamet ettikleri ülkeyi doğrudan ilgilendirmeyen siyasi veya toplumsal meseleleri gündeme getirmeye çalışırlar. Bu kişiler daha çok özgürlük, ifade özgürlüğü, insan hakları ve bilgi etiğini teşvik etmek amacıyla saldırılar düzenlerler. Bu yönüyle hacktivizm, özgün bilgisayar korsanı anlayışının siyasi bir uzantısı niteliğindedir.[247]

Vatansever bilgisayar korsanları ise hacktivistlerden farklı bir gündeme ve farklı bir politik yaklaşıma sahiptir. Bu kişiler, kendilerini düzensiz askerler ya da ülkeleri adına savaşan birer siber milis olarak görürler. Doğaları gereği kozmopolit bir bakış açısından ziyade dar ve milliyetçi bir dünya görüşüne sahiptirler. Vatansever bilgisayar korsanları, kendilerini daima milliyetçi terimlerle tanımlarlar – İsrailli, Filistinli, İranlı vb. Gerçekleştirdikleri saldırılar, kullanılan dil ve söylemlerde açıkça görülen güçlü vatanseverlik ve milliyetçilik duygularıyla motive edilir.

Vatansever bilgisayar korsanlarının eylemleri hedef alınan sistemlerde ciddi hasara yol açabilir. Birçoğu saldırıları ya da misillemeleri düzenlerken ulusal gururu temsil ettiklerini ve

[243] Thomas J. Holt – Brent H. Schell, "Patriotic Hackers: Cyber Warriors Defending Their Homeland", *Journal of Cybersecurity Studies* 1/1 (2015), 45.
[244] N. J. Barata, *"Patriotic Hackers": Non-State Actors Fighting Wars For States,* (Aveiro: University of Aveiro).
[245] Wood, *Patriotic Hackers*, 15.
[246] Rika Isnarti, "The Role of China's Patriotic Hackers and Their Relationship to the Government", *Andalas Journal of International Studies* 4/2 (Kasım 2015), 164.
[247] Michael Dahan, "Hacking for the homeland: Patriotic hackers versus hacktivists", *Research Gate* (Ocak 2013).

kurtardıklarını belirtmektedir. Bazı durumlarda vatansever bilgisayar korsanları kendilerini devletin uzantısı olarak tanımlamakta ve devletin yapmayacağı ya da yapamayacağı şeyleri yapmaktadırlar.[248]

3.2.1.8.Organize Suç Yapıları

Geleneksel organize suç yapılarının dijital ortama uyum sağlamasıyla birlikte, suç örgütleri artık sınır aşan, yüksek düzeyde koordineli ve teknik açıdan son derece sofistike yöntemlerle faaliyet göstermektedir. Fidye yazılımı saldırılarından çevrimiçi dolandırıcılığa, yasa dışı veri ticaretinden kripto varlıkların izinsiz ele geçirilmesine kadar uzanan geniş bir yelpazede eylemler, bu grupların başlıca faaliyet alanlarını oluşturmaktadır. Söz konusu yapılar, çoğu zaman VPN, TOR ağı ve kripto para kullanımı gibi anonimlik sağlayan ve iz sürmeyi zorlaştıran teknolojilerden faydalanarak faaliyetlerini ulusal sınırların ötesine taşımakta; bu durum, klasik kolluk mekanizmalarının yetersiz kalmasına neden olmaktadır. Ayrıca, bazı durumlarda bu grupların devlet destekli olması ya da devletlerin bilgisi dâhilinde hareket etmeleri, uluslararası hukuki sorumluluk tartışmalarını daha da karmaşık hâle getirmektedir. Aşağıda, siber uzaydaki organize suç yapılarından olan siber suç örgütlerine, siber paralı askerlere, 'cyber insider'lara ve siber teröristlere ayrıntılı şekilde yer verilmiştir.

3.2.1.9.Siber Suç Örgütleri

Siber suç örgütleri tehdit ortamındaki en aktif oluşumlardır.[249] Gerçekleştirdikleri filler veri ve altyapıların zarar görmesine, tahrip olmasına, para ve fikri mülkiyetin ve kişisel ve finansal verilerin çalınmasına neden olabilmektedir. Devletler adına faaliyet gösteren *gelişmiş kalıcı tehdit grupları* ile siber suç örgütleri arasında çoğu durumda bir benzerlik vardır. Bununla birlikte, siber suç örgütleri çoğunlukla daha üst düzey bir örgütsel yapıya ve bazı durumlarda ev sahibi devletle sıkı bağlantılara sahiptir. Ev sahibi devletler siber suç örgütlerini siber operasyonlara dâhil edebilir, mali imkanlarından faydalanabilir ve paralı asker olarak

[248] Michael Dahan, "Hacking for the Homeland: Patriotic Hackers versus Hacktivists", *Research Gate* (Ocak 2013).
[249] Paganini, "Non State Actors In Cyberspace: An Attempt To A Taxonomic Classification, Role, Impact And Relations Wıth A State's Socio Economic Structure", 7.

kullanabilirler. Aynı zamanda bu gruplara bir tür dokunulmazlık vaat ederek onları işbirliğine zorlayabilirler.[250]

Siber suç örgütlerinin devletler tarafından yürütülen operasyonlara dâhil edilmesinin en büyük avantajı, bu örgütlerin eylemlerinin devlete atfedilmesini imkânsız hâle getirmese de oldukça zorlaştırmasıdır. Bu tür örgütler, planlanan bir siber saldırı için bilgi, insan kaynağı ve teknik altyapı sağlayarak devletlerin doğrudan sorumluluktan kaçınmasına olanak tanıyabilir.[251]

Siber suç örgütlerinin geçmişine bakıldığında, tarihin en güçlü siber suç örgütlerinden biri olarak 'Rus İş Ağı' (Russian Business Network) öne çıkmaktadır. Bu örgütün, 2008 yılında yaşanan çatışma sırasında Gürcistan'a yönelik gerçekleştirilen siber saldırılara katkıda bulunduğu iddia edilmektedir.[252]

3.2.1.10. Siber Paralı Askerler

"Paralı asker" ifadesi, 12. yüzyıldan bu yana silahlı çatışmalarda savaşmak üzere yerel ya da denizaşırı ülkelerden toplanan kişileri tanımlamak için kullanılmaktadır. [253] Son yıllarda yaşanan hızlı teknolojik gelişmeler ise faaliyetlerini internet ortamında yürüten ve genel olarak 'siber paralı askerler' olarak adlandırılan, daha sofistike ve örgütlü suç oluşumlarının ortaya çıkmasına zemin hazırlamıştır.[254]

Genel bir tanımla siber paralı askerler, belirli siber ağlar ve altyapılara yönelik harekete geçmek için siber saldırı veya savunma operasyonları yürütmek üzere kiralanan kişi, grup veya özel aktörlerdir.[255] Bu kişiler genellikle yetenekli, iyi eğitimli, en son teknolojiler konusunda uygulamalı deneyime sahip ve her sektörde çalışabilecek çok yönlü kişilerdir. Siber paralı askerler "ara aktörler" (*intermediate actors*), "kiralık bilgisayar korsanları" (*hacker-for-hire*) ya da gri şapkalı firmalar (*grey-hat firms*) olarak da tasnif edilebilmektedirler.[256]

---

[250] Paganini, "Non State Actors In Cyberspace: An Attempt To A Taxonomic Classification, Role, Impact And Relations Wıth A State's Socio Economic Structure", 8.
[251] Paganini, "Non State Actors In Cyberspace: An Attempt To A Taxonomic Classification, Role, Impact And Relations Wıth A State's Socio Economic Structure", 8.
[252] Paganini, "Non State Actors In Cyberspace: An Attempt To A Taxonomic Classification, Role, Impact And Relations Wıth A State's Socio Economic Structure", 8.
[253] Sarah Percy, "Mercenaries", *Oxford Bibliographies*, (24 Temmuz 2023).
[254] Fitri Bintang Timur, "Cyber Mercenaries: The Failures Of Current Responses and The Imperative Of International Collaboration", *Observer Research Foundation* (Aralık 2023), 3.
[255] Lorenzo Valeri, "The Information Warrior," *Journal of Financial Crime* 6/1 (1998), 52-53.
[256] Timur, "Cyber Mercenaries: The Failures Of Current Responses And The Imperative Of International Collaboration", 3.

Müşterileriyle ideolojik bir bağı bulunmayan ve sözleşmeye dayalı olarak çalışan bir bilgisayar korsanı grubu olan siber paralı askerler, devletlere saldırgan siber operasyonları dış kaynak yoluyla yürütme imkânı sunmakta ve genellikle makul bir inkâr mekanizması sağlamaktadır. Bu tür bir dış kaynak kullanımı, geleneksel askerî ve teknolojik üstünlüğün etkisini azaltarak, daha küçük devletlerin veya devlet dışı aktörlerin siber uzayda kayda değer bir etki oluşturmasına olanak tanımaktadır.

Özel askeri ve güvenlik şirketlerinde faaliyet gösteren siber paralı askerler, istihbarat toplama, casus yazılım ve kötü amaçlı yazılım geliştirme,[257] veri sızıntılarına yol açma ve hatta dağıtılmış hizmet reddi (DDoS) saldırıları düzenleme gibi çeşitli faaliyetlerde bulunmaktadırlar. Ayrıca, endüstriyel sistemlere zarar verme, hedefin bilgi teknolojisi altyapısını zayıflatma, bilgisayarlara ve ağlara müdahale etme, bilgi çalma ve konum ile bankacılık bilgileri gibi son derece hassas verileri satışa sunma gibi yıkıcı hizmetler de sunmaktadırlar.[258]

3.2.1.11. Cyber Insiders

Cyber insider'lar, bilgisayar ve ağ kaynaklarına meşru erişim yetkisine sahip olan, bu kaynaklara ilişkin bilgileri kullanabilen ancak çalıştıkları işverene, kurumlarına veya bunların bileşenlerine sadık olmayan ve parasal çıkarlar ya da başka sebeplerle bu yapılara ihanet etmeye istekli aktörlerdir. Bu kişiler, geliştirilmesine katkı sağladıkları yazılımlara mantık bombaları yerleştirebilir, sistemlerde arka kapılar açabilir veya küçük, taşınabilir ve kolayca gizlenebilen depolama aygıtları aracılığıyla hassas verileri çalabilirler. Cyber insiderlar, işverenlerine karşı kişisel husumetle hareket edebilir, tepki göstermek amacıyla zarar verebilir ya da gizli bilgileri ifşa etmek, kurumsal sırları rakip şirketlere veya yabancı istihbarat servislerine satmak gibi eylemlerde bulunabilirler. Bu çerçevede söz konusu kişiler, zaman zaman siber casus veya script kiddie gibi davranarak kurum içinden gelen tehditlerin kaynağı hâline gelebilmektedir.[259]

Cyber insider tehdidi, diğer güvenlik açığı temelli saldırılardan farklı olarak, eylemi başlatan kişi tarafından gerçekleştirilen yetkisiz erişime değil, kuruluşun güvenlik sınırları içinde yer alan yetkili kişiler tarafından gerçekleştirilen yetkili erişime dayanmaktadır. Bu

[257] Amnesty International, Hackers For-hire in West Africa Activist in Togo Attacked with Indian-made Spyware, (7 Ekim 2021).
[258] Feike Hacquebord, "Void Balaur: Tracking a Cybermercenary's Activities", (Texas: Trend Micro Research, 2021), https:// documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pd
[259] Frank L. Greitzer - Andrew P. Moore - Dawn M. Cappelli - Dee H. Andrews - Lynn A. Carroll - Thomas D. Hull, "Combating the Insider Cyber Threat", *IEEE Security and Privacy* 6/1 (Ocak-Şubat 2008), 62-64.

nedenle, bir cyber insider tarafından başlatılan herhangi bir yasadışı eylem, izinsiz giriş tespit sistemleri, kayıt tutma mekanizmaları veya uzman sistemler tarafından anormal olarak algılanmayacak; bu durum da söz konusu eylemlerin tespit edilmesini ve engellenmesini son derece güç hâle getirecektir.[260]

3.2.1.12. Siber Teröristler

"Siber terörizm" kavramının açık ve tutarlı bir tanımının yapılmasının önünde bir dizi güçlük mevcuttur. Bununla birlikte siber-terörizm kavramı iki temel fikri ifade eder: siber uzay ve terörizm.[261]

Bu kavrama ilişkin bilgisayar bilimleri profesörü Dorothy Denning, çok sayıda makalesinde ve Mayıs 2000'de Temsilciler Meclisi Silahlı Hizmetler Komitesi önünde konuyla ilgili verdiği ifadede oldukça açık bir tanım ortaya koymuştur:

Siber terörizm, siber uzay ile terörizmin kesişiminde yer alan bir olgudur. Siyasi veya toplumsal hedefler doğrultusunda, bir hükümeti ya da halkı korkutmak veya baskı altına almak amacıyla bilgisayarlara, ağlara ve bu ortamlarda depolanan bilgilere yönelik gerçekleştirilen yasadışı saldırılar ile bu tür saldırı tehditlerini ifade eder. Bir siber saldırının siber terörizm olarak nitelendirilebilmesi için, kişilere veya mallara karşı şiddetle sonuçlanması ya da en azından ciddi düzeyde korku yaratacak ölçüde zarar vermesi gerekir. Ölüme, bedensel yaralanmaya, istismara veya ciddi ekonomik kayıplara yol açan saldırılar bu kapsama örnek olarak gösterilebilir. Kritik altyapılara yönelik ağır etkiler doğuran saldırılar, sonuçlarına bağlı olarak siber terörizm eylemi olarak değerlendirilebilir. Buna karşın, yalnızca zaruri olmayan hizmetleri kesintiye uğratan ya da esas itibarıyla maddi kayıplara neden olan saldırılar siber terör eylemi kapsamında değerlendirilmeyecektir.[262]

Siber terörizm, teknoloji devriminin ve gittikçe artan karşılıklı bağımlılığımızın ortaya çıkardığı arzu edilmeyen sonuçlardan biri haline gelmiştir.[263] Bu kavramın kökleri, internet kullanımındaki hızlı artışın ve ortaya çıkan "bilgi toplumu" tartışmalarının, yüksek düzeyde ağa bağlı ABD'nin karşı karşıya kaldığı potansiyel riskler üzerine çeşitli çalışmalara yol açtığı 1990'ların başına kadar uzanmaktadır.

---

[260] Sigholm, "Non-State Actors in Cyberspace Operations", 14.
[261] Namosha Veerasamy, "A High-level Conceptual Framework of Cyber-terrorism", *Journal of Information Warfare* 8/1 (2009) 44.
[262] Dorothy E. Denning, "Terrorıst Threats To The Unıted States", Commıttee On Armed Servıces House Of Representatıves (23 Mayıs 200).
[263] Mark Henych - Stephen Holmes - Charles Mesloh, "Cyber Terrorism: An Examination of the Critical Issues", *Journal of Information Warfare* 2/2 (2003), 1.

1990 kadar erken bir tarihte, Ulusal Bilimler Akademisi (*National Academy of Sciences*) bilgisayar güvenliği üzerine hazırladığı bir rapora aşağıdaki ifadelerle başlamıştı: "*Risk altındayız. Amerika giderek artan bir şekilde bilgisayarlara bağımlı hale geliyor. Yarının teröristi bir klavye kullanarak bombayla yapabileceğinden daha fazla zarar verebilir*."[264]

Siber teröristler ise, saldırılarını gerçekleştirmek ve toplumda korku yaratmak için bilgisayar ve ağ teknolojilerini kullanan kişilerdir.[265] Siber terörizm hakkında yayınlanan raporlarda, siber teröristler genellikle "sıradan" bilgisayar korsanlarını ya da terörist sanılan diğer aktörleri ifade etmektedir.[266]

3.2.2. Yeni Devlet Dışı Aktörler Olarak Büyük Teknoloji Şirketleri

Amerikalı yazar Francis Fukuyama, "Siyasi Düzenin Kökenleri" adlı eserinde, 16. yüzyılda Kilise'nin nasıl "devlet benzeri özellikler" kazandığını açıklamaktadır. Kilise, kendini meşrulaştırmak amacıyla tek bir kanon yani kilise hukuku oluşturarak; bürokratik bir yapı ve iyi kurumsallaşmış, ayrı bir ruhani otorite alanı geliştirmeyi hedeflemiştir. Her ne kadar yalnızca küçük bir toprak parçası üzerinde hüküm sürse de Kilise'nin gücü ve yarı-devlet niteliği, fiziksel sınırlarla sınırlı olmayan bu ruhani otoriteden kaynaklanmaktaydı. Kilise, sınırların ötesinde ve devletlerin üzerinde bir güç olarak kabul edilmekteydi. Bu durum, Kilise ile egemen devletler arasındaki ilişkiyi kimi zaman gergin, kimi zaman samimi, kimi zaman da rekabetçi fakat tamamen uyumsuz olmayan bir nitelikte sürdürmüştür.[267]

Kilisenin zamanla kazandığı ulusüstü nitelik, 21. yüzyılda siber uzayda ortaya çıkan ve yeni devlet dışı aktörler olarak nitelendirilebilecek *Apple, Meta, Alphabet, Microsoft, Yandex, X, Telegram, Tencent* gibi büyük teknoloji şirketleriyle benzerlik göstermektedir.[268] Bu şirketler, siber uzayın yönetimi ve güvenliğinin şekillendirilmesinde son derece etkili bir rol oynamaktadırlar. Büyük teknoloji şirketleri, kritik dijital altyapıya sahip olup bu altyapıyı işletmekte, siber güvenlik araçları geliştirmekte ve çevrimiçi davranışları düzenleyen norm ve standartları giderek artan ölçüde belirlemektedir. Siber uzayın düzenlenmesine ilişkin politika üretimi de büyük ölçüde bu şirketlerin tekelindedir. Daha açık bir ifadeyle, "teknoloji devleti" olarak adlandırılan bu büyük teknoloji şirketleri, siber uzayın fiili "yasa koyucuları" gibi hareket etmektedir. Ancak bu şirketler, devletlerin aksine, hesap verebilirlik, şeffaflık veya demokratik meşruiyet

[264] Gabriel Weimann, *Cyberterrorism How Real Is the Threat?* (United States Institute Of Peace, 2004), 2.
[265] Sigholm, "Non-State Actors in Cyberspace Operations", 18.
[266] Weimann, *Cyberterrorism How Real Is the Threat?*, 6.
[267] Francis Fukuyama, "*The Origins of Political Order: From Prehuman Times to the French Revolution",* (Farrar, Straus and Giroux. Kindle Edition, chapter 18.
[268] Markus Wagner, "Non-State Actors", *Max Planck Encyclopedia of Public International Law* (Erişim 3 Mart 2024), 1.

ilkelerine bağlı değillerdir. Bu durum, uluslararası hukuk ve insan hakları üzerindeki etkileri bağlamında ciddi endişelere yol açmaktadır. Dolayısıyla hem siber uzay faaliyetlerinin kolaylaştırıcısı hem de düzenleyicisi olarak üstlendikleri bu çift yönlü rol, onları uluslararası hukuk düzeni içerisinde hem benzersiz hem de hukuki statü bakımından belirsiz bir konuma yerleştirmektedir.

Büyük teknoloji şirketleri ulusal ve uluslararası meseleleri etkilemek ve sosyal değişimi tetiklemek için kullanan en önemli devlet dışı aktörler olarak kabul edilebilirler.[269] Örneğin 2001 yılında mobil mesajlaşma ağı Filipinler'de Başkan Estrada'nın devirilmesine yol açmıştır. 2011 yılında Mısır'da Başkan Hüsnü Mübarek'in devrilmesinde Google ve Facebook oldukça etkili olmuştur. [270] Aynı şekilde bu bilgi iletişim teknolojileri ulus ötesi suç ve terör örgütleri gibi saldırgan devlet dışı aktörlerin[271] de benzer şekilde küreselleşmiş iletişimin nimetlerinden faydalanmasına neden olmuştur.[272] Bu bağlamda, Twitter ve Facebook gibi kamuoyunun şekillenmesinde önemli rol oynayan çevrimiçi platformlar, değer yönelimlerini belirleme gücüne sahiptir. Bu platformlar, belirledikleri konuşma kuralları aracılığıyla çevrimiçi içeriği sınırlamakta veya silmekte; bu yolla da uluslararası siber uzay kamuoyunun eğilimlerini doğrudan etkilemektedirler.[273]

Elon Musk ve Bill Gates gibi liderler, teknoloji üstünlüğü, eşitlik, ekoloji ve feminizm gibi konulardaki görüşleriyle küresel kamuoyu algısını etkileyerek, onları takip eden bir dalga başlatabilirler. [274] Bu kişilerin sahibi oldukları büyük teknoloji şirketleri güçlü bir etki oluşturarak toplumların düşünce yapısını ve hareketlerini yönlendirebilirler. [275]

Büyük teknoloji şirketlerinin yükselişiyle birlikte, geleneksel güç odakları arasındaki hiyerarşik ilişkiler gerçek dünyada bulanıklaşmıştır.[276] Özellikle sosyal medya ve finans gibi dijital alanlardaki baskın kontrolü nedeniyle, yerleşik siyasi düzen ve devlet-sermaye

[269] Robert Longley, "What Are Non-State Actors?" *ThoughtCo.*, (Erişim Tarihi 3 Mart 2024).
[270] Alex Warofka, "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar, Meta", (Erişim 14.02.2024).
[271] Rato, M., & Petit, N. (2013). Abuse of dominance in technology-enabled markets: established standards reconsidered? European Competition Journal, 9(1), 1-65.
[272] Wijninga - Oosterveld - Galdiga - Marten, "State And Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies*, 147.
[273] Wijninga - Oosterveld - Galdiga - Marten, "State And Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies*, 147.
[274] Emeritus, "What Companies Fall Under Big Tech? How Do You Land a Job With Them?", (Erişim Tarihi 13 Şubat 2024)
[275] Wijninga - Oosterveld - Galdiga - Marten, "State And Non-State Actors: Beyond the Dichotomy", *Hague Centre for Strategic Studies*, 146.
[276] Jean Burgess-Alice Marwick-Thomas Poell, *"Regulation of and by Platforms",* The SAGE Handbook of Social Media, (London) 254–278.

etkileşimleri tehlikeye girmiştir.[277] Dijital çağda, güç veriye sahip olmakla ilişkilendirilir hale gelmiştir. [278] Joseph Nye, çağdaş küresel güç kaymasının, gücün devletten devlet dışı aktörlere yayılması olarak tanımladığını ve bu yayılmanın kısmen internetin ortaya çıkışıyla beraber bilgi teknolojisinin hızlı gelişimi ve dönüşümüne bağlı olduğunu vurgulamıştır. [279]

Nye, gücün sadece zorlama veya şiddetle ilişkilendirilmediğine inanmaktadır. Bazı güçler, zorlayıcı olmayabilir ve "yumuşak güç" olarak bilinen daha az baskıcı bir doğaya sahip olabilirler. "*Sosyal güç genellikle daha az zorlayıcıdır ve doğası gereği yumuşaktır; ortak haklardan faydalanır, çıkarları etkiler, kamuoyu aracılığıyla baskı uygular, diğer tarafın doğrudan uymasını sağlamak yerine teşvik eder, cesaretlendirir ve etkiler." [280]* Yeni devlet dışı aktörler olarak büyük teknoloji şirketleri de çoğunlukla zorlayıcı olmayan bu yumuşak güce sahiptirler. [281] Bu şirketler geniş veri kaynaklarını kontrol ederek diğer kuruluşları yavaş yavaş etkilemekte ve yönlendirmektedir; bu da gücün giderek "merkezsizleştiği" bir döneme girildiğini göstermektedir. [282]

Büyük teknoloji şirketleri, sahip oldukları teknik kapasite ve dijital yetenekler sayesinde devletlerin güvenliğini sağlama konusunda da önemli roller üstlenebilmektedir. Ancak bu durum, devlet güvenliği açısından belirli riskler de barındırmaktadır. Zira bu aktörler, geleneksel olarak yalnızca devletlerin ya da devletlerin yetkilendirdiği savunma sanayii firmalarının faaliyet alanı olan ulusal güvenliğe ilişkin konularda da etkin bir şekilde rol alabilmektedirler.[283] Örneğin, 2020 yılında Rusya'yla bağlantılı olduğu iddia edilen bilgisayar korsanları ABD devlet kurumlarına ve özel şirketlere sızdığında, bunları ilk tespit eden ve engelleyen Ulusal Güvenlik Ajansı ya da ABD Siber Komutanlığı değil *Microsoft* olmuştu. Bu örnekler, yeni devlet dışı aktör olarak büyük teknoloji şirketlerinin dijital dünyanın omurgasını inşa ettiklerini ve aynı zamanda bu dünyanın polisliğini yapmaya teşebbüs ettiklerini göstermektedir.[284]

Büyük teknoloji şirketlerinin büyük miktarda veriye erişimi, devlete has olan egemenlik ve üstünlük kavramlarını yeniden tanımlarken, fiili bir veri egemeni konumuna doğru da

---

[277] Shuai Feng, "The Principle of Sovereignty and Its Competitors: Order Construction and Evolutionary Logic of Digital Space", *Russian, East European & Central Asian Studies* 04: 96–119. 2022.
[278] Martin Moore, "Tech Giants and Civic Power", Kings Collage London, https://core.ac.uk/download/pdf/51344227.pdf (2016).
[279] Joseph S. Nye, "After The Liberal International Order", Project Syndicate" (Erişim Tarihi 16 Şubat 2024).
[280] Nye, "After The Liberal International Order", *Project Syndicate*" (Erişim Tarihi 16 Şubat 2024).
[281] Hongfei Gu, "Data, Big Tech, and the New Concept of Sovereignty", *Journal of Chinese Political Science*, 1-22.
[282] Michael L. Miller-Cristian Vaccari, "Digital Threats to Democracy: Comparative Lessons and Possible Remedies", *Sage Journals* 25/3, (11 Mayıs 2020) 333-356.
[283] John Gerard Ruggie, "Just Business: Multinational Corporations and Human Rights", (Norton Global Ethics Series) 1st Edition.
[284] Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order", Foreign Affairs, (Erişim 14 Şubat 2024)

ilerletmektedir.[285] Bu aktörler, verilerin kontrolünü ele geçirerek ve teknolojiyi tekellerinde toplayarak siyasi otoriteden bağımsız bir "dijital imparatorluk" oluşturma eğilimindedirler.[286]

Siber çatışmalarda yer alan şirketlerin faaliyetleri iki ana başlık altında sınıflandırılabilir: hukuka uygun eylemler ve hukuka aykırı eylemler. Hukuka uygun eylemler kapsamında, siber savaş faaliyetlerini destekleyen şirketler genellikle bu faaliyetleri bir ulus-devlet adına yürütmektedir. ABD'nde, federal hükümet adına bu tür roller üstlenen pek çok şirket bulunmaktadır. *Northrop Grumman, General Dynamics, Lockheed Martin, TASC* ve *Raytheon* gibi büyük savunma şirketleri, devlete uzmanlık ve kaynak sağlayarak gerekli siber faaliyetlerin yürütülmesini mümkün kılmaktadır.[287]

Yüzyılın ilk on yılında "özgürleştirici teknolojiler"[288] olarak görülen büyük teknoloji şirketleri günümüzde "dijital gangsterler" rolünü oynamakla suçlanmaya başladılar.[289] Her iki niteleme de haklıydı. Örneğin sosyal medya, 2010 yılında başlayan Arap Baharı halk ayaklanmasında kilit bir rol oynamış, 2014 tarihinde başlayan ve halen devam eden Rus işgallerinden bu yana hem Ukrayna vatandaşları hem de siyasi elitler için önemli bir araç olmuştur.[290] 6 Ocak 2021 tarihinde ABD Başkanı Donald Trump'ın destekçilerinin Kongre Binası'na baskın düzenlemesinin ardından Trump'ın[291] Facebook ve Twitter gibi ana akım platformlardan engellenerek uzaklaştırılması bu şirketlerin adeta devlet gibi davranarak cezalandırma yetkisini ellerine aldıklarını göstermektedir.[292] Bu durum, devletlerin tekelinde olması gereken cezalandırma yetkisinin, özel şirketlere kaydığını göstermektedir.[293] Bunlara ek olarak, birçoğu seçim dürüstlüğü, ifade özgürlüğü, mahremiyet veya şiddete teşvik gibi kilit demokratik konularla ilgili olan çeşitli skandallar ve tartışmalar, büyük teknoloji şirketlerinin itibarını ve onlara duyulan güveni zedelemiştir.[294]

---

[285] John Gerard Ruggie, "Just Business: Multinational Corporations and Human Rights", (Norton Global Ethics Series) 1st Edition.
[286] Gu, "Data, Big Tech, and the New Concept of Sovereignty".
[287] Christopher Drew - John Markoff, "Contractors Vie for Plum Work, Hacking for U.S.", *The New York Times* (30 Mayıs 2009).
[288] Larry Diamond-Marc F. Plattner, "Liberation Technology: Social Media and the Struggle for Democracy" (A Journal of Democracy Book).
[289] House of Commons: Digital, Culture, Media and Sport Committee, "Disinformation and 'Fake News': Final Report Eighth Report of Session 2017–19".
[290] Hamza Shaban, "Google For The First Time Outspent Every Other Company To İnfluence Washington n 2017", Washington Post, (Erişim 14 Şubat 2024).
[291] Francesca Sobande -AkaneKanai - Natasha Zeng, "The Hypervisibility and Discourses Of 'Wokeness' in Digital Culture", *Media, Culture and Society* 44/8 (2022), 1576-1587.
[292] Genevieve Lakier, "Informal Government Coercion and The Problem of Jawb "joning", Lawfare (Erişim 13 Şubat 2024).
[293] Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order", Foreign Affairs, (Erişim 14 Şubat 2024)
[294] Susana Coroado, "Leviathan vs Goliath or States vs Big Tech and What The Digital Services Act Can Do About It", Working Papers, Forum Transregionale Studien, (2023). 4.

2019 yılı Aralık ayında başlayan COVID-19 salgınıyla birlikte, büyük teknoloji şirketleri yeni nesil devlet dışı aktörler olarak kamu otoriteleriyle iş birliği arayışına girmiştir. Bu süreçte teknik destek sunarak, kamu hizmetleri ve kamu ürünleri sağlayarak hükümet sistemlerinin işleyişini doğrudan etkilemeye başlamışlardır. Bu gelişmeler, büyük teknoloji şirketlerinin mevcut devlet yapılarından bağımsız şekilde küresel bir aktör olarak hızla yükselmesine zemin hazırlamıştır.[295]

Modern devlet hala güç dengesinin merkezinde bulunmaktadır, [296] ancak büyük teknoloji şirketleri gibi süper güçlere sahip olanlar sessizce güçlü ve belirsiz sınırlara sahip bir güç dengesi oluşturmuş ve böylece merkezi olmayan, çok merkezli bir yapı ortaya çıkmıştır. [297] Bu şirketlerin etkisi ve itibarı, modern dünyada "oligarşileşme" ile birlikte sürekli olarak artmaktadır.[298] Bu aktörler, ulus devletlerdeki yeteneklerini sergilemenin yanı sıra genellikle uluslararası siyasete de katılmaktadır.

Büyük teknoloji şirketleri, yalnızca teknolojik altyapı ve hizmet üretiminde değil, aynı zamanda kural koyma süreçlerinde de giderek artan bir etki alanına sahip olmaktadır. [299] Bu durumun dikkat çekici örneklerinden biri, 2020 yılında faaliyete geçen Facebook Denetim Kurulu'dur (Oversight Board). Söz konusu kurul, Facebook ve Instagram platformlarında içerik düzenlemeye ilişkin emsal teşkil edebilecek kararlar alan, yarı-yargısal ve bağımsız bir mekanizma olarak tasarlanmıştır.

Kurul, Facebook'un en tartışmalı kararlarını dahi geçersiz kılma yetkisine sahiptir. Kararları bağlayıcı nitelikte olup, Facebook CEO'su da dahil olmak üzere şirket içinden herhangi bir müdahaleye kapalı olduğu belirtilmektedir. Bu yönüyle, üyeleri ABD Başkanı tarafından atanan ve ülkenin en yüksek yargı organı olan ABD Federal Yüksek Mahkemesi ile yapısal bazı benzerlikler taşımaktadır.

Çalışmamız açısından özellikle kayda değer bir örnek, Kurul'un 5 Mayıs 2021 tarihinde aldığı karardır. Bu karar, dönemin ABD Başkanı Donald Trump'ın 6 Ocak 2021'de ABD Kongre Binası'nda gerçekleşen şiddet olaylarını övücü nitelikteki paylaşımları nedeniyle Facebook ve Instagram hesaplarının askıya alınmasına ilişkindir.

---

[295] Susana Coroado, "Leviathan vs Goliath or States vs Big Tech and what the digital services act can do about it", Working Papers, Forum Transregionale Studien, (2023). 4.

[296] Susana Coroado, "Leviathan vs Goliath or States vs Big Tech and What The Digital Services Act Can Do About It", Working Papers, Forum Transregionale Studien, (2023). 4.

[297] Li Yan, "The Role and Impact of Nonstate Actors from the Perspective of the Russia—Ukraine Crisis", *China Institutes Of Contemporary International Relations* 32/4 (Temmuz-Ağustos 2022), 65.

[298] Christian Fuchs, "The Digital Labour Theory of Value and Karl Marx in the Age of Facebook, YouTube, Twitter, and Weibo", *Reconsidering Value and Labour in the Digital Age*.

[299] Dal Yong Jin, "The Construction of Platform Imperialism in the Globalization Era", Journal for a Global Sustainable Information Society 11/1 (2013).

Trump'ın hesaplarının kapatılması, teknoloji şirketlerinin merkezlerinin bulunduğu ülkenin en üst siyasi makamlarını dahi kendi dijital ortamlarından uzaklaştırabilecek güçte olduklarını göstermesi bakımından dikkat çekicidir. Böylece, geleneksel olarak mahkemelerin yürüttüğü; ifade özgürlüğü ile diğer hak ve özgürlükler arasındaki çatışmayı dengeleme işlevi, artık şirketler tarafından yerine getirilmeye başlanmıştır.[300]

Sosyal medya platformları aracılığıyla devletler arasında gerçekleşen enformasyon savaşları, Arap Baharı gibi olaylar veya dönemin ABD Başkanı Donald Trump'ın X sosyal medya platformu üzerinden Kuzey Kore'yi nükleer savaşla tehdit etmesi gibi durumlar, büyük teknoloji şirketlerinin rolüyle gerçekleşmektedir. Görüldüğü üzere bu şirketler siber uzayda yeni çatışma alanları oluşturarak faaliyet göstermektedirler.[301]

Büyük teknoloji şirketlerinin, yeni devlet dışı aktörler olarak çatışmalarda üstlendikleri roller farklılık gösterebilmektedir. Bazı durumlarda, bu şirketlerin çatışmalardaki rolleri neredeyse görünmez bir nitelik taşırken; bazı durumlarda ise doğrudan çatışmanın nesnesi hâline gelebilmektedirler. Örneğin, Huawei'nin 5G teknolojisine yönelik kısıtlamalar ya da Çin merkezli *ByteDance* şirketine ait sosyal medya platformu *TikTok*'a getirilen yasaklar, bu şirketlerin uluslararası düzeyde yaşanan çatışmaların doğrudan tarafı hâline geldiğini ortaya koymaktadır.[302]

Büyük teknoloji şirketleri, sağladıkları hizmetler aracılığıyla silahı çatışmalarda ve ayaklanmalarda taraf olabilmektedirler. Örneğin BM, *Facebook/Meta*'yı Myanmar'daki Rohingya soykırımına katkıda bulunduğu iddiasıyla resmi olarak suçlamada bulunmuştur.[303] Meta'nın Etiyopya'da veya İsrail ile Filistin arasında devam eden çatışmalar sırasında, kendi Stratejik Müdahale Ekibi de dahil olmak üzere çok pasif davrandığı veya tam tersi, çatışmanın belirli taraflarına özellikle Filistinlilere karşı acımasızca sansür uyguladığı gözlemlenmiştir. İnsan Hakları İzleme Örgütü, bu durumu belgelemiştir.[304]

Yeni devlet dışı aktörler olarak büyük teknoloji şirketlerinin üçüncü devletlerin teşvikiyle uluslararası çatışmalara taraf olmasının en büyük örneğini Rusya-Ukrayna Savaşı teşkil etmektedir.[305] Ukrayna, sosyal medyayı savaşı kitlesel olarak finanse etmek ve bir bilişim ordusu oluşturmak için

---

[300] Elif Küzeci, *Sayısal Fil: Bilişim Teknolojileri, Devlet ve Hukuk Kesişiminde Bir İnceleme* (İstanbul: İnkılap Yayınevi, 2021), 357-358.
[301] Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order", Foreign Affairs, (Erişim 14 Şubat 2024)
[302] Susana Coroado, "Leviathan vs Goliath or States vs Big Tech and What The Digital Services Act Can Do About İt", Working Papers, Forum Transregionale Studien, (2023). 4.
[303] Ranchordas- De Gregorio- Goanta, "Big Tech War Activism".
[304] Human Rights Watch, *"Video Unavailable" – Social Media Platforms Remove Evidence of War Crimes,* (Erişim 13.02.2024), 25-35.
[305] Henry Farrell - Abraham Newman, "What Happens When Tech Bros Run National Security", Time (Erişim Tarihi 15 Şubat 2024), 1.

kullanmaktadır. [306] Bu bağlamda, eski adı *Twitter* olan *X*'in sahibi Elon Musk'ın savaşın başlangıcında net bir tavır alarak *SpaceX*'e ait *Starlink* uydularını Ukrayna'ya göndermesi Ukrayna'yı desteklediği şeklinde yorumlanmıştır. [307]

Yıllarca platform şirketlerinin casusluk ve çatışmalardan muaf tutulacağı bir "dijital İsviçre" inşa etmeye çalıştıktan sonra, *Microsoft* da gönüllü olarak Ukrayna savaşının dijital cephesinde yer aldı. Başından beri, Rus siber saldırılarını tespit edip bunlara karşı koymak ve önemli bilgileri ABD ve Avrupalı müttefikleriyle paylaşmak için çevrimiçi savaş alanını gözetti. Ukrayna hükümetinin bakanlıklarını buluta taşıyarak, onlara hükümetin kendisi tarafından sağlanamayacak bir seviyede güvenlik sağladı.[308] Ukrayna'ya yardım eden sadece Microsoft değildi. Ulrike Franke ve Jenny Söderström tarafından hazırlanan yeni bir rapora göre[309] *Amazon*, Ukrayna'ya ait verileri özelleştirilmiş bavul büyüklüğündeki "Snowball" sistemlerini kullanarak güvenli bir yere taşıyor ve kritik devlet bilgileri için güvenli depolama sağlıyor.[310]

Rusya-Ukrayna savaşında aktif rol alan yen, devlet dışı aktörlerden bir diğeri de *Google*'dır. *Google*, savaş başladıktan sonra, Ukrayna aleyhine olumsuz içeriklere sansür uygularken, Rusya aleyhine olumsuz içeriklere yer vererek manipülasyon yapmıştır. *Google* ayrıca *YouTube*'daki Rusya lehine olan içerikleri de engellemiştir. [311]

Rusya-Ukrayna Savaşı sürecinde iletişim, tarih boyunca görülmemiş ölçüde geniş bir etki alanı kazanmıştır. Bu bağlamda, Facebook ve Twitter gibi büyük teknoloji şirketleri, sınırlı hesap verebilirliklerine rağmen, savaşın platformlar üzerinden yoğun biçimde yürütülmesine örnek teşkil etmişlerdir.[312] Bu durum, kamu değerlerinin yanı sıra insan haklarının da kısa ve uzun vadede tehlikeye girebileceği anlamına gelmiştir.[313]

Büyük teknoloji şirketlerinin egemen devletleri kontrol etmeye zorlaması bakımından Avustralya hükümeti ile Facebook arasında yaşanan çatışma örnek olarak gösterilebilir. Avustralya hükümeti, Facebook'tan haber içeriği için ödeme yapmasını talep ettiğinde, sosyal

---

[306] Farrell - Abraham Newman, "What Happens When Tech Bros Run National Security", Time (Erişim Tarihi 15 Şubat 2024), 1.
[307] Elon Musk, "Starlink service is now active in Ukraine. More terminals en route", *Twitter,*(27 Şubat 2022, 1:33).
[308] Farrell - Newman, "What Happens When Tech Bros Run National Security".
[309] Ulrike Franke- Jenny Söderström, "Star tech enterprise: Emerging technologies in Russia's war on Ukraine", *European Council on Foreign Relations*, (Erişim Tarihi 15 Şubat 2024).
[310] Russ Mitchell, "How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia", the Seattle Times, (Erişim Tarihi 15 Şubat 2024).
[311] Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order", Foreign Affairs, (Erişim 14 Şubat 2024)
[312] Dal Yong Jin, "Digital Platforms, Imperialism and Political Culture", Routledge New Developments in Communication and Society Research, 1. Baskı.
[313] Sofia Ranchordas-Giovanni De Gregorio-Catalina Goanta, "Big Tech War Activism", *VerfBlog* (Erişim Tarihi 15 Şubat 2023).

medya devi hızla misilleme yaparak Avustralyalı haber kuruluşlarından gelen tüm içeriği sansürledi.[314] Büyük teknoloji şirketlerinin egemen devletleri kontrol altına almaya zorlaması, artık herkesin kabul ettiği basit bir gerçeği ortaya koymuştur: Avustralya ile Facebook arasında yaşanan bu anlaşmazlık, esasen Avustralya gibi egemen bir devlet ile çok uluslu bir teknoloji şirketi arasında, dijital medya platformlarının düzenlenmesine ilişkin bir güç mücadelesidir. Bu bağlamda Facebook, yalnızca büyük bir dijital şirket olmanın ötesine geçmiş; egemen devletlerle pazarlık yapabilecek yetki ve etkiye sahip güçlü bir siyasi aktöre dönüşmüştür.[315]

Büyük teknoloji şirketleri dijital teknoloji ve algoritmalar aracılığıyla artık egemen devletlerin siyasi ekolojisini etkileyebilmektedirler. COVID-19 salgınıyla birlikte insanların günlük yaşamı giderek daha fazla çevrimiçi hale gelirken, büyük teknoloji şirketleri kişisel verileri varlık olarak kullanarak daha büyük bir ekonomik güç elde etmişlerdir. [316] Bu aktörlerin artan etkisi siyasi iletişim üzerindeki kontrollerini daha da güçlendirmiş ve bu durum, bilgi yayma ve siyasi seferberlik üzerindeki baskın etkileri konusunda endişelere yol açmıştır. Bu eğilim, demokratik sistemlerin düzgün işleyişine yönelik önemli bir tehdit oluşturmaktadır.[317]

Bu şirketler, çoğu zaman küçük ölçekli devletlerle rekabet edebilecek düzeyde güç ve kaynağa sahiptir. Teknik alanda faaliyet gösteren büyük teknoloji şirketleri, genellikle iyi organize olmuş yapıları ve yüksek düzeyde eğitimli insan kaynağıyla dikkat çekerler. Siber savaşın yürütülmesinde kullanılabilecek sistemler de dâhil olmak üzere en son teknolojilere ve gelişmiş ekipmanlara erişim imkânına sahiptirler.[318]

[314] Angus Whitley, "Facebook Ends Australia News Blackout After Law Compromise", Bloomberg (Erişim Tarihi 16 Şubat 2024).
[315] Gu, "Data, Big Tech, and the New Concept of Sovereignty".
[316] Gu, "Data, Big Tech, and the New Concept of Sovereignty".
[317] Congjing Ran - Liu Yan, "Dynamic Logic, Mode Selection, and Reconstruction Path of Platform Governance in the Perspective of Data Sovereignty", *Journal of Library Science in China* (16 Şubat 2023), 1–23.
[318] Jason Andress, *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners* (Syngress; İkinci Baskı), 211.

İKİNCİ BÖLÜM

DEVLET DIŞI AKTÖRLERİN ULUSLARARASI SORUMLULUĞU

Mevcut uluslararası hukuk ilkelerine göre, bir devletin devlet dışı aktörlerin fiillerinden dolayı uluslararası hukuk bağlamında sorumlu tutulabilmesi, söz konusu aktörlerin devletin talimatı, yönlendirmesi veya kontrolü altında hareket etmesi ya da devletten kamu gücü kullanma yetkisi almış olmaları durumunda mümkündür. Bu çerçevede, bir devletin siber faaliyetler yürüten bir firmayı sözleşmeye dayalı olarak istihdam etmesi veya bir bilgisayar korsanı grubuna siber saldırı gerçekleştirmesi yönünde doğrudan talimat vermesi halinde, bu saldırılar uluslararası hukuku ihlal ediyorsa, ilgili devlet, verilen talimatların kapsamı aşılmış olsa dahi sorumlu tutulabilir.

Bir devletin uluslararası sorumluluğu yalnızca bireylerin fiillerinin söz konusu devlete atfedilebilmesi durumunda gündeme gelir. Bu bağlamda, bir devletin kendi topraklarında veya yargı yetkisi dâhilinde faaliyet gösteren kişi ve kuruluşların eylemlerinden doğrudan sorumlu tutulması mümkün değildir. Benzer şekilde, faillerin söz konusu devlete mensup olmaları, bir şirketin o devlet sınırları içinde kurulmuş olması veya hatta devlete ait olması, bu eylemlerin devlete atfedilebilmesi bakımından tek başına yeterli bir dayanak teşkil etmez. Bu durum, siber saldırılar özelinde uluslararası hukuka özgü ciddi bir meydan okuma oluşturmaktadır.

Siber uzay bağlamında karşılaşılan en temel sorunlardan biri, saldırı faillerinin kimliğini kesin olarak tespit edebilmek ve bu faillerin eylemlerinin bir devlete ya da diğer uluslararası hukuk süjelerine atfedilip atfedilemeyeceğini belirleyebilmektir. Aşağıda, bu zorlukları aşmak amacıyla uluslararası sorumluluğa ilişkin hükümler ayrıntılı bir şekilde ele alınmaktadır. İncelemede yalnızca 2001 tarihli *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Dolayı Sorumluluğuna İlişkin Taslak Maddeler* ile yetinilmemiş; konuya dair doktrinsel yaklaşımlar ve uluslararası yargı kararları da değerlendirilmiştir. Böylece, siber uzayda faaliyet gösteren yeni devlet dışı aktörlerin sorumluluğunun nasıl tesis edilebileceğine dair sağlam bir hukuki temel oluşturulmuştur.

1.ULUSLARARASI SORUMLULUK HUKUKUNUN TEMELLERİ

Kişinin kendi fiillerine göre hareket etmesi ve bunun sonuçlarını üstlenmesi "sorumluluk" olarak ifade edilebilir. Sorumluluk hukuku, temelini ahlaki değerlerden almaktadır. Pozitif hukuk anlayışının gelişmesiyle birlikte, hukuk düzeni toplum üyeleri arasında adaleti sağlama ve bozulan çıkar dengesini yeniden kurma amacını taşıyan sorumluluk anlayışını pozitif hukuka taşımış; böylece ahlaki olanı normatif olana dönüştürmüştür.[319]

Bir hukuk düzeninde sorumluluk, o hukuk düzeninin "kişi" olarak kabul ettiği varlıklar bakımından geçerlidir. Bu varlıkların, ilgili hukuk düzenince belirlenen yükümlülüklere aykırı hareket etmeleri sorumluluklarını doğurur. Uluslararası hukukun kişileri —başka bir ifadeyle, üyesi— olan devletler, uluslararası örgütler, gerçek kişiler ve şirketler bakımından da, içinde bulundukları hukuk düzeni tarafından belirlenen kurallara aykırı hareket edilmesi uluslararası sorumluluğun doğmasına yol açar. Daha açık bir ifadeyle, uluslararası hukuk düzenince öngörülen yükümlülüklere aykırı davranan uluslararası hukuk kişilerine karşı sorumluluk ileri sürülebilir.

Uluslararası hukuk kişileri, hukuka aykırı fiilleriyle diğer hukuk kişilerine zarar verdiklerinde; zarar veren ile zarar gören arasında, uluslararası hukukun kendisine sonuç bağladığı bir hukuki ilişki doğar. Bu hukuki ilişki, devletin uluslararası sorumluluğu olarak ifade edilebilir.[320]

1.1.Sorumluluk Hukuku Kavramı

Devletin uluslararası sorumluluk hukukunun kökeninin önemli bir kısmı, özel hukuk kişilerinin fiilleri ile yakından ilişkilidir. Özel hukuk kişileri konumundaki yabancılara verilen zararlar, devletin uluslararası sorumluluk hukukunun oluşmasındaki ilk adımlardan birini teşkil etmiştir. Uluslararası hukukta sorumluluk konusunu inceleyen ilk yazarlar, öncelikle devletlerin yabancılara yönelik haksız fiillerinden doğan sorumluluklarını belirlemeye çalışmışlardır. Devletin uluslararası sorumluluğuna ilişkin temel kurallar ise, birkaç yüzyıl boyunca devam eden hakem kararları, kodifikasyon çalışmaları ve akademik projeler sonucunda şekillenmiştir.[321]

---

[319] Enver Bozkurt-Yasin Poyraz- Selcen Erdal, *Devletler Hukuku* (Ankara: Yetkin Yayınları, 11.Bası, 2021), 273.
[320] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 273-274.
[321] Tal Becker, *Terrorism and the State Rethinking the Rules of State Responsibility*, (Kuzey Amerika: Hart Publishing), 11.

"Sorumluluk" ve "yükümlülük" kavramları çoğu zaman birbirilerinin yerine geçerek kullanılmaktadır. Ancak "sorumluluk" kavramı uluslararası hukuk bakımından daha kesin bir anlam ifade etmektedir. Devlet hukuka aykırı bir fiil ya da ihmalden dolayı "sorumlu" tutulduğunda, yükümlülüklerinin ihlalinden doğan hukuki sonuçları üstlenir. Devlet, bu koşullar altında hukuken izin verilen her türlü iyileştirici/telafi edici eylem için uygun adres haline gelir.[322]

Yukarıda aktarılanlardan da anlaşılacağı üzere, uluslararası sorumluluğa ilişkin kurallar başlangıçta örf ve âdet hukuku ile uluslararası yargı organlarının kararları doğrultusunda şekillenmiş; BM tarafından yürütülen kodifikasyon çalışmaları ise devletin uluslararası sorumluluğuna ilişkin kuralların gelişimine önemli katkılar sağlamıştır.

Uluslararası sorumluluğa ilişkin kurallar, geçmişte uluslararası toplumun ihtiyaçlarını karşılamak bakımından yetersiz kalmış ve bu durum, ortak kabul gören ilkeler üzerinde bir uzlaşı sağlanamamasına yol açmıştır. Sorumluluğa ilişkin kuralların gelişmemesinin bir diğer nedeni ise devletlerin farklı egemenlik anlayışlarına sahip olmalarıdır. Başlangıçta, egemen yetkilerle donatılmış devletler, içinde bulundukları toplum hayatını düzenleyen bir kurallaşmayı kabul etmemişlerdir. O dönemdeki hâkim anlayışa göre, devletin üzerinde bir otorite bulunmadığından, devletin uymakla yükümlü olduğu bir kurallar bütünü de mevcut değildir.[323]

19. yüzyılın sonlarına doğru ortaya çıkan anlayışa göre, egemenlik sorumluluğun inkârı değil, aksine onun temel dayanağı olarak görülmüştür. Uluslararası toplumun diğer üyeleriyle birlikte yaşamanın zorunlu kıldığı kurallar gereğince, devletler egemenlik yetkilerini kullanırken bu kuralları göz ardı edemezler. Daha açık bir ifadeyle, sorumluluk ile egemenlik bir bütünün iki tamamlayıcı unsuru olarak değerlendirilmelidir.[324]

Devletin uluslararası sorumluluk hukukunun gelişimindeki bir diğer önemli etken, sınır aşan etkiler doğuran faaliyetlerin ortaya çıkardığı ihtiyaçtır. Bu bağlamda, bir devletin kendi ülkesindeki faaliyetler nedeniyle başka bir devletin ülkesinde ortaya çıkan zararın önlenmesine veya giderilmesine ilişkin ilk kurallar, "iyi komşuluk" ilkesine dayanmaktadır.[325]

Devletlerin ve devlet dışı aktörlerin, devletin uluslararası sorumluluğunun sınırlarına ilişkin kaygılarını değerlendirme sorumluluğu, 34 bağımsız uzmandan oluşan daimi bir organ olan Birleşmiş Milletler Uluslararası Hukuk Komisyonu (UHK) tarafından yürütülen sistematik

---

[322] Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, (London: Cambridge,1953), 163.
[323] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 273-274.
[324] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 274-275.
[325] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 275.

çalışmalar sonucunda gündeme gelmiştir. 1949 yılında UHK, yabancılara ve onların mallarına verilen zararlardan dolayı devletlerin sorumluluklarını düzenlemeye yönelik bir antlaşma taslağı hazırlamak amacıyla bir proje üzerinde çalışma başlatmaya karar vermiştir.

Devletler uzun bir süre, bir devletin kendi topraklarında seyahat eden veya iş kuran başka bir devletin vatandaşına zarar vermesi durumunda, bu zarar eyleminin haksız fiil teşkil ettiği görüşünü benimsemişlerdir. Bu tür fiiller, devletler arasında birçok ihtilafa ve tahkim yargılamasına konu olmuştur. Bu nedenle, UHK ve Birleşmiş Milletler'e üye devletler, ev sahibi devletin yükümlülüklerinin açık bir şekilde belirlenmesinin gelecekteki ihtilafları önleyebileceğine inanmışlardır. Ancak 1960'ların başlarına gelindiğinde, UHK üyeleri arasında bu yükümlülüklerin niteliğine dair önemli anlaşmazlıklar ortaya çıkmıştır.[326] 1949 yılından bu yana, UHK'nin önde gelen akademisyenlerinden sonra gelen kuşaklar da bu proje üzerinde çalışmış ve uluslararası hukuk yükümlülüklerin ihlalinden dolayı devletin uluslararası sorumluluğunu düzenlemek üzere bir dizi taslak madde formüle etmeye çalışmışlardır.

Tüm bu anlaşmazlıklara rağmen, UHK tavsiyesine uygun olarak 2001 yılında BM Genel Kurulu, *"Uluslararası Haksız Fiillerden Dolayı Devletin Uluslararası Sorumluluğu"*na ilişkin 56/83 sayılı kararı kabul etmiştir. Komisyon tarafından hazırlanıp Genel Kurul tarafından onaylanan bu Taslak Maddeler, devletin sorumluluğuna ilişkin kuralların kodifikasyonu yönündeki bugüne kadarki en önemli çabayı temsil etmektedir.[327]

2001 tarihli Taslak Maddeler, bağlayıcı bir uluslararası hukuk kaynağı olmasa da, devletin uluslararası sorumluluğuna ilişkin ilkeler ve uygulamalar bağlamında en kapsamlı ve ayrıntılı bilimsel çalışmayı temsil etmektedir. Taslak Maddeler hazırlanırken devletlerle istişarelerde bulunulmuş ve önde gelen akademisyenlerin on yıllar boyunca katkıları alınmıştır. Bu nedenle Taslak Maddeler, devletin uluslararası sorumluluğuna ilişkin geniş bir mutabakatı yansıtmakta ve otorite sahibi bir kaynak olarak kabul edilmektedir.[328]

Devletin uluslararası sorumluluğu açısından vurgulanması gereken en önemli hususlardan biri, 2001 tarihli Taslak Maddeler'in devletlerin yükümlülüklerini değil, sorumluluklarını düzenlemesidir. Daha açık bir ifadeyle, ihlali uluslararası sorumluluğun doğmasına yol açan kuralın içeriği değil; hukuka aykırı eylem ve ihmallerden dolayı devletin

---

[326] Ian Brownlie, "The Responsibility of States for the Acts of International Organizations", *International Responsibility Today Essays in Memory of Oscar Schachter*, ed. Maurizio Ragazzi (Leiden / Boston: Martinus Nijhoff Publishers- 2005), 90.

[327] International Law Commission, Report of the International Law Commission on the Work of its Fifty-Third Session, 23 April - 1 June and 2 July - 10 August 2001, Official Records of the General Assembly, Fifty-Sixth Session, Supplement No.10, vol. II(2), 2001.

[328] Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford: Oxford University Press, 1995), 146–48.

sorumluluğunu doğuran kurallar Taslak Maddeler tarafından belirlenmiştir. Bu nedenle, birincil değil ikincil kurallar Taslak Maddeler'in kapsamına girmektedir. [329] Örneğin, bir devletin başka bir devletin hava sahasını ihlal etmesi birincil kuralların konusuna girerken, bu ihlal sonucunda sorumluluğun doğma biçimi ikincil kuralların ilgi alanına girmektedir.

Gelişen normlar kümesi tanımlanıp kökenleri analiz edilerek, bu normların devlet dışı aktörlerin fiilleri bağlamında devletin uluslararası sorumluluğuna uygulanmasının makul olup olmadığı eleştirel bir bakış açısıyla değerlendirilebilir.

1.2.Uluslararası Sorumluluğun Şartları

Uluslararası sorumluluğun şartları, diğer bir ifadeyle uluslararası hukuka aykırı fiilin unsurları, Taslak Maddeler'in 2. maddesinde düzenlenmiştir. Buna göre: "Şayet icrai veya ihmal yoluyla işlenen bir davranış, a) uluslararası hukuka göre devlete isnat edilebiliyorsa ve b) devletin bir uluslararası yükümlülüğünün ihlalini oluşturuyorsa, devletin uluslararası haksız fiili vardır."[330] Pazarcı, uluslararası sorumluluğun doğması için dört temel koşulun varlığını aramaktadır: Uluslararası hukuka aykırı bir fiilin veya sonuçlarına uluslararası sorumluluk atfedilen, özde uluslararası hukuka uygun bir faaliyetin bulunması; bu fiil veya faaliyetin bir zarara yol açması; söz konusu fiil veya faaliyetin bir uluslararası hukuk kişisine bağlanması, yani onun fiili veya faaliyeti olarak değerlendirilmesi; ve bu fiil veya faaliyete ilişkin olarak uluslararası sorumluluğu ortadan kaldıran veya etkilerini silen herhangi bir nedenin bulunmaması.[331]

Klasik uluslararası hukuk öğretisinde, uluslararası sorumluluğun şartları arasında kusurlu sorumluluk ile kusursuz (objektif) sorumluluk ayrımı nedeniyle farklı değerlendirmeler yapılmaktadır. Ancak burada biz bu ayrımı dikkate almadan üç temel şart üzerinde duracağız: uluslararası hukuka aykırı bir fiil, zarar ve illiyet (nedensellik bağı).

---

[329] Yücel Acer-İbrahim Kaya, *Uluslararası Hukuk: Temel Ders Kitabı İngilizce Özetli* (Ankara: Seçkin Yayınevi, 10.Bası), 405-406.

[330] Kenan Dülger, *Devletin Uluslararası İnsancıl Hukukun İhlalinden Doğan Sorumluluğu* (İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, 2014) 50.

[331] Hüseyin Pazarcı, *Uluslararası Hukuk,* (Ankara: Turhan Kitabevi, 18.Bası), 441.

1.2.1. Uluslararası Hukuka Aykırı Bir Fiil

Devletin sorumluluğunu doğuran olay, devlete atfedilebilen, uluslararası hukuka aykırı bir fiilin varlığıdır.[332] Taslak Maddelerin 1. maddesine göre, "bir devlet uluslararası hukuka aykırı her fiili, o devletin uluslararası sorumluluğunu doğurur." Bu maddeden ve yukarıda verilen 2. maddeden anlaşılacağı üzere uluslararası toplum düzenine aykırı olan, bu düzenin kurallarıyla çatışan her davranış uluslararası hukuka aykırı fiil ya da haksız fiil olarak adlandırılabilir.[333] İkinci maddede aranan uluslararası haksız fiilden kasıt, uluslararası hukuka göre, yapılması gereken şeyin yapılmaması, yapılmaması gereken şeyin yapılması şeklinde ifade edilebilir.[334]

Devletin uluslararası sorumluluğunu doğuran haksız fiil koşulu, söz konusu fiilin uluslararası hukuka aykırı olmasıdır. Bu bağlamda, bir fiilin iç hukuka aykırı olması, tek başına uluslararası hukuk bakımından sorumluluk doğurması için yeterli değildir. Başka bir deyişle, iç hukuka aykırı bir fiilin uluslararası hukuka da aykırı kabul edilmesi gerekmez. Benzer şekilde, bir fiilin iç hukuk bakımından meşru olması, onun uluslararası hukuk açısından uygun olduğu sonucunu doğurmamaktadır. Bu nedenle, bir fiilin uluslararası sorumluluk doğurabilmesi için yalnızca uluslararası hukuka aykırı olması yeterlidir. Ayrıca, sorumluluk için yalnızca hukuki bir yükümlülüğün ihlali aranır; uluslararası ahlaka veya uluslararası nezaket kurallarına aykırı fiiller uluslararası sorumluluk oluşturmaz.[335]

Uluslararası hukukun asli kaynaklarını oluşturan uluslararası antlaşmalar, uluslararası örf ve âdet kuralları ile hukuk genel ilkeleri, sorumluluk hukuku bakımından da eşit değere sahiptir. Başka bir ifadeyle, ihlal edilen uluslararası hukuk kuralının bir antlaşma, örf ve âdet kuralı veya hukuk genel ilkesi olması, uluslararası sorumluluk hukukunun uygulanmasında herhangi bir farklılık doğurmamaktadır.[336]

Uluslararası hukukun asli kaynaklarından biri olan antlaşmalar bakımından, devletin sorumluluğunu belirlemek daha kolaydır. Çünkü antlaşmalar yazılı metinler olarak devletlerin yükümlülüklerini çoğu zaman açık bir şekilde düzenlemekte ve bu yükümlülüklere aykırı hareket eden tarafları da belirlemektedir. Buna karşılık, uluslararası teamül kurallarının öngördüğü yükümlülüklerin ve bunları ihlal eden fiillerin tespiti, antlaşmalar çerçevesinde

---

[332] Elif Uzun, *Devletin Milletlerarası Hukuka Aykırı Eyleminden Sorumluluğu,* (Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, 2007), 38.
[333] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 276.
[334] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 276.
[335] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 276-277.
[336] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 278.

yapılan tespitlere kıyasla daha zordur. Benzer zorluk, uluslararası hukukun bir diğer asli kaynağı olan hukuk genel ilkeleri açısından da geçerlidir.[337]

1.2.2. Haksız Fiilin Görünüm Biçimleri

Hukuka aykırı veya haksız fiiller, uluslararası hukukta farklı biçimlerde ortaya çıkabilir. Klasik uluslararası hukuk yaklaşımı, haksız fiilleri, fiili oluşturan unsurlar veya meydana gelen zararın hukuki sonuçlarının özelliklerine göre sınıflandırmaktadır. [338] Uluslararası hukukta sorumluluğun bir koşulu olarak haksız fiil, iki temel unsurdan oluşur: aktif bir fiil veya ihmali bir fiil.

Buna göre, haksız fiil, uluslararası hukukun yasakladığı bir fiilin gerçekleştirilmesi veya uluslararası hukukun emrettiği bir davranıştan kaçınılması ile meydana gelir. Başka bir ifadeyle, haksız fiil, aktif bir fiile dayanabileceği gibi, pasif bir davranışla, yani ihmal yoluyla da işlenebilir. Örneğin, Korfu Kanalı Davası'nda Uluslararası Adalet Divanı (UAD), Arnavutluk'un mayınlama faaliyetini gerçekleştirme imkânının teknik olarak bulunmaması nedeniyle bu faaliyetin Arnavutluk'a doğrudan atfedilemeyeceğini; ancak mayınlama faaliyetini bildirmemesi yoluyla ortaya çıkan ihmal nedeniyle sorumlu tutulacağını kararlaştırmıştır.[339]

Mevcut uluslararası hukuk çerçevesinde, bu iki seçim sürecinde gerçekleştirilen siber saldırılar, tek başlarına hukuka aykırı bir müdahale teşkil etmemiş; yalnızca egemenlik ilkesinin ihlali anlamına gelebilecek nitelikte değerlendirilmiştir. Bununla birlikte, bu siber saldırılar kapsamında yer alan etki operasyonları, müdahale yasağı ilkesinin ihlali olarak değerlendirilebilecek durumlar ortaya koymaktadır. Temel mesele, bu operasyonların yalnızca hazırlık aşamasına yönelik fiiller mi yoksa bileşik bir fiilin ayrılmaz bir parçası mı olduğunun belirlenmesidir. Bu bağlamda, aşağıda öncelikle hazırlık eylemleri ile bileşik bir eylemin parçası olan eylemler arasındaki ayrım ele alınmakta ve ardından uluslararası hukuk çerçevesinde bu iki vaka analiz edilmektedir.

[337] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 278.
[338] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 277.
[339] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 277.

1.2.3. Bileşik Eylemle Meydana Gelen İhlal

Uluslararası hukuka aykırı haksız fiil, iki unsurun bir araya gelmesiyle oluşur: devlete atfedilebilir olması ve uluslararası bir yükümlülüğün ihlalini teşkil eden, icrai veya ihmali surette işlenen bir davranış olması.[340] Bununla birlikte, uluslararası haksız fiillerin üç farklı biçimde ortaya çıkabileceği ve bu biçimlerin birbirinden ayrılması önemlidir: tamamlanmış veya anlık fiiller, devam eden fiiller ve bileşik fiiller.

Ani veya tamamlanmış bir uluslararası haksız fiil söz konusu olduğunda, ihlal fiilin gerçekleştiği anda meydana gelir. Bu durumda, fiilin uluslararası haksız fiil olarak nitelendirilebilmesi bakımından ihlalin etkilerinin devam edip etmediği önem arz etmez.[341] Buna karşılık, devam eden bir uluslararası hukuka aykırı fiilde ihlal, fiilin sürdüğü ve uluslararası yükümlülükle uyumsuzluk teşkil ettiği süre boyunca devam eder.[342]

Bileşik fiiller, uluslararası haksız fiilin birden fazla eylem veya ihmali kapsadığı durumları ifade eder. Her bir eylem veya ihmal tek başına uluslararası hukuka aykırılık oluşturmasa da, bu eylem veya ihmallerin birikimiyle ortaya çıkan bileşik fiil uluslararası hukuka aykırılık teşkil edebilir. Bu durum, "Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu" başlıklı Taslak Maddeler'in 15. maddesinde şu şekilde ifade edilmiştir:

"Bütünde haksız olarak tanımlanan bir dizi icrai veya ihmali suretteki davranış nedeniyle bir uluslararası yükümlülüğün ihlali, diğer icrai veya ihmali suretteki davranışlarla bileşik olan ve haksız fiili oluşturmaya yeterli davranışın gerçekleştiği anda meydana gelmiştir."

Böylesi durumlarda ihlal, söz konusu eylem veya ihmaller zincirinin ilk icrai veya ihmali suretteki davranışıyla başlayan tüm süreye yayılır ve bu davranışlar tekrar edildiği ve ilgili uluslararası yükümlülüğe aykırılık devam ettiği sürece sürer.[343]

Bileşik fiil kavramı, uluslararası hukuk bağlamında bir ihlal teşkil etmesi açısından, özellikle siber saldırılar söz konusu olduğunda büyük önem taşımaktadır. Çoğu durumda, siber

---

[340] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğa İlişkin Maddeler*, Madde 2, *Materials on the Responsibility of States for Internationally Wrongful Acts*, 2. baskı, New York: Birleşmiş Milletler Yayınları, 2023.

[341] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğa İlişkin Maddeler*, Article 14(1).

[342] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğa İlişkin Maddeler*, Article 14/2.

[343] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğa İlişkin Maddeler*, Article 15.

saldırılar yalnızca siber uzayla sınırlı kalmayıp daha geniş bir operasyonun parçası olarak yürütülebilir. Bununla birlikte, birçok durumda bazı siber saldırılar, daha geniş operasyonla ilişkili olmalarına rağmen, bileşik bir fiilin unsuru değil, yalnızca hazırlık niteliğinde davranışlar olarak değerlendirilebilir.

Hazırlık fiilleri ile bileşik bir fiilin parçası olan davranışlar arasındaki ayrım, Uluslararası Adalet Divanı (UAD) tarafından *Gabčíkovo–Nagymaros Projesi* davasında ele alınmıştır: "Haksız bir fiil veya suçtan önce sıklıkla, fiil veya suçun kendisiyle karıştırılmaması gereken hazırlık eylemleri gerçekleştirilir. İster anlık ister sürekli olsun, haksız bir davranışın fiilen işlenmesi ile bu davranıştan önceki hazırlık niteliğindeki ve haksız fiil olarak nitelendirilemeyecek davranışlar arasında ayrım yapmak mümkündür."[344]

Dolayısıyla, Divan'a göre hukuka aykırı fiil ile hazırlık eylemleri arasındaki ayrım, söz konusu eylemlerin "alınacak nihai kararı önceden belirlememesi" esasına dayanmaktadır. Bu nedenle, bir eylemin hazırlık niteliğinde mi yoksa hukuka aykırı fiilin gerçek bir parçası mı olduğuna ilişkin ayrım, her somut olay özelinde değerlendirilmelidir.

Siber uzay bağlamında değerlendirecek olursak, siber saldırıların diğer siber saldırılarla ve hatta farklı nitelikteki operasyonlarla birlikte gerçekleştirilmesi oldukça yaygındır. Bu bağlamda, 6 Eylül 2007'de İsrail tarafından Suriye'deki şüpheli bir nükleer reaktöre yönelik gerçekleştirilen hava saldırısı olan *Orchard Operasyonu* iyi bir örnek teşkil etmektedir. Bu hava saldırısından önce, Suriye radar sistemlerini etkisiz hâle getirmeye yönelik siber saldırılar da dâhil olmak üzere bir dizi eylem icra edilmiştir.[345] İsrail'in gerçekleştirdiği hava saldırısı ise Suriye'ye karşı silahlı bir saldırı niteliği taşımaktadır.

Bu noktada sorulması gereken soru, Suriye radar sistemlerini hedef alan siber saldırıların, bileşik bir silahlı saldırının parçası mı yoksa hazırlık niteliğinde bir eylem mi olduğudur. Suriye radar sistemlerinin etkisiz hâle getirilmesi, askeri bir eylemin hazırlık aşamalarını oluşturabilir; ancak İsrail, bu noktada eylemini sonlandırmaya karar verebilirdi. Böyle bir durumda, radarların etkisiz hâle getirilmesi, Suriye'nin egemenliğinin ihlali ve Suriye'ye karşı bir kuvvet tehdidi olarak değerlendirilebilirdi; fakat bu durum tek başına bir silahlı saldırı teşkil etmezdi. Dolayısıyla, siber saldırılar yoluyla radar sistemlerinin etkisiz hâle getirilmesi, hava saldırısının gerçekleştirilmesine yönelik nihai kararı önceden belirlemediği için, bileşik hukuka aykırı fiilin bir parçası değil, yalnızca hazırlık niteliğinde bir eylem olarak değerlendirilmelidir.

---

[344] International Court of Justice (ICJ), Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment (1997), *ICJ Reports*, 7, 54.
[345] Delerue, *Cyber Operastions and International Law,* 244.

Benzer şekilde, Stuxnet saldırısında, santrifüjlere zarar vermeyi amaçlayan kötü amaçlı yazılımdan önce, İran nükleer programının işleyişine dair gerekli bilgileri toplamak amacıyla gerçekleştirilen başka siber saldırılar yapılmıştır.[346] Bu önceki siber saldırılar, hazırlık niteliğinde eylemler olarak değerlendirilmektedir; santrifüjlere fiziksel zarar verilmesi ise, bu eylemleri bileşik bir hukuka aykırı fiilin parçası hâline getirmektedir.

1.2.4. Kusur Sorumluluğu ve Objektif Sorumluluk

Klasik uluslararası hukuka ve uluslararası uygulamaya göre, bir devletin uluslararası sorumluluğunun doğabilmesi için uluslararası hukuka aykırı fiilin kast veya ihmal sonucunda gerçekleşmesi gerekmektedir.[347] Bununla birlikte, bir devletin uluslararası hukuka göre sorumlu tutulabilmesi için kusurun varlığına ihtiyaç olup olmadığı, yani uluslararası yükümlülüklerin sübjektif bir kusur sonucu ihlal edilip edilemeyeceği uzun süre tartışılmıştır.[348] Bu bağlamda iki görüş ileri sürülmüştür. İlk görüşe göre, devletin uluslararası sorumluluğunun doğabilmesi için kusurunun bulunması şarttır. Daha açık bir ifadeyle, bir devletin uluslararası sorumluluğu, uluslararası hukuka aykırı fiilinin bir kusur sonucu işlenmiş olmasına bağlıdır; tesadüfen ortaya çıkan zarar, devletin sorumluluğunu oluşturmaz. Dolayısıyla bu görüşe göre sorumluluk için kusur şarttır ve uluslararası sorumluluğun doğabilmesi için davalı devletin bir kusur işlemiş olması gerekmektedir. Devletlerin sorumluluğunu oluşturan kusur ise, yükümlülüklerini yerine getirmemek veya gerekli özeni göstermemek durumlarında ortaya çıkar.[349]

Kusur teorisi kabul edilirse, devletin sorumluluğunu gerektiren kusurun kime atfedileceğini tespit etmek zor olabilir. Kusur, haksız fiili işleyen, zararı meydana getiren organa mı atfedilecektir? Organın fiili uluslararası hukuka aykırı fakat iç hukuka uygun olabilir.[350] Bununla birlikte yapmakla yükümlü olduğu şeyi yapmış olan organ/ferdin kusurundan bahsetmek mümkün değildir. Bu durumda, bir organ veya bireyin iç hukuk açısından kusurlu bulunmasına rağmen, uluslararası hukuk çerçevesinde kusurlu olduğu söylenemez. Çünkü bu organ veya bireyin uluslararası hukuka aykırı davrandığını bilmesi ya da bilmesi gerektiği iddia edilemez. Diğer tüm hususlardan bağımsız olarak, bu anlamda kabul

[346] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 227-247.
[347] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 279.
[348] Dülger, *Devletin Uluslararası İnsancıl Hukukun İhlalinden Doğan* Sorumluluğu, 71-72.
[349] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 279.
[350] Seha L. Meray, *Devletler Hukukuna Giriş* (Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1. Bası, 1959), 476.

edilen kusur, eylemin nedeni olarak değerlendirilemez ve dolayısıyla isnat edilebilirlik açısından hiçbir önemi yoktur. Kamu görevlisinin yetkisi dışında gerçekleştirdiği eylemlerden dolayı devletin sorumluluğuna gelince, günümüzde neredeyse tamamen terk edilmiş olan özel hukuk kavramları olan 'intihapta kusur' (*seçimde kusur, culpa in eligendo*) — yani devletin memurlarını iyi seçmemiş olması nedeniyle sorumlu tutulması — ve 'nezarette kusur' (*gözetimde kusur, culpa in custodiendo*) — yani devletin kendi organları üzerinde gerekli denetimi yapmamış olması nedeniyle sorumlu tutulması — devletin yapısı ve uluslararası ilişkilerin doğasıyla pek uyumlu değildir. Sonuç olarak varılması gereken nokta şudur ki, uluslararası hukukta organ ya da bireyin manevi durumu genellikle sorumluluğun sebep ve koşulunu oluşturmaz; bu sorun yalnızca devletin uluslararası bir yükümlülüğünü ihlal etmesinden kaynaklanır.[351]

Bu görüşe karşı çıkan bazı yazarlar, devletin uluslararası sorumluluğunu subjektif bir kavram olan kusura değil, uluslararası hukuka aykırı bir haksız fiilin varlığına dayandırmakta ve böylece objektif sorumluluk anlayışını savunmaktadır. Bu yaklaşıma göre, devlete atfedilebilen hukuka aykırı bir fiilin varlığı, devletin sorumluluğunu doğurmak için yeterlidir. Günümüzde uluslararası hukuk uygulaması, devletin objektif sorumluluğunu savunan görüşleri destekler niteliktedir. Bu yaklaşımın yansıtıldığı *Caire Davası*'nda, hakemlik mahkemesi, devlet adına hareket eden görevlilerin fiilleri sebebiyle devletin, herhangi bir kusurlu davranışı olmasa dahi sorumlu tutulacağına karar vermiştir.[352] *Caire Davası* dışında, uluslararası hukukta objektif sorumluluk ilkesinin açıkça kabul edildiği bazı temel alanlar bulunmaktadır. Bunlar arasında nükleer enerjinin barışçıl kullanımı, denizlerin hidrokarbürlerle kirlenmesi ve uzay araçlarının neden olduğu zararlar yer almaktadır. Bu alanlar, uluslararası sorumluluk hukukunun objektif sorumluluk temelinde şekillendiği ve devletlerin kusur aranmaksızın sorumlu tutulduğu önemli örnekler olarak öne çıkmaktadır.[353] 29 Temmuz 1960 tarihli *Nükleer Enerji Alanında Üçüncü Şahıslara Karşı Hukuki Sorumluluğa İlişkin Paris Sözleşmesi* ile 15 Mayıs 1963 tarihli *Nükleer Madde Taşıyan Gemilerle İlgili Hukuki Sorumluluğa İlişkin Brüksel Sözleşmesi*, devletlerin objektif sorumluluğunu düzenleyen temel uluslararası anlaşmalardır. Buna paralel olarak, 29 Kasım 1969 tarihli *Denizlerin Hidrokarbürlerden Kirlenmesi Konusunda Hukuki Sorumluluk Sözleşmesi* de objektif sorumluluk ilkesini esas alarak, gemi sahipleri veya kiracıların denizlerde hidrokarbür kaynaklı kirlilikten doğan zararlardan kusur

[351] Meray, *Devletler Hukukuna,* 476-477.
[352] Caire Davası (Fransa v. Meksika), Arbitral Award, 13 Haziran 1929, Reports of International Arbitral Awards, Cilt V, 540 (5 RIAA 516).
[353] Pazarcı, Uluslararası Hukuk, 445.

aranmaksızın sorumlu tutulmalarını öngörmektedir. Objektif sorumluluğu benimseyen bir diğer önemli uluslararası düzenleme ise 29 Mart 1972 tarihli *Uzay Cisimlerinin Neden Olduğu Zararlar Konusunda Uluslararası Sorumluluğa İlişkin Sözleşme*'dir. Bu sözleşme kapsamında, zarar gören tarafın zararın uzay faaliyetini gerçekleştiren devlet tarafından meydana getirildiğini ispat etmesine gerek kalmaksızın, fırlatan devlet doğrudan sorumlu tutulmaktadır.

Uluslararası yargı organlarının kararlarını inceleyen yazarlar, devletin sorumluluğunu gerektirecek haksız fiillerin kusur esasına göre mi yoksa objektif sorumluluk esasına göre mi değerlendirildiği konusunda kesin bir eğilimin bulunmadığını belirtmektedirler. Hem kusur teorisini benimseyen hem de objektif sorumluluk yaklaşımını esas alan yargı kararları kolaylıkla tespit edilebilmektedir. Bu nedenle bazı yazarlar, her iki görüşü de tamamen reddetmemekte ve her somut olaya uygulanacak ölçütü ayrı ayrı değerlendirmeyi doğru bulmaktadırlar.[354] Bununla birlikte, günümüzde doktrindeki genel eğilimin objektif sorumluluk yönünde olduğu söylenebilir. Objektif sorumluluk teorisini benimseyen yazarlar, sorumluluğu uluslararası hukuk kurallarının yaptırımı olarak görmektedirler.[355]

Sonuç olarak, devletin uluslararası sorumluluğunun doğabilmesi için, devletin uluslararası hukuka göre bir yapmama yükümlülüğüne aykırı hareket etmesi veya bir yapma yükümlülüğünü ihlal etmiş olması yeterli görülmektedir. Başka bir deyişle, uluslararası haksız fiil, bir devletin diğer bir devlet veya devletlerle ilişkilerini düzenleyen hukuki kurallara aykırı bir eylemidir.[356]

Taslak Maddelerde kusurlu sorumluluk veya objektif sorumluluğa ilişkin açık bir hüküm bulunmamaktadır. Bu nedenle, konuyla ilgili genel bir kuralın mevcut olmadığını ve her olayın kendi somut özelliklerine göre değerlendirilmesi gerektiğini ifade etmek gerekir.

1.2.5. Zarar Unsuru

Uluslararası Hukuk Komisyonu, devletin uluslararası sorumluluğunun doğabilmesi için zararın bir unsur olarak aranması gerekliliğini Taslak Maddelerden çıkarmıştır. Bununla birlikte, burada dikkat edilmesi gereken husus, zararın öneminin sorumluluk hukukundan çıkarılmamış olmasıdır. Başka bir deyişle, zarar, Taslak Maddelerden bir unsur olarak aranması

[354] Meray, *Devletler Hukukuna,* 477.
[355] Meray, *Devletler Hukukuna,* 477.
[356] Meray, *Devletler Hukukuna,* 477-478.

gereken bir koşul olmaktan çıkarılmıştır; ancak uluslararası sorumluluk bağlamında etkisi ve önemi devam etmektedir.[357]

Zarar, sorumluluğun ileri sürülebilmesi ve mağdurun tespitinde belirleyici bir rol oynamaktadır. Bununla birlikte, uluslararası haksız fiilin varlığı için, devlete atfedilen bir davranışın mutlaka zarar meydana getirmiş olması şart değildir. Başka bir deyişle, devletin bir uluslararası yükümlülüğüne aykırı her davranışı, zarar doğursun ya da doğurmasın, Uluslararası Hukuk Komisyonu'na göre uluslararası nitelikte bir haksız fiildir ve bu fiilin faili olan devletin uluslararası sorumluluğu doğar. Komisyon tarafından benimsenen görüş de bu doğrultudadır.[358]

Taslak Maddeler'in 31. maddesinin birinci fıkrasında, "Sorumlu devlet, uluslararası haksız fiil ile neden olunan bütün zararı onarmak zorundadır." hükmü yer almaktadır. Aynı maddenin ikinci fıkrasında ise, "Zarar, devletin uluslararası haksız fiilinin sonucu olan maddi ve manevi bütün zararı kapsar." ifadesine yer verilmiştir.[359] Uluslararası Hukuk Komisyonu, söz konusu kuralları oluştururken devlet uygulamalarını ve uluslararası yargı organlarının kararlarını dikkate almıştır. Bu nedenle, ilgili düzenlemeler uluslararası örf ve adet hukuku kurallarını yansıtmaktadır.

Uluslararası sorumluluk, zarardan değil, ihlalden kaynaklanmaktadır. Uluslararası Hukuk Komisyonu'na göre, ihlalden dolayı sorumluluğu doğan bir devletin bu sorumluluktan kaynaklanan yükümlülüklerinin somut olarak ortaya çıkabilmesi ve fiilen yerine getirilebilmesi için zararın varlığı gereklidir. Başka bir ifadeyle, somut bir zarar bulunmadığında devletin sorumluluğu hukuki anlamda mevcut olsa da, ancak somut zararın varlığı halinde bu sorumluluktan doğan onarım yükümlülüğü fiilen uygulanabilir hâle gelmektedir.[360] Zarar, uluslararası haksız fiilin unsurları arasında yer almamaktadır. Bununla birlikte, onarım yükümlülüğünün fiilen ve somut olarak uygulanabilmesi için zararın mevcut olması gerekmektedir.[361]

Devletin uluslararası sorumluluğunun ileri sürülmesi ve mağdurun belirlenmesi bakımından zarar, önemli bir ölçüt teşkil etmektedir. Bununla birlikte, uluslararası haksız fiilin varlığı için devlete atfedilen bir davranışın mutlaka zarar doğurması şart değildir. Uluslararası yükümlülüğe aykırı her davranış, zarar meydana getirip getirmediğine bakılmaksızın,

---

[357] Hakkı Hakan Erkiner, *Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu,* (İstanbul: On İki Levha Yayıncılık, 1.Bası), 109.
[358] Erkiner, *Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu,* 109-110.
[359] Erkiner, Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu, aslı: *International Law Commission, Report of the International Law Commission on the Work of its Fifty-Third Session, 23 April - 1 June and 2 July - 10 August 2001, Official Records of the General Assembly, Fifty-Sixth Session, Supplement No.10*, vol. II(2), 2001, 31/1-2.
[360] Erkiner, *Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu,* 111.
[361] Erkiner, *Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu,* 112.

Uluslararası Hukuk Komisyonu'na göre uluslararası nitelikte bir haksız fiil olarak kabul edilmekte ve bu fiili işleyen devletin uluslararası sorumluluğu doğmaktadır.[362]

Uluslararası sorumluluğun doğabilmesi, ancak uluslararası hukukun koruma alanına aldığı bir hakka yönelik zararın varlığı ile mümkündür. Bir hak teşkil etmeyen doğrudan veya dolaylı çıkarlara verilen zararlar nedeniyle, uluslararası hukuk süjeleri, bu çıkarlarına aykırı davranan devletin sorumluluğunu ileri süremez. Bu çerçevede, uluslararası nezaket kurallarına aykırı davranışlar dostane olmayan eylemler olarak nitelendirilebilir ve devletler arası ilişkileri olumsuz yönde etkileyebilir; ancak bu tür eylemler uluslararası sorumluluk doğurmaz. Benzer şekilde, uluslararası ahlak kurallarına aykırı hareket eden bir devletin de hukuki anlamda sorumluluğu söz konusu olmaz. [363]

Devletin uluslararası sorumluluğunu doğuran zararın, uluslararası haksız fiil veya belirli bir davranış sonucunda meydana gelmiş olması gerekir. Bu çerçevede zarar, doğrudan zarar ve dolaylı zarar olarak ikiye ayrılmaktadır. Doğrudan zarar, uluslararası hukuka aykırı fiilin veya sorumluluk doğuracağı kabul edilen faaliyetin gerekli ve kaçınılmaz sonucunu ifade eder. Dolaylı zarar ise, ilk zarara bağlı olarak ikinci aşamada ortaya çıkan zararlardır. [364] Nitekim 1872 tarihli *Alabama Davası*'nda, hakemlik mahkemesi, İngiltere tarafından silahlandırılarak Güneylilere satılan Alabama gemisinin ABD'ye ait gemileri batırmasını doğrudan zarar olarak değerlendirmiş; buna karşılık gemi sigorta fiyatlarının ve yük taşıma ücretlerinin artmasını dolaylı zarar olarak nitelendirmiş ve bunları uluslararası sorumluluk kapsamında değerlendirmemiştir.[365]

Uluslararası mahkemeler, 20. yüzyılın başlarına kadar yalnızca maddi zararları dikkate alarak devlet sorumluluğunu kabul etmekteydi. Ancak 1923 tarihli *Lusitania Davası*'nda, batırılan gemide hayatını kaybedenlerin yakınlarının uğradığı manevi zararlar da tazminat kapsamına alınmıştır. Bu karar, manevi zararların da uluslararası sorumluluk doğurabileceğini ortaya koyan ilk örneklerden biri olmuştur. Bu gelişme sonrasında, zararın maddi veya manevi nitelikte olması, sorumluluğun tespitinde belirleyici bir unsur olmaktan çıkmıştır. [366] Maddi zarar, uluslararası hukuka aykırı bir fiilden kaynaklanan somut ve ekonomik nitelikteki kayıpları ifade eder. Buna, mülkiyetin kaybı veya tahribatı, kar kaybı ya da objektif biçimde ölçülebilen ve tazmin edilebilen diğer mali zararlar dahildir. Taslak Maddelerin 31(2) numaralı hükmüne göre maddi zarar, bir devletin haksız fiilinden doğan ve ekonomik değeri bulunan her

[362] Erkiner, *Devletin Haksız Fiilden Kaynaklanan Uluslararası Sorumluluğu,* 112-113.
[363] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 284.
[364] Pazarcı, *Uluslararası Hukuk,* 445.
[365] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 284.
[366] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 284.

türlü zararı kapsar.[367] Tazminatın ödenebilmesi için zararın gerçek olması, haksız fiilden kaynaklanması ve parasal olarak ölçülebilir nitelikte bulunması gerekmektedir.

1.2.6. Nedensellik Bağı

Uluslararası hukukta nedensellik kavramı, uyuşmazlıkların çözümünde merkezi bir rol oynamasına rağmen, çoğu zaman yüzeysel ve dağınık biçimde ele alınmaktadır. Uluslararası yargı organlarının nedensellik değerlendirmeleri genellikle tutarsızlık göstermekte, doktrinde ise bu konuda yeterli ve sistematik bir çerçeve henüz oluşmamış bulunmaktadır.[368]

Nedensellik bağı, meydana gelen zarar ile bu zarara yol açan davranış veya olay arasındaki neden-sonuç ilişkisinin varlığını ifade eder. Zarar ile sorumluluğun atfedildiği eylem veya olay arasında böyle bir ilişkinin bulunması zorunludur. Haksız fiillerde ise, haksız fiil ile zarar arasında bu ilişkinin mevcut olup olmadığı incelenir.[369]

Devletin uluslararası sorumluluğu bağlamında nedensellik bağı üç şekilde ortaya çıkar: Birincisi, birincil kurallarda açıkça düzenlenmesi; ikincisi, ikincil kurallarda tazminat yükümlülüğünün bir gereği olarak aranması; üçüncüsü ise yargı kararlarında zararlı sonucun fail ile bağlantısının incelenmesidir. Bununla birlikte, uluslararası hukukta nedensellik genel bir hukuk ilkesi olarak kabul edilmemekte; uygulamada ise fiilî neden ile sorumluluğun kapsamı arasındaki ayrım çoğunlukla karıştırılmaktadır.[370]

Uluslararası hukuk pratiğinde ve yargı kararlarında, uygun nedensellik bağı teorisinin benimsendiği görülmektedir. Nitekim *Maninat* (1905) davasında Fransa-Venezuela Karma Hakem Mahkemesi, hatalı tıbbi teşhis sonucu meydana gelen yaralanma ve sakatlıklardan, bu durumun haksız tutuklamanın bir sonucu olduğu gerekçesiyle Venezuela'yı sorumlu tutmuştur. Mahkeme, kararını "zararın, işlenen haksız fiillerin ne derece doğal ve yakın bir sonucu olduğu" yönündeki değerlendirmeye dayandırmıştır.[371]

Uluslararası hukukta nedensellik değerlendirmesi, genel olarak özel hukukta kullanılan iki aşamalı modele benzemektedir. Bu modelde önce fiilî neden belirlenir, ardından sorumluluğun kapsamı tespit edilir. Uluslararası mahkemeler, nedensellik sorunlarını çözerken özel hukuk ilkelerinden yararlanmakta; ancak uluslararası hukukta nedensellik konusunda

[367] ARS, Articles on Responsibility of States for Internationally Wrongful Acts, md. 31.
[368] Ilias Plakokefalos, "Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity", *The European Journal of International Law* 26/2, (2015), 473-476.
[369] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 285.
[370] Plakokefalos, "Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity", 473-476.
[371] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 285.

henüz tutarlı ve özgün kurallar geliştirilmemiştir. Bu durum, nedensellik konusundaki belirsizliği artırmakla birlikte, özel hukuktan aktarılan kavramlar uluslararası hukuk uygulamasında önemli bir rehber işlevi görmektedir.[372]

2. FİİLİN DEVLETE ATFEDİLMESİ

Uluslararası sorumluluğun doğabilmesi için, sorumluluğa yol açan fiilin bir uluslararası hukuk kişisine atfedilebilir olması ve bu fiilin söz konusu kişiye ait bulunması gerekir. Haksız fiil veya tehlikeli faaliyet bir devlet ya da uluslararası örgütle ilişkilendirilemediği takdirde, uluslararası sorumluluk söz konusu olmaz.[373]

Uluslararası sorumluluk, her şeyden önce devletler arasında ortaya çıkar. Uluslararası hukukta, uluslararası örgütler ile gerçek kişilerin fiillerinden kaynaklanan sorumluluğun ayrı biçimde ele alınması ise klasik doktrinin bir yaklaşımıdır.[374]

2.1.Devletin Uluslararası Hukuka Aykırı Fillerinden Doğan Sorumluluğu

Hiçbir eylem, devletin doğrudan kendisi tarafından gerçekleştirilemez; zira devlet, kendi başına fiilî bir davranışta bulunamaz. Devletin tüzel kişiliği aracılığıyla doğrudan haksız fiil işlemesi esasen mümkün olmadığından, bu tür fiiller ancak devleti temsil eden kişiler veya vatandaşları tarafından gerçekleştirilebilir. Bir haksız fiilin devlete atfedilebilmesi ise, söz konusu fiilin devletin bir organı sıfatıyla gerçekleştirilmiş olmasına bağlıdır.[375] Devlet fiilleri, devletin yetkilileri veya temsilcileri konumundaki bir ya da birden fazla kişi tarafından gerçekleştirilir. Nitekim 1901 tarihli bir hakem kararında da vurgulandığı üzere, "uluslararası hukukun evrensel olarak kabul edilen bir ilkesine göre, bir devletin görevlileri tarafından işlenen uluslararası hukuk ihlalleri, o devletin sorumluluğunu doğurur."[376] Dolayısıyla, devlet eylemi esasen belirli kişi veya kişilerin eylemlerinden ibarettir. Burada önemli olan, bu kişilerin eylemlerinin hangi koşullar altında devlet eylemi sayılacağını ve dolayısıyla devletin uluslararası sorumluluğunu doğuracağını belirlemektir.[377]

---

[372] Plakokefalos, "Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity", 473-476.
[373] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 286.
[374] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 286.
[375] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 286.
[376] Roberto Ago, "Third Report on State Responsibility by Special Rapporteur", *YILC*, (1971) 2/1, 124.
[377] Elif Uzun, *Devletin Uluslararası Hukuka Aykırı Eyleminden Sorumluluğu,* (Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Doktora Tezi, 2007), 80.

Devlete atfedilen fiiller, her şeyden önce devleti temsil eden hükümetin eylemleridir. Her ne kadar devletin fiilleri yalnızca hükümetin fiilleriyle sınırlı olmasa da, hükümetin gerçekleştirdiği eylemler, münhasıran temsil ettikleri devletin fiilleri olarak kabul edilmektedir.[378]

Devletin haksız fiili, yalnızca organları veya temsilcileri aracılığıyla gerçekleşebilir. Uluslararası hukuku ihlal eden bir fiil, doğrudan organ veya yetkililere değil, onların temsil ettiği devlete atfedilir. Bir yetkilinin eylemi devlete atfedildiğinde ise, devlet bu eylemin yol açtığı zararlı sonuçlardan uluslararası hukuk çerçevesinde sorumlu tutulabilir.[379]

2.1.1. Devletin *De Jure* Organları

Bir haksız fiilin devlete atfedilebilmesi için, bu fiilin devlet organları veya resmi görevliler tarafından işlenmiş olması gerekir. Ayrıca, bu organların verdiği yetkiyle gerçekleştirilen fiiller de devlete atfedilebilir. İç hukuk tarafından yetkilendirilen herhangi bir kişi veya organ, uluslararası sorumluluk açısından bir devlet organı olarak kabul edilir.[380]

Organların, iç hukuk uyarınca kendilerine tanınan yetkiler dışında veya bu yetkilere aykırı olarak işledikleri haksız fiiller de devlete atfedilir. Haksız fiili işleyen kişi veya kurumun organ sıfatına sahip olup olmaması ve bu fiili gerçekleştirme yetkisinin bulunup bulunmaması, uluslararası hukuk açısından belirleyici değildir. Temel mesele, organın yetkili olup olmaması değil, haksız fiilin devletin organı gibi hareket eden kişiler tarafından gerçekleştirilip gerçekleştirilmediğidir. Devletin bir organı gibi hareket edilmişse, fiil devlete atfedilmiş sayılır.[381]

Genellikle bir devlet, organlarının ve görevlilerinin yetkilerini iç hukuku aracılığıyla düzenler. Eğer devletin organ ve görevlilerinin eylemleri iç hukuk tarafından tanınmakla birlikte uluslararası hukuk açısından da bir sonuç doğuruyorsa, bu eylemler devletin fiilleri olarak kabul edilir. Ancak, iç hukuka uygun olsa dahi bir eylem uluslararası hukuka aykırı ise, devletin bu eylemden uluslararası düzeyde sorumlu tutulacağı kesindir.[382]

Bir devletin uluslararası sorumluluğunu doğuran fiiller, temel olarak üç yetkisine dayanır: yasama, yürütme ve yargı erkleri. Bunun yanı sıra, bazı durumlarda devlete bağlı

[378] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 286.
[379] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 286.
[380] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 289.
[381] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 289.
[382] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 289.

olarak kamu yetkisi kullanan diğer kuruluşların eylemlerine de uluslararası sorumluluk atfedilebilir.[383]

Devletin fiilleri, esasen uluslararası hukuk tarafından devlete atfedilen gerçek kişilerin fiillerinden ibarettir. Bu nedenle tespit edilmesi gereken husus, hangi gerçek kişi fiillerinin devletin uluslararası yükümlülüklerinin ihlali anlamına geleceğidir. Atfın önemi, organların ve görevlilerin devlete olan ilişkisini ortaya koymak ve bu özel ilişkiyi yasama, yürütme ve yargı organları bağlamında ele almaktır.[384]

2.1.1.1.Yasama

Bir devlet, yasama yetkisini kullanarak gerçekleştirdiği tüm hukuki tasarruflardan dolayı uluslararası sorumlulukla karşı karşıya kalabilir. Sorumluluğa yol açan hukuki işlem, devletin anayasası gibi asli normlara dayanabileceği gibi, kanun, tüzük veya yönetmelik gibi daha alt düzeydeki normlardan da kaynaklanabilir. Bu konuyla ilgili olarak Uluslararası Daimi Adalet Divanı, 26 Temmuz 1927 tarihli *Chorzów Davası* kararında şu ifadeleri kullanmıştır: "Uluslararası hukuk açısından ... iç hukuk düzenlemeleri, mahkeme kararları veya idari tedbirler gibi işlemler, devletlerin faaliyetlerini ve iradelerini gösterir."[385]

Yasama organının tasarrufları, hem aktif fiiller hem de ihmaller yoluyla devletin uluslararası sorumluluğunu doğurabilir. Başka bir deyişle, yasama organı tarafından çıkarılan veya çıkarılmasından kaçınılan yasalar, uluslararası bir yükümlülüğün ihlaline yol açtığında, bu durum devletin sorumluluğunu doğurur.[386]

2.1.1.2.Yürütme

Yürütme, devletin idari faaliyetlerini yürüten tüm birimleri kapsayan ve geniş bir yetki alanına sahip bir kavramdır. Bu nedenle, devletin sorumluluğunun ortaya çıkması bakımından yasama ve yargıya kıyasla daha büyük bir öneme sahiptir. Bu kapsamda kolluk kuvvetleri, silahlı kuvvetler, istihbarat görevlileri, konsolosluk görevlileri ve diğer idari görevlilerin eylemlerinden doğan sorumluluğa ilişkin çeşitli uluslararası mahkeme kararları mevcuttu.[387] Örneğin, ABD-Meksika Hakem Komisyonu tarafından görülen Youmans Davası'nda, ABD

[383] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 290.
[384] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 290.
[385] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 290.
[386] Uzun, *Devletin Uluslararası Hukuka Aykırı Eyleminden Sorumluluğu,* 83.
[387] Uzun, *Devletin Uluslararası Hukuka Aykırı Eyleminden Sorumluluğu,* 85.

askerlerinin emirlerine aykırı hareket ederek kişilere zarar vermesi üzerine, bu fiiller devletin uluslararası sorumluluğu kapsamında değerlendirilmiştir. Hakem heyeti, askerler emir dışına çıksa dahi, devlet organı sıfatıyla hareket ettikleri sürece eylemlerinin devlete atfedileceğini belirtmiştir.[388] Bir diğer örnek ise Nikaragua kararıdır. Bu davada ABD'nin, Nikaragua'daki yarı askeri gruplara sağladığı destek ve istihbarat paylaşımı, devletin sorumluluğu kapsamında ele alınmıştır. Uluslararası Divan, devletin doğrudan veya etkili kontrolü bulunduğu durumlarda, istihbarat görevlilerinin fiillerinin devlete atfedilebileceğini vurgulamıştır.[389]

Uluslararası hukuk uygulamasında, farklı işlevlere sahip yetkililer arasında herhangi bir ayrım yapılmamaktadır. Sivil devlet memurlarının yanı sıra, güvenlik görevlileri, istihbarat görevlileri ve askerlerin gerçekleştirdiği eylemler de devletin uluslararası sorumluluğunu doğurabilir.[390]

Örneğin, 1987 tarihli *Rainbow Warrior Davası*'ndaki hakem kararı, gizli servis ajanlarının eylemleri nedeniyle devletin sorumluluğunu gösteren bir örnektir. Bu davada, Greenpeace gemisi *Rainbow Warrior*, Yeni Zelanda karasularında Fransız gizli servis ajanları tarafından batırılmış ve bir mürettebat üyesi hayatını kaybetmiştir. Hakem heyeti, Fransa'nın, gizli servis ajanlarının fiillerinden dolayı sorumlu olduğuna hükmetmiştir.[391]

Devlet görevlilerinin küçük-büyük veya iç-dış memur şeklinde sınıflandırılması, devletin uluslararası sorumluluğu açısından önemsizdir. Sorumluluk hukukunda bu tür bir ayrım yapılmamaktadır; en alt düzeydeki memurların gerçekleştirdiği fiillerden dolayı da devletin uluslararası sorumluluğu doğabilir.[392]

Bir devlet görevlisinin yetkisini aşarak (ultra vires) gerçekleştirdiği fiillerden dolayı da devletin uluslararası sorumluluğunun doğabileceği genel olarak kabul edilmektedir. Bu husus, 2001 tarihli Taslak Maddeler'in 7. maddesinde açıkça düzenlenmiştir. Maddenin ifadesine göre: "Bir devlet organının davranışı ya da kamu gücü yetkilerini kullanmak üzere yetkilendirilmiş bir kişi veya birimin davranışı, bu organ, kişi veya birim yetkisini aşsa veya talimatlara aykırı hareket etse bile, uluslararası hukuka göre devletin fiili olarak kabul edilir."[393] Devletin, görevlinin yetkisini aşmasından kaynaklanan uluslararası sorumluluğu, görevlinin

[388] Christopher Greenwood, "State Responsibility and Civil Liability for Environmental Damage Caused by Military Operations," *International Law Studies* 69 (1993), 397-415.
[389] Rafael Nieto-Navia, "State Responsibility in Respect of International Wrongful Acts of Third Persons: The Theory of Control", International Law Studies, 69 (1993), 15.
[390] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 292.
[391] Uzun, *Devletin Uluslararası Hukuka Aykırı Eyleminden Sorumluluğu,* 86.
[392] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 292.
[393] International Law Commission (ILC), *Report on the Work of Its Fifty-Third Session (23 April–1 June and 2 July–10 August 2001), General Assembly Official Records Fifty-Fifth Session, Supplement No. 10 (A/56/10)* (New York: United Nations, 2001).

kötü seçilmiş olması veya görevli üzerindeki denetimin yetersizliği kabulüne dayanmaktadır. Böyle bir durumda, devlet kendi iç hukuk düzeniyle sorunu gideremezse, ihmali nedeniyle uluslararası sorumluluğu doğar. Bu tür sorumluluk, hem devletler arasındaki uygulamalarda hem de hakem kararlarında kabul edilmektedir.[394]

2.1.1.3.Yargı

Bir devletin adli memurlarının fiilleri de devlete atfedilebilir ve bu durum, devletin uluslararası sorumluluğunu gündeme getirebilir. Özellikle yabancılar söz konusu olduğunda, bir devletin yargı organlarının eylemlerinden doğan uluslararası sorumluluk, hakkın yerine getirilmesinden kaçınma (*denial of justice*) durumundan kaynaklanır. En yaygın anlamıyla, hakkın yerine getirilmesinden kaçınma, devletin yasama, yürütme ve yargı organlarının haksız fiillerinin sonuçlarını uygun biçimde telafi etmemesi veya bunu reddetmesi anlamına gelir.[395]

2.1.2. Devletin *De Facto* Organları

Atfedilmezlik ilkesinin istisnalarını, devlet dışı aktörlerin fiilleri oluşturmaktadır. Devlet dışı aktörlerin fiilleri, hem Taslak Maddeler hem de yerleşik hukuk uygulamaları çerçevesinde devlete atfedilebilmektedir.

2.1.2.1. Devlet Dışı Aktörlerin Fiillerinden Dolayı Devletin Sorumluluğu

Devletler, uluslararası ilişkilerinde kendi amaçlarını gerçekleştirmek için zaman zaman alışılageldik davranış biçimlerini terk ederek, yani resmi organlarının faaliyetlerinin ötesine geçip resmi organları olmayan özel kişi ve grupları kullanarak uluslararası hukuk kapsamındaki sorumluluklarından kaçınmaya çalışabilmektedir. Ancak uluslararası hukuk çerçevesindeki yargı kararları ve sorumluluğa ilişkin düzenlemeler, devlet örgütlenmesi içinde yer almayan özel kişi ve grupların hukuka aykırı eylemlerinden dolayı devletin sorumluluğunu öngören hükümler geliştirmiştir.

Uluslararası hukukun gelişim sürecini hızlandıran savaşlar ve teknolojik ilerlemeler, devletlerin özel kişi ve grupların fiillerinden de sorumlu tutulmasına yönelik kuralların oluşmasına zemin hazırlamıştır. 18. yüzyılda yaşamış olan Christian Wolff, devleti, kurumları

[394] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 292.
[395] Bozkurt- Poyraz- Erdal, *Devletler Hukuku*, 293.

aracılığıyla faaliyet gösteren soyut bir varlık olarak algılamış; bu yaklaşım, günümüzde "isnat" veya "atıf" doktrinleri olarak bilinen kavramların geliştirilmesine öncülük etmiş ve Wolff'a bu alanda ilk kamu hukukçusu unvanını kazandırmıştır. Wolff'a göre, "özel kişinin fiilleri, üyesi olduğu devletin fiili değildir; çünkü bu fiiller özel kişi tarafından devletin bir üyesi sıfatıyla işlenmemiştir." Bununla birlikte, özel kişi, devletin yöneticisi sıfatına sahip olan bir kişinin emirleri doğrultusunda hareket ettiğinde, devlet bu fiillerden sorumlu tutulur. Bu açıklamadan da anlaşılacağı üzere, özel kişi ile devlet yöneticisi arasında genel bir talimat ve itaat ilişkisi mevcutsa, özel kişinin faaliyetleri devlete atfedilecektir.[396]

De Vattel'e göre, bir devlet, kendi vatandaşlarının ülkeye gelen yabancı devlet vatandaşlarına zarar vermesine veya başka bir devleti incitmesine izin vermeme yükümlülüğü altındadır. Vattel'e göre, bir devlet, kendi vatandaşının ülkede hâkim olan barış ve adalet kurallarına uygun davranmasını sağlayabilecek durumda iken, vatandaşının yabancı bir devlete veya onun bir üyesine zarar vermesine izin verirse, bu durumda söz konusu devlet, sanki kendisi zarar vermiş gibi kabul edilecektir. Görüldüğü üzere, hem Vattel'in hem de Wolff'un görüşlerinde benzerlikler mevcuttur; her ikisi de, devlet ile emir ve itaat ilişkisi içinde olan özel kişilerin fiillerinin devlete isnat edilebileceğini savunmaktadır.[397]

Bununla birlikte, Vattel, görüşünün mutlak olmadığının da farkındadır. Ona göre, oldukça nitelikli bir devlet bile her bir vatandaşının hareketlerini kendi iradesine göre belirleyemez; daha açık bir ifadeyle, devlet vatandaşının her eylemini kontrol edemez ve kendi iradesine mutlak olarak itaat etmesini sağlayamaz. Dolayısıyla, vatandaşlar tarafından işlenen her hukuka aykırı eylemin devlete isnat edilmesi doğru değildir. Bununla birlikte, devlet veya devletin yöneticisi bireyin fiilini onaylar ve uygun bulursa, bu fiil kamusal bir nitelik kazanır ve mağdur taraf, devleti uğradığı zararın gerçek faili olarak kabul edebilir.[398]

20. yüzyılın önemli uluslararası hukukçularından biri olan Lassa Oppenheim, devletin uluslararası sorumluluğunu incelerken, devletin tüzel kişiliğinden hareketle, öncelikle hangi fiillerin devletin fiili sayılacağı sorusunun yanıtlanması gerektiğini vurgulamıştır. Bu çerçevede Oppenheim, devlet yetkilisi veya özel kişilerin, devlet tarafından verilen talimat veya izin doğrultusunda gerçekleştirdiği tüm fiillerin devletin fiili olarak kabul edileceğinin altını çizmiştir.[399] Böylece Oppenheim, resmi organı olmayan özel kişilerin hangi fiillerinin devlete

[396] Bleda Rıza Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi* 11/143-144 (2016), 60-61.
[397] Emer De Vattel, The Law of Nations, ed. Béla Kapossy ve Richard Whatmore (Indianapolis: Liberty Fund, 2008), Kitap II, Bölüm VI, paragraf 71.
[398] Vattel, The Law of Nations, 73-74.
[399] Lassa Oppenheim, *Uluslararası Hukuk: A Treatise*, Cilt I: Barış, 2. Baskı (Londra: Longmans, Green and Co., 1912), 211, paragraf 153.

atfedilebileceğini belirleyerek, günümüzdeki de facto organ kavramının temelini de ortaya koymuştur.

Oppenheim'e göre bir devlet, kendi ülkesinde bulunan vatandaşlarının ve yabancıların diğer devletlere zarar verici fiiller gerçekleştirmesini önleme yükümlülüğü altındadır. Bu yükümlülük, devletin kendi ülkesindeki münhasır egemenliğinden kaynaklanan kontrol ve düzenleme yetkisine dayanmaktadır. Ancak bir devlet, özel kişi ve grupların gerçekleştirdiği her fiili önleyemeyebilir. Bu bağlamda, devletin sorumluluğu, önleyemediği fiiller nedeniyle yalnızca yabancı devlete zarar veren özel kişiyi yargılamak, cezalandırmak ve gerekli zarar tazminini sağlamaktan doğar. Eğer devlet bu sorumluluğunu yerine getirmekten kaçınırsa, bu durum sorumluluğun doğrudan asli sorumluluğa dönüşmesine yol açar ve sonuç olarak devlet, maddi ve manevi tazminat ödemekle yükümlü hale gelir.[400]

Uluslararası Hukuk Komisyonu'nun (UHK) özel raportörü olarak görevlendirilen Roberto Ago, 1971 yılında, devletin de facto organlarıyla ilgili bir sorumluluk hukuku kuralı geliştirilmesini öneren bir rapor sunmuştur. Ago, bu kuralı oluştururken idare hukukunda mevcut olan devletin "de facto memurları" anlayışını esas almış ve bu yaklaşımı uluslararası hukuk alanına uyarlamıştır. Bu çerçevede Ago, özel kişi ve grupların eylemlerinin devlete atfedilmesini, devletin "de facto organları" kavramı kapsamında değerlendirmiştir.[401]

Bu bağlamda, 1974 yılında UHK, devlet adına hareket eden kişi veya kişi gruplarının fiillerinin devlete atfedilebileceğini belirten 8(a) ilkesini ve bu ilkenin, Özel Raportör Ago tarafından devlet sorumluluğuna ilişkin taslak maddeler çerçevesinde geliştirilen yorumunu kabul ettiğinde, maddenin "devlet mekanizmasına fiilen bağlı kişi veya kişi gruplarının fiilleriyle ilgili olduğunu" zımnen beyan etmiş olmuştur.[402]

Doktrinde de kabul edildiği üzere, 8(a) ilkesi, devlet ile bireyler arasındaki ilişkinin "hukuki" değil "fiili" niteliğini dikkate almakta ve bir kişinin hangi koşullar altında devletin fiili temsilcisi veya vekili sayılacağını belirlemektedir.[403]

---

[400] Oppenheim, *International Law*, 211-153.

[401] Roberto Ago, *Third Report on State Responsibility: The Internationally Wrongful Act of the State, Source of International Responsibility*, *The Yearbook of the International Law Commission*, 1971, 2/1, A/CN.4/246 ve Ek.1-3 (New York: United Nations, 1971), 199-274, 262-264, paragraflar 187, 190-191.

[402] Uluslararası Hukuk Komisyonu (ILC), *Document A/9610/Rev.1: Report of the International Law Commission on the Work of Its Twenty-Sixth Session, 6 May–26 July 1974* (*Yearbook of the International Law Commission*, 1974), cilt II(1), 157-330, 283, paragraf 1, erişim 22 Kasım 2024, http://legal.un.org/ilc/guide/9_6.shtml#werprep.; Uluslararası Hukuk Komisyonu (ILC), *Draft Articles on State Responsibility with Commentaries Thereto Adopted by the International Law Commission on First Reading* (Ocak 1997), 32, paragraf 1, erişim 22 Kasım 2024, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf.

[403] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 65.

Bu dönemde, devletin fiili organları olarak tanımlanabilecek kişiler için bir sorumluluk hukuku kuralı geliştirilmesi kuşkusuz tesadüfi değildir. Nitekim Yorum'a göre: "Devletler, çeşitli ve açık nedenlerle, belirli görevleri doğrudan kendileri üstlenmeyi veya bizzat yerine getirmeyi tercih etmezler; bu görevlerin ve işlerin özel kişiler veya özel kişi grupları tarafından üstlenilmesini tercih ederler… Etkililik ilkesinin uluslararası hukuk düzenindeki önemini dikkate alan Komisyon, bu düzenlemede aktör ile devlet arasında var olmayan resmi hukuki ilişkiyi değil, aktör ile devlet arasındaki mevcut gerçek bağı göz önünde bulundurması gerektiğini düşünmektedir."[404]

1945'ten bu yana kurulan iki kutuplu dünya düzeni, devletlerin özel kişiler ve kişi gruplarını tercih etme eğiliminde belirleyici olmuştur. 1949'da Sovyetler Birliği'nin nükleer silahlara sahip olmasıyla birlikte doğrudan savaş yaklaşımı yerini hibrit savaşa bırakmıştır. Devletler, topyekûn bir savaş olasılığından kaçınmak amacıyla, resmi organları yerine resmi bağlantıları tespit edilemeyen devlet dışı aktörleri kullanarak hem savaştan hem de uluslararası sorumluluktan kaçınmayı denemişlerdir. Bu aktörleri örgütlemek veya başka şekilde kontrol etmek; onlara eğitim, silah, istihbarat sağlamak ve kendi ülkesinde barındırmak hukuken askeri saldırı kapsamında incelenmiştir. Ayrıca, BM Şartı çerçevesinde oluşturulan uluslararası hukuk düzenine göre, silahlı saldırı olarak değerlendirilemeyecek fiilleri işleyen özel kişilerin fiillerinden devletin sorumlu tutulup tutulmayacağı sorusu, devletin de facto organları kavramı çerçevesinde ele alınmıştır.[405]

Uluslararası Hukuk Komisyonu'nun (UHK) devlet sorumluluğuna ilişkin kurallarının derlenmesi kapsamında, Madde 8 (a)'nın 1974 ve 1980 taslakları ile yorumu, devlet sorumluluğunun doğabilmesi için, devlet organları tarafından belirli bir hizmetin yerine getirilmesi veya belirli bir görevin ifası amacıyla görevlendirilen kişi veya kişi gruplarının varlığının ve bu tür bir görevin söz konusu organların kışkırtması veya teşviki ile yerine getirildiğinin kanıtlanması gerektiğini ortaya koymaktadır.

Burada özellikle dikkat edilmesi gereken husus, Komisyon'un maddeyi yorumlarken uluslararası hukuktaki etkililik kriterine ve devlet ile özel kişiler arasında fiili/gerçek bir ilişkinin varlığına atıfta bulunmuş olmasıdır. Bununla birlikte, devletin de facto ajanlarının faaliyetlerinden sorumlu olabilmesi için bu ilişkinin etkililik düzeyini hiçbir şekilde

[404] Uluslararası Hukuk Komisyonu (UHK), *Document A/9610/Rev.1: Report of the International Law Commission on the Work of Its Twenty-Sixth Session, 6 May–26 July 1974* (1974), 283, paragraf 2.
[405] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 66-67.

belirtmemiştir. Komisyon'un yorumu, devletin bu kişiler veya kişi grupları üzerindeki kontrolüne ya da bu kontrolün niteliği ve kapsamına dair herhangi bir açıklık içermemektedir.

Gözden kaçırılmaması gereken ikinci nokta ise, Komisyon'un "görevlendirme" fiilini kullanmış olmasıdır. Bu fiil, öncelikle özel kişilerden oluşan bir organizasyon kurmayı ve ardından bu organizasyona belirli bir görev vermeyi ifade etmektedir. Dolayısıyla, ilerleyen satırlarda da görüleceği üzere, UAD tarafından geliştirilen tam bağımlılık testinin temelini oluşturan, özel kişilerden oluşan gruplar kurma veya oluşturma kriterini karşılamaktadır.[406]

2.1.2.2. Madde 5 Bağlamında Devletin Sorumluluğu

Bir devletin, özel kişiler tarafından işlenen uluslararası hukuk ihlallerinden sorumlu tutulup tutulamayacağı sorusu, esasen "devlet eylemi" kavramının tanımıyla doğrudan ilişkilidir. Taslak Maddeler'in 3. maddesine göre, bir devlet fiilinin uluslararası hukuka aykırı olarak nitelendirilmesi hususunda belirleyici olan, iç hukuk değil uluslararası hukuktur. Taslak Maddeler, devletin sorumluluğunun doğabileceği durumlara ilişkin bir dizi kural ortaya koymaktadır. Bu kuralların bir kısmı, özel kişilerin haksız fiilleri veya ihmalleri nedeniyle devletin sorumluluğunu açıkça ya da örtülü bir şekilde öngörmektedir.[407]

Taslak Maddeler'in "*Kamu gücü yetkilerini kullanırken bir kişinin ya da bir birimin davranışı"* başlıklı 5.maddesinde devlet dışı aktörlerin devlete ait kamu gücü yetkilerini kullanmaları için yetkilendirilmiş olmaları halinde bu kişilerin fiillerinin devlete isnat edilebileceğini vurgulamaktadır. Bu maddenin Türkçe tercümesi aşağıda verilmiştir:

"Dördüncü madde kapsamında devlet organı olmayan, fakat bu devletin hukuku tarafından kamu gücü yetkilerini kullanmak için yetkilendirilmiş bir kişinin ya da bir birimin davranışı, olayda bu kişi ya da birim bu nitelikte davrandığı sürece, uluslararası hukuka göre bir devlet fiili olarak kabul edilir."[408]

Taslak Maddelerin 5. maddesi, 4. madde kapsamında devlet organı statüsünde olmayan, ancak yine de kamu gücü kullanma yetkisi verilmiş organların eylemlerinin devlete atfedilmesiyle ilgilidir. Bu madde, giderek yaygınlaşan özel sektör kuruluşlarının devlet organlarının yerine kamu gücü yetkisini kullanması olgusunun yanı sıra, devlet şirketlerinin

[406] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 67-68.
[407] Danwood Mzikenge Chirwa, "The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights", *Melbourne Journal of International Law*, 5, (2004), 205-206.
[408] Uluslararası Hukuk Komisyonu (UHK), *International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Türkçeye çeviren Hakkı Hakan Erkiner, *Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu, A/RES/56/83*, 2001.

özelleştirilmesine rağmen belirli kamusal veya düzenleyici işlevlerini sürdürdüğü durumları da dikkate almayı amaçlamaktadır.[409]

Genel bir terim olan "varlık", devlet organı olmamakla birlikte, devletin yasaları tarafından kamu yetkisi unsurlarını kullanmak üzere görevlendirilebilecek çok çeşitli organları ifade etmektedir. Bunlar arasında kamu şirketleri, yarı kamu kuruluşları, çeşitli türlerde kamu kurumları ve bazı durumlarda, özel şirketler yer alabilir; ancak bunların her birinde, varlığın devlet yasaları tarafından olağan olarak devlet organları tarafından yerine getirilen kamusal nitelikteki işlevleri yerine getirmek üzere yetkilendirilmiş olması ve varlığın davranışının ilgili devlet yetkisinin kullanılmasıyla ilgili olması gerekmektedir.[410] Örneğin, bazı ülkelerde özel güvenlik şirketleri, cezaevi görevlisi olarak hizmet vermek üzere sözleşme yapabilir ve bu kapsamda, mahkeme kararı veya cezaevi yönetmeliklerine dayanarak, kamuya ait yetkileri, örneğin gözaltı ve disiplin yetkilerini kullanabilir. Benzer şekilde, özel veya devlete ait hava yollarına, göç kontrolü veya karantina uygulamalarıyla ilgili belirli yetkiler devredilmiş olabilir. İran-ABD Hakemlik Mahkemesi'nde görülen bir davada, devlet tarafından kurulan ve hayır amaçlı mülkleri yöneten özerk bir vakıf, sıkı bir devlet denetimi altında faaliyet göstermekteydi; yetkileri arasında el konulacak malların tespit edilmesi de bulunuyordu. Mahkeme, bu vakfın özel bir kuruluş değil, kamuya ait bir kuruluş olduğunu ve dolayısıyla mahkemenin yargı yetkisine tabi olduğunu tespit etti. Vakfın idaresi altında olduğu iddia edilen kamulaştırılmış mülkiyet bağlamında ise, bu durumun madde 5 kapsamında değerlendirileceği ifade edildi.[411]

Bir varlığın belirli bir hukuk sisteminin kriterlerine göre kamu veya özel olarak sınıflandırılabilmesi, sermayesinde veya daha genel olarak varlıklarının mülkiyetinde az veya çok devlet katılımının bulunması, yürütme kontrolüne tabi olmaması gibi hususlar bu varlığın eylemlerinin devlete atfedilmesi amacıyla belirleyici kriterler değildir. Bunun yerine, 5. madde gerçek ortak özelliğe, yani bu kuruluşların sınırlı bir ölçüde veya belirli bir bağlamda da olsa kamu gücü otoritesinin belirli unsurlarını kullanma yetkisine sahip olduklarına atıfta bulunmaktadır.[412]

---

[409] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 1.
[410] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 1.
[411] Hyatt International Corporation v. The Government of the Islamic Republic of Iran, *Iran-U.S. C.T.R.*, c. 9, 1985, 72, 88-89.
[412] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 3.

Uluslararası hukukta "kısmen veya tamamen devletin sahip olduğu veya yönettiği kuruluş" niteliğindeki varlıkların eylemlerinin devlete atfedilmesinin gerekçesi, ilgili varlığa devletin iç hukuku tarafından belirli unsurlar açısından kamu gücü yetkisini kullanma yetkisinin verilmiş olmasıdır. Bu tür bir varlığın eylemlerinin uluslararası sorumluluk bağlamında devletin bir fiili olarak kabul edilmesi için, eylemin hükümet faaliyetleriyle ilgili olması gerekmektedir; varlığın başka özel veya ticari faaliyetlerle ilgilenmesi durumunda bu eylemler devlete atfedilmez. Örneğin, belirli polis yetkileri verilen bir demiryolu şirketinin bu yetkileri kullanmasına ilişkin eylemleri uluslararası hukukta devletin bir fiili olarak kabul edilirken, bilet satışı veya demiryolu araçlarının satın alınması gibi diğer faaliyetlerine ilişkin eylemleri bu kapsamda değerlendirilmeyecektir.[413]

Madde 5, bir tüzel kişinin davranışının devlete atfedilmesi amacıyla "kamu gücü yetkisinin" kapsamını mutlak olarak belirlemeye çalışmaz. Belirli bir sınırın ötesinde, neyin "kamu gücü" olarak kabul edileceği, belirli bir topluma, onun tarihine ve geleneklerine bağlıdır. Özellikle önemli olan sadece yetkilerin içeriği değil, aynı zamanda bu yetkilerin bir varlığa nasıl verildiği, hangi amaçlarla kullanılacağı ve varlığın bu yetkileri kullanırken hükümete karşı ne ölçüde sorumlu olduğudur. Bunlar esasen genel bir standardın farklı koşullara uygulanmasına ilişkin meselelerdir.[414]

Madde 5'in formülasyonu açıkça iç hukuk tarafından kamu gücü kullanma yetkisine sahip kuruluşlarla sınırlandırılmıştır. Bu 8. maddedeki bir kuruluşun devletin yönlendirmesi veya kontrolü altında hareket ettiği durumlardan ayırt edilmelidir. Madde 5'in amaçları doğrultusunda, bir kuruluşun yetki kullanması bağımsız bir takdir yetkisi veya hareket etme gücü içerse bile bu madde kapsamına girer; davranışın 8. maddedeki gibi devletin kontrolü altında gerçekleştirildiğini göstermeye gerek yoktur. Öte yandan, 5. madde, örneğin iç hukukun meşru müdafaa veya kendi hakkını koruma gibi gerekçelerle belirli bir davranışı yetkilendirdiği veya haklı gösterdiği durumları kapsamaz; yani vatandaşlara veya yerleşik kişilere genel olarak yetki veren veya davranışlarını izinli kılan durumlar bu kapsama girmez. Söz konusu iç hukuk düzenlemesi, davranışı özellikle kamu gücü kullanma yetkisi olarak yetkilendirmiş olmalıdır; topluluğun işlerinin genel düzenlemesi çerçevesinde bir faaliyete izin verilmesi yeterli değildir.[415]

---

[413] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 5.
[414] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 6.
[415] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 7.

Devletin sahip olduğu ve kontrol ettiği şirketlerin veya işletmelerin ilgili devletin uluslararası yükümlülüklerine aykırı hareket etmesi halinde, bu davranışın devlete atfedilebilir olup olmadığı sorusu ortaya çıkmaktadır. Devletin, ister özel bir kanunla ister başka bir şekilde olsun, başlangıçta bir tüzel kişilik kurması, bu tüzel kişiliğin sonraki davranışlarının devlete atfedilmesi için yeterli bir temel değildir. Tüzel kişiler, her ne kadar devlete ait olsalar ve bu anlamda devletin kontrolüne tabi olsalar da, ayrı kuruluşlar olarak kabul edildiklerinden, 5. madde anlamında devlet otoritesinin unsurlarını kullanmadıkları sürece, faaliyetlerini yürütürken davranışları devlete atfedilemez. Öte yandan, şirketin kamu yetkilerini kullandığına veya devletin bir şirketteki mülkiyet payını veya şirket üzerindeki kontrolünü özellikle belirli bir sonuca ulaşmak için kullandığına dair kanıtların bulunduğu durumlarda, söz konusu davranış devlete atfedilmiştir.[416]

2.1.2.3.Madde 8 Bağlamında Devletin Sorumluluğu

Devletin Sorumluluğuna İlişkin Maddelerin 8. maddesi, özel veya devlet dışı kuruluşların davranışlarının devletlere atfedilmesini düzenlemektedir. *"Devletin yönlendirmesi ya da denetimi altında iken davranış"* başlıklı Madde 8'in Türkçe tercümesi aşağıda verilmiştir:

"Bir kişinin ya da bir grup kişinin davranışı, şâyet bu kişi ya da grup bu davranışı yaparken, devletin tâlîmatları, yönlendirmesi ya da denetimi altında ise, uluslararası hukuka göre devletin fiili olarak kabul edilir."

Madde 8'de kullanılan "kişi veya kişi grubu" ifadesi, madde kapsamına giren davranışların ayrı bir tüzel kişiliği olmayan ancak fiili olarak hareket eden bir gruba ait olabileceği gerçeğini yansıtmaktadır. Dolayısıyla, devlet bir şirket gibi bir tüzel kişiliğin davranışına izin verebilirken, tüzel kişiliği olmayan ancak yine de kolektif olarak hareket eden bireyler veya gruplar topluluğuyla da ilgilenebilir.[417]

Bu hüküm devlet dışı aktörlerin fiillerinden dolayı devleti sorumlu tutabilmek için üç bağımsız kriter öngörmektedir. Bunlar *talimat, yönlendirme* ve d*enetim*dir. Devlet dışı aktörün işlediği fiilin bu kriterlerden herhangi birinin dışında kalması halinde devletin uluslararası sorumluluğu doğmayacaktır.[418] Bununla birlikte devletle devlet dışı aktör arasındaki bağın

[416] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 6.
[417] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001), Article 8, para. 9.
[418] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (2001), Article 8, para. 1.

madde 8'de öngörülen isnat kriterlerini aşması halinde devlet dışı aktör devlete "tam bağımlı" hale gelecek, devlet dışı aktör devletin *de facto* bir organı olarak kabul edilecektir. Bu durumda sorumluluk 8. madde kapsamından çıkarılarak 4. madde[419] kapsamında devletin sorumluluğuna gidilecektir. Bu nedenle, devlet aktörlerin fiillerine ilişkin devletin sorumluluğunun tesis edilebilmesi için madde 8'de öngörülen isnat kriterlerin doğru bir şekilde anlaşılması gerekmektedir.

UHK tarafından 8. maddeye ilişkin yapılan yorumda yukarıda verilen üç özerk kriterden herhangi birinin tespit edilmesinin sorumluluk için yeterli olacağı belirtilmiştir. Ancak bu maddeye ilişkin yapılan yorumun geri kalanı oldukça muğlaktır.[420] Her şeyden önce madde 8'in "*Devletin yönlendirmesi ya da denetimi altında iken davranış"* başlığında ilk kritere yer verilmemiştir.[421] Buna ilaveten Yorum üç isnat teriminden herhangi birinin tanımını vermemekte ve "yönlendirme" ve "kontrol" kelimelerini eş anlamlı olarak ele almaktadır.

Yorum'da üç kriteri bir araya getirme eğilimi oldukça yaygındır. Yorum dışındaki kullanımlarında bile bu üç terimin birbirinin yerine kullanıldığı görülmektedir. Örneğin, Oxford İngilizce Sözlüğü "yönlendirme" terimini tanımlamak için "talimat",[422] "kontrol" terimini tanımlamak için "yönlendirme" terimini kullanmaktadır.[423]

Sorumluluk bahsini çalışan yazarların birçoğu da bu kriterleri karıştırma eğilimi içerisinde olmuşlardır. Bu durum çoğunlukla "yönlendirme" ve "kontrol" kavramlarıyla ilgilidir. UHK tarafından yapılan bu muğlak yaklaşım, Crawford'un eserlerine de yansımıştır. Crawford, devlet sorumluluğu üzerine yazdığı monografide, mahkemelerin ve hakemlerin "yönlendirme" veya "kontrol" terimlerini tek bir atıf standardı yorumlama eğiliminde olduklarını belirterek bu karışıklığı haklı göstermeye çalışmıştır.[424] Ancak monografi bu görüşü

---

[419] Taslak Maddelerin "*Devlet organlarının davranışları"* başlıklı 4.maddesinin Türkçe tercümesi aşağıdaki gibidir: 1. Uluslararası hukuka göre, bir organ, ister yasamaya, yürütmeye, yargıya ilişkin ya da ister başkaca işlevleri yerine getiriyor olsun, bunun devlet örgütlenmesi içindeki durumu ne olursa olsun, ister merkezî idare içinde, ister bir yerel idare niteliğinde olsun, bütün devlet organlarının davranışları devletin bir fiili olarak kabul edilir. 2. Organ, iç hukuka göre bu statüye sahip her kişi ya da birimi kapsar. Uluslararası Hukuk Komisyonu, *Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu (Draft Articles on Responsibility of States for Internationally Wrongful Acts)*, Türkçeye çeviren: Hakan Hakkı Erkiner, 2001, madde 4.

[420] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8.

[421] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8.

[422] *Oxford English Dictionary (OED)*, "Direction", "with a and plural: An instruction how to proceed or act; an order to be carried out, a precept", erişim: 26 Kasım 2024, https://www.oed.com/search/dictionary/?scope=Entries&q=direction&tl=true.

[423] *Oxford English Dictionary (OED)*, "Control", "The fact or power of directing and regulating the actions of people or things; direction, management; command", erişim: 26 Kasım 2024, https://www.oed.com/search/dictionary/?scope=Entries&q=control.

[424] James Crawford, *State Responsibility: The General Part* (Cambridge: Cambridge University Press, 2013), 229-230.

destekleyecek hiçbir davaya atıfta bulunmamıştır. Aşağıda isnat kriterleri her biri müstakil başlık altında incelenmiştir.

2.1.2.3.1. Talimat

Üç kriterden ilki uyarınca, bir devlet, devlet dışı bir aktöre talimatlar vererek bir davranışta bulunmasını talep eder. Bu terim, bir devletin belirli bir eylemde bulunmaya karar verdiğini ve bunu kendi adına yapması için devlet dışı bir kuruluşa talimat vermesini ifade eder. Bu türden bir devlet dışı kuruluş, iç hukuk tarafından devlet otoritesinin unsurlarını kullanma yetkisine sahip olmamalıdır, çünkü bu durumda davranışı Devletin Sorumluluğuna ilişkin Taslak Maddelerin 5. Maddesi kapsamına girecektir.[425]

Madde 8 kapsamında talimatlara göre hareket eden kişi ve kuruluşlardan kasıt devlet tarafından "yardımcılar" olarak istihdam edilen veya belirli görevle görevlendirilen "gönüllüler" olarak üçüncü devletlere gönderilen resmi devlet yapıları dışındaki bireyler anlaşılabilir.[426] Bu kriterin oluşabilmesi için devletin söz konusu davranışı gerçekleştirmeye karar verdiği anda devlet dışı varlığın fiilen devlete tabi olması gerekir. Bu tabi olma durumu basitçe talimatları kabul etme ve ardından bu talimatlara göre hareket etme olgusuyla doğrulanabilir. Bununla birlikte UAD'nın Soykırım davasında belirttiği gibi, talimatlar özellikle "iddia edilen ihlallerin gerçekleştiği her bir operasyonla ilgili olarak" verilmelidir.[427]

Benzer şekilde, devlet ve özel aktör tarafından paylaşılan ortak bir hedefin olması, ikisi arasındaki bağlılığı ve birincisinin ikincisine talimat verdiğini ortaya koyan başka kanıtlar olmadan yeterli değildir. Ortak hedefler siyasi uyumu gösterebilir ve dolayısıyla siyasi atıf için yeterli olabilirken, aynı şey hukuki sorumluluğun tesisi için söylenemez.

Sorumluluğun oluşabilmesi ortaya çıkan fiil, somut unsurları itibariyle talimat veren devlete kadar izlenebilir olmalıdır. Bu, devletin üstlenen fiilin tüm ayrıntılarını tam olarak belirtmesi gerektiği anlamına gelmez. Aksine, kasıtlı olarak muğlak talimatlar verirse, bunlar devletin ortaya çıkan davranış biçiminden sorumlu olmasına yol açacaktır. Bununla birlikte, talimatlar ne kadar açık bir şekilde ifade edilmiş olursa olsun, devlet hukuka aykırı davranışa müsaade etme iradesini ortaya koymalıdır. Örneğin, 1979 İran Devrimi bağlamında, Ayetullah

[425] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5, para 7.
[426] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 2.
[427] International Court of Justice (ICJ), *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, 26 February 2007, para. 400.

Humeyni, Şah'ın geri dönüşünü gerçekleştirmek için İran gençliğine "ABD ve İsrail'e karşı saldırılarını tüm güçleriyle genişletmeleri" çağrısında bulunmuştur.[428] UAD daha sonra Tahran Rehineleri davasında bu genel çağrının "Devletin ABD Büyükelçiliğini işgal etme ve ele geçirme gibi özel bir operasyona girişme yetkisi verdiği" şeklinde yorumlanamayacağına karar vermiştir.[429] Ayetullah'ın açıklaması, kışkırtıcı olsa bile, İran Devleti'nin elçiliği işgal etmeye yönelik özel bir arzusunun tezahürünü içermemektedir.

Bir devlet, verdiği talimatları aşan veya bu talimatların ötesine geçen fiillerden dolayı sorumluluktan kaçınamaz. Uluslararası hukuk uyarınca, devletin *de jure* ya da *de facto* organları tarafından yetki sınırlarını aşarak gerçekleştirilen (*ultra vires*) eylemler, bu kişi veya birimler devletin organı ve iradesinin bir yansıması olarak kabul edildiği için, genel olarak devlete isnat edilir. Eylemin ultra vires olması, devletin sorumluluğunu ortadan kaldırmaz. Bu ilke, yukarıda yer verildiği üzere Taslak Maddeler'inin 7. maddesinde açık bir biçimde düzenlenmiştir. İlgili madde, yetkisini aşan organların fiillerinin devlete isnat edileceğini ve uluslararası sorumluluğa yol açabileceğini hükme bağlamaktadır. Bu bağlamda örneğin, bir devlet, ağlarının risk ve güvenliğine ilişkin tek seferlik bir değerlendirme yapılması görevini özel bir şirkete devrederse ve bu şirketin çalışanları yetkilerini aşarak bu erişimi başka bir devlete karşı siber saldırı düzenlemek için kullanırsa, bu fiilden dolayı devreden devlet tamamen sorumluluktan kurtulamaz. Zira bu kişiler, devletin organı ya da ajanı sıfatıyla hareket ettiklerinden, fiilleri devletin fiili sayılır. Ancak devlet, bu tür *ultra vires* eylemleri önlemek için makul tüm önlemleri aldığını ya da söz konusu eylemleri açıkça yönlendirdiğini veya onayladığını gösterebilirse, bu durum sorumluluğun kapsamını veya niteliğini etkileyebilir.[430] Genel olarak, bir devlet, kendi organı olmayan bireylere yasal talimatlar verdiğinde, bu talimatların uluslararası hukuka aykırı bir şekilde yerine getirilmesi halinde sorumlu olmayacaktır. Ancak, kişiler veya kişi grupları bir devletin etkin kontrolü altında hareket ettiklerinde, belirli talimatlara uyulmamış olsa bile, eylemlerin devlete atfedilmesi için gereken koşullar sağlanmış olur. Bu durumda, söz konusu eylem, devletin kontrolü altında gerçekleşmiş sayılır ve 8. Madde uyarınca devlete atfedilir.[431]

---

[428] International Court of Justice, *United States Diplomatic and Consular Staff in Tehran (Tehran Hostages) (Judgment), ICJ Reports 1980*, 3, parag. 59.
[429] International Court of Justice, *United States Diplomatic and Consular Staff in Tehran (Tehran Hostages) (Judgment)*, parag. 59.
[430] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 8.
[431] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 8.

2.1.2.3.2. Yönlendirme

Yönlendirme kriteri sorumluluk bahsiyle ilgili akademik kaynaklarda belki de diğer iki standart arasında en az incelenmiş olanıdır. Ancak, bu koşulun tarihsel gelişimi incelendiğinde, bu tür bir sınıflandırmanın yanlış olduğu ve bu terimin özerk bir anlama sahip olduğu görülmektedir. Yönlendirme teriminin tam olarak neyi içerdiği literatürde ve uluslararası içtihatta cevapsız kalmaktadır. Bundan dolayı aşağıdaki satırlar önce somut bir kavramsallaştırma geliştirmeyi amaçlamaktadır.

8. madde bağlamında "yönlendirme" kavramının anlamı üzerinde durulan çok az sayıdaki uluslararası davadan biri UAD nezdindeki[432] *Soykırım Davası'*dır.[433] Sözlü savunmalarında, Bosna Hersek adına savunma yapan Alain Pellet, "yönlendirme" terimini talimat teriminden "daha az titiz bir terim" olarak tanımlamıştır. Bu tanımlamaya yargılama sırasında itiraz edilmemiştir.[434] Divan nihai kararında, "Devletin bir organının, haksız fiilin faillerinin hareket etmesini sağlayan talimatı vermesi halinde" yönlendirme kriterinin karşılandığına karar vermiştir. Divan tarafından kullanılan bu ifade, devlet ile söz konusu devlet dışı aktör arasında, basit bir talimatın ötesine geçen ve başka bir şekilde sürdürülmeyen devamlı bir ilişkiye ihtiyaç duyulduğunu ima etmektedir.

Crawford genel olarak yönlendirme ve kontrolü tek bir standart olarak ele alsa da,[435] UAD'nin yukarıda alıntılanan açıklamasından farklı olmayan bir öneride bulunmuştur. "Yönlendirme"nin devam eden bir talimat sürecini veya devlet ile devlet dışı bir kişi arasında ima yoluyla sorumluluğa yol açabilecek bir ilişkiyi işaret ettiğini belirtmiştir. Bu görüşe göre eğer bir devlet resmi organları dışında kişi veya kişi grupları ile bir tabiiyet ilişkisi geliştirir ve bu tür özel aktörlerin davranışlarına rehberlik ederse, bu tür aktörlerin bireysel fiillerinden, bu fiilleri işlemeleri için açık bir talimat olmasa dahi, sorumlu olabilir.

Bu tür bir ast-üst ilişkisinin varlığı farklı şekillerde kanıtlanabilir. US-DRAMS raporunda, Dünya Ticaret Örgütü (DTÖ) Temyiz Organı, çoğu durumda "özel bir kuruluşun yönlendirilmesinin" genellikle "bir tür tehdit veya teşvik" ile kanıtlanabileceğine karar

[432] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Judgment), ICJ Reports 2007*, 43.
[433] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Judgment)*, 43.
[434] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Judgment)*, 396–412.
[435] Crawford, *State Responsibility*, 146.

vermiştir.[436] Bu yaklaşımın burada da kullanılabilir, çünkü hukuki anlamda "yönlendirme"nin varlığını, yönlendiren taraf ile yönlendirilen taraf arasında bulunan ve birincisinden ikincisine doğru tehdit ya da teşvik yoluyla aktarılan bir ast-üst ilişkisinin varlığıyla teyit etmektedir.

2.1.2.3.3. Kontrol

Atıf için madde 8'deki son atıf kriteri, devlet dışı kuruluşların bir devletin "kontrolü" altında hareket ettiği durumlarla ilgilidir. "Kontrol" terimi özerk bir anlama sahiptir, bunu önceki iki kriterden herhangi biriyle eşitlemek yanlış olacaktır.[437]

Her devlet kendi ülkesi üzerindeki egemenliğinin bir sonucu olarak "ülkesinde işlenen özel fiilleri kontrol etme kapasitesine" sahiptir. Ancak, devletin kendi ülkesi üzerinde kontrol sahibi olması, orada işlenen her hukuka aykırı fiili bilmesi gerektiği veya hatta bilmesi gerekebileceği anlamına gelmez.[438] Coğrafi yakınlık veya konumdan kaynaklanan kontrol potansiyeli de atıfta bulunma amaçları doğrultusunda yeterli değildir. Dolayısıyla, devlet ile devlet dışı aktör arasında fiili bir kontrol ilişkisi olmalıdır.

UAD tarafından Bosna Soykırımı Kararı kararında belirtildiği üzere, bir devletin bir devlet dışı aktör üzerindeki kontrol derecesi istisnai düzeyde yüksek olup, söz konusu aktör devletin talimatı dışında bağımsız hareket etme kapasitesine sahip değilse, diğer bir ifadeyle devlete tam bir bağımlılık içinde faaliyet gösteriyorsa, bu durumda devlet ile devlet dışı aktör arasındaki ilişki artık madde 8 kapsamında bir yönlendirme veya denetim ilişkisi olarak değil, devletin de facto bir organı olarak değerlendirilmektedir. Bu tür özel durumlarda, devlet dışı aktörün eylemleri, Taslak Maddeler'in 4. maddesi uyarınca doğrudan devlete atfedilir.[439]

Fakat bu yaklaşım, sadece tam bağımlılık ve fonksiyonel birliktelik koşullarının varlığı hâlinde geçerlidir. UAD, bu ayrımı özellikle Nicaragua ve Bosna davalarında netleştirmiştir. Her ne kadar bir aktörün devletten etkileniyor olması veya bazı eylemlerinin devlet tarafından yönlendirilmesi onun otomatik olarak madde 4 kapsamında değerlendirilmesini sağlamasa da, tam bağımlılık içinde olan yapılar, artık "devlet dışı" değil, devletin bir uzantısı olarak kabul edilmektedir. Bu nedenle, bu tür durumlar, devletin de jure organları (madde 4) ile devlet dışı

---

[436] World Trade Organization, *United States—Countervailing Duty Investigation on Dynamic Random Access Memory Semiconductors (DRAMS) from Korea, Report of the Appellate Body (27 June 2005), WT/DS296/AB/R*, parag. 116.

[437] Kubo Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility", *Journal of Conflict and Security Law*, 21/3 (2016), 420-421.

[438] International Court of Justice, *Corfu Channel Case (United Kingdom v. Albania) (Merits)*, ICJ Reports 1949, 4, 18.

[439] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits*, Judgment of 27 June 1986, I.C.J. Reports 1986, 14.

olup kamu yetkisi kullanan kişi ya da kuruluşlar (madde 5) arasındaki ayrımın ötesinde, doğrudan devletin yapısına fiilen entegre olmuş birimler olarak görülmekte ve devletin uluslararası sorumluluğunu doğurmaktadır.[440]

Yukarı da ifade edildiği üzere, uluslararası içtihatta, özellikle son otuz yılda, devlet dışı aktörlerin eylemlerinin devlete atfı bağlamında iki farklı kontrol testi öne çıkmış ve zaman zaman birbirleriyle yarışan yorumlara konu olmuştur. İlk olarak, UAD Nikaragua davasında[441] "etkin kontrol" testini formüle etmiş ve Bosna Soykırımı davasında yeniden benimsemiştir. İkinci olarak, EYICM Temyiz Dairesi Tadić davasında "genel kontrol" testine rakip olduğu varsayılan bir test önermiştir.[442] Bu nedenle bu iki test bazen sırasıyla "Nikaragua testi" ve "Tadić testi" olarak da anılmaktadır.[443] Ancak, iki test arasında yapıldığı varsayılan seçimin aslında yanlış bir ikilem olduğu ileri sürülmektedir. Bu bakış açısının nedenlerini ortaya koymadan önce, her iki testin unsurlarını incelemek gerekmektedir.

Etkin kontrol testini oluşabilmesi için devletin devlet dışı aktörü desteklemekten daha fazlasını yapması gerekir, örneğin devlet dışı aktörü "finanse etmek, organize etmek, eğitmek, tedarik etmek veya donatmak" gibi. Etkin kontrolün oluşabilmesi için ayrıca devletin operasyonları planlaması, hedefleri seçmesi ve operasyonel destek sağlaması gerekir. Devlet operasyonların planlanmasında, hedeflerin seçilmesinde ve operasyonel desteğin sağlanmasında aktif olarak yer almalıdır. Başka bir deyişle, devlet operasyonun başlatılmasını, yürütülmesini ve sonuçlandırılmasını kontrol edebilmelidir. Bu, potansiyel olarak her haksız fiil üzerinde kontrol gerektirmez, daha ziyade bu tür fiillerin işlendiği daha geniş bir eylem süreci üzerinde kontrol gerektirir.[444] Bununla birlikte, Uluslararası Adalet Divanı'nın (UAD) bu standardı uyguladığı ve her ikisi de olumsuz bir bulguyla sonuçlanan iki önemli davanın da gösterdiği gibi,[445] bu karşılanması gereken yüksek bir eşiktir.

Etkin kontrol testinin oluşabilmesi için, devletin devlet dışı aktörü desteklemenin ötesine geçmesi gerekir; bu destek ister "finanse, örgütleme, eğitim, tedarik veya donatma" şeklinde olsun.[446] Devlet operasyonların planlanmasında, hedeflerin seçilmesinde ve

---

[440] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Judgment)*, 393.
[441] International Court of Justice, *Nicaragua v. United States of America (Merits), Judgment*, ICJ Reports 1986, 14, parag. 33.
[442] International Criminal Tribunal for the former Yugoslavia, *Prosecutor v. Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, Case No. IT-94-1, Appeals Chamber, 2 October 1995, para. 112.
[443] Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility", 420-421.
[444]Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility", 420-421.
[445]Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility", 421.
[446] International Court of Justice, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) (Judgment)*, ICJ Reports 2005, 116, para. 160.

operasyonel desteğin sağlanmasında yer almalıdır.[447] Kısacası, "operasyonun başlangıcını, yürütülme şeklini ve sonunu kontrol edebilmelidir."[448] Bu özellikle her bir olası haksız fiil üzerinde kontrol gerektirmez, sadece bu tür fiillerin işlenebileceği daha geniş bir hareket tarzı üzerinde kontrol gerektirir.[449] Bununla birlikte, UAD tarafından bu standardın uygulandığı iki önemli davanın her ikisinin de olumsuz sonuçlanmasından da anlaşılacağı üzere, gerçek dünyada bile bu çok yüksek bir standarttır.[450]

Öte yandan, genel kontrol testi, Eski Yugoslavya Uluslararası Ceza Mahkemesi (EYCIM) tarafından *Tadić* davasında, "daha düşük bir kontrol derecesi" gerektiren bir test olarak önerilmiştir. Bu test, sonraki içtihatlarla gelişmiş ve *Prlić* kararıyla nihai halini almıştır.[451] Buna göre, genel kontrolün sağlanabilmesi için söz konusu devletin: a) Devlet dışı oluşuma mali ve eğitim yardımı sağlaması, askeri teçhizat temin etmesi ve/veya operasyonel destek sunması, b) Söz konusu oluşumun operasyonlarının organizasyonuna, koordinasyonuna veya planlanmasına katılması, gerekmektedir. Bu iki unsur-yani temel olarak destek ve koordinasyon- yukarıda ele alınan etkin kontrol standardına göre kesinlikle daha az katı bir yaklaşımı temsil etmektedir.

Ancak, bu iki testin, 8. madde kapsamında atıfta bulunulması amacıyla gerekli kontrol standardının iki bağımsız alternatifi anlamına gelmediği ileri sürülmektedir. Bunun en az iki temel nedeni vardır. İlk olarak, EYCIM'nin kendisi bu testin kullanımını sadece organize silahlı gruplarla açıkça sınırlandırmış ve -daha müsamahakâr yaklaşımı altında bile- etkin kontrol testinin "askeri yapılar halinde organize olmayan bireyler veya gruplar" açısından hala geçerli olacağını vurgulamıştır.[452]

İkinci olarak ve çok daha önemli bir şekilde, EYICM Temyiz Dairesi, görünüşte isnat amacıyla geçerli kontrol standardını gözden geçirmeyi ve değiştirmeyi amaçlamış olsa da, aslında devletin sorumluluğu ile ilgili bir meseleye girip girmemesi gerektiği şüphelidir. *Tadić* davasında Temyiz Dairesi'nin ele aldığı mesele, suçlamada belirtilen suçların işlendiği

---

[447] International Court of Justice, *Nicaragua v. United States of America (Merits)*, parag. 112.
[448] Stefan Talmon, "The Responsibility of Outside Powers for Acts of Secessionist Entities", *International and Comparative Law Quarterly* 58/3 (2009), 503.
[449] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, para. 115.
[450] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, ICJ Reports 2007, para. 400.
[451] *Prosecutor v. Kordić and Čerkez*, *Trial Judgment*, IT-95-14/2-T, 26 Şubat 2001, para. 115; *Prosecutor v. Kordić and Čerkez*, *Appeal Judgment*, IT-95-14/2-A, 17 Aralık 2004, para. 36; *Prosecutor v. Nalić and Martinović*, *Trial Judgment*, IT-98-34-T, 31 Mart 2003, para. 198; *Prosecutor v. Tadić*, *Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, IT-94-1-AR72, 2 Ekim 1995, para. 132; Antonio Cassese, *International Law* (Oxford: Oxford University Press, 2005), 657.
[452] Mačák, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility", 422.

dönemde Bosna'daki silahlı çatışmanın hukuki niteliğiydi. Daire, dışarıdan bir devletin, başka bir devlete karşı o devletin topraklarında savaşan bir silahlı grubu kontrol etmesi durumunda, bu çatışmanın uluslararası nitelik kazanacağına karar vermiştir. Ayrıca, uluslararası insancıl hukukun, bir grup bireyin bir devletin kontrolü altında hareket edip etmediğini belirlemek için özel bir kriter sunmadığına da karar vermiştir. Bu nedenle, geçerli *lex specialis* (*özel kural)* kurallarının uygulanabilir olmadığı algısıyla, genel uluslararası hukukta yer alan devlet sorumluluğu normlarını içeren *lex generalis* (*genel kuralı*)'e başvurmuştur.

Ancak, uluslararası insancıl hukukun, devlet sorumluluğu hukukunun *lex specialis*'i olmadığı belirtilmektedir.[453] EYICM'nin analizi, uluslararası hukukun birincil ve ikincil kuralları arasındaki farkın yanlış anlaşılmasından kaynaklanmaktadır. Bir silahlı çatışmanın niteliği, *uluslararası insancıl hukuk* kurallarıyla belirlenirken, devlet sorumluluğu, uluslararası yükümlülüklerin ihlali ve sonuçlarıyla ilgili ikincil kurallarla düzenlenir. Bu nedenle, EYICM'nin önerdiği "genel kontrol" testi, 8. Maddeye uygun kontrol derecesini belirlemek için yeterli değildir.[454] Bu sebeplerle, UAD Bosna Soykırımı davasında bu testi reddetmiştir.[455]

Etkin kontrol testi, 8. maddede belirtilen son kriterin amaçları açısından doğru bir standart olsa da, bu testin siber uzayın gerçeklikleri gibi modern sorunlarla giderek daha az ilgili hale gelmesinin geçerli sebepleri vardır. İlk olarak, devletin uluslararası sorumluluğu hukukunun gelişiminde genel eğilim, daha esnek isnat kurallarına doğru bir yönelim göstermektedir. Bu eğilim, 8. maddenin olgunlaşmasında da kendini göstermiştir; özel raportör Ago'nun "özel suçlama" (yani fiili talimatlar) şeklindeki dar anlayışından, talimatlar, yönlendirme ve kontrolü kapsayan üçlü yapıya doğru bir genişleme olmuştur. Bu genişleyen yaklaşım, belirli hukuk alanlarının evrimini şekillendirmiştir; özellikle terörle mücadele rejimi buna önemli bir örnektir.[456] Bu görüşe göre, bu gelişme, ABD'nin 11 Eylül saldırılarına verdiği tepkinin genel olarak kabul görmesiyle birlikte, "barındırma" veya "destekleme" gibi daha gevşek atıf standartlarının ortaya çıkmasına yol açmıştır. Bununla birlikte, terörle mücadele tedbirlerine dair bu argümanın geçerliliği ne kadar önemli olsa da, siber uzaydaki

[453] Marko Milanović, "State Responsibility for Genocide", *European Journal of International Law* 17/3 (2006), 553-604, https://doi.org/10.1093/ejil/chl019, 553, 587.
[454] Dapo Akande, "Classification of Armed Conflicts: Relevant Legal Concepts", in *International Law and the Classification of Conflicts*, chapter 3 (Oxford: Oxford University Press, 2012), 59–60.
[455] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Judgment)*, 403-406.
[456] Derek Jinks, "State Responsibility for the Acts of Private Armed Groups", *Chicago Journal of International Law* 4/1 (2003), 88-90.

operasyonlarla ilgili benzer gevşek standartların ortaya çıktığını gösteren bir devlet uygulaması henüz bulunmamaktadır.[457]

İkinci olarak, UHK'nin yaklaşımı, belirli durumlarda daha liberal bir testin uygulanmasına olanak tanıyor gibi görünmektedir. Başka bir deyişle, etkin kontrol testi genel olarak geçerli bir kontrol standardı olsa da, bazı durumlar veya bağlamlar daha esnek bir testin kullanılmasını gerektirebilir. UHK'nin yorumlarının dikkatlice incelenmesi, Komisyonun *Nikaragua* testinin istisnasız olarak uygulanmasını şart koşmadığını, aynı zamanda *Tadic* testini tamamen reddetmediğini göstermektedir.[458] Bunun yerine, ikinci teste ilişkin paragrafın sonunda yer alan son derece dolambaçlı bir ifadeyle, bağlama dayalı bir esnekliğe kapı aralamıştır. Bu ifadede, "belirli bir davranışın bir devletin kontrolü altında olup olmadığının ve kontrol edilen davranışın o devlete atfedilip atfedilemeyeceğinin, her bir olay özelinde değerlendirilmesi gereken bir mesele" olduğunu belirtmiştir.[459] Bu temelde, testin katılığının "içeriğe bağlı" olduğu [460] veya "özel durumlarda" çıtanın düşürülebileceği iddia edilmiştir.[461]

Üçüncü olarak, *Nikaragua* testinin, o dönemde doğru bir karar olsa da, sanal dünyada gerçekleşen siber saldırıların modern gerçekliğinden çok uzak olduğu savunulmaktadır. Bu bağlamda, siber uzaydaki operasyonların ortaya çıkardığı zorluklar, Tim Berners-Lee'nin gelecekte *World Wide Web*'in temellerini atmasından üç yıl önce müzakerelerini tamamlayan UAD tarafından öngörülemezdi.[462] Bu durum, *Nikaragua* testinin çevrimdışı dünyada geçerli olmasına rağmen, kontrol kavramının siber alanda yeniden gözden geçirilmesi gerektiğini göstermektedir.[463] Bu görüşü savunanlar, etkin kontrol testi altında "devletlerin bilgi savaşları operasyonlarını gizlemelerinin çok kolay olduğunu" iddia etmektedirler. Sonuç olarak, "genel kontrol standardına benzer daha esnek bir yaklaşımın" siber güvenliği artıracağı öne sürülmektedir.

---

[457] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia: 2014) 92.
[458] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 4-5.
[459] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 5.
[460] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution", *Journal of Conflict & Security Law* 17/2 (2012), 229, 238-239.
[461]Tullio Treves, "International Courts and Tribunals: Alternatives to Treaty Making", *Developments of International Law in Treaty Making*, ed. Rüdiger Wolfrum ve Volker Röben (Springer, 2005), 600.
[462] Tim Berners-Lee, "Information Management: A Proposal", *Internal Memo* (CERN, Mart 1989), 5, http://cds.cern.ch/record/1405411/files/ARCH-WWW-4-010.pdf, erişim tarihi: 28 Kasım 2024.
[463] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations* (Cambridge University Press, 2014), 292.

2.1.2.4.De Facto Organ Yaklaşımının Mahkeme Kararlarına Yansıması

Roberto Ago tarafından geliştirilen de facto organ kavramı, daha sonra Uluslararası Adalet Divanı (UAD) tarafından *Tahran Rehineler Davası*'nda ve ardından *Nikaragua Askeri ve Paramiliter Faaliyetler Davası*'nda uygulanmıştır. Bununla birlikte, Divan söz konusu teoriyi ana hatlarıyla benimsemiş ve kendi özel yorumu doğrultusunda uygulamıştır. Bu durum, Divan'ın kararlarında kullandığı mantık ve dilin tartışmaya açık olduğunu göstermektedir.[464]

De facto organ kavramı açısından Tahran Rehineler Davası, son derece önemli bir yere sahiptir. Bu davada Uluslararası Adalet Divanı (UAD), ABD Büyükelçiliğine yapılan saldırıların ve olayların ilk aşamasındaki eylemlerin hiçbirinin İran'a atfedilemeyeceğine hükmetmiştir. Divan, bu karara varırken Uluslararası Hukuk Komisyonu'nun (UHK) Taslak Madde 8 (8)'nın yorumuna bağlı kalmıştır; buna göre devlet organları, özel kişileri belirli eylemlere teşvik edebilir. Bu bağlamda Divan'a göre, Büyükelçiliğe saldıran kişiler, İran devletinin resmi ajanları veya organları statüsüne sahip olmayan militanlardı. Söz konusu militanların eylemlerinin doğrudan İran'a atfedilebilmesi için, İran'ın yetkili bir organı tarafından görevlendirilmeleri ve İran devleti adına hareket ettiklerinin kanıtlanması gerekir. Bu yaklaşımda Divan, açıkça UHK tarafından tanımlanan de facto organ kavramına dayanmakta; yani belirli bir görevi yerine getirmek üzere görevlendirilen ve bu görevi devletin kışkırtmasıyla yerine getiren kişiler de facto organ olarak kabul edilmektedir.[465]

2.1.2.4.1. Genel Kontrol Testi

De facto organ kuramına ilişkin bir diğer önemli yargı kararı, Eski Yugoslavya için Uluslararası Ceza Mahkemesi'nin (EYİCM) *Tadić* Kararıdır. Bu kararda Mahkeme, de facto organların varlığına ve bunların tespitinde uygulanacak ölçütlere doğrudan atıfta bulunmuş, ayrıca kararın farklı bölümlerinde de facto organ kavramını sıkça kullanmıştır.[466]

Eski Yugoslavya Uluslararası Ceza Mahkemesi (EYİCM) İlk Derece Yargılama Dairesi, 1997 tarihli *Tadić* Kararı'nda, silahlı grupların bir devletin fiilî (de facto) ajanı olarak nitelendirilip nitelendirilemeyeceğini değerlendirirken, Uluslararası Adalet Divanı'nın (UAD)

---

[464] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 68.
[465] *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgement of 24 May 1980, para. 58, http://wwiw.icj-cij.org/docket/index.php?p1=3&p2=3&k=c9&case=64&code=usir&p3=4.
[466] Uluslararası Ceza Mahkemesi Eski Yugoslavya için Uluslararası Ceza Mahkemesi (ICTY), *Prosecutor v. Duško Tadić*, IT-94-1-A, Karar, 15 Temmuz 1999.

Nikaragua davasında benimsediği kriterleri esas almıştır. [467] Bu çerçevede Daire, devlet ile silahlı gruplar arasında bir vekâlet ilişkisi kurulabilmesi için gerekli olan otorite/kontrol ve bağımlılık unsurlarının mevcut olup olmadığını incelemiştir. Daire'ye göre, silahlı grupların faaliyetleri için devletten sağladıkları desteğe bağımlı olmaları tek başına yeterli değildir; devletin, bu bağımlılıktan doğan kontrol yetkisini fiilen kullanması da gereklidir.[468] Bu yaklaşımıyla Daire, UAD'nin *Nikaragua Kararı*'nda ortaya koyduğu isnat edilebilirlik kriterlerini iki ayrı unsur olarak değil, aynı testin birbirini tamamlayan iki öğesi şeklinde yorumlamıştır.[469]

Bununla birlikte, 1999 yılında davayı inceleyen EYİCM Temyiz Dairesi, *Nikaragua* kararında geliştirilen ve devlet ile silahlı gruplar arasındaki ilişkinin yoğunluğunu belirlemek amacıyla kullanılan bağımlılık ve bu bağımlılıktan doğan kontrol kriterlerine dayalı "etkin kontrol" eşiğini oldukça katı bulmuş ve İlk Derece Dairesi'nin bu doğrultudaki yorumunu kabul etmemiştir. Temyiz Dairesi'ne göre etkin kontrol testi, devlet sorumluluğu hukukunun işleviyle bağdaşmamaktadır. Zira bu hukukun amacı, devletlerin resmi organları aracılığıyla yürütülmesi uygun görülmeyen ya da yürütülmesi mümkün olmayan faaliyetleri özel kişi ve gruplara devrederek uluslararası sorumluluktan kaçınmalarını engellemektir.[470] Temyiz Dairesi bu noktada şu tespitte bulunmuştur: "Özel kişilerin fiillerinin devletlere atfedilebilirliğine ilişkin uluslararası hukuk ilkeleri tek tip ve katı kriterlere dayanmamaktadır... Uluslararası hukukun aradığı şart, devletin bu kişiler üzerinde kontrol sahibi olmasıdır. Bu kontrolün derecesi ise her davanın kendine özgü koşullarına bağlıdır."[471] Dolayısıyla, *Nikaragua* kararında öngörülen etkin kontrol testi tek ve her şeyi kapsayan bir standart olarak kabul edilemez; zira devletler ile uluslararası yargı organlarının uygulamaları, daha düşük düzeyde bir kontrolün varlığı halinde dahi devletin sorumlu tutulabileceğini göstermektedir.[472]

Dolayısıyla Temyiz Dairesi, özel kişi veya grupların fiillerinin devlete atfedilmesi bakımından yalnızca Uluslararası Adalet Divanı'nın (UAD) *Nikaragua* kararında uyguladığı

---

[467] Gregory Townsend, "State Responsibility for Acts of De Facto Agents", *Arizona Journal of International and Comparative Law* 14 (1997), 641.
[468] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic aka Dule, IT-94-1-T, Judgment and Opinion of 7 May 1997*, 207, 588, erişim: 19 Kasım 2024, http://www.icty.org/x/cases/tadic/tjug/en/tad-ts705070T2-¢.pdf.
[469] Crawford, *State Responsibility: The General Part*, 151.
[470] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 43-45, para. 108-111, erişim: 19 Kasım 2024, http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf.
[471] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 43-45, para. 116-117.
[472] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*4, 3-45, para.124.

etkin kontrol testini esas almış görünmektedir. Bununla birlikte Temyiz Dairesi, *Nikaragua* kararında UAD tarafından kısmen karma bir yaklaşımla ele alınan tam bağımlılık ve talimat/etkin kontrol testlerini birbirinden bağımsız testler olarak değil, tek bir etkin kontrol ölçütünün ayrıntılandırılması olarak yorumlamıştır.[473]

Temyiz Dairesi'ne göre, etkin kontrol kriteri kendi içinde farklı koşullara göre uygulanabilecek üç ayrı test barındırmaktadır. Bu bağlamda, örgütlenmemiş bireylerin fiilleri ile hiyerarşik bir yapı içerisindeki devlet dışı silahlı grupların faaliyetlerinin devlete atfedilebilmesi için farklı ölçütler uygulanmalıdır. Devlet dışı aktörlerin eylemlerinin devlete isnadı iki temel kategoriye ayrılmaktadır. İlk kategoride, devletin bu eylemler için doğrudan talimat vermesi ve etkin kontrol sağlaması şarttır.[474] İkinci kategoride ise, hiyerarşik bir yapıya sahip silahlı grupların fiillerinin devlete isnadı için devletin bu gruplar üzerinde genel bir kontrol yetkisine sahip olması yeterlidir.[475] Genel kontrolün varlığı için yalnızca askeri veya mali destek sağlanması yeterli görülmemekte; bunun yanında devletin grubun askeri faaliyetlerinin genel planlamasına katkıda bulunması veya bu planlamayı koordine etmesi aranmaktadır.[476]Ancak bu, her bir operasyonun yönetilmesi veya detaylı talimat verilmesi anlamına gelmemektedir.[477] Cassese'ye göre, devletin sağladığı kapsamlı destek ile grubun hiyerarşik örgütlenmesi, devletin bu grubun faaliyetlerinin planlanması ve organizasyonu üzerinde belirleyici bir otoriteye sahip olduğuna işaret etmektedir. Bu ise, söz konusu grupların eylemlerinin devlet otoritesi altında gerçekleştiği yönünde bir değerlendirme yapılmasına imkân tanımaktadır.[478]

Genel kontrol kriteri, devlet ile devlet dışı aktör arasındaki otorite ilişkisinin oldukça düşük bir yoğunluk seviyesinde bulunmasını yeterli görmektedir. Temyiz Dairesi'ne göre, bu kriter kapsamında devletin isnat edilen eylemle doğrudan bağlantısının bulunması yahut devlet dışı aktörün belirli bir düzeyde devletin otoritesi altında hareket etmesi zorunlu değildir. Ayrıca, devletin özel bir yapı üzerindeki otoritesine dayanarak belirli bir eylem için açık talimat vermesi

[473] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 43-45, para.112-114.
[474] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 48, para.118.
[475] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 49-50, para.120-125
[476] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 56, para.130-131.
[477] Uluslararası Ceza Mahkemesi Eski Yugoslavya İçin (ICTY), *Prosecutor v. Dusko Tadic, IT-94-1-A, Judgment of 15 July 1999*, 59, para.137.
[478] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 76-77.

veya genel bir yönlendirmede bulunması da bu kriterin sağlanması açısından gerekli görülmemektedir.[479]

Crawford, bir devletin örgütlü bir devlet dışı aktör grubu üzerinde tam kontrole sahip olması halinde, bu grubun faaliyetlerinin ayrıca incelenmesine gerek bulunmadığını belirtmektedir. Buna karşılık, tam kontrolün mevcut olmadığı durumlarda, mahkemelerin veya uluslararası yargı organlarının her bir eylemi ayrı ayrı değerlendirmesi gerektiğini ifade etmektedir. Ancak *Tadiç Kararı*'nda temyiz dairesi, tam kontrol yerine daha düşük bir eşik olan genel kontrol kriterini benimsemiş ve bu yaklaşım, devlet organları ile devlet organı olmayanlar arasındaki ayrımı en azından isnat edilebilirlik bakımından büyük ölçüde anlamsız hale getirmiştir.[480]

1986–1997 yılları arasında uluslararası yargı organları, özel kişi ve grupların fiillerinin devlete isnat edilebilmesi hususunda Uluslararası Hukuk Komisyonu'nun (UHK) eski 8 (a) maddesine dayalı olmakla birlikte farklı ve çoğu kez muğlak testler geliştirmiştir. Bu testler, devletin sorumluluğu bakımından yeknesak ve tutarlı bir standart ortaya koymaktan uzak kalmıştır. Ancak 2001 yılında, UHK raportörü James Crawford tarafından hazırlanan ve kabul edilen taslak maddelerin nihai versiyonunda, eski 8 (a) maddesi köklü biçimde yeniden formüle edilmiştir. Nihai 8. maddeye göre, bir kişi veya grubun fiili, devletin talimatı, yönlendirmesi veya kontrolü altında gerçekleştirilmişse devlete isnat edilebilir.[481] Bu değişiklikle birlikte, orijinal taslaktaki "devletin hesabına hareket eden kişiler" ibaresi terk edilmiş ve yerine talimat ile etkin kontrol esaslı bir test benimsenmiştir. Söz konusu dönüşüm, özellikle Uluslararası Adalet Divanı'nın *Tahran Rehineler Davası* ile *Nikaragua* Kararı'nda geliştirdiği içtihatlardan etkilenmiştir. Böylece Crawford'un öncülüğünde hazırlanan nihai metin, devlet sorumluluğuna ilişkin daha açık, sistematik ve öngörülebilir bir çerçeve sunmayı hedeflemiştir.

Nihai taslaktaki 8. madde, özel kişi ve grupların fiillerinin devlete isnat edilebilmesi için orijinal taslaktaki "devlet tarafından teşvik edilme" kriterini içtihatlarla uyumlu hale getirerek netleştirmiş ve üç somut kriter çerçevesinde formüle etmiştir. Buna göre, devletin talimatları, direktifleri veya kontrolü altında gerçekleştirilen eylemler devlete isnat edilebilecektir ve bu unsurların her biri tek başına yeterli kabul edilmektedir. Maddeye eklenen yorumda, devletin özel kişilere belirli bir eylem için doğrudan talimat vermesi açık ve kolay saptanabilir bir durum olarak görülürken; direktifler veya kontrol altında gerçekleşen eylemlerin daha karmaşık

[479] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 77.
[480] J Crawford, *International Law*, 152.
[481] James Crawford, *Les Articles de la C.D.I. sur la Responsabilité de l'État* (Paris: Pédone, 2004), 130.

hukuki sorunlar doğurabileceği vurgulanmıştır. Özellikle "kontrol" kriterinin kapsamı konusunda önemli bir belirsizlik bulunduğu ifade edilmektedir. Cassese'ye göre, 'kontrol uygulamak', kişi üzerinde bir güç veya otoriteye sahip olmak anlamına gelir; ancak bu otoritenin kapsamı ve yoğunluğu uluslararası hukuk bakımından net olarak belirlenmemiştir. Talimat ve yönlendirme kriterlerinin dışında bırakılması halinde, bir devletin eylemler üzerinde kontrol uygulayıp uygulamadığının hangi ölçütlere göre belirleneceği sorusu ortaya çıkmaktadır. UHK'nun kabul ettiği test bu belirsizliğe açık bir çözüm sunmamaktadır. Nitekim Crawford da 8. maddenin yorumunda, her bir eylemin devletin kontrolü altında olup olmadığının ve bu kontrol derecesinin devlete isnadı gerektirip gerektirmediğinin somut olayın koşullarına göre değerlendirileceğini belirterek söz konusu belirsizliği teyit etmektedir.[482]

2.1.2.4.2. Etkin Kontrol Testi

Uluslararası Adalet Divanı (UAD), 1986 tarihli Nikaragua'da Askeri ve Paramiliter Faaliyetler Davası'nda de *facto organ* kavramını dolaylı biçimde de olsa kapsamlı şekilde ele almıştır. Divan, söz konusu kararında, özel kişi ve grupların eylemlerinin devlete isnat edilip edilemeyeceğini iki farklı açıdan incelemiştir.[483]

Divan, kararında, hukuka aykırı eylemlerde bulunan düzensiz grupların bir devletten fiilen bağımsız olmadığı ve kadrolarının söz konusu devlet tarafından oluşturulup, organize edilip komuta edildiği durumlarda, bu grupların eylemlerinin devlete atfedilmesinin, artık yalnızca eylemlere katılım veya teşvik gibi mekanizmalarla açıklanamayacağını vurgulamıştır.[484] Gerçekten de Divan, ABD tarafından "oluşturulduğu" ve komuta edildiği ima edilen UCLA (*Unilaterally Controlled Latino Assets*) gruplarına ilişkin değerlendirmesinde, söz konusu devletin, bu oluşumların varlıkları ve operasyonel yetenekleri tamamen ABD'ye bağlı olmak kaydıyla, eylemlerine genel talimatlar vermesi veya eylemlerinin planlanması ve desteklenmesine genel düzeyde katılım sağlaması durumunda, söz konusu hukuka aykırı eylemlerin ABD'ye atfedilmesini yeterli görmüştür.[485]

---

[482] Crawford, *Les Articles de la C.D.I. sur la Responsabilité de l'État*, 133.
[483] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 69.
[484] Uluslararası Adalet Divanı (UAD), *Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986*, para. 114, erişim: 19 Kasım 2024, http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=66&case=70&code=nus&p3=4.
[485] Uluslararası Adalet Divanı (UAD), *Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986*, para. 75-86.

Bu davada UAD, Nikaragua'da faaliyet gösteren rejim karşıtı "kontralar" ile ABD arasındaki ilişkinin, bir taraftan kontralar bakımından bağımlılık, diğer taraftan ise ABD bakımından kontralar üzerinde otorite olup olmadığını ortaya koyması gerektiğini belirtmiştir.[486] Bu bağlamda, vekillik testi olarak bilinen bağımlılık ve kontrol kriteri, devlet ile kendi organları arasında var olan müvekkil-vekil ilişkisinin, devlet ile devlet organı olmayan kişiler arasında da mevcut olup olmadığını; silahlı grupların devletin organı olarak kabul edilip edilemeyeceğini, vekilin müvekkile bağımlılığını, onun nam ve hesabına hareket etmesini ve bu bağımlılıktan kaynaklanan müvekkilin vekil üzerindeki yetki ve kontrolünü tespit etmeyi amaçlamaktadır. Divan, kontralar ile ABD arasındaki bağımlılık ve kontrol ilişkisini, ABD'nin kontra kuvvetlerinin liderlerini seçmesi, işe alması ve onlara ödeme yapmasının yanı sıra organizasyon, eğitim, teçhizat temini, operasyonların planlanması, hedeflerin belirlenmesi ve operasyonel desteğin sağlanması gibi unsurlar üzerinden değerlendirebileceğini ifade etmiştir. Divan'a göre bu ilişkinin belirlenmesindeki temel amaç, söz konusu silahlı grubun kendisini örgütlediği, finanse ettiği ve komuta ettiği iddia edilen ABD'den gerçek anlamda bağımsız olup olmadığını tespit etmektir.[487]

Kontraların faaliyetlerini ABD'ye atfetmenin gerekçelerini detaylı şekilde inceleyen Divan, somut davanın koşullarında şu sonuca ulaşmıştır: "ABD'nin Nikaragua'da faaliyet gösteren kontralara sağladığı geniş çaplı desteğe rağmen, kontraların tüm faaliyetleri üzerinde ABD adına hareket ettiklerini kabul ettirecek derecede bir yetkiye sahip oldukları açıkça ortaya konulamaz. ABD'nin kontralara yönelik katılımı ve hatta kendisine son derece bağımlı bir güç üzerindeki genel kontrolü, ek kanıtlar yoksa, insan hakları veya insancıl hukuk ihlali teşkil eden eylemlerin ABD tarafından emredildiği veya dayatıldığı anlamına gelmez."[488] Bu değerlendirme sonucunda Divan, kontra kuvvetlerinin tamamen ABD'ye bağımlı ve onun yetki ve talimatlarına tabi bir örgüt olmadığını tespit etmiş; dolayısıyla, belirli bir bağımsızlığa sahip bu kuvvetlerin faaliyetlerinin tamamının ABD'ye atfedilemeyeceği sonucuna varmıştır.[489]

Bununla birlikte, Divan etkin kontrol kriterini alternatif bir yaklaşım olarak ortaya koymuş ve söz konusu eylemlerin başka yollarla ABD'ye atfedilebileceğini belirtmiştir. Divan'a göre, "Amerika Birleşik Devletleri'nin sorumluluğunun doğabilmesi için, ilke olarak, bu hukuk ihlallerinin gerçekleştiği askeri ve paramiliter operasyonlar üzerinde etkin bir

[486] Uluslararası Adalet Divanı (UAD), *Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986*, para. 109.
[487] Uluslararası Adalet Divanı (UAD), *Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986*, para. 114.
[488] Uluslararası Adalet Divanı (UAD), *Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986*, para. 114.
[489] James Crawford, *State Responsibility, The General Part,* 148.

kontrole sahip olduğunun kanıtlanması gerekir."[490] Bu değerlendirmeyi yaparken Divan, BM Genel Kurulu'nun 3314 (XXIX) sayılı Kararı'nın 3(g) maddesini kapsamlı bir biçimde incelemiştir. Söz konusu hüküm, Türkçeye çevrildiğinde şu şekildedir: "Bir devlet tarafından veya bir devlet adına, diğer bir devlete karşı yukarıda listesi verilen fiillere varan veya o ölçekte olan silahlı kuvvet fiillerini icra eden silahlı çetelerin, grupların, gayri nizami askerlerin veya paralı askerlerin gönderilmesi veya bu gibi fiillere önemli ölçüde karışılması."[491]

Söz konusu hükümden anlaşılacağı üzere, bir devletin düzenli silahlı kuvvetlerini göndermeksizin, silahlı çeteler, gruplar, düzensiz unsurlar veya paralı askerleri başka bir devlete karşı silahlı saldırı gerçekleştirmek üzere sevk etmesi ya da bu tür eylemlere kayda değer düzeyde katılım göstermesi, silahlı saldırı kapsamında değerlendirilir. Bu düzenleme, dolaylı yollarla, yani vekil unsurlar aracılığıyla gerçekleştirilen saldırı biçimlerini de kapsayacak şekilde getirilmiştir.[492]

Uluslararası Adalet Divanı, 3(g) maddesinin örf-adet hukukuna dayanan bir ilkeyi yansıttığını kabul etmiş ve vekil aktörler aracılığıyla gerçekleştirilen silahlı saldırıların, uygun koşullar altında bir devlete atfedilebilir nitelikte saldırı fiilini teşkil edebileceğini belirtmiştir. Bununla birlikte, Divan yalnızca mali destek sağlanmasının, lojistik veya istihbarat desteği verilmesinin tek başına silahlı saldırı eşiğini aşmaya yetmeyeceğini; ancak bir devletin silahlı grupları doğrudan sevk etmesi veya onların saldırı niteliğindeki eylemlerine önemli düzeyde katılım göstermesi hâlinde bu eylemlerin 3(g) maddesi kapsamında saldırganlık sayılabileceğini vurgulamıştır. Bu değerlendirmede Divan, gerçekleştirilen eylemlerin ölçeği ve etkilerinin, düzenli silahlı kuvvetler tarafından gerçekleştirilen klasik bir saldırı ile karşılaştırılabilir nitelikte olması gerektiğinin altını çizmiştir.[493]

Divan, somut olayda Amerika Birleşik Devletleri'nin Nikaragua'daki kontralara eğitim, mali kaynak ve silah sağlayarak önemli ölçüde destek verdiğini tespit etmiştir; ancak bu desteğin, ABD tarafından doğrudan gerçekleştirilen bir silahlı saldırı olarak nitelendirilemeyeceği sonucuna varmıştır. Bununla birlikte, Divan, söz konusu desteğin silahlı grupların gönderilmesi veya onların saldırı niteliğindeki eylemlerine anlamlı düzeyde katılım

[490] Uluslararası Adalet Divanı (UAD), *Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986*, para. 109 -116.
[491] Birleşmiş Milletler Enformasyon Merkezi (UNIC-Ankara), *Saldırı'nın (Tecavüzün) Tanımı: Birleşmiş Milletler Genel Kurulu'nun 3314 (XXIX) sayılı ve 1974 Tarihli Kararı* (Ankara: Birleşmiş Milletler Enformasyon Merkezi, 2002).
[492] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Lahey: Uluslararası Adalet Divanı, 1986).
[493] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Lahey: Uluslararası Adalet Divanı, 1986).

göstermesi durumunda, 3(g) maddesi kapsamında bu eylemlerin saldırganlık teşkil edeceğini belirtmiştir.[494]

Divan tarafından yapılan bu değerlendirme, devletlerin etkili biçimde kontrol ettiği veya önemli ölçüde destek verdiği devlet dışı silahlı aktörlerce gerçekleştirilen düşmanca eylemler karşısında devlet sorumluluğu anlayışını geliştirmiş ve böylece vekil aktörler aracılığıyla yürütülen saldırganlık faaliyetlerinin hukuki denetimden kaçmasının önlenmesine katkı sağlamıştır.[495]

Uluslararası Hukuk Komisyonu (UHK) tarafından hazırlanan 2001 tarihli Taslak Maddeler'in 8 (a) maddesi ve bu maddenin yorumunda yer alan kriterlerle tam olarak uyumlu değildir. Esas itibariyle Divan, UHK'nın "devlet adına hareket eden özel kişi ve kişi gruplarının eylemlerinin devlet eylemi olarak kabul edileceği" şeklindeki nispeten basit ifadesi yerine, devlet tarafından oluşturulmayan devlet dışı özel grupların hukuka aykırı faaliyetlerinin devlete atfedilebilmesi için bu gruplar ile devlet arasında "bağımlılık ve otorite" ile kısmi bir bağımlılık ve otorite ilişkisini somutlaştıran "etkin kontrol" kriterlerine dayalı iki test uygulamaktadır. Ancak doktrin, Komisyon'un özel kişi gruplarını belirli bir görevi veya fiili yerine getirmeye kışkırtma/teşvik etme ifadesinin zımnen devlet ile özel kişiler arasında bir otorite ilişkisini içerdiğini; dolayısıyla Divan'ın belirli bir fiilin yerine getirilmesini emretme ve dayatma ifadelerine özgü otorite ve bağımlılık ilişkisinin de aslında devlet sorumluluğu hukukunda de facto organ teorisinin hem teoride hem de pratikte bir bütünlük teşkil ettiğini ifade etmektedir.[496]

2.1.2.4.3. Kontrol Testlerinin Karşılaştırılması

Uluslararası Adalet Divanı (UAD), 2007 tarihli *"Soykırımın Engellenmesi Konvansiyonunun Uygulanması"* davasında, devletin de facto organlarının veya ajanlarının faaliyetlerinden doğan sorumluluğu yeniden ele almış ve 1986 tarihli Nikaragua davası çerçevesinde doktrinde tartışılan isnat kriterlerini açıklığa kavuşturmuştur. Divan'a göre, "de facto organ" terimi, hukuken devlet organı olmayan ancak devlete sıkı bir şekilde bağlı ve kontrol altında bulunan kişi ve grupları ifade etmektedir. Nikaragua davasında belirtilen "tam

[494] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Lahey: Uluslararası Adalet Divanı, 1986).
[495] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (Lahey: Uluslararası Adalet Divanı, 1986).
[496] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 72-73.

bağımlılık" kriteri uyarınca, bu aktörlerin devletle ilişkisi o kadar yakın ve yoğun olmalıdır ki, onları devlete ait kabul etmek mümkün olsun. Tam bağımlılık yalnızca maddi ve finansal destekle sınırlı olmayıp, aynı zamanda hangi eylemlerin, ne zaman ve nasıl gerçekleştirileceğine dair karar süreçlerinde devletin belirleyici olmasını da kapsamaktadır. Bu bağlamda, devlet dışı aktörlerin gerçek anlamda otonom olmaması, yani bağımsız bir hareket serbestisinden yoksun olması gerekmektedir.[497]

Divan, özel kişiler ve grupların faaliyetlerinin devlete atfedilmesinde, bu aktörlerin devletin resmi (de jure) organlarıyla arasında tam bir bağımlılık ilişkisi bulunmasa bile, devletin talimatları, yönlendirmesi veya sıkı kontrolü altında hareket ettikleri takdirde devlet sorumluluğunun doğabileceğini vurgulamıştır. Ancak Divan, de facto organ kavramını ve buna ilişkin isnadı değerlendirirken, UHK tarafından de facto organlar için geliştirilmiş olan kapsamlı çerçeve yerine, Devletin Sorumluluğuna İlişkin Madde 4'ü referans almıştır. Oysa UHK'nin 1971–2001 döneminde şekillenen taslaklarında, de facto organ kuramı Madde 8(a) kapsamında ele alınmış ve devlet dışı aktörlerin devlete atfedilebilirliğini somut kriterlerle belirleyen bir yapı geliştirilmiştir. Divan'ın Madde 4'ü esas alması, hem teorik hem de uygulamalı açıdan bazı tutarsızlıklar yaratmış; özellikle devlet organları ile devlet dışı aktörler arasındaki sınırın belirlenmesinde ve isnat kriterlerinin uygulanmasında belirsizlikler doğurmuştur. Bu yaklaşım, devlet sorumluluğu hukukunda de facto organ kuramının bütüncül ve sistematik çerçevesi ile Divan uygulamaları arasındaki uyumsuzluğu açıkça ortaya koymaktadır.[498]

2001'de kabul edilen Nihai Taslak Metin'te Madde 8, de facto organ kavramını içermemekte olup, organ tanımı yalnızca Madde 4 kapsamında yapılmaktadır. Bu durum, doktrinde de vurgulandığı üzere, Madde 8'in de facto organ teorisini kapsamadığını ortaya koymaktadır. Bu nedenle, doktrinde de facto organ kavramı çoğu zaman UAD'nin Nikaragua davasında benimsenen dar anlamının ötesinde daha geniş bir şekilde kullanılmakla birlikte, kavramın kesin bir tanımı bulunmadığından anlamı çoğu zaman muğlaktır. Öte yandan, Nikaragua kararında öne çıkan "tam bağımlılık" kriteri ne UHK'nin 1996 taslağında ne de 2001'deki nihai metinde benimsenmiş; bunun yerine UHK, Madde 4(2) uyarınca, iç hukukta organ statüsü tanınmasa dahi, devletin geniş organ tanımı çerçevesinde bu kişi ve grupların eylemlerinin devlete isnat edilebileceğini öngörmüştür. Bu yaklaşım, devlet sorumluluğu

[497] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 79.
[498] Uluslararası Adalet Divanı, *Bosna-Hersek-Sırbistan ve Karadağ Davası (Soykırım Suçunun Önlenmesi ve Cezalandırılması Sözleşmesi)*, 26 Şubat 2007 tarihli karar, paragraf 391- 397, http://www.icj-cij.org/docket/files/91/13685.pdf.

hukukunda de facto organ teorisinin belirsizliklerini korumakla birlikte, devlet dışı aktörlerin eylemlerinin devlete atfedilmesi için esnek bir çerçeve sunmaktadır.[499]

Crawford'un yorumlarına göre, UAD içtihatlarında de facto organ kavramı, yalnızca devletin tam bağımlılığı altında bulunan kişi ve gruplarla ilişkilendirilmekte; devlet dışı aktörlerin ise yalnızca devletin de jure organlarına yakın bir ilişki içinde olmaları hâlinde de facto organ kabul edilebileceği vurgulanmaktadır. Bu bağlamda, Ago'nun Taslak Madde 8(a) kapsamında geliştirilen de facto organ kuramının, Madde 4 çerçevesinde ele alınması, hem teorik açıdan daha tutarlı hem de uygulamada daha kapsayıcı bir çözüm sunmaktadır.

Divan, Soykırımın Önlenmesi Davası'nda, Nikaragua kararındaki yaklaşımı esas almış, ancak devletin talimatı veya kontrolü altındaki kişilerin de facto organ olarak değerlendirilmemesi yönündeki anlayışın tartışmalı unsurlar içerdiğini ortaya koymuştur. Bu yaklaşım, faillerin devletle olan bağını yeterince açıklayamamakta ve sorumluluğun kapsamını daraltmaktadır. Divan, özel kişiler ve grupların devletin de facto organları olup olmadığını belirlemek için Madde 8'in üç kriterinden oluşan testi uygulamış; bunlar arasında özellikle "etkin kontrol" kriterinin, uluslararası hukukta sorumluluğun tespiti bakımından doğru ve ölçütlü bir yaklaşımı yansıttığını vurgulamıştır. Bunun aksine, EYİCM'nin "genel kontrol" yaklaşımının, devlet sorumluluğu ile devlet organlarının eylemleri arasındaki bağlantıyı zayıflattığı ve uluslararası sorumluluk normlarıyla uyumsuz olduğu Divan tarafından ifade edilmiştir.

De facto organ kavramı doktrinde, UAD tarafından kullanılan dar kapsamın ötesinde daha geniş bir biçimde yorumlanmakla birlikte, kavramın net bir tanımı bulunmamaktadır. Nikaragua davasında öne sürülen "tam bağımlılık" standardı, yüksek bir ispat eşiği getirmesi nedeniyle uygulamada sınırlı bir etki göstermektedir. Milanović ve bazı diğer hukukçular, UAD'nin de facto organ kuramını, devlet dışı aktörlerin yalnızca istisnai durumlarda, devletin iradesini icra eden araçlar olarak kabul edildiği özel bir yaklaşım olarak değerlendirmektedir. Bu bağlamda, devlet dışı aktörlerin eylemlerinin devlete isnadı, yalnızca doğrudan talimat, etkin kontrol veya denetim unsurlarına dayandırıldığında mümkün olmakta; aksi hâlde, sorumluluğun ortaya çıkması güçleşmekte ve bu durum devletlerin sorumluluktan kaçmasına zemin hazırlamaktadır.[500]

[499] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 81.
[500] Marko Milanovic, "State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plücken", *Leiden Journal of International Law*, 22, 2009, 307-324, 312.

De facto organ kuramında, özel kişi ve grupların yalnızca devlete her alanda tam bağımlılık hâlinde faaliyet göstermesi gerektiği yönündeki yorum, gereksiz bir kriter eklemesi olarak değerlendirilmektedir. 2001 tarihli Taslak Maddeler'in 8. maddesi, talimat verme ve yönlendirme unsurlarını zaten devletin otoritesine tabi olmayı içermektedir. Bu nedenle, ayrı bir tam bağımlılık kriteri oluşturmanın gerekliliği ve yerindeliği, özellikle içtihatta bu kuramın uygulanmasına dair somut örneklerin bulunmadığı dikkate alındığında tartışmalıdır.[501] UHK Taslak Maddeleri hazırlanırken, tam bağımlılık ve de facto organ kavramları açısından kapsamlı ve kesin bir çerçeve geliştirilmemiş; devlet dışı aktörlerin devletle ilişkisi kontrollü ve somut olay bazında değerlendirilmiştir. Bu yaklaşım, devletin sorumluluğunu daha gerçekçi biçimde ele almakta ve uluslararası uygulamayla uyumlu bir çerçeve sunmaktadır.

Özetle, özel kişi ve grupların devletin de facto organı olarak kabulü, Uluslararası Adalet Divanı'nın Soykırım Davası ve Nikaragua davasında ortaya koyduğu yüksek bağımlılık ve etkin kontrol kriterlerine dayanmaktadır. Bu kriterler, teorik tartışmalara konu olsa da, devlet sorumluluğu hukukunda hâlen temel bir referans noktası olarak kabul edilmektedir.

Özel kişi ve grupların eylemlerinin devletin de facto organ kuramı çerçevesinde devlete atfedilmesi, Divan'ın Soykırım davasındaki kararı ve bazı doktrin yazarlarına göre, Devletin Uluslararası Sorumluluğuna İlişkin Taslak Maddeler'in 4. maddesi kapsamında ele alınmaktadır. Bu bağlamda, söz konusu kişiler ve gruplar de facto veya de jure ayrımı yapılmaksızın devletin bir organı olarak kabul edilmekte ve dolayısıyla 8. madde kapsamında değil, doğrudan 4. madde uyarınca değerlendirilir. Bu yaklaşım, yalnızca teorik bir ayrım olmayıp, devlet sorumluluğu hukuku bakımından önemli sonuçlar doğurmaktadır.[502]

Devletin organları, kendilerine tanınan devlet otoritesini kullanarak yetkilerini aşar veya verilen talimatlara aykırı hareket ederlerse (*ultra* vires *eylemler*), bu fiiller Devletin Uluslararası Sorumluluğuna İlişkin Taslak Maddeler'in 7. maddesi uyarınca doğrudan devlete isnat edilir. Bu çerçevede, Divan'ın Soykırım davasında benimsediği şekilde de facto organ kuramı, devletin de jure organlarının eylemlerinden doğan sorumluluğunu düzenleyen 4. madde kapsamında ele alınırsa, bu organların devlet otoritesi çerçevesinde gerçekleştirdikleri tüm eylemler —hukuka aykırı olsalar dahi— devletin sorumluluğunu doğuracaktır. Dolayısıyla de facto organlar bakımından da de jure organlara uygulanan isnat kuralları geçerli olacaktır.[503]

[501] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 85-86.
[502] Milanovic, "State Responsibility for Acts of Non-State Actors", 313.
[503] Crawford, *State Responsibility*, 126.

Bu durum, Taslak Maddeler'in 4, 5 ve 6. maddelerinde yer alan atıf kuramları bakımından geçerli olmakla birlikte, 8. madde kapsamında özel bir düzenlemeye tabidir. Devletin yalnızca özel kişilere belirli bir eylemi gerçekleştirmeleri yönünde talimat vermesi veya onları yönlendirmesi yeterli değildir; bu kişilerin gerçekleştirdiği eylemler, ancak devlet tarafından etkin biçimde kontrol ediliyorsa devlete isnat edilebilir. Bu bağlamda, devletin etkin denetimi altında hareket eden özel aktörlerin *ultra vires* niteliğindeki fiilleri dahi 8. madde kapsamında devlete atfedilebilir.[504] Milanovic'in de belirttiği üzere, burada tartışma konusu olan husus, *ultra vires* eylemlerin 8. madde kapsamında hareket eden özel kişi ve gruplara atfedilip atfedilemeyeceği değil; bu tür eylemlerin devlete isnat edilebilmesi için gerekli olan ispat eşiğinin son derece yüksek olmasıdır. Söz konusu yüksek ispat standardı ise uygulamada ciddi güçlükler doğurmaktadır.[505]

Doktrinde ve Uluslararası Hukuk Komisyonu'nun Devletin Sorumluluğuna İlişkin Taslak Maddeler'in hazırlanma sürecinde, tam bağımlılık ilkesine dayalı ve devletin de jure organlarıyla tamamen eşdeğer kabul edilen bir de *facto organ* kuramının geliştirilmesi uygun bulunmamaktadır. Devlet sorumluluğu hukuku açısından *de facto* organlar teorisi; devlet dışı aktörlerin, devletin talimatı, yönlendirmesi veya denetimi altında hareket etmeleri çerçevesinde değerlendirilmelidir. Bu yaklaşım, hem öğretide hem de Komisyon'un uzun süredir benimsediği genel anlayışla örtüşmektedir. Dolayısıyla *de facto* organların Taslak Maddeler'in 4. maddesinde yer alan *de jure* organlarla kategorik olarak eşdeğer sayılması yerine, her somut olayın koşullarına göre değerlendirme yapılmasına ve bu çerçevede daha esnek kriterler içeren 8. madde kapsamında ele alınmasına imkân tanınması daha yerinde olacaktır. Bu yaklaşım, uluslararası hukukun genel sistematiği ve devletlerin fiilî uygulamalarıyla daha uyumludur.[506]

2.2. Atfın Teorik Temelleri

2.2.1. Özel Fiillerin Atfedilmemesi İlkesi

Bir devletin uluslararası sorumluluğu, icrai fiil veya ihmal yoluyla gerçekleştirilen bir davranış uluslararası hukuka göre devlete atfedilebiliyor ve devletin bir uluslararası yükümlülüğünü ihlal ediyorsa doğar. Bu durumda, söz konusu davranış devletin uluslararası

[504] Crawford, *Les Articles de la C.D.I. sur la Responsabilité de l'Etat*, 130, para. 9.
[505] Milanovic, "State Responsibility for Acts of Non-State Actors", 314.
[506] Kurtdarcan, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin *De Facto* Organı Kavramı Üzerine Kısa Bir Değerlendirme", 84.

haksız fiili olarak kabul edilir.[507] UHK Taslak Maddelerinin 2. maddesinde açıkça ifade edilen bu temel ilke, Uluslararası Daimi Adalet Divanı,[508]Uluslararası Adalet Divanı[509] ve devletin sorumluluğuna ilişkin önde gelen birçok çalışmada defalarca teyit edilmiştir.[510]

Devletin uluslararası hukuk sorumluluğu, resmi organları veya temsilcileri aracılığıyla gerçekleştirilen hukuka aykırı fiillerle ortaya çıkar. Geleneksel bakış açısına göre, devletin özel kişilerin fiillerinden doğrudan sorumluluğu, yalnızca bu kişilerin devlet adına hareket ettiği kabul edildiği durumlarda söz konusu olur.

Uluslararası sorumluluk bağlamında devlet yalnızca kendi haksız fiillerinden hukuken sorumlu olduğundan, devletle ilgisi olmayan özel kişilerin davranışları devletin sorumluluğunu tetikleyemez; bu, özel kişilerin fiillerinin devlete atfedilemeyeceğine dair genel ilkedir. Bu ilke, *de jure* ve *de facto* temsilcileri aracılığıyla faaliyet gösteren devletlerin uluslararası düzeyde hak ve yükümlülüklerin birincil taşıyıcıları olarak algılanmasından kaynaklanmakta ve uluslararası hukuk sistemi açısından önemli sonuçlar doğurmaktadır.

2.2.2. Kolektif Sorumluluk Teorisi

Orta Çağ'da devletin uluslararası sorumluluğu bağlamında kabul edilen görüş, kökenlerini Roma hukukundaki *jus gentium*'a dayanan feodal kolektif sorumluluk kavramlarından almaktaydı.[511] Buna göre, bir grup, üyeleri tarafından işlenen fiillerden doğrudan sorumlu tutuluyordu.[512] Uluslararası hukukun oluşum sürecinde, devlet organları tarafından gerçekleştirilen haksız bir fiil nedeniyle o devlete karşı misilleme yapılmasına izin veren bir misilleme doktrini benimsenmiştir. Bu yaklaşım, devlet organı tarafından

---

[507] Hakkı Hakan Erkiner (çev.), *Uluslararası Haksız Fiilden Ötürü Devletin Uluslararası Sorumluluğu*, aslı: *International Law Commission, Report of the International Law Commission on the Work of its Fifty-Third Session, 23 April - 1 June and 2 July - 10 August 2001, Official Records of the General Assembly, Fifty-Sixth Session, Supplement No.10, vol. II(2), 2001*.

[508] *Uluslararası Daimi Adalet Divanı, Phosphates in Morocco Davası, Ön İtirazlar (1938), PCIJ (Ser. A/B) No. 74, 10 (14 Haziran), 28.*

[509] *Uluslararası Adalet Divanı, United States Diplomatic and Consular Staff in Tehran (ABD v. İran)*, [1980] ICJ Rep 3 (24 Mayıs), 29; *Military and Paramilitary Activities in and against Nicaragua (Nikaragua v. ABD)*, [1986] ICJ Rep 14 (27 Haziran), 117–18; *Case Concerning the Gabčíkovo–Nagymaros Project (Macaristan v. Slovakya)*, [1997] ICJ 7 (25 Eylül), 54.

[510] Clyde Eagleton, *The Responsibility of States in International Law* (New York: NYU Press, 1928), 6–7; Ian Brownlie, *System of the Law of Nations: State Responsibility Part I* (Oxford: Clarendon Press, 1983), 23; James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge: CUP, 2002), 4.

[511] Jan Hessbruegge, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law", *New York University Journal of International Law and Politics* 36/4 (2004), 276-79.

[512] EJ de Aréchaga, "International Responsibility", *Manual of Public International Law*, ed. M. Sørensen (New York, NY: St Martin's Press, 1968), 531- 558.

gerçekleştirilen haksız fiili kolektif unsurun fiili olarak kabul etmekte ve karşı önlem alınmasını haklı kılmaktaydı.[513]

Sonraki dönem hukukçuları, bu yaklaşımı yumuşatarak, devletin tüm özel kişilerin davranışlarından kaynaklanan zararlardan sorumlu olduğunu ileri sürmüşlerdir. William Hall gibi hukukçular daha katı bir sorumluluk teorisi benimseyerek, "bir devletin kendi ülkesinde gerçekleşen tüm eylem ve ihmallerden mutlaka sorumlu olduğunu" savunmuş; ancak devletin kendi kusuru bulunmadığı durumlarda bu sorumluluktan kurtulabileceğini öne sürmüşlerdir.[514] Clyde Eagleton ise devletin "birey bir fiil gerçekleştirdiği andan itibaren sorumlu olması gerektiğini" ileri sürerken, iç hukuk yollarının bu sorumluluğu ortadan kaldırmak için bir araç olarak hizmet edeceğini belirtmiştir.[515]

Devletlerin egemen eşitliği ilkesinden önce var olan kolektif sorumluluk doktrininden, özel kişilerin fiillerinin devlete atfedilemeyeceği ilkesine doğru kayış, kademeli ancak belirgin bir şekilde gerçekleşmiştir. Bu atfedilemezlik ilkesi, Hugo Grotius tarafından uluslararası alanda öne çıkarılmış ve hukuki sorumluluğun kusura dayandığı kavramlardan ilham almıştır. Kolektif, tıpkı birey gibi, kendi kusuru ortaya konmadan sorumlu tutulamazdı.

Son dönemlerde, özel kişilerin verdikleri zararlardan sorumlu tutulmayı öngören "Mutlak veya Katı Devlet Sorumluluğu" teorisi, uluslararası hukukta ve uygulamada, önceki kolektif sorumluluk doktrinlerini anımsatacak şekilde ortaya çıkmıştır. Uzay faaliyetlerinden nükleer testlere ve çevresel zararlara kadar uzanan çeşitli alanlarda, akademisyenler ve devletler, devletin kusurlu davrandığına dair kanıtlara bağlı olmaksızın bir sorumluluk doktrinini savunmuş veya kabul etmişlerdir.[516]

Ancak bu teoriler kural değil, istisnadır. İç hukukta benzerlerine paralel olarak, mutlak veya kesin sorumluluk teorisi öncelikle aşırı tehlikeli faaliyetler için maddi tazminat sağlama amacıyla, genellikle ekonomi politikası ve "risk tahsisi" gerekçeleriyle savunulmaktadır.[517] Daha da önemlisi, hâkim görüşe göre, bu durumlarda dahi devlet genellikle özel zarardan

---

[513] Lauterpacht (ed.), *The Collected Papers of Hersch Lauterpacht*, 3 (Cambridge: Cambridge University Press, 1970), 251, 258; FV García Amador, "Fifth Report on State Responsibility", *Yearbook of the International Law Commission* 2 (1960): 41, UN Doc A/CN.4/125, 61.

[514] We Hall, *A Treatise on International Law*, 2. bs. (Oxford: Clarendon Press, 1884), 193.

[515] Clyde Eagleton, "Measure of Damages in International Law", *Yale Law Journal* 39 (1929-30): 52, 56; Roy Emerson Curtis, "The Law of Hostile Expeditions as Applied by the United States", *The American Journal of International Law* 8/1 (Ocak 1914), 1-37, 35.

[516] Hersch Lauterpacht, "The Subjects of International Law," içinde *International Law. Being the Collected Papers of Hersch Lauterpacht, Volume I: The General Works*, der. E. Lauterpacht (Cambridge: Cambridge University Press, 1970), 136–50; akt. Andrea Bianchi (ed.), *Non-State Actors and International Law* (Londra: Routledge, 2009), 1. Bs. 50.

[517] Hersch Lauterpacht, "The Subjects of International Law", *International Law. Being the Collected Papers of Hersch Lauterpacht, Volume I: The General Works*, der. E. Lauterpacht (Cambridge: Cambridge University Press, 1970), 136-150; akt. Andrea Bianchi, *Non-State Actors and International Law* (Londra: Routledge, 2009), 60.

hukuken sorumlu tutulmaz; ancak yine de söz konusu zararı telafi etmesi gerekir. Bu nedenle, mutlak veya kesin sorumluluk teorisi, çağdaş uluslararası hukukta neredeyse evrensel kabul gören, özel kişilerin fiillerinin devlete atfedilemeyeceği genel ilkesini ortadan kaldırmaz.

2.2.3. Suç Ortaklığı Teorisi

Yukarıda belirtildiği üzere, Grotius, kolektif veya mutlak sorumluluk teorilerinden kaynaklanmayan özel kişilerin fiilleri için devlet sorumluluğu teorisini ilk formüle edenlerden biridir. Grotius, genel olarak devletin kendi vatandaşlarının haksız fiillerinden sorumlu olmayacağını ileri sürmüştür. Ancak, devletin *patientia* veya *receptus* kavramları aracılığıyla özel kişilerin fiillerine "suç ortağı" olması hâlinde, devletin sorumluluğunun doğabileceğini savunmuştur.[518]

Bu görüşe göre, devlet, özel kişinin haksız fiilinden haberdar olmasına rağmen gerekli tedbirleri almayarak (*patientia*) veya suçluyu iade etmeyerek ya da cezalandırmayarak (*receptus*), haksız fiili onayladığını göstermiş ve böylece fiilin eşit bir tarafı hâline gelmiştir. Dolayısıyla, devletin sorumluluğu yalnızca bireyin fiilinden değil, devletin bu fiili önleyememesi veya cezalandıramaması yoluyla fiile zımnen iştirak etmesinden doğmaktadır.

Emerich de Vattel, 1758 yılında kaleme aldığı eserinde Grotius'un yaklaşımını sürdürmüştür. Vattel, özel kişilerin fiilleri için devletin mutlak sorumluluğunu reddederek, bu tür fiillerin devlete yalnızca devletin fiili onaylaması veya tasdik etmesi, yani "hareketin gerçek sahibi" hâline gelmesi durumunda atfedilebileceğini ileri sürmüştür.[519] Vattel, patientia ve receptus kavramlarını benimseyerek şu görüşleri savunmuştur:

"*… Tebaasının adil ve barışçıl bir şekilde hareket etmesini sağlama gücüne sahip bir egemen, onların yabancı bir ulusu incitmesine izin verirse, o ulusa kendisinin doğrudan incitmesinden daha az yanlış yapmış olmaz. Tebaasından birinin işlediği kötülüğü onarmayı, suçluyu cezalandırmayı veya nihayetinde onu teslim etmeyi reddeden bir hükümdar, kendisini de bir bakıma bu fiile ortak etmiş olur ve bundan sorumlu hâle gelir…*"[520]

Birkaç yıl sonra William Blackstone, suç işleyen failleri cezalandırmayan bir hükümdarın "tebaasının suçuna ortak olduğunu ya da yataklık etmiş" olacağını

[518] Hugo Grotius, *De Jure Belli Ac Pacis*, c. 2, çev. JB Scott (1646), 523–26.
[519] Emmerich de Vattel, *The Law of Nations or, the Principles of Natural Law: Applied to the Conduct and to the Affairs of Nations and Sovereigns*, 2, çev. CG Fenwick (New York, NY: Legal Classics Library, 1916), 72.
[520] de Vattel, *The Law of Nations*, 71-75.

vurgulamıştır.[521] Bu doktrini gerekçelendirirken, Blackstone dönemin uluslararası hukukuna göre, kişisel olarak işlenen hakaretlerin savaşa girmek için bir bahane olabileceği gerçeğinden hareket etmiştir. Özel haksız fiiller ile silahlanma arasındaki bu bağlantı nedeniyle, hükümdarın, yabancı savaşın felaketlerini kendi toplumunun üzerine çekmemesi için, yabancı tebaaya karşı işlenen özel haksız fiilleri cezalandırmaya teşvik etmesi önemli görülüyordu.[522]

İlk hakem kararlarının önemli bir kısmı, özel kişilerin görevlerini kötüye kullanmaları bağlamında devletin sorumluluğunu ortaya koymak için suç ortaklığı teorisine başvurmuştur. Bu davaların çoğu, devletin devlet dışı aktörü yargılayamadığı veya hukuka aykırı olarak sorumluluğu isnat ettiği durumlarda, "adaletin reddi" nedeniyle devletin sorumluluğunu tespit etmiştir. Örneğin, 1874 tarihli *Montijo Davası*, Panama'ya giden bir ABD gemisinin, ülkedeki devrimci faaliyetlere katılan kişiler tarafından ele geçirilmesi ve bu kişilere af çıkarılması ile ilgiliydi. Birleşik Devletler-Kolombiya Komisyonu, davada Panama aleyhine verdiği kararda, "bu yönde açık bir hüküm bulunmasa dahi, af ilan edenin, affettiği kişilerin daha önce üstlendiği yükümlülükleri kendi yükümlülüğü olarak kabul ettiği" görüşünü benimsemiştir.[523]

1903'te İtalyan-Venezüella Komisyonu önünde görülen *Poglioli Davası*'nda, Yargıç Ralston, davacıları öldürmeye teşebbüs eden dört kişinin yakalanıp cezalandırılmamasından dolayı Venezüella'nın hukuki sorumluluğunu değerlendirmiştir. Ralston, suç ortaklığı teorisini savunan görüşleri inceledikten sonra, "yetkililerin suç ortaklığını ve adaletin inkarını" tespit etmiştir.

Benzer şekilde, *Hammer Davası*'nda Temsilci Findlay, Venezüella'nın sorumluluğunu, "bir devletin, başka bir devletin vatandaşlarına yapılan haksızlıklardan, suçlunun hesap vermeden veya işlediği suçtan dolayı cezalandırılmadan serbestçe dolaşmasına izin verildiği her durumda sorumlu olduğunu" savunmuştur.[524]

Suç ortaklığı teorisinin savunucuları, kendi dönemleri için daha makul bir devlet sorumluluğu modeli ortaya koymuşlardır. Egemen devlet ile özel hukuk kişisi arasındaki temel ayrım uluslararası düzende yerleşik hâle geldikçe, devlet dışı aktörlerin davranışları için otomatik sorumluluk kavramlarının içi giderek boşalmıştır. Suç ortaklığı teorisi, genel atfedilemezlik ilkesini benimseyerek, devletin kusuru olmadan sorumlu olamayacağı fikrini

---

[521] William Blackstone, *Commentaries on the Laws of England*, c. 4, der. W. Morrison (London: Cavendish, 2001), 68.

[522] Blackstone, , *Commentaries on the Laws of England*, 68.

[523] *The Montijo Davası* (ABD / Kolombiya), 1875, JB Moore, *History and Digest of International Arbitrations to which the United States has been a Party*, c. 2, Washington: Government Printing Office, 1898, 1421, 1438.

[524] *Narcisa de Hammer Davası (Amerika Birleşik Devletleri / Venezuela), 1885, JB Moore, History and Digest of International Arbitrations to which the United States has been a Party, 3, Washington: Government Printing Office, 1898, 2969.*

kabul etmiştir. Aynı zamanda, suçu önleme veya özel hukuk kişisini sorumlu tutma bakımından yetersizliği nedeniyle devleti fiilin bizzat tarafı sayarak, özel hukuk kişilerin fiilleri için devletin sorumluluğunu tesis etmeye çalışmıştır.

1925'te Meksika-Amerika Birleşik Devletleri Genel Talepler Komisyonu'nda görülen *Janes Davası*, özel hukuk kişilerin fiillerinden dolayı devletin uluslararası sorumluluğunun gelişiminde önemli bir dönüm noktasını temsil etmektedir. Dava, ABD vatandaşı Byron Everett Janes'in öldürülmesi nedeniyle Janes ailesi adına ABD tarafından açılan tazminat talebini içermekteydi. Janes, Meksikalı bir maden şirketinin eski çalışanı tarafından herkesin gözü önünde öldürülmüştü. ABD, Meksikalı yetkililerin suçlunun yakalanması ve cezalandırılması konusunda gerekli özeni göstermemesi nedeniyle Meksika'nın ölümden sorumlu tutulması gerektiğini ileri sürmüştü.[525]

Davanın somut delillerini inceledikten sonra, Komisyon'un çoğunluğu, uluslararası kararlarda bu tür davalarda devletin sorumluluğunu, "bireyin devletle bir tür suç ortaklığına ve devleti bireyin kabahatinin sonuçlarından sorumlu tutmaya" dayandırma eğilimini not etmiştir. Komisyon burada çok önemli bir ayrım yapmıştır:

"Suç ortaklığı varsayımına dayanan bir gerekçeye göre, devletin işlenmesi planlanan zarar verici suçu bildiği, bunu önleyebileceği, ancak bazı nedenlerle sorumluluğunu oluşturacak şekilde bunu yapmadığı durumlarda sorumluluğu doğar mı? Bu, bir müdahale etmeme durumudur. Bu davadaki devletin uluslararası sorumluluğunu oluşturan suç, suçlunun şahsi sorumluluğundan ayrı, kendine özgü bir sorumluluktur. Suçlu, bir Amerikan vatandaşını öldürdüğü için sorumludur; devlet ise suçluyu özenle soruşturma ve uygun şekilde cezalandırma görevini yerine getirmediği için sorumludur. Cezalandırmama bir tür onaylama olarak düşünülse bile—Komisyon'un görüşüne göre bu şüphelidir—bir suçu onaylamak hiçbir zaman o suça ortak olmakla özdeş görülmemiştir." [526]

Komisyon böylece Meksika'yı, özel hukuk kişilerin fiilleriyle devlet arasında herhangi bir suç ortaklığı iddiasında bulunmaksızın, ayrı bir suç olan adaletin yerine getirilmemesi fiilinden sorumlu tutmuştur. Tazminatın belirlenmesi söz konusu olduğunda, Komisyon, devletin suçu ile özel hukuk kişisinin suçunun "köken, karakter ve etki" bakımından farklı olması nedeniyle, tazminatın yalnızca özel hukuk kişisinin fiilinden kaynaklanan zararla hesaplanamayacağını belirtmiştir. Komisyon, bu tür davalardaki tazminat uygulamalarını inceledikten sonra, Meksika'nın borçlu olduğu zararın, cezalandırmadaki başarısızlık nedeniyle

[525]Amerika Birleşik Devletleri - Birleşik Meksika Devletleri Karma Hakem Mahkemesi (ABD-BMDKHM), K. 1925, *Reports of International Arbitral Awards*, 4, 82.
[526]ABD-BMDKHM, K. 1925, 89.

davacıların maruz kaldığı bireysel mağduriyet ile "devletin tutumundan kaynaklanan güvenlik eksikliği"nden doğduğunu ileri sürmüştür.[527]

Janes Davası'nın suç ortaklığı teorisini eleştirmekle birlikte tamamen reddetmediği belirtilmelidir. Dava, yalnızca önlememe bağlamında teorinin geçerliliğini kabul etmekle kalmamış, aynı zamanda "suçluların kovuşturulmaması ve cezalandırılmaması … düzenli olarak gerçekleşiyorsa, bu durum bir engellememe veya önlememe niteliği kazanabilir ve bu şekilde ele alınabilir" hükmünü ortaya koymuştur.[528]

Bununla birlikte, Janes Davası'ndaki değerlendirme, hakem heyetlerinin ve hukukçuların Komisyon'un ihtiyatlı analizinin ötesine geçerek suç ortaklığı teorisinin otoritesini bütünüyle sorgulamalarının yolunu açmıştır. Dava, devletin haksız fiili ile bunun sonucunda ortaya çıkan zararın, özel kişilerin fiilinden temel anlamda farklı olduğunu vurgulayarak, suç ortaklığı teorisinin yapay karakterini ortaya koymuştur.

Suç ortaklığı teorisi, kamusal ve özel alan arasındaki farklılıkları yeterince dikkate almadığı için hukukçuların gözünde sürdürülemez hâle gelmiştir. Suç ortaklığının cezai diline başvuranlar, devletin ihmal yoluyla, bir şekilde kasıtlı olarak suçun işlenmesini kolaylaştıracak koşulları oluşturduğunu ve dolayısıyla bundan sorumlu tutulması gerektiğini ima etmişlerdir. Sorumluluk konusunu inceleyen akademisyenler, devletin sorumluluğunun her türlü kusur veya kötü niyetten ziyade uluslararası yükümlülüklerin "objektif" ihlallerine dayandırılması gerektiğine giderek daha fazla ikna oldukça, "devletin suç ortaklığı" kavramı savunulamaz hâle gelmiştir.

Devletin, suçun işlenmesinde özel hukuk kişisiyle birlikte hareket edebileceği varsayımı, dönemin hâkim görüşlerine göre hatalıydı. Bu görüşü savunanlara göre, devlet ve özel hukuk kişisi yalnızca farklı hukuki yükümlülüklere tabi olmakla kalmayıp, aynı zamanda farklı hukuki dünyalarda yer aldıklarından birlikte hareket edemezler. Uluslararası Hukuk Komisyonu'nun (UHK) devlet sorumluluğu konusundaki ikinci özel raportörü Roberto Ago'nun ifadesiyle: "Özel hukuk kişisi uluslararası bir yükümlülüğü ihlal edemeyeceğine göre, özel hukuk kişisi ile devlet arasında böyle bir ihlal amacıyla suç ortaklığı düşünülemez." [529]

---

[527] ABD-BMDKHM, K. 1925, 89.

[528] ABD-BMDKHM, K. 1925, 89-90.

[529] Roberto Ago, *Devletin Uluslararası Hukuka Aykırı Eylemi, Uluslararası Sorumluluğun Kaynağı: Devlet Sorumluluğu Üzerine Üçüncü Rapor*, BM Uluslararası Hukuk Komisyonu, belge no. A/CN.4/246 ve Ek 1-3, *Uluslararası Hukuk Komisyonu Yıllığı*, 1971, 2/1, 96.

2.2.4. Göz Yumma Teorisi

Janes Davası'nda kararın verildiği dönemde, bazı hukukçular, suç ortaklığı teorisinin biraz değiştirilmiş bir versiyonunu tasarlayarak teoriyi sürdürmeye çalışmışlardı. Bu hukukçular, suç ortaklığı teorisine yöneltilen yapaylık eleştirilerinden açıkça etkilenmişlerdir. Bunun yerine, devletin özel kişilerin fiillerinden suç ortaklığı yoluyla değil, suçu önleme veya cezalandırmadaki başarısızlıklarının fiili onaylama ya da "göz yumma" anlamına gelmesi nedeniyle sorumlu olduğunu ve böylece fiili kendi fiilleri haline getirdiğini öne sürmüşlerdir. Suç ortaklığı teorisinin savunucuları zaman zaman suç ortaklığı ve göz yumma kavramlarını birbirinin yerine kullanmış olsalar da, bu kavramlar artık hukuken farklı biçimde ele alınmaktaydı. Bu yaklaşımı benimseyenlerden bazıları, Janes Davası'ndaki Amerikan Komiseri Fred Nielsen'in karşı oy görüşünden destek almıştır. Nielsen, göz yumma teorisini güçlü bir şekilde savunarak şunları belirtmiştir:

"Bir devletin, yabancılara zarar veren kişileri cezalandırmak için uygun adımları atmadığı takdirde bu suça göz yumduğu ve dolayısıyla sorumlu hale geldiği yönünde defalarca öne sürülen teori ne mantık dışıdır ne de keyfidir. Devlet, birey tarafından işlenen bir suçu cezalandırmak için harekete geçmediğinde, bu suçu hoş gördüğünü söylemek mantığa aykırı değildir ve 'göz yumma' kavramının uygun anlamı çarpıtılmamış olur. Aynı şekilde, uygun cezai önlemlerin ihmal edildiği kanıtlandığında devletin suçtan sorumlu tutulabileceği de açıkça görülmektedir."[530]

Amerikalı hukukçu Charles Hyde, 1928'de yayımladığı eserinde, birçok uluslararası tahkim mahkemesinin tazminatları özel kişinin neden olduğu maddi zarara göre değerlendirdiği gerçeğinden hareketle, göz yumma teorisini destekleyen kanıtlar ortaya koymuştur. Hyde, bunun devletin özel kişilerin haksız fiillerinden doğrudan sorumlu tutulduğunu gösterdiğini ileri sürmüştür. Devletin özel kişilerin fiillerinden sorumluluğunu açıklarken Hyde, suça ortaklık ile göz yumma arasındaki ayrımı açıklamak amacıyla Nielsen'in mantığına atıfta bulunmuştur:

"Devlet, yargılama yapmayı ihmal ettiğinde, başvurana zarar verenlerin haksız fiillerini onayladığı veya göz yumduğu ve dolayısıyla bu fiillerden sorumlu olduğu varsayılmalıdır. Göz yumma teorisi, görünürde şiddet eylemlerine ortaklık isnat eden yaklaşımdan daha tatmin edici

[530] ABD-BMDKHM, K. 1925, 32.

bir açıklama sunar. Bir devlet, faile ortak olmadan da ihmal yoluyla bir davranışa göz yumabilir."[531]

Bu görüşlerin ortak özelliği, özel kişilerin davranışlarının, devletin kusurlu davranışı sonucunda bir şekilde devlet fiiline dönüşebileceği varsayımıdır. Göz yumma teorisine göre, devletin özel kişinin fiili karşısında eylemsiz kalması, bu fiili kendi fiili olarak kabul ettiğine dair resmi bir onay ile eşdeğer kabul edilir.

Ancak, devletin özel kişiye ait bir fiili dolaylı olarak göz yumarak kendi fiili haline getirebileceği düşüncesi, söz konusu fiilin tamamen özel olmadığını düşündürmektedir. Özel fiillerin devlete atfedilmemesi ilkesinin aksine, göz yumma teorisi kapsamında kamusal ve özel alan arasındaki sınır sabit değil, değişkendir. Devletin, özel aktörü sorumlu tutmak için gerekli özen yükümlülüğünü yerine getirerek fiili özel olarak nitelendirdiğini göstermesi gerekmektedir; bu yapılmadığında ise fiilin tamamen özel nitelikte olmadığı ve devlete atfedilebileceği ortaya çıkar.[532]

Clyde Eagleton'ın ileri sürdüğü gibi, eğer devlet yalnızca kendi fiilinden sorumluysa, tazminat "devletin fiili veya ihmaliyle" ölçülmelidir. Ancak uygulamada, tazminat çoğunlukla "asli fiilden kaynaklanan zararla" ölçülmüş ve bu durum, Eagleton'ın "teori ile pratik arasında çarpıcı bir tutarsızlık" olarak nitelendirdiği bir sonucu doğurmuştur. Suç ortaklığı veya göz yumma teorilerinin geçerliliğini sorgulayan ve devletin yalnızca kendi kusurundan sorumlu olduğunu savunan hukukçular, bu anomaliyi açıklamak zorunda kalmıştır.

Bu saklı karine, göz yumma teorisinin, özel fiillerin devlete atfedilmemesi ilkesinin temellerine meydan okuduğunu göstermektedir. Teori, devletin yükümlülüklerini yerine getirmediği sürece özel fiiller dolayısıyla doğrudan sorumluluğu öngördüğünden, kusursuz ya da katı sorumluluk doktrinine daha yakın bir yaklaşımı temsil etmektedir.[533]

2.2.5. Ayrı Suç Teorisi

Suç ortaklığı ve göz yumma teorilerinin her zaman belli başlı savunucuları bulunmakla birlikte, özel kişilerin fiilleri nedeniyle devletin sorumluluğu üzerine yürütülen tartışmalarda uzun süredir hakim olan görüş, devletin fiillerinin özel kişilerin fiilleriyle

[531] Charles Hyde, "Concerning Damages Arising From Neglect to Prosecute," *American Journal of International Law* 22/1 (1928), 140-142; Edwin Borchard, *The Diplomatic Protection of Citizens Abroad* (New York: Banks Law Publishing, 1915), 217.
[532] Hyde, "Concerning Damages," 142.
[533] Tal Becker, *Terrorism and the State Rethinking the Rules of State Responsibility*, (Kuzey Amerika: Hart Publishing), 24.

ilişkilendirilemeyeceği ilkesidir. Bu ilke, haksız fiil ile devletin bu fiile ilişkin kusuru arasında net bir ayrım yapılmasını gerektirmektedir.

Devlet yalnızca kendi organlarının ve birimlerinin hukuka aykırı fiillerinden hukuken sorumlu tutulabiliyorsa, özel kişilerin fiilleri nedeniyle devlet dışı aktörlerin veya diğer devletlerin zarar görmesi durumunda devletin sorumluluğunu açıklamak için alternatif bir kuramsal çerçeveye ihtiyaç vardı. İşte bu ihtiyaç, "Ayrı Suç Teorisi" (*The Separate Delict Theory*)nin ortaya çıkmasına yol açmıştır.[534] Günümüzde uluslararası hukukta sıklıkla atıfta bulunulan bu teori, tarihsel gelişimi ve bağlamı açısından ise çoğu zaman göz ardı edilmektedir.

Ayrı Suç Teorisi, devlet sorumluluğunun tamamen özel kişilerin fiillerinden kaynaklanabileceği fikrini reddeder; zira fiil, ya doğrudan (kolektif sorumluluk yoluyla) ya da dolaylı olarak (suç ortaklığı veya göz yumma yoluyla) devlete atfedilebilir. Teoriye göre devletin sorumluluğu, yalnızca suçu önleme ve cezalandırma bakımından gerekli özen yükümlülüğünü ihlal etmesi nedeniyle ortaya çıkar.

Bu teoriyi savunanlar, devletin sorumluluğunun her zaman kendi kusuruna dayandığını vurgulamışlardır. Özel fiil devlete atfedilemediği sürece, devlet hiçbir şekilde fiilin kendisinden sorumlu tutulamaz; sorumluluk yalnızca bu fiille ilgili olarak işlediği kusurdan kaynaklanır. Janes Davası'ndaki anlayışı takip eden bu yaklaşım, özel fiili yalnızca harici bir olay olarak kabul ederken, devletin sorumluluğunu hem açıklamakta hem de devletin hukuka aykırı davranışıyla sınırlamaktadır.

2.3. Uluslararası Hukukta Kodifikasyon Süreçleri ve Atıf

2.3.1. Lahey Kodifikasyon Konferansı

İkinci Dünya Savaşı öncesi dönemde gerçekleştirilen en önemli kodifikasyon çalışması, kuşkusuz 1930 tarihli Lahey Kodifikasyon Konferansı olmuştur. 1925 yılında, Milletler Cemiyeti Genel Kurulu'nun uluslararası hukukun kodifikasyonunu gerçekleştirme talebini takiben, bir Uzmanlar Komitesi, devletin yabancılara veya onların mallarına verdiği zarar nedeniyle sorumlu olabileceği durumları incelemeye başlamıştır.[535] Komite 1926'da elde ettiği sonuçları devletlere sundu. Bu sonuçlar "ister ulusal ister yabancı olsun, özel kişiler tarafından

[534] Becker, Terrorism and the State: Rethinking the Rules of State Responsibility, 26.

[535] League of Nations Committee of Experts for the Progressive Development of International Law, *Questionnaire No. 4, on Responsibility of States for Damage Done in their Territories to the Person or Property of Foreigners* (Cenevre: League of Nations, 1926), V3, C.46.M.23.1926.V; yeniden basım: F. V. García Amador, "First Report on State Responsibility," *Yearbook of the International Law Commission*, Cilt 2 (1956), Birleşmiş Milletler Belgesi A/CN.4/96, 173, 221.

yabancılara verilen zararın devletin sorumluluğunu içermediği" ve bu tür durumlarda devletin sorumluluğunun ancak "devletin kendisinin bir ödevi ihlal etmesi" halinde ortaya çıkacağı görüşünü içermekteydi. Bu yaklaşım, devletlerin Komite tarafından hazırlanan önerilere verdikleri yanıtlarla da açıkça desteklenmiştir. Örneğin Almanya, "…sorumluluk özel kişilerin eylemlerinden kaynaklanmaz"[536] görüşünü savunmuştur. Bu görüşe göre "bir devletin sorumluluğu yalnızca kendi yetkililerinin fiil veya ihmallerinden kaynaklanabilecek ve hiçbir zaman özel kişilerin fiillerinden kaynaklanmayacaktır." Japonya, "devletin prensip olarak özel kişilerin fiillerinden sorumlu tutulmaması gerektiğini" belirtmiştir.[537] Benzer şekilde Polonya da "devlet hiçbir zaman özel kişilerin fiillerinde sorumlu tutulamaz" görüşünü savunmuştur.[538] ABD de yukarıdaki devletlerle benzer görüşleri paylaşarak aşağıdaki ifadelere yer vermiştir: "Devlet, özel kişilerin yabancılara yönelik haksız fiillerinden sorumlu değildir." ABD'ye göre, sorumluluğun doğması için, özel kişilerin fiillerinden bağımsız olarak, devletin bir kusurunun bulunması şarttır.[539]

Lahey Kodifikasyon Konferansı'nda tartışılan çeşitli formülasyonların, Janes Davası'ndaki bulgunun aksine, bir devletin kendi haksız fiili nedeniyle sorumluluğunun ortaya çıkmasının ardından, devletin genellikle yalnızca özel bir fiilin sebep olduğu zarardan değil, fiilin devletin eylemsizliğinden ya da sorumlulukları yerine getirmemekten kaynaklandığı durumlarda sorumlu tutulduğunu ima ettiği gözlemlenmiştir. Örneğin, Konferans için hazırlık yapan Komite, "devletin, özel bir kişi tarafından bir yabancıya verilen zarardan sorumlu tutulabileceği durumun, fiilin kendisinde değil, devletin davranışında—yani düzeni sağlama görevini yerine getirmemesinde—bulunduğu" sonucuna varmıştır.[540] Benzer şekilde, Konferans için hazırlanan tartışma raporlarının çoğunda, özel kişiler tarafından verilen zarardan dolayı devletin sorumluluğundan bahsedilmiştir. Buna göre bir devlet ayaklanma, isyan veya toplumsal şiddete katılan kişiler tarafından bir yabancının şahsına veya malına verilen zarardan sorumlu değildir. Bununla birlikte bu devletin yabancıyı korumak veya suçluyu cezalandırmak için gerekli özeni göstermediği durumlarda özel kişi tarafından verilen zarardan dolayı

[536] Preparatory Committee of the Conference for the Codification of International Law, *Bases of Discussion* (Cenevre: League of Nations, 1929), V3, C.75.M.69.1929.V; yeniden basım: Shabtai Rosenne (ed.), *League of Nations Conference for the Codification of International Law*, Cilt 2 (Dobbs Ferry, NY: Oceana Publications, 1975), 540–542.
[537] Shabtai Rosenne, *League of Nations Conference for the Codification of International Law*, Cilt 2 (Dobbs Ferry, NY: Oceana Publications, 1975), 635.
[538] Shabtai Rosenne, *League of Nations Conference for the Codification of International Law*, Cilt 2 (Dobbs Ferry, NY: Oceana Publications, 1975), 655.
[539] Shabtai Rosenne, *League of Nations Conference for the Codification of International Law*, Cilt 2 (Dobbs Ferry, NY: Oceana Publications, 1975), 694.
[540] Shabtai Rosenne, *League of Nations Conference for the Codification of International Law*, Cilt 2 (Dobbs Ferry, NY: Oceana Publications, 1975), 518.

sorumluluğu oluşmaktadır. Af durumlarında devletin zarar verenin sorumlu olduğu ölçüde zarardan sorumlu olacağı öngörülmüştür. Devletin sorumluluğunun yalnızca zarara neden olan fiil meydana geldikten sonra uygun önlemleri almamasından ileri geldiği durumlarda ise, devlet yalnızca bu tür önlemleri tamamen veya kısmen almamış olmasından kaynaklanan zararı gidermekle yükümlüdür. Konferans'ta ilk okumada kabul edilen Taslak Maddelerin 10. maddesi bu karışıklığın giderilmesine yardımcı olmamıştır. Bu maddeye göre "Özel kişiler tarafından yabancılara veya mallarına verilen zararla ilgili olarak, devlet yalnızca zarara neden olan fiilleri önlemek, gidermek veya cezalandırmak için gerekli tedbirleri almaması halinde sorumludur."[541]

10. madde tek başına okunduğunda, devletin tam olarak hangi fiillerden sorumlu olduğunun net olmadığı görülmektedir. Başka bir deyişle, bu maddeden devletin sorumluluğunun yalnızca kendi fiilleriyle mi sınırlı olduğu yoksa özel kişilerin fiillerini de kapsayıp kapsamadığı anlaşılmamaktadır. Katılımcı devletler, özel kişilerin fiillerinin prensipte devlete atfedilemeyeceğini vurgulamış olsalar da, maddede sebep olunan zarara ilişkin sorumluluğa yapılan atıflar, anlaşılır bir hukuki metin oluşturulmasını engellemekte ve özel kişiler tarafından verilen zararla ilgili olarak devletin sorumluluğunun kapsamı konusunda bir dizi belirsizlik yaratmaktadır.

Dolayısıyla Konferans, devlet sorumluluğu konusundaki çalışmalarını hiçbir zaman tamamlayamadı.[542] Zaman yetersizliği ve konunun karmaşıklığı nedeniyle delegeler taslak maddeleri daha fazla açıklığa ve ayrıntıya kavuşturamadılar. Sonuç olarak, kodifikasyon girişimleri neticesinde, haksız özel fiillerin devlete atfedilemeyeceği ve devletin sorumluluğunun, özel fiilin kendisinden ziyade, devletin bu tür fiillerle ilgili eylemsizlikleri veya ihmalleri sonucunda oluştuğu görüşü hakim olmuştur.[543]

2.3.2. García Amador'dan Ago'ya Kodifikasyon Süreci

Uluslararası Hukuk Komisyonu, 1949'daki ilk oturumunda, kodifikasyon için uygun görülen konular arasında hem yabancılara yönelik muameleyi hem de devletin uluslararası

[541] *Text of Articles Adopted in First Reading by the Third Committee of the Conference for the Codification of International Law* (Cenevre: League of Nations, 1930), V17, C.351(c)M.145(c). 1930. V; F. V. García Amador, *First Report on State Responsibility*, 225–226.
[542] Shabtai Rosenne, *The International Law Commission's Draft Articles on State Responsibility* (Dordrecht: Nijhoff, 1991), 2–17.
[543] American Law Institute, *Second Restatement of the Law, 2 Foreign Relations Law of the United States*, Bölüm 183 (1965).

sorumluluğunu incelemiştir.[544] Diğer konulara daha fazla öncelik verilmesi nedeniyle, Genel Kurul 1953 yılına kadar UHK'dan "devletin sorumluluğuna ilişkin uluslararası hukuk ilkelerinin kodifikasyonunu" [545] üstlenmesini talep etmiş ve Komisyon 1955 tarihine kadar Kübalı FV García Amador'u bu konu için özel raportör olarak atamıştır.

García Amador'la birlikte birçok hukukçu atfedilemezlik ilkesini desteklemiştir. İlk raporunda Garcia Amador, devletin özel fiillere ilişkin sorumluluğunun "fiilin kendisinden değil, devletin fiille ilgili davranışından kaynaklandığını" ileri sürmüştür.[546] Bu düşünce ikinci raporunda da tekrarlanmış ve "devlete atfedilen şeyin esasen zarara neden olan (özel) fiil veya eylem değil, daha çok uluslararası bir görevin yerine getirilmemesi" olduğunu belirtmiştir.[547]

Garcia Amador'un 1961 yılında sona eren UHK üyeliği döneminde, devletin sorumluluğuna ilişkin çalışmalar oldukça sınırlı ilerleme kaydetmiş ve adeta bir çıkmaza girmişti. Ertesi yıl Komisyon, konunun geleceğini değerlendirmek amacıyla İtalyan hukukçu Roberto Ago başkanlığında bir alt komite oluşturdu.

Alt komitenin raporunda, hukuki yükümlülüklerin ihlalinden kaynaklanan devlet sorumluluğuna ilişkin kuralların, uluslararası hukukun maddi ya da "birincil" kurallarından ayrılması gerektiği önerilmiştir.[548] Raporun ana hatları, "özel kişilerin fiillerinin devlete isnadı" ve "bu tür durumlarda uluslararası sorumluluğun gerçek kaynağı" gibi hususları da kapsayan isnat sorununu içermekteydi.

Her ne kadar bu kavramlar o dönemde henüz kullanılmamış olsa da, devlet sorumluluğuna ilişkin "ikincil" kurallar ile uluslararası hukukun "birincil" kuralları arasında yapılan ayrım, Komisyon'un yalnızca yabancılara verilen zararlar konusuyla sınırlı kalmaktan kurtulmasını ve devlet sorumluluğunun daha geniş boyutunu bir bütün olarak kodifiye etmeye odaklanmasını mümkün kılmıştır.[549]

---

[544] *Report of the International Law Commission*, UN GAOR, 4. Sessiyon, Ek No 10, Birleşmiş Milletler Belgesi A/925 (1949). UHK bu kararını büyük ölçüde Hersch Lauterpacht'ın Genel Sekreter için hazırladığı ve önemli bir öngörüyle sorumluluk sorununun yabancılara zarar verme alanını "aştığını" savunduğu bir memorandumа dayandırmıştır; bkz. *Survey of International Law in relation to the Work of Codification of the International Law Commission*, Birleşmiş Milletler Belgesi A/CN.4/1/Rev.1 (1948), para 98.

[545] Genel Kurul Kararı 799 (VIII), Birleşmiş Milletler Genel Kurulu (UN GAOR), 8. Sessiyon, Ek No 17, Birleşmiş Milletler Belgesi A/799 (1953).

[546] García Amador, FV, *First Report on State Responsibility* (1956) 2 Yearbook of the International Law Commission 104, 182, UN Doc A/CN.4/96., 187.

[547] García Amador, FV, *Second Report on State Responsibility* (1957) 2 Yearbook of the International Law Commission 104, 121, UN Doc A/CN.4/106., 121

[548] *Report of the Sub-Committee on State Responsibility* (1963) 2 Yearbook of the International Law Commission 227, UN Doc A/CN.4/152.

[549] Daniel M. Bodansky - John R. Cook, "Symposium: The ILC's State Responsibility Articles", *American Journal of International Law*, 96/4 (2002,) 780.

2.3.3. Ayrı Suç Teorisinin Komisyon Görüşmeleri

İkinci özel raportör olarak görevlendirilen Roberto Ago, 1969–1980 yılları arasında sekiz rapor sunmuştur. Ago'nun üçüncü ve dördüncü raporları, isnat meselesine ve uluslararası hukuk bakımından bir fiilin "devlet fiili" olarak nitelendirilmesine odaklanmıştır. 1972 yılında yayımlanan dördüncü raporunda ise, özel kişilerin fiilleri bağlamında devlet sorumluluğu konusu kapsamlı bir şekilde ele alınmıştır. Bu raporda Ago, yabancılara zarar verilmesine ilişkin birincil kuralların gölgesinde kalmadan, uygulanabilir hukuki ilkelerin sistematik ve net bir analizini ortaya koyabilmiştir. Söz konusu rapor, günümüzde dahi ayrı suç teorisinin en kapsamlı ve güçlü açıklaması olma özelliğini korumaktadır.

Ago, konuya ilişkin giriş niteliğindeki değerlendirmesinde, teorik olarak özel kişilerin fiillerinin de bir devlet fiili olarak kabul edilmesine engel bulunmadığını ifade etmiştir.[550] Bununla birlikte, uygulamada yalnızca devletin "teşkilatının" bir parçasını oluşturan kişilerin fiillerinin bu şekilde nitelendirildiğini gözlemlemiştir.[551]

Ago, ilgili hukuki kaynakları yorumlarken, "telafi edilecek olanın, bunun sonucunda ortaya çıkabilecek zarar değil, devletin kusuru" olduğu görüşünü savunmuştur.[552] Özel Raportör "Devletin bireyin fiilinden değil, bireyin fiiliyle bağlantılı olarak bazı organlarının genellikle ihmalkar davranışlarından sorumlu olduğunu"[553] ileri sürmüş ve "Devletin kendi topraklarında özel aktörler tarafından neden olunan zarardan sorumlu olmamasına ilişkin temel ilkeye"[554] atıfta bulunmuştur. Bu bağlamda Ago, ayrı suç teorisini aşağıdaki terimlerle açıklamıştır:

"Birey olan ve birey olarak kalan kişilerin —yani devletle hiçbir kurumsal bağı bulunmayan kişilerin— fiil ve ihmalleri, uluslararası hukuk kapsamında devlete isnat edilemez ve devlet fiili olarak nitelendirilemez. Bu nedenle, söz konusu fiiller devletin diğer devletlere karşı sorumluluğunu doğurmaz. Devlet, uluslararası düzeyde yalnızca kendi organlarının eylemlerinden ve çoğunlukla da ihmallerinden sorumludur. Devletin sorumluluğu, bireyin eyleminden değil; organlarına koruma sağlama yükümlülüğü yükleyen genel veya özel bir yükümlülüğün ihlal edilmesinden kaynaklanmaktadır."[555]

---

[550] Roberto Ago**,** "Third Report on State Responsibility", *Yearbook of the International Law Commission*, 2 (1971), s. 199, 233, UN Doc A/CN.4/226.
[551] Ago, Third Report**,** *Yearbook of the International Law Commission*, 2 (1971), 233.
[552] Roberto Ago**,** "Fourth Report on State Responsibility", *Yearbook of the International Law Commission*, 2 (1972), 99, UN Doc A/CN.4/264.
[553] Ago, Fourth Report**,** *Yearbook of the International Law Commission*, 2 (1972), 99.
[554] Ago, Fourth Report**,** *Yearbook of the International Law Commission*, 2 (1972), 106.
[555] Ago, Fourth Report**,** *Yearbook of the International Law Commission*, 2 (1972), 123.

Ago, ilgili uluslararası hukuk kaynaklarını ayrıntılı biçimde inceledikten sonra Komisyon'a şu sonucu sunmuştur: "Uluslararası yargı kararları ve devlet uygulamalarında mevcut olan ilkelere göre, özel kişilerin fiillerinin devlete atfedilmediği görülmektedir. Bununla birlikte, özel kişilerin fiillerinin devlete atfedilmesine ilişkin bu kesin olumsuz sonuç, devletin bu tür fiiller bağlamında hiçbir şekilde uluslararası sorumluluğa sahip olamayacağı anlamına gelmemelidir. Ancak kural olarak, devletin sorumluluğu yalnızca bireylerin fiillerine karşı pasif tutum sergileyerek uluslararası bir yükümlülüğünü ihlal eden devlet organlarının eylemlerinden doğabilir. Dolayısıyla bireyin fiili, devletin davranışının haksızlığını ortaya çıkaran harici bir unsur, başka bir deyişle bir katalizör niteliği kazanabilir."[556]

Uzun bir içtihat geleneği ile Ago'nun ulaştığı sonuçlar, ayrı suç teorisinin geniş kabul gören bir hukuk doktrini olarak benimsendiği yönündeki görüşü desteklemektedir. Bu yaklaşıma göre devlet, özel kişilerin fiillerinden değil; yalnızca kendi fiillerinden sorumludur. Devletin sorumluluğu, hukuka aykırı davranışta bulunan aktör ile devlet arasındaki vekâlet benzeri bir ilişkiye dayandırılmaktadır. Bu çerçevede, devlet görevlilerinin ve organlarının fiilleri devlete isnat edilebilirken, tamamen özel aktörlerin eylemleri ne devlete isnat edilebilir ne de devletin sorumluluğunu doğurabilir. Dolayısıyla devletin hukuki sorumluluğu, esasen vekâlet ilişkisinin bir fonksiyonu olarak görülmekte; özel kişilerin fiillerine ilişkin isnat ilkeleri de doğal olarak bu anlayıştan beslenmektedir.[557]

2.3.4. Atfedilemezlik İlkesi ve İstisnaları

Roberto Ago'nun savunduğu ilkeler, 1975 yılında UHK tarafından hazırlanan Taslak Maddeler'in I. Bölümü'nde herhangi bir itirazla karşılaşmadan kabul edilmiştir. Komisyon'da ve akabinde Genel Kurul'un Altıncı Hukuk Komitesi'nde yürütülen tartışmalar sırasında, hem uzmanlar hem de devletler Ago'nun kapsamlı yorumunu övmüş ve ortaya koyduğu uluslararası hukuk kuralını güçlü biçimde desteklemiştir. [558]

Her ne kadar başlangıçta Ago tarafından önerilen metinden farklı bir üslup tercih edilmiş olsa da, Komisyon'un benimsediği düzenleme genel olarak devletin yalnızca devlet sıfatıyla hareket eden özel kişilerin fiillerinden sorumlu tutulabileceğini; buna karşılık, hiçbir koşulda özel fiillerin bizzat kendisinden sorumlu kılınamayacağını teyit etmiştir.[559]

---

[556] Ago, Fourth Report**,** *Yearbook of the International Law Commission*, 2 (1972), 126.
[557] Becker, *Terrorism and the State Rethinking the Rules of State Responsibility*, 42.
[558] *Uluslararası Hukuk Komisyonu Yıllığı,* 1.
[559] Roberto Ago, "Devletin Sorumluluğu Üzerine Dördüncü Rapor," *Uluslararası Hukuk Komisyonu Yıllığı,* 2, (1972), 71..

Devletin uluslararası sorumluluğun doğabilmesi için devletle birey arasında bir vekâlet ilişkisinin varlığını arayan görüş iki şekilde Taslak Maddelerin zımni bir parçası haline gelmiştir. Birincisi, yalnızca devlet adına hareket ettiği düşünülen kişilerin davranışların devletin sorumlu tutulabileceği davranışlarla bir tutulacağını teyit eden genel atıf ilkesidir. İkinci olarak, bu vekâlet ilişkisinden yoksun özel davranışların atfedilebilir olmayacağı ve ima yoluyla da olsa doğrudan devlet sorumluluğuna yol açamayacağı teyit edilmiştir. UHK metninin taslak 11. maddesi, ilk okumada kabul edildiği şekliyle bu görüşü destekler niteliktedir. Buna göre: (1) Devlet adına hareket etmeyen bir kişinin veya bir grup kişinin davranışı, uluslararası hukuk kapsamında devletin bir fiili olarak değerlendirilmeyecektir; (2) 1. Paragraf, söz konusu paragrafta atıfta bulunulan kişi veya kişi grubunun davranışıyla bağlantılı olan ve 5 ila 10. maddeler uyarınca devletin bir fiili olarak kabul edilecek olan diğer davranışların devlete atfedilmesine halel getirmez.[560]

UHK tarafından yapılan Yoruma göre, bu kural sadece uluslararası yapılageliş hukukunu yansıtmakla kalmayıp, evrensel olarak uygulanabilir niteliktedir. Yorumun son paragraflarında bu kuralın "uluslararası hukuk ilişkilerinde giderek daha fazla kabul gören kriterlere uygun" olduğu ve "özel kişinin içinde bulunduğu koşullar ve davranışlarından etkilenen menfaatlere bakılmaksızın geçerli olduğu" belirtilmiştir.[561] Komisyon, bu kuralın "çağdaş uluslararası yaşamın ihtiyaçlarını tam olarak karşıladığını ve değiştirilmesi gerekmediğini" savunarak istisnalar getirilmesini reddetmiştir.[562]

Taslak 11. madde, beşinci özel raportör James Crawford'un 1998 yılında UHK'nun devlet sorumluluğu projesini tamamlamaya yönelik yönlendirme çabaları kapsamında yeniden ele alınmasına kadar Komisyon tarafından herhangi bir müdahaleye tabi tutulmamıştır. Crawford, ilk raporunda söz konusu kuralın geçerliliğini sorgulamamış; ancak kuralın kabulünün ardından Genel Kurul'un Altıncı Komitesi'nde yapılan tartışmalarda bazı devletlerce dile getirilen yararına ilişkin görüşleri raporunda yinelemiştir.

Crawford, Taslak Maddelerde bu maddenin yer almasının, uluslararası hukukta devlet ile devlet dışı aktörler arasında prensipte net bir ayrım yönünde kaydedilen önemli bir evrimin sonucu olduğunu belirtmiştir. Öte yandan, maddenin bağımsız bir işlevsel içeriğe sahip olmayan olumsuz bir düzenleme olduğunu vurgulamıştır. Bu düzenleme, UHK'nın diğer isnat

[560] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Draft Articles on State Responsibility for Internationally Wrongful Acts*, 2(2), (1975).
[561] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Draft Articles on State Responsibility for Internationally Wrongful Acts* (Taslak Madde), Yıllık Rapor 1975, Cilt 2, 70, 82, BM Dokümanı A/CN.4/SER.A/1975/Add.1.
[562] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Draft Articles on State Responsibility for Internationally Wrongful Acts*, 82.

maddelerinin tersine, UHK kuralları uyarınca devletin fiili olarak nitelendirilemeyen özel fiillerin devlete isnat edilemeyeceğini teyit eden, dolayısıyla biraz döngüsel bir önerme niteliği taşımaktadır.[563]

Crawford'un, 11. maddenin UHK'nin nihai taslağından çıkarılması yönündeki önerisi Komisyon tarafından kabul edilmiştir.[564] Dolayısıyla, UHK Taslak Maddeleri'nin Genel Kurul tarafından kabul edilen son hâli, Ago'nun bu konudaki yoğun çabalarının açık bir izini taşımamaktadır. Ancak bu durum, kuralın kabul edilmiş otoritesine gölge düşürdüğü şeklinde yorumlanamaz. Aksine, Taslak Madde 11'in çıkarılması, kuralda algılanan herhangi bir değişiklikten değil; içeriğinin UHK'nın isnat ilkelerinin dokusuna o kadar derinlemesine işlemiş olmasından ve açıkça ifade edilmesinin gereksiz görülmesinden kaynaklanmıştır. Bu açıdan, Taslak Madde 11'in silinmesi, kuralın kazandığı önemli statüyü ifade eden bir durum olarak değerlendirilebilir.

Crawford'un da belirttiği üzere, UHK'nın atıf ilkeleri "…kümülatif olmakla birlikte aynı zamanda sınırlayıcıdır: belirli bir yükümlülüğün yokluğunda, bir devlet, pozitif isnat ilkelerinin kapsamına girmeyen herhangi bir kişi veya kuruluşun davranışlarından sorumlu tutulamaz…" Bu görüş, yalnızca hukukçuların çalışmalarında değil, aynı zamanda UHK Yorumunda da açık bir biçimde yansıtılmaktadır.[565]

Ago'nun raporunu izleyen yıllarda uluslararası hukuk uygulaması, büyük ölçüde özel fiiller bakımından devlet sorumluluğunu vekâlet temelli bir yaklaşımla ele almıştır. Uluslararası Hukuk Komisyonu tarafından hazırlanan metnin kabulünü takip eden dönemdeki uluslararası içtihat incelendiğinde, özel fiillere ilişkin sorumluluk bağlamında vekâlet paradigmasının uygulanarak devletin sorumluluğuna gidildiği açıkça görülmektedir.

2.3.4.1. Tahkim Kararları

20. yüzyılın başlarından itibaren tahkim mahkemeleri, devletin suç ortaklığı ve "ayrı suç teorisi" ilkelerini benimseme yönünde bir yaklaşım sergilemiştir. Bu davalar genellikle, devletin yabancılara karşı işlenen haksız fiilleri önleme veya kovuşturma yükümlülüğünü

[563] James Crawford, "First Report on State Responsibility," *BM Dokümanı*, 31–32.
[564] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Elliinci Oturum Tutanakları*, Yıllık Rapor 1998, 1.
[565] James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge: Cambridge University Press, 2002), 5; James Crawford, "The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: A Retrospect," *American Journal of International Law* 96 (2002), 874, 878–879.

yerine getirmediği iddialarını içermekte olup, doğrudan ya da dolaylı olarak devlet sorumluluğunun yalnızca devletin kendi kusurundan kaynaklandığını öne sürmektedir.

İlk hakem kararları, özel fiillerin devlete atfedilemezlik ilkesine önemli ölçüde vurgu yapmıştır. Örneğin, Lovett Davası Şili'de yerel garnizon valisinin isyancılar tarafından öldürülmesiyle ilgilidir. Bu davada, 1892 tarihli ABD-Şili Talepler Komisyonu, uluslararası hukuk otoritelerinin hemfikir olduğunu belirterek, "bir devletin uyruklarından biri tarafından verilen zararın o devletin kendisi tarafından yapılmış sayılmayacağı ilkesi"ni açıkça vurgulamıştır.[566] 1903'teki Sambiaggo Davası'nda ise hakem, temel bir ilke olarak gördüğü şekilde, "Bir devlet, tıpkı bir birey gibi, yalnızca temsilcilerinin fiillerinden ya da sorumluluğunu açıkça üstlendiği fiillerden sorumlu tutulur" ifadesini kullanmıştır.[567] Bu ilke, 1906 tarihli Underhill[568] ve 1920 tarihli *Home Frontier and Foreign Missionary Society* gibi diğer davalarda da benzer şekilde dile getirilmişti.[569]

Max Huber'in 1925 tarihli, *İspanyol Fas'ındaki İngiliz Mülkleri Davası*'na ilişkin ünlü kararı, ayrı suç teorisini desteklemesi bakımından *Janes Davası*'nı tamamlayıcı niteliktedir. Huber genel hatlarıyla şunları belirtmiştir:

"…devlet, ayaklanma olaylarından doğrudan sorumlu değildir; [ancak] devlet, yetkililerin sonuçları mümkün olduğunca hafifletmek için yaptıklarından veya yapmadıklarından sorumlu olabilir. Kamu yetkililerinin eylem veya eylemsizliklerinden doğan sorumluluk, yetkililerin kontrolü dışındaki ya da onlara açıkça düşman olan kişilere isnat edilebilecek eylemlerden doğan sorumluluktan önemli ölçüde farklıdır…" [570]

Menebhi olayının somut incelemesinde Huber, Fas'ın uluslararası alanında İspanyol bölgesi sakinleri tarafından işlenen sınır ötesi hırsızlıklara ilişkin olarak İspanya'nın sorumluluğunu değerlendirmiştir. Somut olayda Huber, hırsızlıkların önlenememesi nedeniyle İspanya'nın doğrudan sorumluluğu bulunmadığına karar vermiş ve İspanya'nın failleri kovuşturma yükümlülüğüne ilişkin sorumluluğunu ele almıştır. Hakem, İspanya'nın "suçluları parayı iade etmeye teşvik etmek veya onları cezalandırmak için herhangi bir şey yapmadığını" tespit etmiş ve bu eylemsizliği uluslararası bir yükümlülüğün ihlali olarak değerlendirmiştir.

Huber ayrıca şunları belirtmiştir:

---

[566] Frederick H. Lovett (United States v. Chile) (1892), yeniden basım: J. B. Moore, *History and Digest of International Arbitrations to Which the United States Has Been a Party*, 3 (1898), 2991.
[567] Sambiaggo Davası (Italy v. Venezuela) (1903), *10 Reports of International Arbitral Awards* 499, 512.
[568] Underhill Davası (United Kingdom v. Venezuela) (1903), *9 Reports of International Arbitral Awards* 155, 159.
[569] Home Frontier and Foreign Missionary Society of the United Brethren in Christ v. United Kingdom (1920), *R. Intl Arb. Awards* 6, 44.
[570] Uluslararası Tahkim Mahkemesi (UTA), *Spanish Zone of Morocco Case v. Spain*, K. 2 (1923), 641-642.

"Zararın tamamının sorumluluğunu, belki bu konuda ihmali olsa da, zararın doğrudan nedeni olan olaylardan kesinlikle sorumlu olmayan bir hükümete (İspanya'ya) yüklemek hiçbir koşulda haklı görülemez… İspanya'nın sorumluluğu, zarara neden olan asıl olayın koşullarına değil, yalnızca adli yardım koşullarına dayanmaktadır." [571]

Huber'in bu kararı, özel kişilere ait haksız fiillerin önlenmemesi veya cezalandırılmaması nedeniyle devletin sorumluluğunun, genel atfedilemezlik ilkesine bir istisna teşkil etmediği yönündeki pozisyonu netleştirmiştir. Görüldüğü üzere, devletin sorumluluğu yalnızca özel kişilerin haksız fiilleri karşısında devletin ihmallerinden kaynaklanmaktadır. Başka bir deyişle, sorumluluk devletin söz konusu fiile iştirak etmesi (suç ortaklığı yapması) veya göz yumması nedeniyle doğmamaktadır.

Benzer bir sonuç, 1933 yılında ABD'nin Panama'da sarhoş bir grup tarafından yaralanan vatandaşı adına açtığı Noyes Davası'ndan da çıkarılabilir. Komisyon, devlet dışı aktörlerin davranışlarından dolayı herhangi bir devlet sorumluluğunun doğmayacağını teyit etmiştir. Panama, yalnızca resmi makamlarının "bu olayla bağlantılı davranışlarından veya düzeni sağlama, suçları önleme ya da suçluları kovuşturma ve cezalandırma görevlerini yerine getirmedeki genel başarısızlıklarından" sorumlu tutulabilirdi.[572] Somut olayda Panama'nın böyle bir kusuru tespit edilememiştir. Bu dava, devletin sorumluluğunun ya belirli bir olaya ilişkin görevini kötüye kullanmasından ya da düzeni sağlamada daha genel bir başarısızlıktan kaynaklanabileceğini ortaya koymuştur.

2.3.4.2.Tahran Rehinlere Davası

Dava, Tahran'daki ABD Büyükelçiliğinin ele geçirilmesi ile Tebriz ve Şiraz'daki ABD Konsolosluklarına yapılan saldırılar ve öğrenci militanların ABD'lileri rehin almasının ardından ortaya çıkmıştır. Bu vaka, Uluslararası Adalet Divanı'nın (UAD) isnat ve sorumluluk konularını detaylı biçimde incelediği ilk karar olma özelliğini taşımaktadır.[573] Divan'ın, Büyükelçiliğe el konulması ve devlet yetkililerinin eylemsizliğini ele aldığı "ilk aşama" incelemesi, tamamen özel nitelikte olduğu düşünülen haksız davranış karşısında devletin sorumluluğu sorununun değerlendirilmesine yöneliktir. Ancak aşağıda ele alınacak kararın en dikkat çekici kısmı, ele geçirmenin "ikinci aşaması" ile ilgilidir; burada Divan, militanların

[571] Uluslararası Tahkim Mahkemesi (UTA), *Spanish Zone of Morocco Case v. Spain*, K. 2 (1923), 709-710.
[572] Uluslararası Tahkim Mahkemesi (UTA), *Walter A. Noyes (United States) v. Panama*, K. 6 (1933), 308, 311.
[573] Uluslararası Adalet Divanı (UAD), *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States v Iran)*, [1980] ICJ Rep 3 (24 Mayıs 1980).

devam eden eylemlerini daha sonra onaylaması nedeniyle sorumluluğu doğrudan İran'a atfetmiştir.

Divan, Humeyni'nin ABD hedeflerine saldırıya teşvik etmesinin, elçiliği ele geçirmek için özel bir yetki sağladığı ve öğrenci militanları de facto devlet ajanlarına dönüştürdüğü yönündeki ABD argümanını reddetmiştir. Nitekim Uluslararası Adalet Divanı, elçiliğin ele geçirilmesinin, daha sonra iktidara gelen devrimci hükümet tarafından tasvip edilmesinin bile, elçiliğin ilk ele geçirilişinin bağımsız ve özel niteliğini değiştirmediğini tespit etmiştir.[574] Dolayısıyla öğrencilerin davranışları, İran tarafından onaylanana kadar özel nitelikte olup devlete atfedilemez olarak değerlendirilmiştir.

Divan ayrıca, ABD Büyükelçiliği ve Konsolosluklarına el konulmasının doğrudan İran'a isnat edilemeyeceğini; ancak bunun, "İran'ın bu saldırılarla ilgili herhangi bir sorumluluktan muaf olduğu" anlamına gelmediğini belirtmiştir; çünkü İran'ın kendi davranışları, uluslararası yükümlülükleriyle çelişmiştir. Dolayısıyla Divan'a göre, "ilk aşamada" İran, el koyma fiilinin kendisinden değil, Büyükelçiliği ve personelini korumada veya el koyma başladıktan sonra müdahale ederek sonlandırmada tamamen başarısız olduğu için sorumlu tutulmuştur.[575] Divan, İran'ın yükümlülüklerinin ve ABD'nin yardım çağrılarının farkında olduğunu, bu yükümlülükleri yerine getirmek için gerekli araçlara sahip olduğunu ve buna rağmen "bu yükümlülüklere uymakta tamamen başarısız olduğunu" tespit etmiştir.[576]

Bu yaklaşımı benimseyen Divan, Diplomatik ve Konsolosluk İlişkilerine dair Viyana Sözleşmeleri kapsamındaki pozitif önleme ve koruma yükümlülüklerine dayanarak, İran'ın ihmallerinden dolayı devlet sorumluluğunu ileri sürmüş; ancak öğrenci militanların eylemlerinden kaynaklanan doğrudan sorumluluğu reddetmiştir. Böylece Divan, devlet yetkililerinin eylemsizliğine, düşmanca özel davranışları teşvik eden bir politikanın eşlik ettiği ve ABD yerleşkesine el konulmasını kolaylaştırmak amacıyla tasarlanmış olabileceği durumlarda bile, devlet sorumluluğunun kapsamını sınırlandırarak vekil yaklaşımının geçerliliğini kabul etmiştir.[577]

Olayların ikinci aşaması, İranlı öğrenciler tarafından ABD Büyükelçiliğinin işgalinin tamamlanmasını ve Tebriz ile Şiraz'daki Konsoloslukların ele geçirilmesini takiben ortaya çıkan olaylar serisini kapsamaktadır. Bu aşamayla birlikte öğrencilerin eylemleri doğrudan İran'a isnat edilmiştir. Buna yol açan temel neden, dönemin İran dini lideri Ayetullah

[574] UAD, *Reparation for Injuries Suffered in the Service of the United Nations*, 1949 ICJ, 36.
[575] UAD, *Reparation for Injuries Suffered in the Service of the United Nations*, 1949 ICJ, 32-33.
[576] UAD, *Reparation for Injuries Suffered in the Service of the United Nations*, 1949 ICJ, 32.
[577] Uluslararası Adalet Divanı (UAD), United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), K. 30 (1 Kasım 1979).

Hümeyni'nin 17 Kasım 1979 tarihli fermanıdır. Söz konusu ferman, ABD Büyükelçiliği'nin "casusluk ve komplonun merkezi" olduğunu ve "İslami harekete karşı çıkan kişilerin bulunduğu bu yerin uluslararası diplomatik koruma hakkına sahip olmadığını" iddia ederek başlamaktadır. Humeyni, elçilik binalarının ve rehinelerin mevcut durumlarının, ABD'nin eski Şah'ı yargılamak için iade etmesi ve mülkünün İran'a teslim edilmesine kadar devam edeceğini açıkça ilan etmiştir.[578]

Divan'a göre:

"…Ayetullah Humeyni ve İran Devleti'nin diğer organları tarafından söz konusu eylemlere onay verilmesi ve bu eylemlerin aralıksız devam etmesi, devam etmekte olan Büyükelçilik işgalini ve rehinelerin tutulmasını İran Devleti'nin eylemleri hâline dönüştürmüştür. Militanlar, işgali gerçekleştirenler ve rehineleri hapsedenler, bu aşamadan sonra artık İran Devleti'nin ajanları hâline gelmişlerdir; bu nedenle onların eylemlerinden dolayı İran Devleti uluslararası sorumludur…"[579]

2.3.4.3.İran-ABD Talepler Mahkemesi

İran-Amerika Birleşik Devletleri Talepler Mahkemesi, 1981 yılında İran ile Amerika Birleşik Devletleri arasında yaşanan rehine krizi ve diplomatik ilişkilerin kesilmesini takiben, bu sorunları çözmek amacıyla müzakere edilen Cezayir Bildirileri çerçevesinde kurulmuştur. Mahkeme, iki ülke arasındaki ekonomik ve diplomatik ilişkilerin kesintiye uğramasından doğan talepleri çözümlemek üzere tesis edilmiş bir uluslararası tahkim merciidir. Özellikle özel hukuk kişileri ve devletlerin maruz kaldığı zararlarla ilgili taleplerin—örneğin yatırım uyuşmazlıkları, mülkiyetin kamulaştırılması ve diğer mali taleplerin—tarafsız bir ortamda çözülmesini amaçlamaktadır. Bu tür bir mahkemenin kurulmasındaki temel gerekçe, taraflar arasındaki siyasi gerilimler nedeniyle ulusal mahkemelerde adil bir yargılamanın sağlanamayacak olmasıdır.[580]

Mahkemenin yetki alanı, ABD vatandaşlarının İran'a karşı, İran vatandaşlarının ABD'ye karşı ve doğrudan iki devlet arasında ileri sürülen talepleri kapsamaktadır. Mahkeme; sözleşme ihlalleri, mülkiyetin kamulaştırılması ve İran Devrimi'nin ardından uygulamaya konulan yaptırımlar nedeniyle ortaya çıkan özel hukuk ve kamu hukuku nitelikli ihtilafları

[578] Yusuf Aksar, *Temel Metin ve Davalarla Uluslararası Hukuk,* (Ankara: Seçkin Yayınevi, 2017), 365.
[579] Tahran Rehineler Davası (US Diplomatic and Consular Staff in Tahran Case (US v. Iran), ICJ Reports, 1980, 3)
[580] Homayoun Maf, "A Review of the Iran-United States Claims Tribunal", *Mision Juridica* 13/19 (Aralık 2020), 98-107.

karara bağlama yetkisine sahiptir. Ayrıca, birçok uyuşmazlığın karşılıklı taleplere dayalı olması nedeniyle Mahkeme karşı talepleri de inceleme yetkisine sahiptir. [581]

İran-Amerika Birleşik Devletleri Talepler Mahkemesi'nin emsal teşkil eden kararlarından biri, İran-Irak Savaşı sırasında ABD tarafından İran'a ait petrol platformlarına yönelik gerçekleştirilen askerî saldırılarla ilgilidir. Mahkeme, bu saldırıların savaş eylemi niteliği taşımasına rağmen, Cezayir Bildirileri ya da Mahkemenin yetkisi çerçevesinde bağlayıcılığı bulunan uluslararası hukuk yükümlülüklerinin ihlali anlamına gelmediği sonucuna varmıştır. Bunun yanı sıra, ABD tarafından İran'a ait malvarlıklarının –özellikle İran Merkez Bankası'na ait varlıkların– dondurulmasına ilişkin uyuşmazlıklar bağlamında Mahkeme, devletlerin yargı bağışıklığı (*sovereign immunity*) ilkesini, özel şahısların alacak haklarıyla dengeleyerek, uluslararası yatırım hukuku ve devlet sorumluluğu hukuku bakımından önemli içtihatlar geliştirmiştir.[582]

Yabancılara verilen zararlara ilişkin devlet sorumluluğu *İran-ABD Talepler Mahkemesi* nezdinde de atfedilmezlik ilkesi ve ayrı suç teorisi çerçevesinde incelenmiştir. Mahkeme, ABD'li yetkililer tarafından yapılan haksız sınır dışı etme, kamulaştırma ve sözleşme ihlali konularını değerlendirmiştir. Mahkeme, İran'ın yabancıları koruma görevini açıkça yerine getirmediği ifade etmiştir.[583] Bununla birlikte İran her ne kadar özel faaliyetleri bir şekilde yönlendirse bile, Mahkeme devlet dışı aktörlerin fiillerinden dolayı İran'a doğrudan sorumluluk atfetme konusunda, açık bir vekalet ilişkisi olmaksızın, isteksiz olduğunu göstermiştir.

İran-ABD Talepler Mahkemesi'nde görülen ve İslam Devrimi öncesi ile sırasında yaşanan olaylara ilişkin önemli bir hukuki uyuşmazlık olarak öne çıkan *Short/İran davasında*[584] davacı Alfred Short, İslam devrimi öncesinde ve sırasında özel kişiler tarafından gerçekleştirilen taciz ve korkutma eylemlerinin İran'dan ayrılmasına ve buna bağlı olarak mal kaybına yol açtığını iddia etmiştir. Davacı, bu eylemlerin İran'a atfedilebileceğini ve sınır dışı edilme eyleminin doğrudan devlet tarafından yapıldığını ileri sürmüştür.

Daire'nin çoğunluğu Taslak Maddelere atıfta bulunduktan sonra, bir devletin yeni hükümeti haline gelen devrimci bir hareketin üyelerinin davranışlarının bir devlet fiili olarak kabul edileceğini,[585] ancak "devrim destekçilerinin fiillerinin devlete isnat edilemeyeceğine"

[581] Maf, "A Review of the Iran-United States Claims Tribunal", 107.
[582] Maf, "A Review of the Iran-United States Claims Tribunal", 107.
[583] David D. Caron, "Attribution Amidst Revolution: The Experience of the Iran–United States Claims Tribunal", American Society of International Law Proceedings 84 (1990), 51, 65.
[584] *Short v. Islamic Republic of Iran, Award No. 312-11135-3, 14 Temmuz 1987, 16 Iran–United States Claims Tribunal Reports 76 (1987).*
[585] Birleşmiş Milletler Uluslararası Hukuk Komisyonu (BMUHK), *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğuna İlişkin Taslak Maddeler*, 2001, md. 10.

karar vermiştir.[586] Davacı, devrim liderleri tarafından verilen belirli direktiflere işaret edemediği veya ayrılmasına yol açan eylemlere bizzat karışan devrimci ajanları tespit edemediği için, İran hukuka aykırı fiillerden sorumlu tutulamamıştır.

Yargıç Brower, yazdığı muhalefet şerhinde çoğunluğun görüşünü çeşitli gerekçelerle eleştirmiştir. İlk olarak, Ayetullah Humeyni'nin Amerikan karşıtı düşmanca açıklamalarının, ABD vatandaşlarını İran'dan sınır dışı etmeye yönelik kasıtlı bir politikanın parçası olduğunu ve başıboş bir şekilde örgütlenmiş taraftarların eylemlerinin yeni hükümete mal edilebileceğini savunmuştur.[587] Ayrıca, bu koşullar altında Mahkeme'nin, ABD vatandaşlarının ülkeyi terk etmelerinin İran tarafından haksız bir şekilde sınır dışı edilmelerinin sonucu olduğuna dair çürütülebilir bir karine oluşturması gerektiğini belirtmiştir. Açık bir ifadeyle Brower, Humeyni'nin "sınır dışı etme coşkusunu bastırmadaki başarısızlığının… ortaya çıkan sonuçların sorumluluğunun kendisine atfedilmesine izin vermesi gerektiğini" vurgulamıştır. Brower'in muhalefet şerhi, diğer Mahkeme kararlarında sınırlı yankı bulmuştur.

Genel bir kural olarak, Mahkeme kararları devlet sorumluluğunun kapsamını kısıtlamakta ve bu tür davalarda devletin sorumluluğunu ortaya koymak isteyen davacılardan, *vekâlet* ilişkisini kanıtlamalarını şart koşan yüksek bir kanıt standardı talep etmektedir. Örneğin, Short davasından birkaç ay sonra karara bağlanan *Rankin/İran* davasında Mahkeme,[588] devrim ajanlarına verilen özel direktiflerin davacının ülkeyi terk etmesine ve mal kaybına yol açtığını davacının ispat etmesi gerektiğini teyit etmiştir. Mahkemeye sunulan kanıt olarak, ülkeyi yabancılardan arındırmaya yönelik genel ve yaygın bir resmi politikanın varlığı, Rankin'in ülkeyi terk etmesinden İran'ın doğrudan sorumlu olduğunu göstermek için yeterli olmamıştır.

İran'ı sınır dışı etme veya mal kaybından sorumlu tuttuğu davalar da dâhil olmak üzere, Mahkeme, açık ve kanıtlanmış bir vekâlet bağı olmadan özel fiillerin devlet sorumluluğunun kaynağı olamayacağı görüşünü desteklemiştir. Yeager/İran davasında[589] davacı, İran Devrim

---

[586] Short, K. 312-11135-3 (14 Temmuz 1987), 85.

[587] Rankin v. Islamic Republic of Iran (Rankin), K. 326-10913-2 (3 Kasım 1987), *Iran–United States Claims Tribunal Reports* 17 (1987), 135; Arthur Young & Co. v. Islamic Republic of Iran (Arthur Young), K. 338-484-1 (1 Aralık 1987), *Iran–United States Claims Tribunal Reports* 17 (1987), 245; Hilt v. Islamic Republic of Iran (Hilt), K. 354-10427-2 (16 Mart 1988), *Iran–United States Claims Tribunal Reports* 18 (1988), 154; Leach v. Islamic Republic of Iran (Leach), K. 397-195-1 (15 Kasım 1989), *Iran–United States Claims Tribunal Reports* 23 (1989), 233.

[588] Rankin v. Islamic Republic of Iran (Rankin), K. 326-10913-2 (3 Kasım 1987), *Iran–United States Claims Tribunal Reports* 17 (1987), 135; Arthur Young & Co. v. Islamic Republic of Iran (Arthur Young), K. 338-484-1 (1 Aralık 1987), *Iran–United States Claims Tribunal Reports* 17 (1987), 245; Hilt v. Islamic Republic of Iran (Hilt), K. 354-10427-2 (16 Mart 1988), *Iran–United States Claims Tribunal Reports* 18 (1988), 154; Leach v. Islamic Republic of Iran (Leach), K. 397-195-1 (15 Kasım 1989), *Iran–United States Claims Tribunal Reports* 17 (1989), 233.

[589] Yeager v. Islamic Republic of Iran (Yeager), K. 326-10583-2 (1987**),** *Iran–US Cl. Trib. Rep.* 17 (1987), 92; AJJ de Hoogh, "Articles 4 and 8 of the 2001 ILC Articles on State Responsibility, The Tadić Case and Attribution

Muhafızları mensuplarının kendisinin İran'dan ayrılmasına neden olduğunu kanıtlayabilmiştir. Muhafızlar, kamu görevlerini yerine getirdikleri ve ayırt edici kol bantlarıyla tanımlanan yerel bir milis teşkil ettikleri için Mahkeme, onları yeni kurulmakta olan Hümeyni hükümetinin de facto bir unsuru olarak kabul etmiştir. Sonuç olarak Daire, "İran'ın bir yandan hükümet otoritesinin devrimci 'Komiteler' veya 'Muhafızlar' tarafından kullanılmasını hoş göremeyeceğini ve aynı zamanda onlar tarafından işlenen haksız fiillerin sorumluluğunu reddedemeyeceğini" tespit etmiştir.[590] Bu süreçte Daire, Amerikan karşıtı faaliyetleri teşvik eden planlı bir devlet politikasını teyit etmiş olmasına rağmen, söz konusu davranışın özel nitelikte olması halinde İran'ın bundan sorumlu olmayacağını vurgulamıştır.[591]

Haksız kamulaştırma ile ilgili davalarda, Mahkeme tarafından UHK'nin 2001 tarihli Taslak Maddelerine açık ya da dolaylı bir şekilde dayanılarak benzer tespitler yapılmıştır.[592] Bu tür davalarda, devletin özel mülkiyetin kamulaştırılmasından doğrudan sorumlu tutulamayacağı; bu tür davranışları hoş görse veya teşvik etse bile, söz konusu kişilerin özellikle devlet adına hareket ettiği kanıtlanmadığı sürece devletin sorumluluğunun doğmayacağı vurgulanmıştır. Bu nedenle, örneğin *Pereira/İran*[593] ve *Computer Sciences Corp./İran* davalarında[594] Mahkeme, el koyma fiillerini gerçekleştiren Devrim Muhafızlarını İran ajanları olarak gördüğü için, davacının mülkünün bir kısmının kamulaştırılmasından İran'ı sorumlu tutmuştur.

İran tarafından etkin bir şekilde kontrol edilen şirketler tarafından gerçekleştirildiği iddia edilen ihlalleri içeren bir vakada, Mahkeme, devlet müdahalesine ilişkin açık bir kanıt bulunmadığı sürece, söz konusu şirket eyleminin özel ve ticari nitelikte kabul edilmesi gerektiğine ve İran'a atfedilemeyeceğine karar vermiştir.[595] Başka bir davada Mahkeme, devlete ait bir bankanın davacının mülkiyetindeki malı kontrol etmesini veya ele geçirmesini, devletin sorumluluğunu oluşturmayacağını belirtmiştir. Mahkemeye göre banka, ticari bir kuruluş sıfatıyla faaliyet göstermekte olup, kamu yetkisini kullandığını gösterecek herhangi bir

---

of Acts of Bosnian Serb Authorities to the Federal Republic of Yugoslavia", *British Yearbook of International Law* 72 (2001), 255, 271.

[590] İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 17 (1987), *Iran–US Cl. Trib. Rep.*, 92-105.

[591] Gregory Townsend, "State Responsibility for Acts of De Facto Agents," *Arizona Journal of International and Comparative Law* 14 (1997), 635-879.

[592] Charles Nelson Brower ve Jason D. Brueschke, *The Iran–United States Claims Tribunal* (The Hague: Nijhoff, 1998), 442-471; Akira Mouri, *The International Law of Expropriation as Reflected in the Work of the Iran–US Claims Tribunal* (Dordrecht: Nijhoff, 1994), 177-191.

[593] İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 5 (1984), *Iran–US Cl. Trib. Rep.*, 198.

[594] İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 5 (1984), *Iran–US Cl. Trib. Rep.*, 269.

[595] İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 12 (1986), *Iran–US Cl. Trib. Rep.*, 335, 348-349; İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 10 (1984), *Iran–US Cl. Trib. Rep.*, 228.

olgusal temel bulunmamaktadır.[596] Mahkeme, kamu iktisadi teşebbüsünün farklı tüzel kişiliğine saygı göstererek, bu tür teşebbüslerin hukuka aykırı fiillerinin devlete atfedilmesinden kaçınmıştır. Böylece, atfedilmezlik ilkesi, davranışın kurumsal ticari faaliyet bağlamında gerçekleşmiş olması koşuluyla, devletin bizzat davranışın sahibi olduğu durumlarda bile devletin sorumluluğunu reddetmiştir.[597]

3. DEVLETİN ŞİRKET EYLEMLERİNDEN DOLAYI SORUMLULUĞU

3.1. Şirketlerin İnsan Hakları İhlalleri Nedeniyle Devletin Sorumluluğu

Devlet, yürütme, yasama, yargı organları ile polis, ordu ve benzeri kamu görevlilerinin tüm eylem ve ihmallerinden sorumludur. [598] Bu durum, devlet organları veya görevlileri tarafından yetkilerinin görünürdeki sınırlarının ötesinde gerçekleştirilen eylemler için de geçerlidir. Bir eylem ya da ihmal devlete atfedilebiliyorsa ve bu davranış, bir antlaşma ya da uluslararası teamül hukuku çerçevesinde doğan bir yükümlülüğün ihlaline yol açmışsa, devlet uluslararası hukuk nezdinde sorumlu tutulur.[599]

Devletin sorumluluğuna ilişkin bu kuralların uluslararası insan hakları hukukuna uygulanabilir olduğu genel olarak kabul edilmektedir ve bu durum UHK'nin Taslak Maddelerinde ve Şerhinde açıkça belirtilmiştir. Nitekim, insan haklarına ilişkin kuruluşlar da devletin sorumluluğuna ilişkin genel kuralları, önlerine gelen insan hakları meselelerinin kilit yönlerine hem açıkça[600] hem de zımnen uygulamışlardır.[601]

Uluslararası insan hakları hukuku kapsamındaki bir devletin yükümlülükleri sadece ülkesiyle sınırlı değildir. Başlıca uluslararası insan hakları sözleşmeleri, devletin yükümlülüklerini hem bir devletin ülkesindeki bireylere hem de bir devletin yargı yetkisine tabi

[596] İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 9 (1985), *Iran–US Cl. Trib. Rep.*, 206, 238-239.
[597] J. Chalmers, "State Responsibility for Acts of Parastatals Organized in Corporate Form," *American Society of International Law Proceedings* 84 (1990), 84.
[598] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 4, para 6.
[599] Robert McCorquodale - Penelope Simons, "Responsibility Beyond Borders: State Responsibility for Extraterritorial Violations by Corporations of International Human Rights Law," *The Modern Law Review* 70/4 (2007), 601.
[600] Inter-American Court of Human Rights (I-ACtHR), *Awas Tingni v. Nicaragua*, *International Human Rights Reports* (IHRR), 2001, 153.
[601] Rick Lawson, "Out of Control. State Responsibility and Human Rights: Will the ILC's Definition of the 'Act of State' Meet the Challenges of the 21st Century?," *The Role of the Nation-State in the 21st Century*, ed. Maartje Castermans, Frans van Hoof ve Janneke Smith, 115; John Cerone, "Out of Bounds? Considering the Reach of International Human Rights Law," *Center for Human Rights and Global Justice Working Paper Number 5, 2006*, New York School of Law, 26, http://www.nyuhr.org/research_publications.html (Erişim: 5 Mart 2007).

olan bireylere açıkça genişletmektedir.[602] Amerikalılar Arası İnsan Hakları Komisyonu, ülkesel yargı yetkisi hakkında aşağıdaki ifadelere yer vermiştir:

"Madde 1(1) anlamında "yargı yetkisi" teriminin yalnızca ülke toprakları ile sınırlı ya da bu toprakları kapsayan bir terim olmadığını" belirtmiştir. Komisyon, bunun yerine, Amerikan Sözleşmesi'ne taraf olan bir devletin, belirli koşullar uyarınca, temsilcilerinin o devletin toprakları dışında etki doğuran veya üstlenilen eylem ve ihmallerinden sorumlu olabileceği görüşündedir."[603]

Avrupa İnsan Hakları Mahkemesi[604] ve İnsan Hakları Komitesi (İHK)[605] de benzer açıklamalar yapmıştır. Bu yargı yetkisi kavramı, yargı yetkisi tesis edilebildiği takdirde[606] bir devlet için ülkesi dışında da insan hakları konusunda potansiyel yasal yükümlülükler doğurabilir. [607] Buna göre, bir devletin güvenlik güçlerinin bu devletin ülkesi dışında bir kişiyi yakalaması, gözaltına alması ve işkence yapması ve devletin kendi vatandaşının pasaportunu başka bir devletteki konsolosluklarından birinde alıkoyması durumunda, devletler İHK tarafından Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'ni ("UMSHS") ihlal etmiş ve dolayısıyla uluslararası sorumluluğu doğmuş olur. İHK ayrıca İsrail'in işgal ettiği topraklardaki[608] bireylerle ilgili olarak MSHUS kapsamında yükümlülükleri olduğu ve Belçika'nın Somali'de BM barış gücü olarak görev yapan kuvvetleriyle ilgili olarak bu tür yükümlülükleri olduğu görüşünü benimsemiştir.[609] Bu ilke, İHK'nin Genel Şerhinde yinelenmiştir:

"Bir Taraf Devlet, kendi ülkesinin sınırları içinde bulunmasa bile, yetki ve fiilî kontrolü altında bulunan herkese Sözleşme'de belirtilen haklara saygı göstermeli ve bu hakları güvence

---

602 Amerikan İnsan Hakları Sözleşmesi (AİHS), 1969, md. 1/1.**;** Avrupa İnsan Hakları Sözleşmesi (AİHS), 1950, md. 1.**;** Ekonomik, Sosyal ve Kültürel Haklar Komitesi (CESCR), *Genel Yorum No. 8: Ekonomik Yaptırımlar ile Ekonomik, Sosyal ve Kültürel Haklara Saygı Arasındaki İlişki*, BM Dok. E/C.12/1997/8 (12 Aralık 1997), 7.

603 Amerika Devletleri İnsan Hakları Komisyonu, *Saldano v. Arjantin***,** Rapor No. 38/99 (11 Mart 1999), [17].; Amerika Devletleri İnsan Hakları Komisyonu, *Coard ve diğerleri v. Amerika Birleşik Devletleri*, Rapor No. 109/99 (29 Eylül 1999), [37].

604 European Court of Human Rights (ECtHR), *Drozd ve Janousek v. Fransa ve İspanya***,** Başvuru No. 127 47/8 (1992) 14 EHRR 745, [91]; Avrupa İnsan Hakları Sözleşmesi (AİHS), 1950, md. 1.

605 Medeni ve Siyasi Haklar Uluslararası Sözleşmesi (MSHUS), md. 2/1. İnsan Hakları Komitesi (İHK), *Genel Yorum No. 31(80): Taraf Devletlere Sözleşme Tarafından Yüklenen Genel Hukuki Yükümlülüğün Niteliği*, BM Dok. CCPR/C/21/Rev.1/Add.13 (26 Mayıs 2004), [3].

606 İnsan Hakları Komitesi (İHK), *Montero v. Uruguay*, Bireysel Başvuru No. 106/81, Görüşler (31 Temmuz 1983).

607 İnsan Hakları Komitesi (İHK), *López Burgos v. Uruguay*, Bireysel Başvuru No. 52/79, Görüşler (29 Temmuz 1981), [12.3].

608 İnsan Hakları Komitesi (İHK), *İsrail'e İlişkin Sonuç Gözlemleri* (1999), BM Dok. CCPR/C/79/Add.93, [10].

609 İnsan Hakları Komitesi, Belçika'ya İlişkin Sonuç Gözlemleri (1998), BM Dok. CCPR/C/79/Add.97, [14].

altına almalıdır. Bu yükümlülük, söz konusu yetki veya fiilî kontrolün hangi koşullarda elde edildiğinden bağımsız olarak geçerlidir."[610]

Aynı şekilde, Amerikalılar Arası İnsan Hakları Komisyonu, bireyler üzerinde bir kontrol uygulaması varsa, söz konusu topraklar üzerinde etkin bir kontrol olsun ya da olmasın, bir konunun bir devletin yargı yetkisi dahilinde olduğunu tespit etmek için yeterli olabileceğini belirtmiştir.[611] Komisyon, "ilke olarak, soruşturmanın, sözde mağdurun milliyeti veya belirli bir coğrafi alanda bulunup bulunmadığına değil, devletin, belirli koşullar altında, yetki ve kontrolü altındaki kişilerin haklarını gözetip gözetmediğine dayanması gerektiğini" belirtmiştir.[612] Bu bağlamda, *Alejandre v. Küba* davasında,[613] Küba ajanlarının uluslararası sularda iki sivil uçağı düşürerek tüm dört pilotu öldürmesi olayında, Komisyon, mağdurların Küba ajanlarının yetkisi altında olduklarına ve dolayısıyla Küba ajanlarının yargı yetkisine tabi olduklarına dair koşulların "kesin delillerini" tespit etmiştir.

Kontrol için daha düşük bir eşik testi Avrupa İnsan Hakları Mahkemesi tarafından *Ilascu v Moldova ve Rusya* davasında,[614] Moldovalı ayrılıkçı rejimin (MRT) suçunun Rusya'ya atfedilmesiyle ilgili olarak uygulanmıştır. Mahkeme, Rusya'nın MRT'ye siyasi ve askeri destek sağladığı ve MRT'nin "Rusya Federasyonu'nun etkin otoritesi ya da tam tersine en azından belirleyici etkisi altında" kaldığı bu davada, Rusya'nın Transdniestrian bölgesinin etkin kontrolünde olduğuna karar vermemekle birlikte, gerekli kontrol derecesinin mevcut olduğunu değerlendirmiştir.[615] Bu durum, Mahkeme'nin, devlet dışı aktörlerin başka bir ülkedeki eylemlerinin, devletin bu aktörler üzerinde yargı yetkisine sahip olduğunu ve dolayısıyla AİHS kapsamında ülke dışı yükümlülükleri bulunduğunu düşündürecek şekilde bir devlete atfedilebileceğini tespit etmesi için yüksek derecede etkin kontrol gerektirmediğini ortaya koymaktadır.

---

[610] İnsan Hakları Komitesi, *Genel Yorum No. 31(80): Taraf Devletlere Sözleşme Tarafından Yüklenen Genel Hukuki Yükümlülüğün Niteliği*, yukarıda n. 25, [10].

[611] Ralph Wilde, "Legal 'Black Hole'?: Extraterritorial State Action and International Treaty Law on Civil and Political Rights" (2005) 26 Michigan JIL 739, 802; ve bkz. David Cassel, "Extraterritorial Application of Inter-American Human Rights Instruments" F. Coomans ve M. Kamminga (der.), *Extraterritorial Application of Human Rights Treaties* (Antwerp: Intersentia, 2004) 175-181, 175.

[612] Coard ve diğerleri v. Amerika Birleşik Devletleri, 37.

[613] Alejandre v. Küba, Amerika Devletleri İnsan Hakları Komisyonu, Başvuru No. 11.589, Rapor 86/99, 29 Eylül 1999.

[614] Avrupa İnsan Hakları Mahkemesi, *Ilascu ve Diğerleri v. Moldova ve Rusya*, Başvuru No. 48787/99, Büyük Daire Kararı, 8 Temmuz 2004. Erişim: https://hudoc.echr.coe.int/eng?i=001-61886.

[615] Uluslararası Adalet Divanı (UAD), Soykırım Suçunun Önlenmesi ve Cezalandırılması Sözleşmesi'nin Uygulanması Davası (Bosna-Hersek/Sırbistan ve Karadağ)**,** Karar, 2007, [398-407], erişim: 10 Nisan 2007, http://www.icjcij.org/icjwww/idocket/ibhy/ibhyjudgment/ibhy_ijudgment_20070226_frame.htm**;** Marko Milanovic**,** "State Responsibility for Genocide"**,** *European Journal of International Law* 17,(2006) 553-585-586.

Kontrol testi için bir diğer örnek olarak *Loizidou v. Turkey* davası gösterilebilir. Bu dava AHİM'in devletlerin ülke dışındaki fiillerinden dolayı doğan sorumluluğun değerlendirildiği önemli bir karardır. 1974 Kıbrıs Barış Harekatı'ndan sonra Türkiye'nin fiilen kontrol ettiği Kuzey Kıbrıs ait mülküne erişimi engellen Kıbrıslı Rum vatandaşı Titina Loizidou, Türkiye aleyhine AİHM'ye başvurmuştur. Mahkeme, Türkiye'nin söz konusu bölge üzerinde "etkin kontrol" sahibi olduğunu ve bu nedenle Kuzey Kıbrıs'taki insan hakları ihlallerinden sorumlu tutulabileceğini belirtmiştir. Bu karar, AİHM içtihadında etkin kontrol testinin şekillenmesinde dönüm noktası olmuştur; çünkü Mahkeme, bir devletin yalnızca kendi sınırları içindeki değil, fiilen kontrol ettiği başka topraklardaki fiillerinden de Avrupa İnsan Hakları Sözleşmesi uyarınca sorumlu olabileceğini açıkça ortaya koymuştur.[616]

Bir diğer örnek olarak *Al-Skeini v. United Kingdom* davası gösterilebilir. Bu dava, 2003 yılında İngiltere güçlerinin işgali altındaki Irak'ta sivillerin ölümüyle sonuçlanan olaylara ilişkindir. Başvurucular, ölen yakınlarının yaşam haklarının ihlal edildiğini ve etkin soruşturma yürütülmediğini ileri sürmüştür. AİHM, İngiltere'nin Irak'taki belli bölgelerde kamu gücünü kullandığını ve dolayısıyla AİHS m.1 anlamında yargı yetkisini icra ettiğini kabul etmiştir. Mahkeme, bir devletin başka bir ülkede kamu gücü kullandığı durumlarda bireyler üzerinde yetki ve kontrol sahibi olması nedeniyle Sözleşme kapsamındaki yükümlülüklerinin devam ettiğini vurgulamıştır.[617]

Uluslararası Adalet Divanı (UAD) tarafından verilen Duvar hakkındaki Danışma Görüşünde ise İsrail'in işgal altındaki Filistin topraklarıyla ilgili olarak MSHS, ESKHUS ve Çocuk Hakları Sözleşmesi (ÇHS) kapsamında yükümlülükleri olduğunu ve MSHS'nin "bir devletin kendi ülkesi dışında yargı yetkisini kullanırken gerçekleştirdiği eylemler bakımından uygulanabilir" olduğunu ifade etmiştir.[618] Bu görüş, UAD tarafından Demokratik Kongo Cumhuriyeti ve Uganda davasında, Uganda'nın Demokratik Kongo Cumhuriyeti topraklarındaki eylemleriyle ilgili olarak UMSHS, ÇHS ve Afrika İnsan ve Halkların Hakları Şartı'nın uygulandığı sonucuna varılarak teyit edilmiştir.[619] Nitekim bu son davada Divan daha da ileri giderek "uluslararası insan hakları araçlarının, bir devletin kendi toprakları dışında, özellikle de işgal altındaki topraklarda yargı yetkisini kullanırken gerçekleştirdiği eylemler

[616] Avrupa İnsan Hakları Mahkemesi (AİHM), *Loizidou v. Turkey (Merits)*, B. No. 15318/89 (18 Aralık 1996).
[617] Avrupa İnsan Hakları Mahkemesi (AİHM), *Al-Skeini and Others v. the United Kingdom*, B. No. 55721/07 (7 Temmuz 2011).
[618] Uluslararası Adalet Divanı (UAD), *Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 9 July 2004, General List No. 131, 106-109; McCorquodale - Simons, "Responsibility Beyond Borders," 603-604.
[619] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Merits (2006) 45 ILM 271, para. 217.

bakımından uygulanabilir olduğunu" kaydetmiştir.[620] UAD bu sonuca varırken, tüm devletlerin (sadece işgalci güçlerin değil) (bir devletin taraf olduğu) uluslararası insan hakları sözleşmeleri kapsamındaki yükümlülüklerinin ve zorunlu olarak uluslararası teamül hukukunun bir parçası olan tüm insan haklarının, bir devletin kendi toprakları dışındaki eylemleriyle ilgili olarak uygulanabilir olduğunu belirlemektedir.

3.2. Şirketlerin Ülke Dışı Faaliyetlerinden Dolayı Devletin Sorumluluğu

Devletin sorumluluğuna ilişkin 2001 tarihli Taslak Maddeler, şirketin uluslararası hukuku ihlal eden fiillerinin bir devlete atfedilmesini, iki durumda uluslararası sorumluluğa yol açacak şekilde mümkün kılmaktadır. Birincisi, devletin şirkete kamu gücünü kullanma yetkisi vermesi; ikincisi ise şirketin devletin "talimatları, yönlendirmesi veya kontrolü altında" hareket etmesidir. Buna ek olarak, devletin şirket faaliyetlerine yardım ve destek vererek başka bir devletin veya şirketin işlediği uluslararası haksız fiile iştirak etmesi halinde de devlet, uluslararası hukuk bakımından sorumlu olacaktır. Bu durumların tamamında, söz konusu fiiller ilgili devletin toprakları dışında işlenmiş olsa dahi devlete atfedilebilir.

Bu kapsamda ayrıca, Taslak Maddelerin 11.maddesine yer vermek gerekir. Bu madde devletin sorumluluğunu doğurabilecek özel bir durumu düzenlemektedir. Bu maddenin Türkçeye çevrilmiş hali aşağıda verilmiştir:

"Önceki maddelere göre devlete isnat edilemeyen bir davranış, bu devlet tarafından söz konusu davranışın kendi davranışı olarak tanındığı ve benimsendiği hâlde ve ölçüde, uluslararası hukuka göre bu devletin fiili olarak kabul edilir."[621]

Bu maddeden de görüldüğü üzere, bir devlet başlangıçta kendisine ait olmayan bir eylemi sonradan açıkça benimser veya tasvip ederse, söz konusu fiil devlete aitmiş gibi değerlendirilecektir. Böylece, öncesinde herhangi bir organik ya da işlevsel bağ bulunmayan kişi veya grupların fiilleri, devletin açıkça sahiplenmesiyle ona isnat edilebilir. Ancak bu tür bir sahiplenmenin örtük yani zımni değil, açık ve kararlı bir şekilde yapılmış olması gerekir. Bu duruma örnek olarak 1980 tarihli Tahran Rehineler Davası gösterilebilir. Uluslararası Adalet Divanı, başlangıçta bireysel hareket eden öğrencilerin Tahran'daki ABD Büyükelçiliğini işgal etmelerinin, İran makamlarının bu eylemleri açıkça benimsemeleri sonucunda devlete atfedilebilir hale geldiğine karar vermiştir. Dolayısıyla Madde 11, devletin doğrudan emir

[620] McCorquodale - Simons, "Responsibility Beyond Borders", 604.
[621] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5.

vermediği veya kontrol etmediği fiilleri dahi, sonradan benimsemesi yoluyla kendi eylemi haline getirmesini sağlayan bir isnat yoludur.

Şirketlerin ülke dışı eylemleri bağlamında, sanayileşmiş devletlere ait İhracat Kredi Ajansları (*Export Credit Agencies* – ECAs) önemli bir örnek teşkil etmektedir. Bu ajanslar, devlet organı olmamakla birlikte ayrı tüzel kişilikler olarak faaliyet göstermektedir. Ulusal yasalar, düzenlemeler veya işlevlerini yerine getirmelerini sağlayan resmi tüzüklerle yetkilendirilmişlerdir. Bu çerçevede ECAs'a, ulusal şirketlerin ticaret ve sınır ötesi yatırımlarını doğrudan veya dolaylı olarak destekleme ve geliştirme sorumluluğu verilmiştir. Görevlerini yerine getirirken ECAs, çoğu zaman yabancı devletlerde ticari faaliyetlerde bulunmaktadır. Örneğin, uluslararası ticari ortaklıklar kurmak amacıyla resmi hükümet heyetlerinin yurt dışı ziyaretlerine katılabilir veya yerel pazarlarda iş fırsatları yaratmak ve piyasa verilerini toplamak için başka ülkelerde ofisler açabilirler. Ancak ECAs'ın bu tür sınır ötesi faaliyetleri sırasında insan haklarını ihlal etmesi – örneğin, istihbarat toplama sürecinde mahremiyet hakkını çiğnemesi – halinde, söz konusu eylemler devlete atfedilebilir ve bu durum uluslararası hukuk kapsamında devletin sorumluluğunu doğurabilir.[622]

Bu tür durumlarda, kamu gücü yetkisiyle donatılmış şirketin ülke dışı faaliyetleri devlete atfedilebilir. Bu tür faaliyetlerin uluslararası insan hakları hukukunu ihlal ettiği durumlarda veya şirketin yetkisini aştığı durumlarda devletin uluslararası sorumluluğu doğacaktır.[623]

İhracat Kredi Ajansları (*İKA*), ulusal şirketlerinin küresel pazarlardaki rekabet gücünü artırmak amacıyla onlara geniş bir hizmet yelpazesi sunmaktadır. Bu hizmetler, ihracat kredisi sağlama ve risk sigortası sunmaktan diğer devletlerde önemli bağlantılar geliştirmeye ve yurtdışındaki hükümet ticaret heyetlerine katılmaya kadar uzanmaktadır. Daha önce de tartışıldığı üzere, İKA'nn eylemleri çoğu durumda devlete atfedilebilmektedir. Devlet şirketinin doğrudan yabancı yatırımlarını desteklemek amacıyla bu tür hizmetleri sağlaması, uluslararası hukuka aykırı fiillerde devlete yardım ve yataklık etme olarak değerlendirilebilir.[624] Örneğin, bir devlet veya onun İKA'sı, ulusal şirketlerinin başka bir devletteki faaliyetleri için krediler, siyasi risk sigortası veya yatırım garantileri gibi finansman desteği sunabilir. Bu türden bir durumda, ev sahibi devlet, şirketin veya onun bağlı kuruluşunun kendi ülkesinde uluslararası insan hakları yükümlülüklerini (örneğin uluslararası çalışma haklarının korunması gibi) ihlal

[622] McCorquodale - Simons, "Responsibility Beyond Borders," 606-607.
[623] *International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts*, Madde 7.
[624] McCorquodale - Simons, "Responsibility Beyond Borders," 612.

ederek faaliyet göstermesine izin veriyorsa ve şirketin ana devletinin de benzer uluslararası insan hakları yükümlülükleri bulunuyorsa, ana devletin uluslararası hukuka aykırı bir fiile yardım ve yataklık ettiği sonucuna varılabilir.[625]

Ana devletin, şirketlerin ülke sınırları dışındaki faaliyetlerinde suç ortağı olduğu durumlarda görülmektedir. Taslak Maddeler yalnızca devletlerin sorumluluğunu ele alsa da, diğer aktörlerin sorumluluğa başvurma veya sorumluluk üstlenme olasılığını dışlamamaktadır. Bireylerin giderek artan sayıda uluslararası suça ilişkin uluslararası sorumluluğa maruz kalabilecekleri artık kabul edilmektedir. Buna ek olarak, şirketlerin ve diğer ticari kuruluşların uluslararası hukuk uyarınca uluslararası suç işlememe yükümlülükleri olduğu ve bu nedenle uluslararası suç teşkil eden fiillere iştirak ve bu fiillerin işlenmesi nedeniyle uluslararası sorumluluğa maruz kalabilecekleri görüşü de yaygın bir şekilde savunulmaktadır.[626]

Bu nedenle, ana devletin bir şirkete, ana devlet tarafından işlenmesi halinde uluslararası haksız fiil teşkil edecek fiillerin işlenmesinde veya bu fiillere iştirak edilmesinde yardım veya destek vermesi halinde, en azından yardım veya desteğin "bu fiile önemli ölçüde katkıda bulunduğu" durumlarda, söz konusu devlet uluslararası sorumluluk altına girecektir. Dolayısıyla, ana devletin bir şirkete, örneğin "rejim değişikliği" amacıyla destek vererek ya da İKA aracılığıyla kredi, siyasi risk sigortası veya yatırım garantileri sağlayarak yardım etmesi ve şirketin uluslararası suç teşkil eden insan haklarını ihlal etmesi halinde, bu devlet uluslararası insan hakları hukuku kapsamında sorumluluk altına girebilir.[627] Yukarıdaki durumlarda devletin suç ortaklığı nedeniyle sorumlu tutulabilmesi için, devletin haksız fiilin işlenmesine yardımcı olduğunu veya yardım ettiğini bilmesi gerekir.

Bağlı şirketlerin ayrı bir tüzel kişilik olduğu ve bu nedenle ana şirketlerinden zorunlu olarak farklı olduğu; uluslararası hukuk bakımından ana şirket ile bağlı şirketin, her birinin kendi devletlerinin münhasır yargı yetkisine tabi olduğu uzun zamandır ileri sürülmektedir.[628] Bu görüş büyük ölçüde Uluslararası Adalet Divanı'nın (UAD) *Barcelona Traction Davası* kararına dayanmaktadır.[629] Ancak, söz konusu karar hem kendi bağlamı —yani uluslararası hukuktaki diplomatik koruma amacıyla verilmiş olması— hem de çok uluslu şirketler (ÇUŞ'ler) dâhil olmak üzere kurumsal gruplara ilişkin anlayıştaki gelişmeler ışığında yeniden

[625] McCorquodale - Simons, "Responsibility Beyond Borders," 612.
[626] Andrew Clapham**,** "State Responsibility, Corporate Responsibility, and Complicity in Human Rights Violations", *Responsibility in World Business: Managing Harmful Side-Effects of Corporate Activity*, mlf. Lars Bomann-Larsen ve Oddny Wiggen (Tokyo: United Nations University Press, 2004), 50-81.
[627] Ricardo Israel Zipper**,** "Politics and Ideology in Allende's Chile", *Journal of Latin American Studies* 22/1-2 (Mart 1990), 169-176.
[628] N. L. Dubin, "The Direct Application of Human Rights Standards to, and by, Transnational Corporations", *The Review of the International Commission of Jurists* 61 (1999), 35.
[629] Uluslararası Adalet Divanı (ICJ), K. 1970 ICJ Reports 3 (5 Şubat 1970).

değerlendirilmelidir.[630] Devlet uygulamalar şirketler gruplarının yasal yapısını devlet düzenlemelerinden kaçınmak amacıyla kullanma eğilimleriyle başa çıkmak için çeşitli yaklaşımlar sergilemektedir.[631] Bazı mahkemelerin, birçok uluslu şirketin yalnızca teorik olarak ayrı bölümlerini değil, tüm faaliyetlerini dikkate alarak yabancı ana şirketleri bir devletin yargı yetkisine dâhil etme yönündeki uygulamaları uzun bir geçmişe sahiptir. Örneğin, ABD'de "işletmenin birliği veya bütünleşmesi" ve "alter ego olarak hareket etme" gibi geniş teoriler geliştirilmiş ve yabancı ana şirketin ABD'de fiilen mevcut, yerleşik veya "bulunabilir" olduğu hukuken kabul edilmiştir. Benzer şekilde, Avrupa Adalet Divanı'nın rekabet davalarındaki yaklaşımı, kurumsal grup yapısının parametrelerini ve grup içindeki ilişki gerçekliğini incelemeyi içermektedir.[632]

İfade edilmesi gereken bir diğer husus devletlerin uluslararası hukuk kapsamında şirketin ülke dışı faaliyetleri üzerinde kural koyucu ve yargısal yargı yetkisi kullanma konusunda geniş yetki ve kapasiteye sahip olduğudur. Buna ek olarak, söz konusu şirketin bir ana şirket olduğu durumlarda, ana devlet, uluslararası hukuk uyarınca, ana şirketin söz konusu bağlı iştiraklere belirli bir hareket tarzı dayatmasını veya herhangi bir sözleşmeye belirli şartlar eklemesini talep ederek, tamamen sahip olduğu veya kontrol ettiği yabancı bağlı iştirakleri dolaylı olarak düzenleme hakkına sahiptir.[633]

Son zamanlarda kabul gören bir görüşe göre, çok uluslu bir şirket tek bir varlık olarak değerlendirildiğinde, her birimi belirli bir işlevi yerine getirir ve ana şirket uzmanlık, teknoloji, denetim ve finans sağlar. Ana şirketin bu işlevlerle ilgili ihmalleri zarara yol açarsa, sorumluluk ona ait olur. Benzer şekilde, uluslararası hukuk kapsamında her devlet, ülke sınırları dışında zarara yol açacak şekilde hareket etmeme yükümlülüğüne sahiptir. Bu yükümlülük, devletin bu faaliyetler üzerinde kontrol sahibi olması gereken durumlarda sınır ötesi çevresel ve insan hakları etkilerini de kapsar. Devlet, ulusal faaliyetlerinin başka devletlere veya halklara zarar vereceğini bilmesi hâlinde bu zararı önlemekle yükümlüdür; aksi hâlde sorumluluk doğar. Bu sorumluluk, uluslararası insan hakları hukuku kapsamında, devletin ülkesindeki kişiler üzerinde etkili kontrol ve düzenleme önlemleri almasını gerektiren özen yükümlülüğünün bir parçasıdır. Günümüzde, devletlerin kendi topraklarındaki şirketlerin faaliyetlerini yeterince denetlememesi nedeniyle bu yükümlülüğün ihlal edildiği birçok örnek bulunmaktadır.

[630] Janet Dine, *The Governance of Corporate Groups* (Cambridge: Cambridge University Press, 2000), 65
[631] Dine, *The Governance of Corporate Groups*, 63.
[632] McCorquodale - Simons, "Responsibility Beyond Borders," 616.
[633] McCorquodale - Simons, "Responsibility Beyond Borders," 616.

Ev sahibi devletler, şirketin yabancı iştiraklerinin ülke dışı faaliyetlerini kontrol etmek için bazı araçlara sahiptir; bir devletin ev sahibi devlette bu tür bir faaliyetin insan hakları üzerindeki etkisi hakkında "yeterli bilgiye" sahip olması halinde, ev sahibi devletin "bu amaçla yasal düzenlemeler yaparak riski önleme ve azaltma" yükümlülüğü vardır. Bu yükümlülüğün yerine getirilmemesi, uluslararası sorumluluğun doğmasına yol açan gerekli özen yükümlülüğünün ihlali anlamına gelecektir.[634] Artık devletlerin kendi uyruğu olan şirketlerin (veya bu şirketlerin yabancı iştiraklerinin) ülke dışındaki faaliyetlerinde insan haklarını ihlal eden eylemlerde bulunabileceklerini bilemeyecekleri düşünülemez. Bazı ülke dışı şirket faaliyetlerinin insan hakları, özellikle de ekonomik, sosyal ve kültürel haklar üzerindeki olumsuz etkileri artık çok iyi belgelenmiştir.[635]

Bu bağlamda, bir şirketin yabancı iştirakinin eylemleri doğrudan ana devlete atfedilemese de, ana devletin ana şirket üzerinde yeterli kontrole sahip olduğu ve iştirakin insan hakları hukukunu ihlal etme olasılığı hakkında yapıcı bilgiye sahip olduğu ve bu tür faaliyetlerin insan hakları üzerindeki etkilerine ilişkin olarak gerekli özen yükümlülüğü uygulanmasını gerektirdiği ileri sürülebilir. Bu yükümlülük, bir devletin, bu tür faaliyetlerin yabancı bir yan kuruluş aracılığıyla yürütüldüğü durumlarda bile, bu tür kuruluşların uluslararası insan hakları hukukunu ihlal ederek faaliyet göstermemesini sağlamak için makul adımlar atmasını gerektirir. Söz konusu yükümlülük, bunlarla sınırlı olmamakla birlikte, ana devletin iç mevzuatı yürürlüğe koymasını, insan hakları açısından etkili değerlendirmeler yapılmasını, bu tür etkilerin daha sonra hafifletilmesini ve ana devletin yargı organlarında bir çözüm yolu sağlanmasını gerektirebilir.[636]

3.3. Kamu Gücü Yetkisi Kullanan Şirketler

Bir şirketin yürüttüğü faaliyetler, bu şirket tamamen bir devlete ait olsa ya da devletin bu şirket üzerinde kontrol gücü bulunsa dahi, ilk bakışta uluslararası hukuk kapsamında bir devlete atfedilemez.[637] Bununla birlikte, kamu veya kamu gücü fonksiyonlarını icra eden özel kuruluşların eylemlerinin bir devlete atfedilmesi uzun zamandır tartışılmaktadır. Bu tür bir atıf,

---

[634] McCorquodale - Simons, "Responsibility Beyond Borders," 619.

[635] ECOSOC, *The Realization of Economic, Social and Cultural Rights: The Relationship between the Enjoyment of Human Rights, in particular, International Labour and Trade Union Rights, and the Working Methods and Activities of Transnational Corporations*, UN Doc E/CN.4/Sub.2/1995/11 (1995), [58], [61-64], [91]; ECOSOC, *Human Rights Principles for Transnational Corporations and Other Business Enterprises, Introduction*, UN Doc E/CN.4/Sub.2/2001/WG.2/WP.1/Add.1 (2002).

[636] McCorquodale - Simons, "Responsibility Beyond Borders," 623.

[637] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5.

bazı kamu işlevlerini sürdüren devlet kuruluşlarının özelleştirilmesindeki artışla birlikte daha da gerekli hale gelmiştir.[638]

Bir davranışın devlete atfedilebilmesi için, şirketin davranışının "diğer özel veya ticari faaliyetlerle değil, devlet faaliyetleriyle" ilişkili olması gerekmektedir.[639] Şirketin davranışının devlete atfedilebilmesi için kilit faktör, şirketin devlet tarafından mülkiyet derecesi değil, kamu gücünü kullanma yetkisidir.[640]

Bir şirketin ana devletin talimatları doğrultusunda hareket etmesi halinde, bu tür eylemlerin devlet faaliyeti teşkil etmesine gerek yoktur. UHK, "yardımcı olarak istihdam edilen veya komşu ülkelere "gönüllü" olarak gönderilen veya yurtdışında belirli görevleri yerine getirmeleri için talimat verilen" kişi veya kuruluşları buna örnek olarak göstermektedir. Bu konu, Irak'ta işgalci güçler tarafından gerçekleştirilen (hukuka aykırı) eylemlerin başlangıcından bu yana daha da belirgin hale gelmiştir. Burada, ilgili devletler tarafından istihbarat sağlamaktan bu tür askeri eylemleri desteklemek için devlet altyapısını yeniden oluşturmaya kadar çok çeşitli hizmetler sunmak üzere ne kadar çok sayıda özel şirketle sözleşme yapıldığı ortaya çıkmıştır.[641] Nitekim Ebu Gureyb'de (ve başka yerlerde) mahkumlara yönelik kötü muamelenin ortaya çıkmasının ardından yapılan soruşturmalar, bu kötü muamelelerin bir kısmının özel şirket çalışanları tarafından yapıldığını göstermiştir.[642]

3.4. Devletin Talimatıyla/ Yönlendirmesiyle Hareket Eden Şirketler

Bir şirket, devletin kamu gücü yetkilerini kullanmıyorsa veya böyle bir yetkiyi kullandığı kanıtlanamıyorsa, faaliyetleri yalnızca devletin "talimatları doğrultusunda hareket etmesi veya devletin yönlendirmesi ve kontrolü altında bulunması" durumunda devlete atfedilebilir. Bu tür durumlarda, şirketin davranışları ancak ilgili faaliyetin doğrudan devletin talimatı veya kontrolü kapsamında olması halinde devlete atfedilebilir; devletin kontrolüne yalnızca dolaylı olarak bağlı olan faaliyetler bundan hariç tutulur. Bununla birlikte, bir şirketin ana devletin kontrolü altında hareket ettiği ve belirli talimatları göz ardı ettiği veya bu

[638] Adam McBeth, "Privatising Human Rights: What Happens to the State's Human Rights Duties when Services are Privatised?" (2004) 5 *Melbourne Journal of International Law* 133.
[639] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5.
[640] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 5.
[641] Major Susan S. Gibson, "Lack of Extraterritorial Jurisdiction over Civilians: A New Look at an Old Problem", *Military Law Review* 148 (1995), 114.
[642] Mark W. Bina, "Private Military Contractor Liability and Accountability after Abu Ghraib", *John Marshall Law Review* 39 (2005), 1237.

talimatlara aykırı davrandığı durumlarda dahi, söz konusu eylemleri yine de devlete atfedilebilir. Bu, devletin uluslararası hukuktaki sorumluluğunun, kontrol ve gözetim ilişkisine dayalı olarak genişletilmesine imkân tanıyan temel bir prensibi yansıtmaktadır.[643]

UAD'nin Nikaragua davasındaki testi, devlet dışı aktörlerin bir devlet tarafından kontrol edildiğinin tespiti için bu kadar yüksek bir eşik oluşturduğu için eleştirilmiştir. Ancak, bu test UAD tarafından Soykırım Sözleşmesi'nin uygulanmasına ilişkin 2007 tarihli kararında desteklenmiştir.

Şirketlerin devletler tarafından ülke dışı askeri faaliyetlerinde, ticarette ve diğer alanlarda giderek daha fazla kullanılmasıyla birlikte, bu şirketlerin faaliyetlerinin devlete atfedilmesi olasılığı açıkça ortaya çıkmaktadır. Bu tür faaliyetlerin uluslararası insan hakları hukukunu ihlal ettiği durumlarda, şirketin talimatlara aykırı davrandığı durumlar da dahil olmak üzere, devletin uluslararası sorumluluğu doğacaktır.[644]

[643] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, Article 8, para 1.
[644] McCorquodale - Simons, "*Responsibility Beyond Borders*," 611.

ÜÇÜNCÜ BÖLÜM

SİBER EYLEMLER VE SORUMLULUK

Çalışmanın bu bölümü, siber saldırıların uluslararası hukuk açısından haksız fiil teşkil edebileceği çeşitli durumları ele almaktadır. Öncelikle belirtilmesi gereken, mevcut uluslararası hukukta siber saldırıları doğrudan yasaklayan genel bir kuralın bulunmadığıdır. Başka bir ifadeyle, devletler arasında gerçekleştirilen siber saldırıları açıkça yasaklayan spesifik bir uluslararası hukuk normu mevcut değildir. Bu tür eylemler genellikle dostane olmayan ya da düşmanca faaliyetler olarak değerlendirilmektedir.

Siber saldırıları doğrudan yasaklayan bir kural olmamasına rağmen, birçok durumda gerçekleştirilen bir siber saldırı belirli uluslararası hukuk normlarının ihlalini oluşturabilir. Örneğin, yabancı bir devletin bilgisayar sistemlerine yönelik bir siber saldırı, uluslararası hukukun temel ilkelerinden biri olan egemenlik ihlali veya müdahale yasağı prensibinin ihlali anlamına gelebilir. Bu çerçevede, bu bölümde siber uzaydaki devlet dışı aktörler tarafından ihlal edilebilecek uluslararası hukuk normları ele alınacaktır. Bunlar; egemenliğin ihlali, müdahale yasağı, kuvvet kullanma yasağı ve insan hakları ihlalleridir.

1. DOSTANE OLMAYAN FİİL OLARAK SİBER EYLEMLER

Yukarıda belirtildiği gibi, uluslararası hukukta siber saldırıları doğrudan yasaklayan açık bir kural bulunmamaktadır. Devlet destekli devlet dışı aktörler tarafından gerçekleştirilen siber saldırıların hukuka uygunluğu ise casusluk faaliyetleriyle karşılaştırılabilir. Daha açık bir ifadeyle, uluslararası hukukta casusluğu yasaklayan özel bir kural mevcut değildir.

Kanaatimizce, devletlerin siber saldırıları doğrudan yasaklayan özel uluslararası hukuk kuralları kabul etmeleri birkaç nedenle oldukça olası değildir. Öncelikle, devletler bu gri alanda hareket etme yeteneklerinin hukuk tarafından kısıtlanmasını istemezler. Ayrıca, bir siber saldırının düşmanca ya da dostane olmayan bir niyet taşıyıp taşımadığını ayırt etmek çoğu zaman zor olabilmektedir.

Uluslararası hukukun siber uzaya uygulanabilirliği üzerine önemli çalışmalardan biri olan Tallin El Kitabı 2.0'da, siber saldırıları yasaklayan doğrudan bir kurala yer verilmemekle birlikte, mevcut diğer kurallar incelendiğinde siber saldırıların yasaklanmasının amaçlandığı

anlaşılmaktadır. Buna ek olarak, siber saldırıları yasaklayan genel bir kuralın yokluğu, Tallin El Kitabı 2.0'ın üçüncü kuralında ifade edilen devletlerin siber saldırıları yürütme özgürlüğü kavramından ayrı tutulmalıdır.[645]

Her ne kadar uluslararası hukukta siber saldırıları doğrudan yasaklayan açık bir kural bulunmasa da, bu saldırılar dostane olmayan ve düşmanca eylemler olarak nitelendirilebilir. Daha açık bir ifadeyle, bir devlet tarafından diğer bir devlete yönelik, uluslararası hukuka aykırı olmamakla birlikte aleyhte durum, ihmal veya nezaketsizlik teşkil eden fiiller dostane olmayan fiil olarak tanımlanabilir. Ancak, bu tür fiiller genellikle doğrudan hukuki sonuç doğurmaz.[646]

Nikaragua davasında dostane olmayan fiillerin uluslararası hukuk kapsamında yasaklanmadığını açıkça belirten UAD şu ifadelere yer vermiştir:

"Bu türden bir ödev (dostane olmayan fiillerden bulunmaktan kaçınma) elbette bir antlaşmada açıkça belirtilebilir veya hatta antlaşma metninden çıkan zorunlu bir sonuç olarak ortaya çıkabilir; ancak uluslararası teamül hukuku açısından, bu tür geniş kapsamlı bir kuralın varlığının devlet uygulamalarında kanıtlanmış olduğu açıkça görülmemektedir." [647]

Uluslararası hukukta dostane olmayan fiilleri yasaklayan açık bir düzenleme olmamasına rağmen, bu tür fiillerden kaçınılması gerektiği Birleşmiş Milletler Antlaşması'nın 2. maddesinin 2. paragrafı ve 33. maddesi ile "Birleşmiş Milletler Antlaşması Uyarınca Devletler Arasında Dostane İlişkiler ve İşbirliğine İlişkin Uluslararası Hukuk İlkeleri Bildirisi"nden çıkarılabilir.[648] Buna göre, "Uluslararası bir uyuşmazlığa taraf olan devletler ve diğer devletler, uluslararası barış ve güvenliğin korunmasını tehlikeye atacak şekilde durumu ağırlaştırabilecek her türlü eylemden kaçınacak ve Birleşmiş Milletler'in amaç ve ilkelerine uygun hareket edeceklerdir." [649]

Bununla birlikte, bu metinlerin hiçbiri, bu tür fiillerden kaçınmak adına bağlayıcı bir hukuki yükümlülük getirmemektedir. Bu nedenle, hem Nikaragua Kararı hem de söz konusu düzenlemeler, uluslararası hukukun dostane olmayan fiilleri yasaklamadığını açıkça ortaya koymaktadır.

Siber uzaydaki yeni devlet dışı aktörlerin, devletlerin desteğiyle gerçekleştirdiği siber operasyonlar, uluslararası hukuk açısından kesinlikle yasaklanmış ya da tamamen izin verilmiş

---

[645] Michael N Schmitt - Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 16.
[646] Dagmar Richter, "Unfriendly Act", *Max Planck Encyclopedias of International Law (MPIL),* (Ocak 2013), 1.
[647] Internatinal Court of Justice (ICJ), I.C.J. Reports 1986, (12 Kasım 1986).
[648] Richter, "Unfriendly Act", 1.
[649] Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations', *Birleşmiş Milletler Genel Kurulu* (24 Ekim 1970), Kanun No: UNGA Res 2625 (XXV), 103.

fiiller olarak nitelendirilemez. Devlet dışı aktörler tarafından gerçekleştirilen bu operasyonların bazı biçimleri ve sonuçları, egemenlik ilkesi, müdahale yasağı ve insan hakları ihlali gibi uluslararası hukukun temel normlarını ihlal edebilir. Burada özellikle vurgulanması gereken önemli bir nokta şudur: Devlet dışı aktörlerin yaptığı bir siber operasyon dostane olmayan veya düşmanca bir fiil olarak değerlendirilebilir, ancak bu her zaman uluslararası hukuk bakımından hukuka aykırı olduğu anlamına gelmez. Öte yandan, belirli bir siber operasyon uluslararası hukukun ilgili normlarını ihlal ettiğinde hukuka aykırı hale gelecektir.

Dolayısıyla, devlet dışı aktörler tarafından gerçekleştirilen ve devlet tarafından desteklenen siber eylemler, dostane olmayan fiiller olarak değerlendirilmektedir. Başka bir ifadeyle, bu tür fiiller uluslararası hukuk açısından hukuka aykırı sayılmamaktadır. Bu duruma verilebilecek en önemli örnek ise siber casusluk faaliyetleridir.

Uluslararası hukukta siber casusluk fiillerini doğrudan yasaklayan genel bir kural bulunmamaktadır. Ancak, siber casusluk bazı durumlarda uluslararası hukukun belirli normlarına aykırı olabilir. Tallinn Manual 2.0'ın 32. Kuralı da bu konuda benzer bir yaklaşım benimsemektedir. Buna göre, "Bir devlet tarafından barış zamanında gerçekleştirilen siber casusluk tek başına uluslararası hukuku ihlal etmese de, uygulama şekli açısından uluslararası hukuka aykırılık teşkil edebilir." [650] Ancak Kural 32, bu konudaki karmaşık durumu iki temel nedenle daha da zorlaştırmaktadır.

İlk olarak, Kural 32, Tallinn Manual 2.0'ın 'uluslararası hukuk tarafından düzenlenmeyen siber operasyonlar' konusunu ele alan 5. Bölümünde yer almakta olup, devlet dışı aktörler tarafından yürütülen ve uluslararası hukuk tarafından yalnızca sınırlı durumlarda düzenlenen siber operasyonlara ilişkin Kural 33 ile birlikte değerlendirilmiştir.[651] Siber casuslukla ilgili Kuralın bu bölümde yer alması, siber operasyonların hukuka uygunluğunun siber espiyonaj amacıyla gerçekleştirilip gerçekleştirilmediğine bağlı olarak değişiklik göstereceğini ifade etmektedir. Başka bir deyişle, Tallinn Manual 2.0'ın diğer bölümlerinde ele alınan farklı amaçlara sahip siber operasyonların aksine, siber casusluk faaliyetlerinin kendine özgü bir hukuki rejime tabi olduğu ima edilmektedir.

İkinci olarak, Tallinn El Kitabı'nın 32. Maddesi, casusluğun genel olarak uluslararası hukuk tarafından yasaklanmaması durumuna rağmen, casusluk faaliyetlerinin uluslararası hukukun bazı temel normlarını ihlal edebileceği yönündeki geleneksel ve yaygın görüşü esas almaktadır. Madde 32'nin şerhi, bu yaklaşımı açık ve detaylı biçimde ortaya koymaktadır.[652]

[650] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 168.
[651] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 168.
[652] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 172.

Bununla birlikte, Kural 32'ye ve diğer ilgili kurallara ilişkin Şerhin bazı bölümleri, siber casusluk konusunda genel bir yasak bulunmadığını ve siber casusluk faaliyetlerinin casusluk amacıyla yürütüldükleri sürece her zaman hukuka uygun sayılacağını savunan azınlık yaklaşımını destekliyor gibi görünmektedir.[653] Diğer bir deyişle, bu yaklaşım, söz konusu faaliyetlerin casusluk amacının, bu faaliyetlerin hukuka aykırılığını engelleyen bir durum olarak görülme eğiliminde olduğunu ifade eder. Kural 32'nin Şerhinde geliştirilen iki örnekten özellikle 9. paragrafta yer alan örnek dikkat çekicidir:

Uzmanlar, belirli bir ciddiyet eşiğine ulaşan uzaktan siber casusluğun uluslararası hukuku ihlal edip etmediği konusunda fikir birliğine varamamıştır. Örneğin, bir devletin başka bir devletin askeri siber sistemlerine rızası olmadan uzaktan eriştiği ve gigabaytlarca gizli veriyi uzun bir süre boyunca dışarı sızdırdığı bir durumu ele alalım. Uzmanların çoğunluğu, sızma eyleminin ciddiyetine bakılmaksızın hiçbir uluslararası hukuk yasağını ihlal etmediği görüşündedir. Uzmanlara göre uluslararası hukuk ihlalini oluşturan husus, sızma eyleminin yoğunluğu değil, kullanılan yöntemin hukuka aykırı olup olmadığıdır. Bununla birlikte, bazı uzmanlar, belirli bir noktada hedef devletin maruz kaldığı sonuçların o kadar ağır olduğunu (örneğin nükleer fırlatma kodlarının sızdırılması) ve operasyonun egemenliğin ihlali anlamına geldiğini (Kural 4) savunmaktadır.[654]

Uzmanlar, başka bir devletin yönlendirmesi veya kontrolü (Kural 17) altında hareket eden bir kişi tarafından bir devletin ülkesinde bulunan bir bilgisayara USB flash bellek yerleştirilmesi gibi yakın erişimli siber casusluk operasyonlarının hukuka uygunluğu konusunda da görüş birliğine varamamıştır. Çoğunluk, bu tür bir faaliyeti siber casusluk olması nedeniyle değil, kişinin başka bir devletin ülkesinde rızası olmaksızın bu işlemi gerçekleştirmesi sebebiyle egemenliğin ihlali olarak değerlendirmiştir. Buna karşılık, bazı uzmanlar, casusluk eylemlerinin egemenlik ihlali (Kural 4) ve müdahale yasağına (Kural 66) istisna teşkil ettiğini savunarak, bu faaliyetin hukuka aykırı olmayacağı görüşünü benimsemiştir.[655]

Sonuç olarak, siber casusluk faaliyetlerinin hukuka uygunluğu, diğer siber operasyonların hukuka uygunluğundan farklılık göstermemektedir: Siber casusluk için genel bir yasak bulunmamaktadır, ancak kullanılan siber operasyonlar uluslararası hukukun belirli normlarını ihlal edebilir. İncelenecek genel uluslararası kamu hukuku normlarının —yani ülkesel egemenlik, müdahale yasağı, kuvvet kullanma yasağı ve uluslararası insan hakları

[653] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 172.
[654] Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 4.
[655] Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 66.

hukuku— ihlaline ek olarak, siber casusluk eylemleri diplomatik ve konsolosluk hukuku, uluslararası ticaret hukuku, Dünya Ticaret Örgütü hukuku ve fikri mülkiyet hukuku gibi belirli uluslararası hukuk dallarının normlarını da ihlal edebilir. Buna rağmen, tek başına siber casusluk eylemlerinin dostane olmayan fiiller olarak değerlendirilmesi gerektiği ve dolayısıyla bu eylemlerden doğrudan bir uluslararası sorumluluğun doğmayacağı anlaşılmaktadır.

2.TEMEL ULUSLARARASI HUKUK NORMLARINI İHLAL EDEN SİBER EYLEMLER

2.1. Devletlerin Egemen Eşitliğini İhlal Eden Siber Saldırılar

Ülkesel egemenlik bir devlete iç sular, karasuları, takımada suları, hava sahası, kara ülkesi ve eklentileri üzerinde tam ve münhasır yetki vermektedir.[656] Devlet dışı aktörler tarafından gerçekleştirilen devlet destekli siber operasyonlar hedef devletin ülkesel egemenliğini ihlal edebilir.

2.1.1. Devlet Egemenliği

Mevcut uluslararası hukuktaki egemenlik kavramı, uluslararası hukukun en temel ilkelerinden biridir. Egemenlik, devletlerin egemen eşitliği ilkesine dayanır. Bu bağlamda uluslararası hukuk, egemen devletlerin üzerinde daha yüksek bir otoritenin bulunmadığını kabul etmekle birlikte, devletlerin gönüllü ve istekli olarak bu hukukla bağlı olmayı seçtiği, bağımsız ve bir arada yaşayan devletlerin hukukudur.[657] Bu husus, Uluslararası Daimi Adalet Divanı tarafından Lotus davasında açıkça ifade edilmiştir:

"Uluslararası hukuk, bağımsız devletler arasındaki ilişkileri düzenlemektedir. Bu nedenle, devletleri bağlayan hukuk kuralları, sözleşmelerde veya genel hukuk ilkeleri olarak kabul edilen ve birlikte var olan bu bağımsız topluluklar arasındaki ilişkileri düzenlemek ya da ortak amaçlara ulaşmak amacıyla oluşturulan teamüllerde ifade edildiği şekilde, devletlerin kendi özgür iradelerinden kaynaklanmaktadır." [658]

[656] Ram Prakash Anand, *Sovereign Equality of States in International Law* (Haryana: Hope India Publication, 1986), 197; James Crawford, *Brownlie's Principles of Public International Law*, (Oxford: Oxford University Press, 2012), 201.
[657] Anand, *Sovereign Equality of States in International Law,* 22.
[658] Permanent Court of International Justice (PCIJ)**,** *The Case of the SS "Lotus" (France v. Turkey)*, Series A, No. 10 (7 Eylül 1927), 18.

Bu çerçevede, egemenlik ilkesinin temel unsurlarına da değinmek gerekmektedir. Egemenlik ilkesinin temel unsurları şunlardır: "Bir toprak parçası ve onun daimi nüfusu üzerinde yargı yetkisi; müdahale yasağı ilkesi; ve uluslararası hukukla bağlı olmaya rıza gösterme."

2.1.1. Ülkesel Egemenlik

Ülkesel egemenlik, devletin kara ülkesi, iç suları, takımada suları, karasuları, deniz yatağı ve toprak altı ile bu alanların üzerindeki hava sahasını kapsamaktadır. Bu ilke, devlete kendi ülkesi ve eklentileri üzerinde tam ve münhasır yetki tanımaktadır. [659] Ülkesel egemenliğin iki temel özelliği bulunmaktadır: Devletin ülkesi üzerinde fonksiyonlarını yerine getirme hakkı ve bu hakkın münhasırlığı. Bu bağlamda, ülkesel egemenlik iki ana boyuta sahiptir: Pozitif boyut, devletin ülkesi üzerindeki münhasır yetkisini ifade ederken; negatif boyut ise diğer devletlerin haklarını koruma yükümlülüğünü göstermektedir.

Ülkesel egemenlik, devletlerarası ilişkilerin temelini oluşturmakta olup, bunun doğal sonucu olarak devletin yargı yetkisi ve müdahale yasağı ilkeleri ortaya çıkmaktadır. Ayrıca, bu ilke kuvvet kullanma ve müdahale yasağı ilkeleriyle yakından ilişkilidir ve bazı durumlarda bu ilkeler arasında belirli ölçüde örtüşme görülebilmektedir.

2.1.2. Siber Uzay Üzerinde Ülkesel Egemenlik

Ülkesel egemenlik ilkesi, bir devletin kara ülkesi, iç suları, takımada suları, karasuları, deniz yatağı ve toprak altı ile bu alanların üzerindeki hava sahasını kapsamaktadır. Bu durumda şu soru gündeme gelmektedir: Ülkesel egemenlik siber uzayı da kapsar mı? Bu soruya yanıt ararken, ABD Savunma Bakanlığı tarafından yapılan siber uzay tanımına yer vermek oldukça yerinde olacaktır:

"Siber uzay, bilgi ortamı içinde; İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ile denetleyiciler dahil olmak üzere, bilgi teknolojisi altyapılarının ve bu altyapılarda bulunan verilerin birbirine bağımlı ağlarından oluşan küresel bir alandır." [660]

Siber uzay kurgusal bir alan olmasına rağmen, somut ve gerçek altyapılara sahiptir. Başka bir ifadeyle, siber uzayın ve internetin fiziksel mimarisini oluşturan bilgisayar ağları ve

[659] Malcolm N. Shaw, *International Law* (Cambridge: Cambridge University Press, 2021), 61.
[660] US Department of Defense (DOD), "Cyberspace" (erişim 26 Nisan 2025).

bunların bileşenleri gerçek varlıklardır ve bu varlıklar devletlerin ülkesel egemenliği kapsamında yer almaktadır.

Bu durumda şu soru gündeme gelmektedir: Devletlerin ülkesel egemenliği bilgisayar ağlarını da kapsamakta mıdır? [661] Birleşmiş Milletler Genel Kurulu tarafından görevlendirilen Uluslararası Hukuk Uzmanları Grubu (UNGGE), 2013 raporunda bu konuya ilişkin aşağıdaki hususlara dikkat çekmiştir:

"Devlet egemenliği ve egemenlikten kaynaklanan uluslararası normlar ve ilkeler, devletlerin bilişim teknolojileri (BİT) ile ilgili faaliyetlerini yürütmeleri ve kendi ülkelerindeki BİT altyapısı üzerindeki yargı yetkileri için geçerlidir." [662]

Bu raporun BM Genel Kurulu'na sunulmasının ardından hiçbir devlet bu konuda görüş ayrılığı bildirmemiş veya çekince koymamıştır. Örneğin, İsveç, raporun sonuçlarına ilişkin olarak, "Devletlerin egemenlik yetkilerini siber uzaya genişletmelerinin uluslararası hukuk, insan hakları ve bireylerin temel özgürlükleri de dahil olmak üzere tüm uluslararası yükümlülüklerle uyumlu olması gerektiğini" vurgulamıştır. [663] Ancak, bu rapor ve sonraki deklarasyonların bağlayıcı olmayan uluslararası hukuk belgeleri olduğu ve yalnızca yumuşak hukuk niteliği taşıdığı unutulmamalıdır.

Egemenlik ilkesinin siber uzay ve bilgisayar ağlarını da kapsadığına dair en önemli göstergelerden biri, bugüne kadar hiçbir devletin ülkesel egemenliğin kendi toprakları içindeki bilişim teknolojileri (BİT) altyapılarını kapsayacak şekilde genişletilmesine itiraz etmemiş olmasıdır. Daha açık bir ifadeyle, devletler ülkesel egemenlikleri çerçevesinde ve ayrıca yargı yetkilerini kullandıkları alanlarda bulunan bilgisayar ağlarının fiziksel altyapıları üzerinde kontrol yetkisini kullanmaktadırlar. Literatür de bu yaklaşımı desteklemektedir.[664]

Egemenlik ve yargı yetkisi kavramları çoğu zaman birbirine karıştırılmakta ve birbirinin yerine kullanılmaktadır. Oysaki, her iki kavram birbirinden farklı anlamlar taşımaktadır.[665]

---

[661] United Nations General Assembly (UNGA), *Developments in the Field of Information and Telecommunications in the Context of International Security*, Res. 66/24 (13 Aralık 2011), para. 4.

[662] United Nations General Assembly (UNGA), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (24 Haziran 2013), UN Doc A/68/98, para. 20.

[663] Sweden, *Submission by Sweden to UNGA Resolution 68/243 Entitled "Developments in the Field of Information and Telecommunications in the Context of International Security"* (12 Eylül 2014).

[664] Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace", Katharina Ziolkowski (ed.), *Peacetime Regime for State Aktivities in Cyberspace* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2013), 190–191; Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies* 89 (2013), 123, 128–131; Andrey L. Kozik, "The Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace", *Baltic Yearbook of International Law* 14 (2015), 93, 97–103.

[665] Anand, *Sovereign Equality of States in International Law,* 28.

Devletin yargı yetkisi, egemenlik, egemen eşitlik ve içişlerine müdahale yasağı ilkelerine dayanır. Bu bağlamda yargı yetkisi, hukuken hak ve yükümlülüklere sahip olma ve bunları uygulama ile tüzel ve gerçek kişilerin fiillerini denetleme yetkisini ifade eder. Bir devlet, ülkesel egemenliği altındaki alanlar üzerinde yargı yetkisine sahiptir. Ayrıca, kendi vatandaşları ile kayıtlı gemileri, uçakları ve uzay araçları üzerinde ülke dışında da yargı yetkisini kullanabilir. Böylece, bir devletin yargı yetkisi, kara ülkesi, karasuları, takımada suları ve hava sahasında bulunan siber altyapıları da kapsayacak şekilde genişlemektedir. Bunun yanı sıra, o devletin bayrağını taşıyan gemilerde, tescil ettiği uçaklarda ve uydulardaki siber altyapılar da devletin yargı yetkisi kapsamına dahildir.[666]

2.1.3. Egemenliğin İhlali Bakımından Siber Eylemler

Egemenlik ilkesinin ihlali, yalnızca bir devlet tarafından diğer bir devlete karşı gerçekleştirilen veya bir devlete atfedilebilecek bir fiilden kaynaklanabilir. Başka bir ifadeyle, sadece bir devlete atfedilebilen siber operasyonlar, egemenlik ilkesinin ihlali olarak değerlendirilebilir.

Klasik uluslararası hukukta yerleşmiş geleneksel görüşe göre, yalnızca devletler ve uluslararası örgütler, uluslararası hukukun süjeleri olarak kabul edilmektedir.[667] Hak ve yükümlülük sahibi olabilme durumlarına göre gerçek kişiler de uluslararası hukukun süjeleri arasında değerlendirilebilmektedir. Bununla birlikte, bir uluslararası anlaşma, taraflar böyle bir iradeye sahip olmadıkça, tek başına gerçek kişiler için hak ve yükümlülük doğurmaz. Bu ilke, Uluslararası Daimi Adalet Divanı tarafından *Danzig Yargı Yetkisi* davasında şu şekilde teyit edilmiştir:

"Uluslararası hukuka oldukça iyi yerleşmiş bir ilkeye göre, bir uluslararası anlaşma olan Beamtenabkommen'in, kendi başına özel kişiler için doğrudan haklar ve yükümlülükler doğurmayacağı kolayca kabul edilebilir. Ancak, tarafların niyetine göre, bir uluslararası anlaşmanın asıl amacı, bireysel hak ve yükümlülükler oluşturan ve ulusal mahkemeler tarafından uygulanabilir olan bazı belirli kuralların benimsenmesi olabilir."[668]

---

[666] Joachim Zekoll, "Jurisdiction in Cyberspace", *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization*, ed. Günther Handl, Peer Zumbansen ve Joachim Zekoll (Boston: Martinus Nijhoff Publishers, 2012), 341; Joanna Kulesza, *International Internet Law* (New York: Routledge, 2012), 1–30.
[667] Shaw, *International Law*, 188.
[668] Daimi Uluslararası Adalet Divanı, *Jurisdiction of the Courts of Danzig (Advisory Opinion)*, Series B, No. 15 Collection of Judgments (1928), 17.

Ayrıca, insan hakları hukuku gibi alanlarda, gerçek kişilere ve diğer aktörlere haklar tanıyan ve yükümlülükler getiren antlaşmaların sayısı giderek artmaktadır.[669] Bununla birlikte, ülkesel egemenlik söz konusu olduğunda, yalnızca devletlerin fiilleri ülkesel egemenliğin ihlalini teşkil edebilir. Başka bir ifadeyle, bireyler kendi başlarına bir devletin ülkesel egemenliğini ihlal edemezler.[670]

Bir bireyin bir devletin ülkesine izinsiz girişi, eğer bir devlete atfedilebiliyorsa, bu durum söz konusu devletin ülkesel egemenliğini ihlal ettiği anlamına gelebilir; ancak bireyin kendisi, kişisel olarak bu egemenliği ihlal etmiş sayılmaz. Bu fiil, yalnızca ilgili devletin iç hukukunun ihlali niteliğini taşır. Bu bağlamda, ancak devlet müdahalesini ortaya koyan somut kanıtların bulunması hâlinde egemenlik ihlalinden söz edilebilir.

Bir devlet veya devlet destekli devlet dışı aktör tarafından gerçekleştirilen siber operasyonların, hedef devletin ülkesel egemenliğini hangi yollarla ihlal edebileceği tartışılırken temel bir ayrım yapılması gerekmektedir. Bazı siber operasyonlar, hedef sistemlere kötü amaçlı yazılım yerleştirilmesi suretiyle gerçekleştirilebilir; diğer bir ifadeyle, hedef sistemin güvenliği ihlal edilerek sisteme doğrudan sızılır. Bununla birlikte, diğer bazı siber operasyonlar, hedef sistemlere fiziksel olarak nüfuz edilmeksizin uzaktan gerçekleştirilir ve çeşitli etkiler doğurabilir. Hizmet engelleme (DoS) saldırıları buna iyi bir örnektir. Bu iki senaryo temel alınarak üçüncü bir senaryodan da söz edilebilir: Siber operasyonlar sonucunda ülkesel egemenlik ihlali, hata veya ihmal sonucu kazara meydana gelebilir.

2.1.3.1. Yabacı Bir Sisteme Nüfuz Eden Siber Eylemler

Siber uzay kurgusal bir alan olduğundan, burada gerçekleştirilen operasyonlar da doğası gereği birbirinden oldukça farklıdır. Örneğin, bazı siber saldırıların gerçekleşebilmesi için öncelikle hedef sisteme fiziksel veya mantıksal olarak nüfuz edilmesi gerekmektedir. Bu bağlamda *Stuxnet* saldırısı örnek olarak gösterilebilir. *Stuxnet*'in zarar verebilmesi için öncelikle hedefteki nükleer santralin bilgisayar sistemine bulaşması gerekmiştir. Buna karşılık, siber casusluk faaliyetleri, bazı durumlarda verilerin toplandığı devletin ülkesinden yalnızca transit geçiş sırasında da gerçekleştirilebilir. Bu noktada şu soru ortaya çıkmaktadır: "Yabancı bir sisteme nüfuz eden bir siber saldırı, hedef devletin egemenliğini ihlal eder mi?"

[669] Shaw, *International Law*, 188.
[670] James Sloan, "Prosecutor v. Dragan Nikolic: Decision on Defence Motion on Illegal Capture", *Leiden Journal of International Law* 16 (2003), 541-548.

Doktrinde, bu soruya ilişkin üzerinde mutabık kalınmış bir cevap henüz bulunmamaktadır. Örneğin, bazı yazarlar, yabancı sistemlere nüfuz eden siber saldırıların egemenlik ilkesinin ihlali anlamına gelmeyeceğini ileri sürmektedir.[671] Bu görüşü savunan Benedikt Pirker, casusluğun uluslararası hukuk kapsamında yasaklanmadığını ileri sürerek şu sonuca varmaktadır: "Aynı kuralların muhtemelen siber uzay için de geçerli olduğu kabul edilebilir; yabancı bilgisayar sistemlerine izinsiz girişler bu nedenle mutlak surette hukuka aykırı değildir. Nitekim casusluk, devletler arasında oldukça yaygın bir uygulamadır."[672] Kanaatimizce bu görüş isabetli değildir. Diğer bir ifadeyle, siber operasyonların yabancı sistemlere izinsiz girişinin ülkesel egemenliği ihlal etmeyeceği sonucuna varmak oldukça güçtür. Zira siber saldırılara ilişkin genel bir yasağın bulunmaması, ajanlar tarafından gerçekleştirilen her fiilin uluslararası hukuk kapsamında yasaklanmadığı veya mutlaka izin verildiği anlamına gelmez. Bir devletin ülkesinde, başka bir devletin ajanları tarafından gerçekleştirilen casusluk faaliyetleri, o devletin egemenliğini ihlal eder. Bir devlet tarafından hedef devletin ülkesinde gerçekleştirilen her türlü izinsiz fiilin, hedef devletin ülkesel egemenliğini ihlal ettiği açıktır. Aşağıda yer verilen örnekler, aynı sonucun siber saldırılar için de geçerli olduğunu ortaya koymaktadır.

Bu örnekler arasında en çarpıcı olanı, 2008 BND skandalıdır. 2008 yılında Alman dış istihbarat servisi Bundesnachrichtendienst (BND), Haziran ile Kasım 2006 tarihleri arasında Afganistan Ticaret ve Sanayi Bakanı ile Alman Der Spiegel gazetesinde görev yapan bir gazeteci arasındaki iletişimi izlemiştir.[673] BND, bu sızma fiilini gerçekleştirmek amacıyla Afganistan Ticaret ve Sanayi Bakanlığı'nın bilgisayar ağına Truva atı casusluk yazılımını yerleştirmiştir. Mevcut uluslararası hukuk çerçevesinde, bir Alman gazeteci ile bir Afgan bakan hakkında casusluk yapılmasının tek başına uluslararası hukuka aykırı bir fiil teşkil etmediği açıktır. Ancak egemen bir devletin resmi organlarının bilgisayar sistemlerine Truva atı yazılımı yerleştirilmesi, açıkça Afganistan'ın ülkesel egemenliğinin ihlali anlamına gelmektedir.

Yukarıda verilen örnek çerçevesinde, bir devletin hava sahasına yabancı bir uydu yerleştirmek suretiyle gerçekleştirilen basit bir izinsiz giriş fiilinin, ülkesel egemenliğin ihlali anlamına geldiği açıkça ortaya konmuştur. Sovyetler Birliği'ne ait *Cosmos 954* uydusunun

---

[671] Jeffery Hunker, Joseph Margulies ve Bonnie Hutchinson, *Role and Challenges for Sufficient Cyber-Attack Attribution* (2008), 66.

[672] Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace", *NATO Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE Publications, 2013), 212.

[673] "BND Scandal: How German Spies Eavesdropped on an Afghan Ministry", *Spiegel Online*, 28 Nisan 2008, https://www.spiegel.de/international/germany/bnd-scandal-how-german-spies-eavesdropped-on-an-afghan-ministry-a-550212.html.

düşmesi vakası da bu iddiayı destekleyen bir örnek teşkil etmektedir.[674] Nitekim, uydunun Kanada topraklarına düşmesinin ardından Kanada tarafından da benzer bir yaklaşım benimsenmiştir: "Cosmos 954 uydusunun Kanada hava sahasına girmesi ve uydudan çıkan tehlikeli radyoaktif enkazın Kanada topraklarında birikmesi, Kanada'nın egemenliğinin ihlalini teşkil etmektedir. Bu ihlal; uydunun izinsiz girişi, bu izinsiz girişin zararlı sonuçları, tehlikeli radyoaktif kalıntıların varlığının Kanada'ya verdiği zarar ve Kanada'nın kendi ülkesinde gerçekleştirilecek fiilleri belirleme egemenlik hakkına müdahale edilmesi ile ortaya çıkmıştır."[675]

Egemenliğin ihlali bağlamında, devletler sıklıkla ülkesel egemenliklerinin uçaklar veya gemiler tarafından ihlal edildiğini iddia etmektedir. Bugüne kadar gerçekleşen vakaların büyük bir çoğunluğunda, önceden izin alınmaksızın bir devletin ülkesel egemenliği altındaki bir alana giriş fiili, egemenlik ihlali için yeterli kabul edilmiştir. Diğer bir ifadeyle, ihlal için belirli bir fiil veya zararın meydana gelmesi şart koşulmamıştır.[676] Bu bağlamda, örneğin bir devletin karasularında tespit edilen yetkisiz bir yabancı denizaltının varlığı, söz konusu devletin ülkesel egemenliğinin ihlali anlamına gelecektir.[677]

Bu sonuç, siber operasyonlara da genişletilebilir. Daha açık bir ifadeyle, bir siber saldırı yabancı bir devletin ülkesindeki siber yapılara izinsiz nüfuz ederse, bu durum o devletin ülkesel egemenliğinin ihlali anlamına gelecektir.[678] Buna karşılık, casusluk faaliyetleri yürüten bir devletin kendi ülkesinden geçen verileri izleme yoluyla gerçekleştirdiği siber casusluk operasyonu, diğer devletin ülkesel egemenliğini ihlal etmeyecektir.

Bununla birlikte, birçok siber saldırı hedef devletin ülkesel egemenliğini ihlal edecek niteliktedir. Casusluk durumlarında olduğu gibi, devletler her vakayı bu şekilde tanımlayıp kamuoyuna açıklamayabilir. Ancak bu durum, ülkesel egemenlik ilkesinin ihlali olabileceği gerçeğini değiştirmez. Bir devletin belirli bir durumu bu şekilde nitelendirme veya nitelendirmeme nedenleri hukuki değil, daha çok siyasi sebeplere dayanmaktadır.

---

[674] *Statement of Claim, Claim against USSR for damage caused by Soviet Cosmos 954*, Department of External Affairs, Ottawa, 23 Ocak 1979; 1972 tarihli Liability Convention, Article II; J. A. B. Note, *Fordham International Law Journal*, 1984, 255–285.

[675] "Claim against the Union of Soviet Socialist Republics for Damage Caused by Soviet Cosmos 954", *International Legal Materials* 18 (1979), 18.

[676] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986*, I.C.J. Reports 1986, 128.

[677] Swedish Armed Forces (SAF), "Confirmed Submarine in the Stockholm Archipelago", *Swedish Armed Forces*, 14 Kasım 2014, erişim 29 Nisan 2025, www.forsvarsmakten.se/en/news/2014/11/confirmed-submarine-in-the-stockholm-archipelago/.

[678] Heinegg von Heintschel W., "Chapter 1: The Tallinn Manual and International Cyber Security Law", *Yearbook of International Humanitarian Law* 15 (2012), 3; Heinegg von Heintschel W., "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies* 89 (2013), 123.

2.1.4. İstem Dışı Egemenlik İhlali

Yukarıda, bir siber saldırının bir devletin ülkesel egemenliğini ihlal edebileceği farklı senaryolar ele alınmıştır. Ancak, egemenlik ihlalinin hata veya ihmal sonucu gerçekleşmesi durumunda farklı bir değerlendirme yapılıp yapılamayacağı sorusu henüz yanıt bulmamıştır.

Hata veya ihmal sonucu ülkesel egemenliğin ihlaline ilişkin önemli bir örnek, Sovyetler Birliği'ne ait *Cosmos 954* uydusunun düşüşüdür. Uydu, 24 Ocak 1978 tarihinde kontrolden çıkarak Kanada'nın kuzeybatısına düşmüştür. Bu olayda, Sovyetler tarafından Kanada'nın ülkesel egemenliğinin kasıtlı olmayan bir şekilde ihlal edildiği kabul edilmiştir. Ancak ihlal istem dışı olsa da, bu durum ülkesel egemenliğin ihlali olarak değerlendirilmiştir.[679]

Günümüze kadar siber uzay, istemsiz bir şekilde veya belirli bilgisayar sistemlerini hedef almaksızın tüm dünyaya yayılan kötü amaçlı yazılımlara dair birçok örnek sunmaktadır. Bu bağlamda, örneğin *Stuxnet* kötü amaçlı yazılımı İran'daki bir nükleer tesise zarar vermek amacıyla tasarlanmış; ancak dünya genelinde yayılmıştır. Bu yazılımın, diğer devletlerin ülkesel egemenliği kapsamındaki bilgisayar sistemlerine nüfuz etmesi nedeniyle, bu devletler egemenliklerinin ihlal edildiğini açıkça ileri sürebilirlerdi. Bu tür örneklerde, egemenlik ilkesinin ihlal edilip edilmediğinin tespitine yönelik değerlendirmelerde, bulaşan sistemlerin ve dolayısıyla etkilenen devletlerin doğrudan hedef alınmamış olmasının bir önem taşıyıp taşımadığı tartışmaya açıktır. Ancak mevcut uluslararası hukuk kapsamında, bu durumun olayın hukuki nitelendirmesini değiştirmediği açıktır.

Bu örnekler, başka bir soruyu gündeme getirmektedir: Hata veya ihmal, ülkesel egemenliğin ihlalinin hukuka aykırılığını ortadan kaldıran haller arasında sayılabilir mi? Mücbir sebep ve beklenmedik olaylar, bu tür durumlarda hukuka aykırılığı ortadan kaldırabilecek uygun hukuki araçlar olarak değerlendirilebilir. Mücbir sebep, bir devletin kontrolü dışında gelişen, karşı konulamaz bir kuvvet veya öngörülemeyen bir olayın gerçekleşmesi sonucu, yükümlülüğünü yerine getirmesini fiilen imkânsız hale getiren hallerde hukuka aykırılığı kaldırır.

Siber uzay kapsamında, bazı siber saldırıların, "öngörülemeyen bir olayın" sonucu olarak gerçekleşmesi teorik olarak mümkün görünmektedir. Ancak, mücbir sebebin, bu durumu ileri süren devletin eylemlerinden kaynaklanan bir fiilin hukuka aykırılığını ortadan kaldırmayacağı açıktır. Bu husus, Devletin Sorumluluğuna İlişkin Taslak Maddeler'in Şerhinde

[679] Alexander F. Cohen**,** "Cosmos 954: The International Law of Satellite Accidents," *International Incidents: The Law That Counts in World Politics*, ed. W. Michael Reisman ve Andrew R. Willard (Princeton: Princeton University Press, 1988), 68–84.

de açıkça belirtilmiştir.[680] Buna göre, "ilgili devletin ihmali veya kusurundan kaynaklanan durumlarda hukuka aykırılık devam etmektedir; sonuç olarak gerçekleşen zarar kaza eseri ve kasıtsız olsa dahi" bu durum geçerlidir.[681] Dolayısıyla, kötü amaçlı bir yazılımın istemsiz bir şekilde yayılması, etkilenen devletlerin ülkesel egemenliklerinin ihlalini teşkil edecektir.

Egemenlik ilkesi kapsamında aktarılan hususlar, siber saldırıların hedef devletin ülkesel egemenliğini ihlal edebileceğini ortaya koymaktadır. Devlet destekli siber saldırılar, fiziksel bir zarar meydana getirmese, herhangi bir somut zarar üretmese ya da nüfuz istemsiz bir şekilde gerçekleşmiş olsa dahi egemenlik ilkesinin ihlali gerçekleşebilir. Yabancı bir sisteme yalnızca sızma veya bu sistemde etkilerin ortaya konması, egemenlik ilkesinin ihlali için yeterlidir. Sızma ve etkilerin derecesi, ihlalin ciddiyetini ve sonuçlarını belirler; bu hususlar ise devletin uluslararası sorumluluğunun kapsamını belirlerken belirleyici rol oynar.

2.1.4.1.Bir Devletin Başka Bir Devletin Ülkesinde Yetki Kullanması

Lotus davasında Uluslararası Daimi Adalet Divanı, bir devletin kendi otoritesini başka bir devletin ülkesinde kullanmasının uluslararası hukukun ihlalini teşkil edeceğine hükmetmiştir. Karara göre: "Uluslararası hukuk tarafından bir devlete getirilen ilk ve en önemli sınırlama, eğer aksine izin veren bir kural yoksa, bir devletin başka bir devletin ülkesinde herhangi bir şekilde yetki kullanamayacağıdır." [682]

Siber operasyonlar, devletlere yetkilerini başka bir devletin ülkesinde kullanmaları için görece kolay bir imkân sunabilir. Ancak bu durum, söz konusu diğer devletin egemenliğinin ihlali anlamına gelir. Aşağıda yer alan iki senaryo, bu durumu açıklayıcı niteliktedir.

İlk senaryoya göre, bir devlet kanun uygulama faaliyetlerinin kendi yetki alanıyla sınırlı olması sebebiyle siber operasyonlara başvurma eğiliminde olabilir. Başka bir devletten, o devletin ülkesinde bulunan bir kişiye karşı harekete geçmesini talep eden bir devlet, kimi durumlarda ev sahibi devletin harekete geçmemesi nedeniyle hayal kırıklığına uğrayabilir. Ancak siber uzay, başka bir devletin ülkesinde bulunan bir kişiye karşı uzaktan harekete geçmek için çeşitli araçlar sunmaktadır. Bu çerçevede, siber saldırılar da dâhil olmak üzere, yabancı bir devletin ülkesinde onun rızası olmaksızın gerçekleştirilen her türlü devlet fiili,

[680] Birleşmiş Milletler Uluslararası Hukuk Komisyonu (BM UHK), *Uluslararası Hukuka Aykırı Fiillerden Dolayı Devletlerin Sorumluluğuna İlişkin Maddeler*, BM Genel Kurulu'nun 56/83 Sayılı Kararına Ek, 53. Oturum (2001), md. 23/1.
[681] Birleşmiş Milletler Uluslararası Hukuk Komisyonu, *Uluslararası Hukuka Aykırı Fiillerden Dolayı Devletlerin Sorumluluğuna İlişkin Maddeler*, md. 23/2 (a).
[682] Uluslararası Daimi Adalet Divanı, *The Case of the S.S. Lotus (Fransa v. Türkiye)*, Judgment of 7 Eylül 1927, PCIJ Series A No. 10, 18.

ülkesel egemenliğin ihlali anlamına gelir. Örneğin, bir devlet, yurt dışında bulunan bir bilgisayar korsanının daha fazla siber operasyon gerçekleştirmesini engellemek amacıyla söz konusu kişinin bilgisayarını bozabilir veya imha edebilir. Benzer şekilde, bir devlet, yurt dışında bulunan bir terör örgütü liderini, bu kişinin aracının kontrol sistemine müdahale ederek ve bir trafik kazasına neden olarak öldürebilir.[683]

İkinci senaryo, Uluslararası Adalet Divanı'nın içtihadından hareketle açıklanabilir. Korfu Kanalı davasında Birleşik Krallık, Arnavutluk karasuları içinde delil toplamak amacıyla ülke sınırları dışında zorlayıcı tedbirler uygulamıştır. Mahkeme, Kraliyet Donanması'nın bu fiillerinin Arnavutluk'un egemenliğini ihlal ettiğine hükmetmiştir. Bu yaklaşım uyarınca, başka bir devletin ülkesinde bulunan sunuculardaki delilleri ele geçirmek amacıyla gerçekleştirilecek siber operasyonlar da hedef devletin egemenliğinin ihlali anlamına gelecektir.[684] Sonuç olarak, yabancı bir sisteme nüfuz eden siber saldırılar, siber müdahalenin amacına bakılmaksızın, etkilenen devletin ülkesel egemenliğinin ihlalini teşkil eder.

2.1.4.2.Zarar Koşulunun Olmaması

Uzaktan gerçekleştirilen siber operasyonların bir devletin ülkesinde vuku bulmasının hukuki niteliği, uluslararası hukukta hâlen belirsizliğini korumaktadır. Uzmanlar, bu tür operasyonların hukuka uygunluğunu iki temel ölçüt üzerinden değerlendirmektedir: (1) hedef devletin ülkesel bütünlüğüne yönelik müdahalenin derecesi ve (2) devletin doğrudan kamusal işlevlerine müdahale edilip edilmediği veya bu işlevlerin gasp edilip edilmediği.

Birinci ölçüte ilişkin olarak, uzmanlar meseleyi üç farklı düzeyde analiz etmektedir: (1) fiziksel zarar, (2) işlevsellik kaybı ve (3) işlevsellik kaybı eşiğinin altında kalan, ancak yine de ülkesel bütünlüğün ihlali niteliği taşıyan durumlar.[685] Uzmanların büyük bir bölümü, fiziksel hasar veya yaralanmanın egemenlik ihlali tespitinde yeterli olduğunu teyit etmektedir. Bununla birlikte, bazı yazarlar bu hususun belirleyici bir unsurdan ziyade, dikkate alınması gereken unsurlardan yalnızca biri olduğunu vurgulamaktadır.[686] Benzer şekilde, uzmanlar, başka bir devlette bulunan siber altyapının işlev kaybına neden olan dolaylı bir etkileşimin bazen egemenlik ihlaline yol açabileceği konusunda hemfikir olmuş, ancak bu ihlalin kesin eşiği

[683] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It", WIRED, 21 Temmuz 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[684] Uluslararası Adalet Divanı (UAD), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986*, I.C.J. Reports 1986, s. 128, para. 251.
[685] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 20.
[686] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 20.

konusunda bir uzlaşıya varılamamıştır.[687] Bununla birlikte, fiziksel hasara veya işlev kaybına yol açmayan bir siber saldırının egemenlik ilkesinin ihlalini oluşturup oluşturmadığı ve eğer oluşturuyorsa hangi durumlarda oluşturduğu hususunda bir fikir birliği sağlanamamıştır.

İkinci temele ilişkin olarak ise uzmanlar, bir siber saldırının fiziksel hasar, yaralanma veya işlev kaybına yol açıp açmadığına bakılmaksızın egemenlik ilkesinin ihlali olarak değerlendirilebileceğini ifade etmişlerdir.[688]

Uzmanların, bir siber saldırı yoluyla gerçekleştirilen egemenlik ihlalinin belirli bir zarar (*harm*) eşiğine bağlı olduğunu değerlendirmeleri oldukça dikkate değerdir. Benzer bir görüş, Tallin El Kitabı'nın ilk baskısında da yer almaktadır:

"Bir devlet tarafından, diğer bir devlette bulunan siber altyapıya yönelik gerçekleştirilen siber saldırı, ilgili devletin egemenliğini ihlal edebilir. Bu operasyonun hasara (*damage*) yol açması halinde kesinlikle bir ihlal meydana gelir. Ancak Uluslararası Uzmanlar Grubu, örneğin faaliyetleri izlemek amacıyla kullanılan zararlı yazılımlar gibi fiziksel hasara yol açmayan kötü amaçlı yazılım yerleştirilmesi gibi fiillerin egemenlik ihlali oluşturup oluşturmadığı konusunda bir uzlaşı sağlayamamıştır." [689]

Bu yaklaşıma göre, siber saldırılar, fiziksel etki oluşturup oluşturmama durumlarına bağlı olarak birbirinden ayrılabilir.[690] Bununla birlikte, bu yaklaşım iki açıdan dikkat çekici ve tartışmaya açıktır. İlk olarak, devletin uluslararası sorumluluğu hukukunda genel kural olarak bir uluslararası hukuka aykırı fiilin varlığı için zarar meydana gelmesi şart değildir. Ancak, bu tür unsurların gerekip gerekmediği, ihlale konu birincil yükümlülüğün içeriğine bağlı olup, bu konuda evrensel nitelikte bir kural bulunmamaktadır. İkinci olarak, Tallinn El Kitabı sürecine katılan uzmanların daha önce de belirttiği üzere, bir devletin başka bir devletin ülkesine veya ulusal hava sahasına, o devletin izni olmaksızın ya da uluslararası hukuka uygun bir gerekçe bulunmadan fiziksel olarak girmesi, egemenlik ihlali teşkil eder.[691] Bu bağlamda, kanaatimizce siber uzay bakımından da farklı bir yaklaşım benimsemeye gerek bulunmamaktadır. Başka bir ifadeyle, bir devletin diğer bir devletin bilgi ve iletişim teknolojileri (BİT) altyapısına sızması suretiyle egemenlik ihlalinin gerçekleşmesi, herhangi bir zarar eşiğinin aşılmasına bağlı

[687] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 20-21.
[688] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 21-22.
[689] Schmitt – Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 16.
[690] Katharina Ziolkowski, "General Principles of International Law as Applicable in Cyberspace", *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2013), 163.
[691] International Law Commission (ILC), *Commentary to the Articles on State Responsibility*, 2 *Yearbook of the International Law Commission* (Part II) (2001), 31, 36.

olmamalıdır. Daha açık bir ifadeyle, siber uzay kaynaklı fiillerin egemenlik ihlali teşkil edebilmesi için zarar eşiğinin varlığı şart koşulmamalıdır.

Zarar şartı, siber müdahale sonucunda fiziksel bir etkinin varlığını gerektirse de, bu tür bir şartın varlığına ilişkin herhangi bir hukuki dayanak bulunmamaktadır. Günümüze kadar gerçekleşen devlet uygulamaları, bu konudaki mevcut hukuku teyit edebilir veya değiştirebilir. Siber saldırı fiziksel hasar oluşturduğunda, bu durumun egemenlik ihlali olarak değerlendirilme ihtimali, herhangi bir fiziksel hasar veya zarar oluşturmayan saldırılara kıyasla daha yüksektir. Ancak teorik açıdan değerlendirildiğinde, her iki durumda da ülkesel egemenliğin ihlali söz konusudur. Bununla birlikte, devletlerin kendilerine yönelik gerçekleştirilen bir fiili ülkesel egemenliğin ihlali olarak değerlendirip değerlendirmemeleri genellikle siyasi mülahazalara dayanmaktadır. Ayrıca, günümüze kadar yeni devlet dışı aktörler tarafından gerçekleştirilen devlet destekli siber saldırılara ilişkin oluşmuş devlet uygulamaları oldukça sınırlıdır. Dolayısıyla, bu tür saldırılara karşı gelişmiş bir örf ve adet hukuku kuralı da bulunmamaktadır.

Kanaatimizce, devletler açısından zarar şartı aramak makul değildir. Bu durum, hukuki olmaktan çok siyasi bir argümana dayanmaktadır. Daha açık bir ifadeyle, zarar oluşturmayan siber müdahalelerin uluslararası hukuku ihlal etmediğinin kabul edilmesi halinde, her devlet diğerlerinin sistemlerine hukuka uygun şekilde nüfuz edebilir. Bu durumda bir devlet, yabancı bilgisayar sistemlerine "hukuka uygun" biçimde kötü amaçlı yazılımlar yerleştirebilir; örneğin, savaş alanını hazırlamak amacıyla arka kapılar veya mantık bombaları yükleyebilir. Ancak, bu araçlar fiilen kullanıldığında egemenlik ihlali gerçekleşmiş sayılacaktır. Gerçek dünyadan bir örnek vermek gerekirse, bu mantıkla bir devletin diğer bir devletin ülkesine zaman ayarlı bombalar yerleştirmesi o devletin ülkesel egemenliğini ihlal etmeyecektir; ancak bu bombalar patlatıldığında ihlal meydana gelecektir.

2.1.4.3.Hedefin Niteliği ve Enfoksiyon Araçları

Gerçek dünyada, bir devlet adına hareket eden bir kişinin başka bir devletin sınırlarını geçmesi halinde ülkesel egemenlik ihlali meydana gelir. Bu kapsamda, ülkesel egemenlik bir devletin ülkesinde bulunan BİT altyapılarını da kapsar. Siber uzayda ise sınırın ne zaman aşıldığını tespit etmek oldukça zordur; çünkü siber uzayda görünür veya somut bir sınır bulunmamaktadır ve veriler sürekli olarak bir sunucudan diğerine geçerken fiili sınırları aşmaktadır.

Devlet dışı aktörler tarafından gerçekleştirilen, devlet destekli bir siber saldırının, diğer bir devletin ülkesinde bulunan herhangi bir BİT altyapısını doğrudan enfekte etmesi,

etkilerinden bağımsız olarak, o devletin ülkesel egemenliğinin ihlali anlamına gelecektir. Ancak burada, yalnızca transit geçiş ile sistemin fiilen ihlal edilmesi arasında bir ayrım yapmak gerekmektedir.

Hukuka aykırı bir ihlal yalnızca bilgisayarların veya sunucuların bulunduğu devletin ülkesel bütünlüğüne zarar vermektedir. Buna karşılık, hedef alınan sunuculardaki verilere sahip olan diğer bir devletin ülkesel egemenliği bu durumdan etkilenmez. Bu bağlamda, örneğin A devletine ait verilerin B devletinin ülkesinde bulunan bir sunucuda saklandığı durumda, C devleti tarafından desteklenen ve bu sunucuyu enfekte eden siber saldırılar yalnızca B devletinin ülkesel egemenliğini ihlal etmiş sayılacaktır. Diğer bir ifadeyle, bu durum A devletinin ülkesel egemenliğinin ihlali anlamına gelmeyecektir.

Siber sızma dolaylı olduğunda durum daha da karmaşıklaşmaktadır. Bu çerçevede, örneğin *Stuxnet* saldırısı vakasında, nükleer santralin bilgisayar sistemine virüs bulaşmasının virüslü bir USB bellek aracılığıyla gerçekleştiği ileri sürülmektedir. 2008 yılında ise ABD Savunma Bakanlığı, bir ABD askeri üssünün otoparkında bulunan virüslü bir USB bellek nedeniyle askeri bilgisayar ağlarına yönelik ciddi bir saldırıya maruz kalmıştır. Her iki örnekte de sızma dolaylı görünse de, siber saldırıların hedefinin doğrudan etkilenen yabancı sistemler olduğu açıktır. Bu çerçevede, bu tür durumların mağdur devletin ülkesel egemenliğinin ihlali anlamına geldiği ileri sürülebilir.[692]

Bir diğer olası senaryoya göre, bir kişi, ister devlet memuru olsun ister olmasın, yurt dışına seyahat ederek bilgisayarını bir yabancı devletin bilgisayar sistemine bağladığında ve bu sırada bilgisayarı bir virüsle enfekte olduğunda, dönüşte bu virüsü kendi ülkesinin ağında yayabilir. Bu durum iki farklı benzetmeyle açıklanabilir: İlk olarak, yurt dışında bir hastalığa yakalanan bir kişinin ülkesine döndüğünde bu hastalığı yaymasına; ikinci olarak ise, bir kişinin yurt dışından bomba satın alıp bunu ülkesinde patlatmasına benzetilebilir. Her iki benzetmede de bir devletin diğerinin ülkesel egemenliğini ihlal edip etmediğinin belirlenmesi zor görünmektedir. Bu durum, siber saldırılar bağlamında farklı saldırı senaryolarına yol açabilecek çeşitli karmaşık durumları gündeme getirmektedir.

---

[692] William J. Lynn III, "Defending a New Domain", *Foreign Affairs* 89 (2010), 97; Infosecurity Magazine, *Worm that Wreaked Havoc for US Military Likely a Progenitor of Red October* (12 Mart 2014), https://www.infosecurity-magazine.com/news/worm-that-wreaked-havoc-for-us-military-likely-a/; Noah Shachtman, "Under Worm Assault, Military Bans Disks, USB Drives", *WIRED* (19 Kasım 2008), https://www.wired.com/2008/11/army-bans-usb-d/; Noah Shachtman, "Hackers, Troops Rejoice: Pentagon Lifts Thumb-Drive Ban (Updated)", *WIRED* (18 Şubat 2010), https://www.wired.com/2010/02/hackers-troops-rejoice-pentagon-lifts-thumb-drive-ban/; Ellen Nakashima, "Cyber-Intruder Sparks Response, Debate", *The Washington Post* (6 Aralık 2011), https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response debate/2011/12/06/gIQAxLuFgO_story.html; Noah Shachtman, "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)", *WIRED* (25 Ağustos 2010), https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/.

İlk senaryo olarak, A devletinden özel bir kişinin, bilerek ya da bilmeyerek, B devletinde bulunan özel bir kişiden kötü amaçlı yazılım (*malware*) bulaşmış bir cihaz veya yazılım satın alması ve bu kötü amaçlı yazılımın ardından kendi ülkesindeki bilgisayarlara yayılması durumu ele alınabilir. Bu durumda, fail bir devlet olmadığı için ülkesel egemenlik ihlali de gerçekleşmeyecektir. Ancak, kötü amaçlı yazılımın bir devlet tarafından oluşturulmuş olması halinde dahi, failin B devletinin kontrolü altında hareket ettiğinin kanıtlanmaması durumunda hukuki durum değişmez. Failin B devletinin kontrolü altında hareket ettiğinin ispatlanması halinde ise olayın hukuki nitelendirmesi farklı olacaktır.

İkinci senaryoda ise, eğer alıcı A devleti veya onun adına hareket eden bir ajan, satıcı ise özel bir kişi ise bu durum ülkesel egemenliğinin ihlali teşkil etmeyecektir.

Üçüncü senaryoda, eğer A devletinden özel bir kişi, B devletinden veya B devleti adına hareket eden bir kişiden bir mal satın alırsa, bu durumun A devletinin ülkesel egemenliğinin ihlali olarak değerlendirilebileceği düşünülebilir. Bu senaryoda, B devleti kasıtlı olarak, kötü amaçlı yazılımın hedef devlette yayılmasını veya belirli sistemleri hedef almasını sağlamak amacıyla, enfekte edilmiş bir cihaz ya da yazılım satmıştır. Ancak, B devletinin savunması, alıcının durumdan haberdar olup olmadığını sorgulamak üzerine kurulabilir. Böyle bir durumda, alıcının farkındalığına bağlı olarak, bu fiilin A devletinin ülkesel egemenliğinin ihlali sayılıp sayılamayacağı daha tartışmalı hale gelebilir.

Dördüncü ve son senaryoda ise, A devletinin, B devleti tarafından enfekte edilmiş bir cihaz veya yazılımı, enfeksiyondan habersiz olarak B devletinden satın aldığı durum ele alınabilir. Bu senaryoda, kötü amaçlı yazılım A devletinin ülkesinde bulunan BİT altyapılarına zarar vermeye başladığında, B devletinin A devletinin ülkesel egemenliğini ihlal ettiği sonucuna varılabilir. Ancak bu ihlal, yalnızca A devletinin kötü amaçlı yazılımın varlığından habersiz olması durumunda geçerli olacaktır. Bazı durumlarda, bir devlet farklı amaçlarla kötü amaçlı kod içeren bir cihaz veya yazılımı bilerek satın alabilir. Bu tür hallerde, enfeksiyon A devletinin sistemlerinde yayılsa bile, satış yapan devletin A devletinin ülkesel egemenliğini ihlal ettiği yönünde bir değerlendirme yapılamaz.

Sonuç olarak, hukuka aykırı yani yetkisiz şekilde devlet dışı aktörler tarafından gerçekleştirilen ve devlet tarafından desteklenen herhangi bir siber saldırının, diğer bir devlete müdahale teşkil etmesi durumunda, ilgili devletin ülkesel egemenliği ihlal edilmiş sayılacaktır. Ayrıca, yalnızca bir devletin diğer bir devletin ülkesel egemenliğini ihlal edebileceği hususu unutulmamalıdır.

2.1.4.4.Yabancı Bir Sisteme Nüfuz Etmeyen Siber Saldırılar

Bazı siber operasyonlar, hedef sisteme doğrudan sızmaksızın da etkiler oluşturabilmektedir. Bu bağlamda, örneğin DDoS saldırıları, BİT altyapısını aşırı taleplerle yükleyerek işlevsiz hale getirmeyi amaçlamaktadır. Bu tür bir senaryoda, her bir talep tek başına hukuka aykırı veya zarar verici olmasa da, eş zamanlı olarak çok sayıda talebin bir araya gelmesi hedef sistemin olağan işleyişini bozmakta ve aksamalara yol açmaktadır.

Hedef sisteme herhangi bir sızma gerçekleşmediği ve dolayısıyla doğrudan bir egemenlik ihlali oluşmadığı durumlarda, bu tür fiillerin hedef devletin ülkesel egemenliğini ihlal edip etmediği belirsizliğini korumaktadır. Kanaatimizce, bir devletin diğer bir devletin ülkesinde izinsiz olarak gerçekleştirdiği her türlü fiil, ilgili devletin ülkesel egemenliğini ihlal eder.

DDoS saldırılarında, hedef devletin BİT altyapısına herhangi bir kötü amaçlı kod enjekte edilmediği için doğrudan bir sızma fiili gerçekleşmemektedir. Bununla birlikte, DDoS saldırıları hedef devletin ülkesel egemenliği kapsamında etkiler oluşturur. Örneğin, bu saldırılar bir sunucunun yavaşlamasına veya kullanılamaz hale gelmesine neden olabilir. Dolayısıyla, bu tür saldırılar hedef devletin ülkesinde olumsuz etkiler oluşturduğu için izinsiz (*unauthorized)* fiiller olarak değerlendirilmekte ve ilgili devletin ülkesel egemenliğini ihlal ettiği sonucuna varılabilir.

Saldırıya uğrayan devlet açısından, altyapısına yönelik düşük yoğunluklu dahi olsa etkilerin oluşması, DDoS saldırılarının tespitini kolaylaştırmaktadır. Yukarıda belirtildiği üzere, ülkesel egemenliğin ihlali olarak nitelendirme bakımından belirli bir yoğunluk eşiği ya da fiziksel zarar şartı aranmamaktadır. Bununla birlikte, fiziksel zararların varlığı veya yoğunluğu, bir devletin egemenliğinin diğer bir devlet tarafından ihlal edildiğini açıkça ve alenen ilan etmesini teşvik eden önemli bir faktör olabilir. Kanaatimizce, bu sonuca DDoS saldırıları için de ulaşılabilir. Özellikle fiziksel etkiler üreten siber saldırıların, fiziksel olmayan etkiler üreten saldırılara kıyasla ülkesel egemenliğin ihlali olarak nitelendirilme olasılığının daha yüksek olduğu göz önünde bulundurulduğunda, bu değerlendirme daha da güçlenmektedir.

Egemenlik ilkesi, yalnızca bir devlet tarafından, ya kendi fiilleriyle ya da kontrolü altındaki kişilerin fiilleriyle ihlal edilebilir. Bu bağlamda, bir DDoS saldırısının egemenlik ilkesinin ihlali olarak değerlendirilebilmesi için saldırının bir devlete atfedilebilir olması gerekmektedir. Ancak, atfetme süreci çoğu durumda oldukça karmaşık hatta imkânsız olabilir; çünkü bu tür saldırılar genellikle birçok kişinin ve çeşitli coğrafi bölgelerden kontrol edilen

zombileşmiş bilgisayarların eşzamanlı katılımıyla gerçekleştirilmektedir. Örneğin, Estonya, Gürcistan ve Litvanya'ya yönelik büyük çaplı DDoS saldırılarının aynı anda birden fazla ülkeden kaynaklandığı tespit edilmiştir.[693]

2.2. Müdahale Yasağı İlkesi ve Siber Eylemler

2.2.1. Müdahale Yasağı Kavramı

Müdahale yasağı ilkesi, genellikle iki farklı ilkeyi kapsamaktadır. Bunlardan ilki bir devletin başka bir devletin iç ve dış işlerine müdahaleyi yasaklayan "müdahale yasağı" ilkesidir. Diğeri ise bir devletin diğer bir devletin ülkesel bütünlüğüne müdahaleyi yasaklayan egemenlik ilkesidir. Egemenlik ilkesi yukarıda detaylı bir biçimde incelenmiştir. Bununla birlikte bu iki ilke, genellikle "müdahale yasağı ilkesi" olarak adlandırılan aynı madalyonun iki yüzü olarak görülmekte ve çoğu zaman birbiriyle karıştırılmaktadır.[694] Örneğin, UAD'nın Nicaragua Davası kararında[695] geliştirdiği müdahale yasağı ilkesinin tanımı, her iki unsuru da kapsamaktadır. Bu bölümün amacı doğrultusunda, müdahale yasağı ilkesi, bir devletin başka bir devletin iç ve dış işlerine müdahaleyi yasaklayan ilkeyi ifade etmek için kullanılmaktadır. Müdahale yasağı ilkesi siber saldırılar için de geçerlidir.[696]

Genel anlamda, müdahale yasağı ilkesi, kuvvet kullanma yasağı ve egemenlik ilkesi ile de yakından ilişkilidir. Bu örf-adet hukuku ilkesi toprak bütünlüğüne saygı ve devletlerin egemen eşitliği ilkesine dayanmaktadır.[697]

Müdahale yasağı ilkesi, BM Şartı'nın 2. maddesinde çok boyutlu olarak düzenlenmiştir. Maddenin birinci fıkrası, üye devletlerin egemen eşitliğini teyit ederek müdahale yasağının temelini oluşturur. Dördüncü fıkra ise, herhangi bir devletin ülkesel bütünlüğüne veya siyasal bağımsızlığına karşı kuvvet kullanmasını yasaklamakta ve dolayısıyla kuvvet içeren müdahaleleri hukuka aykırı kabul etmektedir. Altıncı fıkra, BM üyesi olmayan devletlerin de bu ilkelere uygun davranmaları gerektiğini belirterek müdahale yasağının evrensel niteliğini pekiştirmektedir. Yedinci fıkra ise, BM'in bir devletin iç yetki alanına giren konulara

[693] Delerue, *Cyber Operastions and International Law,* 227.
[694] Pierre-Marie Dupuy ve Yann Kerbrat, *International Law*, (Paris: Editions Economica, 2008), 130; Pierre-Kerbrat, *International Law*, 130, Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-intervention", *Baltic Yearbook of International Law* 14 (2015), 137-144.
[695] Uluslararası Adalet Divanı, *Nicaragua/United States of America (Merits)*, para. 202.
[696] Krzysztof Ziolkowski, "Computer Network Operations and the Law of Armed Conflict", *Military Law and Law of War Review* 49 (2010), 164.
[697] Uluslararası Adalet Divanı, *Nicaragua/United States of America (Merits)*, para. 202.

müdahalesini yasaklayarak, iç işlere müdahale yasağı ilkesini kurumsal düzeyde güvence altına almaktadır.[698]

Nikaragua Davası kararında Uluslararası Daimi Adalet Divanı, müdahale yasağı ilkesinin kapsamını aşağıdaki şekilde açıklığa kavuşturmuştur:

"Müdahale yasağı ilkesi, tüm devletlerin veya devlet gruplarının diğer devletlerin iç ve dış işlerine doğrudan ya da dolaylı olarak müdahale edilmesini yasaklar. Yasaklanan müdahale, devlet egemenliği ilkesi gereği her bir devletin serbestçe karar verebileceği konulara ilişkin olmalıdır. Bu konular arasında siyasi, ekonomik, sosyal ve kültürel sistemin seçimi ile dış politikanın belirlenmesi yer alır. Bir müdahale, bu tür seçimlerde serbest iradeye dayalı olması gereken tercihleri zorlayıcı yöntemlerle etkilemeye çalıştığında hukuka aykırı hale gelir. Yasaklanan müdahalenin tanımlayıcı unsuru ve esasını oluşturan zorlayıcılık unsuru, özellikle askeri eylem gibi doğrudan kuvvet kullanımı veya başka bir devlet içindeki yıkıcı ya da terörist silahlı faaliyetleri desteklemek gibi dolaylı yöntemler kullanıldığında açıkça görülebilir."[699]

Dolayısıyla, bu ilke her bir devletin özgürce karar verebileceği; örneğin, "siyasi, ekonomik, sosyal ve kültürel bir sistemin seçimi ile dış politikanın belirlenmesi" gibi konulara yönelik doğrudan veya dolaylı müdahaleyi yasaklamaktadır.[700] Nikaragua Davası kararında, yasaklanan müdahalenin üç temel özelliği ortaya konmuştur: Birincisi, müdahale bir devletin diğer bir devlete karşı gerçekleştirdiği bir fiil olmalıdır. Bununla birlikte, özel bir kişi veya grubun gerçekleştirdiği bir fiil de bir devlete atfedilebiliyorsa, hukuka aykırı müdahale olarak değerlendirilebilir. İkincisi, hukuka aykırı müdahale, hedef devletin özgürce karar verebileceği, iç veya dış işlerine ilişkin konulara yönelik olmalıdır. Üçüncüsü ise, zorlayıcı unsur, hukuka aykırı müdahalenin temel bileşenini oluşturmalıdır. Hukuka aykırı müdahale, hedef devletin iç veya dış işlerine doğrudan ya da dolaylı şekilde müdahale ederek onu zorlamaya yönelik bir girişim niteliği taşımalıdır.[701]

Müdahale yasağı ilkesi, uluslararası örf ve adet hukukunun yerleşik bir kuralı olarak kabul edilmekle birlikte, bazı durumlarda devletler tarafından bu ilkeye karşı istisna iddiaları ileri sürülmektedir. Ancak, bu tür istisna iddiaları uluslararası hukuk tarafından genel olarak tanınmamaktadır. Nitekim UAD, Nikaragua kararında, ABD'nin müdahale yasağını ihlal eden

---

[698] Georg Nolte, "Article 2 (7)", *The Charter of the United Nations: A Commentary*, ed. Bruno Simma vd. (Oxford: Oxford University Press, 2012), 284-285.
[699] Uluslararası Adalet Divanı, *Nicaragua/United States of America (Merits)*, para. 205.
[700] Sean Watts**,** "Low-Intensity Cyber Operations and the Principle of Non-Intervention", *Baltic Yearbook of International Law* 14 (2015), 153-155.
[701] Gaetano Arangio-Ruiz**,** "Article 2(7)", *The Charter of the United Nations: A Commentary*, ed. Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus; yardımcı ed. Nikolai Wessendorf, 3. Baskı, Cilt 1 (Oxford: Oxford University Press, 2012), 260–261.

eylemlerini haklı göstermek amacıyla ileri sürdüğü "insani müdahale" ve "demokratik rejimleri destekleme" gerekçelerini açıkça reddetmiştir. Bu bağlamda, müdahale yasağına getirilebilecek hukuken geçerli istisnalar oldukça sınırlı olup, Divan bu tür istisna iddialarını uluslararası hukukun bir parçası olarak kabul etmemiştir.[702]

İç savaş veya isyan hareketlerinin yaşandığı bir ülkedeki protestoculara veya isyancılara destek amacıyla başka bir devletin müdahalede bulunması, hukuka aykırı müdahalenin en yaygın örneklerinden biridir.[703] Çünkü iç savaşlar ve bir devletin kendi ülkesinde bulunan isyancılarla ilişkileri genellikle o devletin iç işleri kapsamında değerlendirilir. Hukuka aykırı bir müdahale, hedef devletin ülkesel bütünlüğüne yönelik bir ihlal veya kuvvet kullanımı içermese dahi bu şekilde nitelendirilebilir. Diğer bir ifadeyle, ülkesel bütünlüğün ihlali veya kuvvet kullanımı, hukuka aykırı müdahalenin zorunlu koşulları değildir.[704] Bu bağlamda, örneğin ekonomik baskı genellikle ne bir egemenlik ihlali ne de kuvvet kullanımı olarak değerlendirilmekle birlikte müdahale yasağı kapsamında değerlendirilebilir.

Müdahale yasağı ilkesi ile ilgili olarak UAD önünde görülen üç dava büyük önem taşımaktadır. Bu ilke, ilk kez Korfu Boğazı Davası'nda UAD tarafından uygulanmış ve Divan, aynı tutumunu Nikaragua Davası ile Silahlı Faaliyetler Davası'nda teyit etmiştir.[705]

Korfu Boğazı Davası'nda, hukuka aykırı müdahale, Kraliyet Donanması'nın Boğazı'nda bir mayın tarlası bulunduğuna ilişkin deliller toplaması ve gerçekleştirdiği mayın temizleme operasyonuyla vücut bulmuştur.[706] Bu davada, UAD, müdahalenin uluslararası hukuka uygunluğu sağlamak ve delil toplamak amacıyla gerçekleştirilmiş olmasının, fiilin hukuka aykırılığını ortadan kaldırmadığına karar vermiştir.

UAD, Nikaragua Davası kararında, hukuka aykırı müdahale oluşturabilecek veya oluşturmayacak çeşitli örnekler sunmuştur. Bu bağlamda, UAD, ABD'nin Eylül 1984 sonuna kadar Nikaragua'daki "kontra" güçlerinin askeri ve paramiliter faaliyetlerine mali destek, eğitim, silah temini, istihbarat sağlama ve lojistik destek yoluyla verdiği desteğin yasaklanmış bir müdahale teşkil ettiğine hükmetmiştir. Ayrıca Divan, silahlı muhalif grupların silahlandırılması ve eğitilmesinin yanı sıra, yalnızca mali kaynak sağlama fiillerini de hukuka

[702] Uluslararası Adalet Divanı, *Nicaragua/United States of America (Merits)*, para. 205.
[703] Shaw, *International Law*, 832-841.
[704] Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", 145-148.
[705] Uluslararası Adalet Divanı, *Corfu Channel Davası (Birleşik Krallık v. Arnavutluk)*, Esas Hakkında Karar, 9 Nisan 1949, ICJ Reports 1949, 4-35; Uluslararası Adalet Divanı, *Askerî ve Paramiliter Faaliyetler Davası (Nikaragua v. Amerika Birleşik Devletleri)*, Esas Hakkında Karar, 27 Haziran 1986, ICJ Reports 1986, 14-150; Uluslararası Adalet Divanı, *Kongo Cumhuriyeti Topraklarında Silahlı Faaliyetler Davası (Kongo Demokratik Cumhuriyeti v. Uganda)*, Karar, 19 Aralık 2005, ICJ Reports 2005, 168-227.
[706] Uluslararası Adalet Divanı, *Corfu Channel Davası*, 4-35.

aykırı müdahale olarak değerlendirmiştir.[707] Bununla birlikte, Divan, 1981 Nisan ayında ekonomik yardımın kesilmesi, aynı dönemde ABD'nin Nikaragua'dan şeker ithalatı kotasını yüzde doksan oranında düşürmesi ile 1985 Mayıs ayında uygulanan ticaret ambargosunun müdahale yasağını ihlal etmediğine hükmetmiştir.[708]

Silahlı Faaliyetler Davası'nda UAD, Uganda'nın Demokratik Kongo Cumhuriyeti'nde faaliyet gösteren düzensiz güçlere sağladığı aktif ekonomik, askeri ve mali destek ile yürüttüğü askeri ve paramiliter faaliyetleri, müdahale yasağı ilkesinin ihlali ve hukuka aykırı kuvvet kullanımı olarak değerlendirmiştir.[709]

2.2.2. Müdahale Yasağına Aykırı Siber Eylemler

Hukuka aykırı müdahalenin üç temel unsuru bulunmaktadır: (1) bir devletin diğer bir devlete karşı gerçekleştirdiği bir fiil, (2) bu fiilin diğer devletin özgür iradesiyle karar verme yeteneği üzerinde baskı oluşturmayı amaçlaması ve (3) söz konusu yeteneği sınırlaması. Bu unsurlar çerçevesinde, aşağıda siber uzay kaynaklı bazı siber saldırı örneklerinin hukuka aykırı bir müdahale teşkil edip etmediği incelenecektir.

2.2.2.1.Sony Pictures Entertainment Olayı

Sony Pictures Entertainment saldırısı, müdahale yasağı ilkesinin siber uzaydaki kapsamını belirlemek açısından önemli bir örnek teşkil etmektedir. Japonya merkezli *Sony Corporation*'ın Amerikan iştiraki olan *Sony Pictures Entertainment*, 2014 yılında bir siber saldırıya uğramış ve şirketten önemli miktarda veri çalınmıştır. Saldırganlar, elde ettikleri verileri kamuoyuyla paylaşmıştır. Saldırının amacı, Kuzey Kore lideri Kim Jong-un'a yönelik bir suikastı konu alan *The Interview* adlı filmin gösteriminin iptal edilmesini sağlamak olarak belirtilmiştir. Amerika Birleşik Devletleri yetkilileri, saldırının Kuzey Kore tarafından desteklendiğini iddia etmiş; ancak Kuzey Kore, bu saldırıyla herhangi bir ilgisinin bulunmadığını ifade etmiştir.[710]

---

[707] Uluslararası Adalet Divanı, *Nicaragua/United States of America (Merits)*, para. 242.
[708] Uluslararası Adalet Divanı, *Nicaragua/United States of America (Merits)*, para. 228.
[709] Uluslararası Adalet Divanı, *Askerî ve Paramiliter Faaliyetler Davası (Nikaragua v. Amerika Birleşik Devletleri,* 14-150
[710] David E. Sanger ve Nicole Perlroth, "U.S. Said to Find North Korea Ordered Cyber Attack on Sony", *The New York Times*, 17 Aralık 2014, https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

Bu saldırıya ilişkin olarak, Aralık 2014'te ABD Ulusal Güvenlik Bakanı Jeh Johnson yaptığı açıklamada, "Sony Pictures Entertainment'a gerçekleştirilen siber saldırı, yalnızca bir şirket ve çalışanlarına karşı yapılmış bir saldırı değil; aynı zamanda ifade özgürlüğümüze ve yaşam biçimimize yönelik bir saldırıdır." ifadelerini kullanmıştır.[711] Ulusal Güvenlik Bakanı tarafından yapılan bu açıklama, ABD'nin içişlerine yönelik bir müdahaleye verilen bir tepki olarak değerlendirilebilir.

Müdahale yasağı ilkesinin ihlalinin gerçekleşebilmesi için öncelikle bir fiilin bir devlet tarafından başka bir devlete karşı gerçekleştirilmiş olması gerekmektedir. *Sony Pictures Entertainment*'a yönelik siber saldırıda failin kimliği kesin olarak tespit edilememiştir; bu nedenle, Kuzey Kore'nin söz konusu saldırıyı gerçekleştirdiği açık ve net biçimde ortaya konulamamıştır. Bununla birlikte, bu saldırının Kuzey Kore tarafından gerçekleştirildiği varsayıldığında, hukuka aykırı bir müdahalenin oluşabilmesi için gerekli olan ilk kriterin karşılandığı sonucuna ulaşılabilir. Müdahale yasağı ilkesinin ihlali için ayrıca mağdurun bir devlet olması gerekmektedir. Ancak, müdahalenin dolaylı şekilde gerçekleşebileceği de kabul edilmektedir. Bu bağlamda, bir devletin yabancı bir şirkete karşı gerçekleştirdiği eylem, dolaylı olarak başka bir devletin iç işlerine müdahale niteliği taşıyabilir ve bu nedenle müdahale yasağı ilkesinin ihlali kapsamında değerlendirilebilir.[712]

İkinci ve üçüncü unsur bakımından, hukuka aykırı bir siber müdahalenin varlığından söz edilebilmesi için, bir devletin normal şartlarda kendi iradesiyle karar verebileceği konularda bu devleti zorlamayı amaçlaması gerekir. Bu çerçevede, "ifade özgürlüğü" ve "yaşam biçimi" gibi kavramlar, bir devletin kendi örgütlenmesine ilişkin karar verme yetkisinin bir parçası olarak kabul edilir. Ancak, özel bir eğlence şirketini hedef alan söz konusu siber saldırıların, ABD'ye karşı doğrudan veya dolaylı bir zorlayıcı eylem teşkil ettiğini ileri sürmek oldukça güçtür.

Sony Pictures Entertainment'a yönelik siber saldırılar; şirketin iç yazışmalarının kamuya sızdırılması, filmlerin yayımlanmasında gecikmeler, bazı filmlerin yasa dışı olarak çevrim içi paylaşılması ve nihayetinde şirketin ekonomik açıdan zor duruma düşmesi gibi sonuçlar doğurmuştur. Ancak bu gelişmeler, Amerika Birleşik Devletleri üzerinde doğrudan veya dolaylı bir zorlayıcı etki yaratmamıştır. Somut olay verileri ve müdahale yasağı ilkesinin

[711] ABD Ulusal Güvenlik Bakanlığı (DHS), "Statement by Secretary Johnson on Cyber Attack on Sony Pictures Entertainment" (19 Aralık 2014), https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.

[712] Maziar Jamnejad ve Michael Wood, "The Principle of Non-intervention", *Leiden Journal of International Law* 22/2 (2009), 372-373.

kriterleri birlikte değerlendirildiğinde, söz konusu saldırının müdahale yasağı ilkesinin ihlali niteliği taşımadığı sonucuna ulaşılmaktadır.

2.2.2.2. Stuxnet Saldırısı

Stuxnet saldırısı, bugüne kadar siber uzay kaynaklı kuvvet kullanımı olarak değerlendirilen tek vaka olarak kabul edilmektedir. Bu saldırı sonucunda İran'ın nükleer programı hedef alınmış, sistemler enfekte edilerek işleyişi bozulmuş ve özellikle bazı santrifüjler fiziksel olarak tahrip edilmiştir.

Saldırının temel amacı, İran'ı nükleer programında değişiklik yapmaya ve askeri nükleer hedeflerinden vazgeçmeye zorlamaktı. İran'ın nükleer programı ise bazı devletler ve yorumcular tarafından hem sivil hem de askeri amaçlara hizmet eden çift kullanımlı bir faaliyet olarak değerlendirilmiştir. Her ne kadar bir devletin enerji ve askeri politikalarına belirli yeni antlaşmalar aracılığıyla sınırlamalar getirilebilse de, bu tür düzenlemeler aksi belirtilmedikçe devletin içişleri kapsamına girer. Bu bağlamda, Stuxnet saldırısının arkasında bir devletin bulunduğu iddiası doğrulanırsa, bu durum bir devletin başka bir devleti, enerji ve askeri politikalarını değiştirmeye zorlamak suretiyle gerçekleştirdiği hukuka aykırı bir müdahale olarak nitelendirilebilir.[713] Ancak burada vurgulanması gereken husus, söz konusu saldırının failinin kesin olarak tespit edilememiş olmasıdır. Genel kanı, bu zararlı yazılımın Amerika Birleşik Devletleri ve İsrail'in, diğer bazı devletlerin de desteğiyle tasarlanıp gerçekleştirildiği yönünde olsa da, bu durum yalnızca iddia düzeyinde kalmıştır.

2.2.2.3. Estonya'ya Karşı Gerçekleştirilen Siber Saldırılar

Müdahale yasağı ilkesine ilişkin önemli örneklerden biri, 2007 yılında Estonya'ya yönelik gerçekleştirilen siber saldırılardır. Tallinn'deki Sovyet dönemine ait bir heykelin başka bir yere taşınmasının ardından, kamu kurumları, bankalar, medya kuruluşları ve parlamentoya ait sistemler büyük çaplı DDoS saldırılarıyla hedef alınmış; devletin dijital altyapısı ciddi şekilde kesintiye uğramıştır. Saldırıların, Rusya ile bağlantılı gruplarca gerçekleştirildiği öne sürülmüş, ancak doğrudan devlet sorumluluğu tespit edilememiştir. Buna karşın, eğer saldırılar

[713] Terry D. Gill ve Kinga Tibori-Szabó, *The Use of Force and the International Legal System* (Cambridge: Cambridge University Press, 2023), 234-235.

bir devletin yönlendirmesiyle yapılmış olsaydı, bu durum Estonya'nın iç işlerine yönelik bir müdahale olarak değerlendirilirdi.[714]

2.2.2.4. 2016 ABD Seçimlerine Müdahale

2016 ABD başkanlık seçimlerinde yapılan siber bağlantılı saldırılar son dönemlerin en önemli saldırıları arasında yer almıştır. Bunlardan ilki Demokrat Parti'nin başkan adayı ve dönemin ABD Dışişleri Bakanı Hillary Clinton'ın e-posta tartışmaları ve Dışişleri Bakanı olarak görev yaptığı dönemde kullandığı kişisel e-posta sunucusundaki gizli bilgilerin sızdırılmasıdır.[715] İkincisi ise Demokratik Ulusal Komite'nin (DNC) hakclenmesidir. Üçüncüsü ise, otuz dokuz ABD eyaletindeki seçmen veri tabanlarının ve yazılım sistemlerinin hacklenmesidir.[716] Sonuncusu ise, ABD'de yoğun olarak kullanılan oy kullanma makinelerinin hacklendiği iddiasıdır.[717] [718]

Genel olarak, bu siber saldırıların arkasında Rusya Federasyonu'nun olduğu iddia edilmiştir. Saldırıları gerçekleştirenlerin, Rusya'nın Ana İstihbarat Teşkilatı (GRU) ile Federal Güvenlik Servisi (FSB) olduğu öne sürülmüştür. Ancak, Rusya Federasyonu bu iddiaları kesinlikle reddetmiştir. Öte yandan, Demokratik Ulusal Komite (DNC) ağlarına yönelik sızma sorumluluğunu, "*Guccifer 2.0*" takma adını kullanan "yalnız bir hacker" üstlendiğini belirtmiştir.[719]

DNC'yi hedef alan çeşitli siber saldırılar farklı amaçlara ve hedeflere yönelikti. Bu saldırılar sonucunda, Demokratik Parti'nin Cumhuriyetçi Parti'nin başkan adayı Donald Trump hakkında yürüttüğü araştırmaların yer aldığı veri tabanına erişim sağlanmıştır.[720]

---

[714] Terry D. Gill ve Kinga Tibori-Szabó, *The Use of Force and the International Legal System*, 234.

[715] United States Federal Bureau of Investigation (FBI), *Hillary R. Clinton* (2016), https://vault.fbi.gov/hillary-r.-clinton.

[716] Michael Riley ve Jordan Robertson, "Russian Hacks on U.S. Voting System Wider than Previously Known", *Bloomberg*, 13 Haziran 2017, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[717] Ellen Nakashima, "National Intelligence Director: Hackers Have Targeted 2016 Presidential Campaigns", *The Washington Post*, 18 Mayıs 2016, https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html.

[718] Brian Barrett, "America's Electronic Voting Machines Are Scarily Easy Targets", *WIRED*, 2 Ağustos 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/; Lily Hay Newman, "Voting Machines Are Still Absurdly Vulnerable to Attacks", *WIRED*, 28 Eylül 2018, https://www.wired.com/story/voting-machine-vulnerabilities-defcon-voting-village/.

[719] Thomas Rid, **"**All Signs Point to Russia Being behind the DNC Hack", *Motherboard*, 25 Temmuz 2016, https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack.

[720] David E. Sanger ve Nick Corasaniti, "D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump", *The New York Times*, 14 Haziran 2016, https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

Gerçekleştirilen bu siber saldırıların hangi saikle yapıldığı hala gündemdeki önemli sorulardan biridir.[721] Saldırıların, 2016 ABD başkanlık seçimleri için yürütülen kampanyayı etkilemeyi veya manipüle etmeyi amaçladığı iddia edilmiştir.[722] Varsayımlardan biri, bu saldırıların amacının, Rusya Federasyonu'nun lideri Vladimir Putin ve Rus hükümetinin Hillary Clinton yerine Donald Trump'ı tercih etmesi sebebiyle, Donald Trump'ın bir sonraki ABD Başkanı olarak seçilmesini kolaylaştırmak olduğu yönündedir.[723]

Uluslararası hukuk çerçevesinde bu olayı değerlendirecek olursak, öncelikle siyasi faaliyetlere müdahalenin müdahale yasağı ilkesinin ihlali anlamına gelip gelmediği sorusu gündeme gelmelidir.[724] Bir devletin başka bir devletin seçim sürecine müdahalesi, bir devletin diğerinin iç örgütlenmesini ve hükümetini serbestçe belirleme yetisini kısıtlayan bir tür zorlamayı ifade eder.[725] Ancak bir devletin başka bir devlette yapılan seçimlere karşı sergilediği tutum her zaman müdahale anlamına gelmez. Bu bağlamda örneğin, bir devletin başka bir devletteki aday lehine açıkça tercihini ifade etmesi sıkça karşılaşılan olağan bir durumdur; bu, hukuka aykırı bir müdahale teşkil edebilir ancak genellikle kamuoyunda bu şekilde kınanmaz. Mevcut örnekte, Rusya Devlet Başkanı'nın Donald Trump lehine yaptığı çeşitli açıklamalar bu durumu yansıtmaktadır.[726] Bununla birlikte, seçimlere yönelik müdahale aktif bir boyut kazandığında, örneğin Rusya Federasyonu'nun istihbarat topluluğu tarafından verilerin hacklenmesi ve çalınan bilgilerin yayınlanması durumunda, bu açıkça hukuka aykırı bir

[721] Susan Hennessey, "What Does the US Government Know about Russia and the DNC Hack?", *Lawfare*, 25 Temmuz 2016, https://www.lawfareblog.com/what-does-us-government-know-about-russia-and-dnc-hack.
[722] David E. Sanger ve Eric Schmitt, "Spy Agency Consensus Grows That Russia Hacked D.N.C.", *The New York Times*, 26 Temmuz 2016, https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.
[723] Bruce Schneier, "By November, Russian Hackers Could Target Voting Machines", *The Washington Post*, 27 Temmuz 2016, https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/; Shane Harris ve Nancy A. Youssef, "FBI Suspects Russia Hacked DNC; U.S. Officials Say It Was to Elect Donald Trump", *The Daily Beast*, 25 Temmuz 2016, https://www.thedailybeast.com/articles/2016/07/25/fbi-suspects-russia-hacked-dnc-u-s-officials-say-it-was-to-elect-donald-trump.html.
[724] Michael Wood, "The Principle of Non-intervention in Contemporary International Law: Non-interference in a State's Internal Affairs Used to be a Rule of International Law: Is It Still?", *Chatham House*, International Law Discussion Group Meeting, 2007, 7.
[725] Jack Goldsmith, "Yet More Thoughts on the DNC Hack: Attribution and Precedent", *Lawfare*, 27 Temmuz 2016, www.lawfareblog.com/yet-more-thoughts-dnc-hack-attribution-and-precedent.
[726] Andrew Roth, "Putin Says Trump Is 'Absolute Leader' in U.S. Presidential Race", *The Washington Post*, 17 Aralık 2015, https://www.washingtonpost.com/world/putin-no-major-gaps-with-washington-over-efforts-to-end-syria-conflict/2015/12/17/a178255e-a431-11e5-8318-bd8caed8c588_story.html; Andrew Roth, "Russia Denies DNC Hack and Says Maybe Someone 'Forgot the Password'", *The Washington Post*, 15 Haziran 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/russias-unusual-response-to-charges-it-hacked-research-on-trump/.

müdahale anlamına gelir.[727] Benzer şekilde, seçim sonuçlarını değiştirmek amacıyla oylama makinelerinin manipüle edilmesi de açıkça hukuka aykırı bir müdahale teşkil eder.[728]

Müdahale yasağına ilişkin olarak, ABD seçimlerinden iki gün sonra ABD Dışişleri Bakanlığı'nın hukuk danışmanı tarafından yapılan konuşmada şu hususlara değinilmiştir:

"Bu bağlamda, müdahale yasağını açıklığa kavuşturma konusunda karşılaştığımız zorlukları göz önünde bulunduralım. Uluslararası Daimi Adalet Divanı'nın Nikaragua Davası kararında ifade edildiği üzere, uluslararası örf ve adet hukuku tarafından benimsenen bu kural, devletlerin her bir devletin egemenlik ilkesi uyarınca özgürce karar verme hakkına sahip olduğu konularda —örneğin siyasi, ekonomik, sosyal ve kültürel sistemlerin seçimi gibi— baskı oluşturacak eylemlerde bulunmalarını yasaklamaktadır. Genellikle bu kural dar bir örf-adet hukuku kuralı olarak görülse de, devletlerin siber faaliyetleri bu yasağı ihlal edebilir. Örneğin, bir devletin başka bir devletin seçim yapma yeteneğine müdahale eden veya başka bir devletin seçim sonuçlarını manipüle eden siber saldırıları, müdahale yasağını açıkça ihlal eder. Bu nedenle, şeffaflığın artırılması amacıyla devletlerin, siber uzaydaki faaliyetlere yönelik müdahale yasağı ilkesinin uygulanmasına dair daha kapsamlı çalışmalar yapması gerekmektedir."[729]

2016 ABD seçimleri bağlamında, hacklenen dosyaların kamuoyuna açıklanması müdahale yasağı ilkesinin ihlali anlamına gelmektedir. Ancak hackleme eylemi, bu sürecin sadece hazırlık aşamasını oluşturmakta olup, dosyaların kamuoyuna açıklanmasından ayrı değerlendirilmelidir. Çünkü fail, hackleme işleminden sonra durmaya karar vererek dosyaların açıklanmasına devam etmeyebilirdi. Bu nedenle, hukuki açıdan hackleme ve dosyaların çalınması ile bu bilgilerin kamuoyuna açıklanması iki ayrı fiil olarak ele alınmalıdır. Bu kapsamda, seçim sürecini etkilemek amacıyla dosyaların kamuoyuna açıklanması müdahale yasağının ihlali iken, hackleme ve dosya çalınması ABD'nin egemenliğinin ihlali sayılmakla birlikte hukuka aykırı bir müdahale oluşturmaz.

Brian J. Egan, yukarıda atıf yapılan siber uzaya uygulanabilir uluslararası hukuka ilişkin konuşmasında, "başka bir devletin ülkesinde bulunan bilgisayarlar veya diğer ağa bağlı cihazlara yönelik uzaktan gerçekleştirilen siber saldırıların, uluslararası hukukun doğrudan ihlalini oluşturmadığını" belirtmiştir. Egan'a göre, bu tür siber saldırıların uluslararası hukukun

[727] Duncan B. Hollis**,** "Russia and the DNC Hack: What Future for a Duty of Non-intervention?", *Opinio Juris*, 27 Temmuz 2016, http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/.

[728] Michael N. Schmitt**,** "The Use of Cyber Force and International Law", *The Oxford Handbook of the Use of Force in International Law*, ed. Marc Weller (Oxford: Oxford University Press, 2015), 1116.

[729] Brian J. Egan**,** "International Law and Stability in Cyberspace", *Berkeley Journal of International Law* 35/1 (2017), 169-180.

doğrudan ihlalini teşkil etmesi için somut bir zarar meydana gelmiş olması gerekmektedir.[730] Dolayısıyla Egan, siber saldırılardan kaynaklanan uluslararası hukuk ihlallerinin oluşabilmesi için zarar eşiğinin aşılmasını şart koşmaktadır. Mevcut davada ise, DNC dosyalarının hacklenmesinin bu zarar eşiğini aşıp aşmadığının ve dolayısıyla bir ülkenin egemenliğinin ihlali olarak değerlendirilip değerlendirilemeyeceğinin tespit edilmesi gerekmektedir.

2.2.2.5. 2017 Fransa Seçimlerine Müdahale

En önemli siber müdahale örneklerinden biri de 2017 Fransa başkanlık seçimlerinde yaşanmıştır. Bu seçim sürecinde siber güvenlik açıkları ile Emmanuel Macron ve partisi "En Marche!" aleyhinde yürütülen dezenformasyon kampanyaları öne çıkmıştır.

5 Mayıs 2017 tarihinde, Emmanuel Macron'un seçim kampanyasından sızdırılan gigabaytlarca e-posta ve belge çevrimiçi olarak yayımlandı; bu olay daha sonra "Macron Sızıntıları" (*Macronleaks*) olarak adlandırıldı. Belgeler ilk olarak 5 Mayıs 2018 tarihinde Pastebin platformunda "*EMLEAKS*" başlığıyla yayımlandı[731] ve ardından *4chan forumu*nda ve sosyal medya ağlarında paylaşıldı. 31 Temmuz'da ise *WikiLeaks*, sızdırılan belgelerin birçoğunu "Macron Kampanya E-Postaları" başlığı altında yeniden yayımladı.

Yapılan bu siber saldırıların arkasında, APT 28 olarak da bilinen ve genellikle "Fancy Bear" adıyla anılan; Rusya'nın Askeri İstihbarat Teşkilatı GRU'ya bağlı olduğu iddia edilen grup yer almaktadır. Bu grup, 2017 Fransa Cumhurbaşkanlığı seçimleri sırasında yürütülen kimlik avı kampanyası ve diğer siber saldırılardan sorumlu tutulmaktadır. [732] Ancak, 1 Haziran 2017 tarihinde Fransa Ulusal Siber Güvenlik Ajansı (ANSSI) Başkanı Guillaume Poupard, saldırının o kadar genel ve basit olduğunu ifade ederek, "bunu neredeyse herkes yapmış olabilir" açıklamasında bulunmuştur.[733] Bununla birlikte, Fransa hükümeti, Emmanuel Macron'un seçilmesinden önce veya sonra gerçekleşen bu siber saldırıları ve genel olarak seçim kampanyası sırasında yaşanan müdahale girişimlerini, herhangi bir yabancı ülkeye resmi olarak atfetmemiştir.[734]

---

[730] Egan, "International Law and Stability in Cyberspace", 209-211.
[731] EMLEAKS, "EMLEAKS" (*Pastebin*, 5 Mayıs 2017), http://archive.fo/eQtrm.
[732] Feike Hacquebord, *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat* (A Trend Micro Research Paper, 2017), 13, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm.
[733] Martin Untersinger, "MacronLeaks: L'enquête Pointe Vers un Piratage 'Simple et Générique'", *Le Monde*, 2 Haziran 2017, https://www.lemonde.fr/pixels/article/2017/06/02/macronleaks-l-enquete-pointe-vers-un-piratage-simple-et-generique_5137945_4408996.html.
[734] Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume ve Janaina Herrera, *Information Manipulation: A Challenge for Our Democracies'*, Policy Planning Staff (CAPS, Ministry for Europe and Foreign

ABD seçimlerine yapılan siber müdahalede olduğu gibi, "En Marche!" hareketine yönelik siber saldırı fiilleri ile ele geçirilen belgelerin kamuoyuna açıklanması fiillerinin birbirinden ayrılması gerekmektedir; çünkü bu eylemler iki farklı fiil olup, tek bir bütünün parçaları olarak değerlendirilemezler. Bu durum, bu iki fiilin hukuki niteliklerinin de farklı olmasını beraberinde getirir.

İlk fiil, "En Marche!" partisine yönelik hackleme eylemidir. Bu eylem, yalnızca hazırlık niteliğinde olup, seçim sürecine müdahale etmeyi amaçlayan daha geniş bir bileşik eylemin parçası değildir. Bununla birlikte, daha önce DNC hacklemesinde görüldüğü gibi, failler yalnızca hackleme ile kalıp ele geçirilen dosyaların kamuoyuna açıklanmasına geçmeme kararı alabilirdi. Bu nedenle, "En Marche!" hackleme olayı ile seçim sürecine müdahale girişimi iki ayrı eylem olarak değerlendirilmelidir. Daha açık bir ifadeyle, dosyaların hacklenmesi ve çalınması Fransa'nın egemenliğinin ihlali anlamına gelirken, uluslararası hukuk açısından hukuka aykırı bir müdahale oluşturmaz.[735]

İkinci fiil ise, dosyaların kamuoyuna açıklanması ve yayılması yoluyla "En Marche!" partisinin ve adayının itibarını olumsuz etkilemeye yönelik çeşitli eylemleri kapsayan bileşik bir fiildir. Bu durum, 2016 ABD seçimlerine yapılan müdahaleden farklıdır; çünkü yayımlanan belgelerin bir kısmı değiştirilmiş veya tamamen uydurulmuştur. Ancak belgelerin değiştirilmiş ya da uydurulmuş olması, bu fiilin asıl amacını—yani Fransa'nın seçim sürecinin işleyişi üzerinde baskı oluşturmayı—değiştirmemektedir. Ayrıca belgelerin bir kısmının uydurma olması ya da sürecin amatörce yürütüldüğüne dair iddialar, fiilin hedefini ve niyetini etkilememektedir. Bu nedenle, söz konusu fiilin müdahale yasağı ilkesinin ihlali olarak değerlendirilmesi muhtemeldir.

Bu müdahale vakıasının hukuka aykırı bir müdahalenin üç temel kriterini karşılama olasılığı oldukça yüksektir. Öncelikle, müdahale yasağı ihlalinin gerçekleşebilmesi için müdahalenin bir devlet tarafından diğer bir devlete karşı gerçekleştirilmiş olması gerekmektedir. Somut olayda, Fransa 2017 seçimlerine yönelik bu müdahale girişimi resmen herhangi bir devlete atfedilmemiş olsa da, genel kanaat bu müdahaleden Rusya'nın sorumlu olduğu yönündedir. Ayrıca, hukuka aykırı bir müdahale, hedef devletin özgürce karar verebileceği ve iç ya da dış işlerini kapsayan konularla ilgili olmalıdır. Bu bağlamda, seçim süreçleri devletlerin iç işlerine giren ve özgürce karar verebilme yetkisi kapsamında yer alan konular arasında bulunmaktadır. Son olarak, hukuka aykırı bir müdahale, hedef devlete ait iç

Affairs) ve the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces) (Paris: Ağustos 2018), https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

[735] Delerue, *Cyber Operastions and International Law,* 254.

veya dış işlere doğrudan ya da dolaylı müdahale ederek baskı oluşturma amacı taşımalıdır. Bu nedenlerle, 2017 Fransa cumhurbaşkanlığı seçimlerine yönelik müdahale girişimi, eylemin yabancı bir devlete atfedilmesi durumunda hukuka aykırı müdahale teşkil etme ihtimali taşımaktadır.[736]

2.2.3. İç Savaş Esnasında Siber Müdahale

Bir devletin başka bir devletteki iç savaş ya da isyancılara destek amacıyla müdahalede bulunması, müdahale yasağı ilkesinin en yaygın ihlallerinden biridir. İç karışıklıklar ve iç savaşlar, bir devletin iç işleri kapsamında değerlendirilir. Bu çerçevede, bir devletin başka bir devlete karşı isyancılara destek vermek amacıyla siber saldırılar düzenlemesi, müdahale yasağı ilkesinin ihlalini oluşturabilir. Ayrıca, bu siber saldırıların siber savaş eşiğinin altında kalması, söz konusu fiillerin hukuka aykırı müdahale niteliğini ortadan kaldırmaz.[737]

Siber uzayın kendine özgü yapısı nedeniyle, bir devlet isyancılara destek vermek amacıyla çeşitli imkanlara sahip olmaktadır. Örneğin, düşük yoğunluklu bir siber saldırı yoluyla ilgili devletin iletişim sistemlerini hedef alarak isyancılara avantaj sağlanabilir. Bu tür saldırılar kuvvet kullanımı olarak değerlendirilmez; ancak müdahale yasağı ilkesinin ihlaline yol açar.

1999 Kosova Savaşı, bu bağlamda önemli bir örnek teşkil etmektedir.[738] Kosova Kurtuluş Ordusu, Yugoslavya Federal Cumhuriyeti'nin askeri kuvvetlerine karşı NATO'dan hava desteği almıştır. Ayrıca, ABD Hava Kuvvetleri'nin Sırp iletişim ağlarını kontrol altına almak ve Sırp ordusu ile yetkililere ait hassas verilere erişim sağlamak amacıyla siber saldırılar gerçekleştirdiği iddia edilmiştir. Özellikle ABD Hava Kuvvetleri'nin, Sırp telekomünikasyon ağlarına erişim için uydular ve özel olarak dönüştürülmüş uçaklar kullandığı belirtilmiştir.[739] Bu siber saldırılar, NATO üyesi yabancı devletlerin bir iç savaş sırasında isyancılara destek vermesi anlamına geldiği için, müdahale yasağı ilkesinin ihlali olarak değerlendirilebilir.

---

[736] Delerue, *Cyber Operastions and International Law,* 254.
[737] Delerue, *Cyber Operastions and International Law,* 257.
[738] NATO, "Operation Allied Force", 23 Mart - 10 Haziran 1999, https://www.nato.int/kosovo/all-frce.htm.
[739] James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2002), 70; aktaran Dimitrios Delibasis, *The Right to National Self-Defence in Information Warfare Operations* (England: Arena Books, 2007), 33–34.

2.2.4. Siber Casusluk ve Müdahale Yasağı İlkesi

Siber casusluk, genel olarak veri toplama faaliyetlerinden oluşan bir fiil olup, tek başına müdahale yasağı ilkesinin ihlali anlamına gelmez. Bir devletin başka bir devletten veri toplaması, hedef devletin karar alma özgürlüğünü etkilemeyi amaçlayan bir cebir eylemi oluşturmaz. Bu durum, casusluk faaliyetinin hedef devletin ülkesinde gerçekleştirilip egemenliğinin ihlal edilip edilmediğine bakılmaksızın değişmez. Ancak, elde edilen veriler hedef devleti zorlamaya yönelik bir amaçla kullanılabilir. Bu bağlamda, siber casusluk faaliyetleri tek başına hukuka aykırı müdahale teşkil etmese de, hedef devleti zorlamayı amaçlayan bileşik bir eylemin hazırlık aşaması veya ayrılmaz parçası olarak değerlendirilebilir ve bu nedenle hukuka aykırı müdahale niteliği taşıyabilir.[740] Dolayısıyla, yeni devlet dışı aktörler tarafından bir devlette bulunan bilgisayarlara ve ağlara izinsiz nüfuz edilerek gerçekleştirilen casusluk faaliyetleri, ilgili devletin ülkesel egemenlik ilkesinin ihlali olarak değerlendirilecektir.

Yukarıda aktardıklarımızdan hareketle, siber saldırıların birçok durumda müdahale yasağı ilkesinin ihlalini oluşturabileceğini açıkça ifade edebiliriz. Ayrıca, müdahale yasağı ilkesinin üç temel unsuru—bir devletin diğer bir devlete karşı gerçekleştirdiği, hedef devletin özgürce karar alma yetisini kısıtlayarak onu zorlamayı amaçlayan bir eylem—siber saldırılar açısından da geçerlidir. Başka bir deyişle, bu kriterler siber saldırılar için de diğer tüm devlet faaliyetlerinde olduğu gibi uygulanabilir niteliktedir.

Buraya kadar aktardıklarımızdan hareketle, çoğu devlet tarafından gerçekleştirilen veya devlet desteğiyle yürütülen siber saldırıların, hedef devleti zorlamak amacı taşıdığı ve bu nedenle müdahale yasağı ilkesinin ihlaline yol açabileceği sonucuna varılabilir. Bu bağlamda, siber saldırıların hukuka aykırılığının temel dayanağının büyük ölçüde müdahale yasağı ilkesinin ihlali olduğu söylenebilir.

2.3. İnsan Hakları ve Siber Uzay

Modern uluslararası insan hakları hukuku, 1945 sonrasında devlet yetkisini sınırlamak ve keyfi uygulamaları önlemek amacıyla devlet merkezli bir çerçeve olarak geliştirilmiştir. Bu çerçevede devletler, insan hakları ihlallerinden sorumlu tutulmakta ve özel aktörlerin faaliyetleri üzerinde düzenleyici bir rol üstlenmektedir. Ancak dijital teknolojinin

[740] Delerue, *Cyber Operastions and International Law,* 258.

yaygınlaşması ve büyük teknoloji şirketlerinin küresel ölçekte faaliyet göstermesi, insan hakları hukukunun geleneksel devlet merkezli yapısıyla uyum sorunları doğurmaktadır. Günümüzde dijital insan haklarının korunması, birey ile devlet arasındaki ilişkiden ziyade, birey ile teknoloji şirketleri arasındaki güç dinamiklerine bağlı hâle gelmiştir. Büyük teknoloji şirketleri, geniş kullanıcı tabanları, uluslararası faaliyet alanları ve hızlı teknolojik gelişimleri nedeniyle devletlerin geleneksel düzenleme mekanizmalarının ötesinde bir etki alanına sahiptir. Bu şirketler, ifade özgürlüğü, özel hayatın gizliliği ve eşitlik gibi temel hakların küresel ölçekte kullanımını doğrudan etkileyebilmekte ve bazı dijital hakların korunmasında, çevrimdışı dünyada devletlerin sağlayamadığı sorumlulukları üstlenebilmektedir.[741]

İnsan hakları hukukunun büyük teknoloji şirketlerine uygulanması için geliştirilen yaklaşımlar arasında, BM İnsan Hakları Konseyi'nin *İş ve İnsan Hakları* gündemi çerçevesinde belirlenen yükümlülükler, şirketlerin kurumsal politikalar yoluyla insan hakları normlarını işleyişlerine dahil etmesi ve özel prosedürler aracılığıyla denetlenmeleri yer almaktadır. Bu bağlamda 2011 tarihli Birleşmiş Milletler İş ve İnsan Hakları Rehber İlkeleri (*UNGP*), şirketlerin insan haklarına saygı göstermesini doğrudan tanıyan önemli bir çerçeve sunar. UNGP, devletlerin işletmeleri denetleme, düzenleme ve insan hakları ihlallerine karşı koruma yükümlülüğünü öne çıkarırken, şirketlerin insan haklarını ihlal eden etkileri önlemesini, olumsuz etkileri düzeltmesini, insan hakları politikaları oluşturmasını, etki değerlendirmesi yapmasını ve raporlama yapmasını zorunlu kılar. Ayrıca şirketlerin etkili şikâyet mekanizmaları kurması ve faaliyetleri boyunca insan haklarına saygı göstermesi, gönüllü taahhütlerden bağımsız olarak gereklidir.[742]

Büyük teknoloji şirketlerinin küresel ölçekte bireylerin temel haklarını doğrudan etkileyebilecek konumları, UNGP çerçevesinde özel bir önem taşır. İnternet ve dijital platformların yaygın kullanımı, şirketlerin veri kontrolü, algoritmik karar süreçleri ve kullanıcı deneyimlerine dair sundukları hizmetler, dijital hakların korunmasını doğrudan etkiler ve devletlerin geleneksel insan hakları uygulamalarının ötesinde sorumluluklar yükler.

UNGP'nin hukuken bağlayıcı olmaması ve gönüllü uygulamalara dayanması, şirketlerin sorumluluklarını fiilen sınırlayabilmektedir. Bu eksiklikler, BM İnsan Hakları Konseyi'nin Hukuken Bağlayıcı Araç (*LBI*) taslak çalışmalarıyla giderilmeye çalışılmaktadır.

---

[741] Yuval Shany, "Big Tech Companies' Obligations under International Human Rights Law", *Cabridge University Press,* (2025), 58, 3–27, 4-5.

[742] Surya Deva, "Treating Human Rights Lightly: A Critique of the Consensus Rhetoric and The Language Employed by the Guiding Principles", *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?*, ed. Surya Deva ve David Bilchitz (Cambridge: Cambridge University Press, 2013), 78/94.

LBI, devletlere şirketleri insan hakları ihlallerinden korumak ve uluslararası haklara saygıyı güvence altına almak için güçlü düzenleyici yükümlülükler getirirken, şirketlerin kontrolü altındaki üçüncü tarafların ihlallerini önleme sorumluluğunu doğrudan vurgular. Bu düzenleme, özellikle büyük teknoloji şirketlerinin tedarik ve değer zincirleri üzerinden dijital hakların korunmasına yönelik sorumluluklarını genişletmekte ve çevrim içi faaliyetler sonucu ortaya çıkabilecek ihlallere karşı daha sistematik bir önlem mekanizması sağlamaktadır.[743]

Sonuç olarak, UNGP ve LBI çerçeveleri, büyük teknoloji şirketlerinin insan haklarına saygı göstermesi gereken doğrudan sorumluluklarını tanımlamakta ve devletlerin bu şirketleri denetleme yükümlülüklerini güçlendirmektedir. Bu düzenlemeler, dijital insan haklarının korunmasında devlet merkezli yaklaşımı genişletirken, büyük teknoloji şirketlerinin küresel ölçekte hak ihlallerini önleme ve kullanıcı haklarını güvence altına alma sorumluluklarını ön plana çıkarmaktadır. Teknolojik dinamizm ve yapısal sınırlamalara rağmen, bu çerçeveler dijital hakların korunmasında hem devletlerin hem de şirketlerin yükümlülüklerini bütüncül bir şekilde ortaya koyan temel bir referans işlevi görmektedir.

2.3.1. İnsan Haklarının Siber Saldırılara Uygulanabilirliği

Bazı siber saldırılar, belirli koşulların varlığı halinde gerçek kişilerin ve grupların haklarını ihlal edebilir; diğer bir ifadeyle, siber saldırılar insan hakları ihlallerine yol açabilmektedir. Bu durum üç farklı senaryo çerçevesinde ele alınabilir. Birinci senaryoda, A devleti kendi toprakları içinde bulunan yabancı gerçek kişilerin insan haklarına müdahale eden bir saldırı gerçekleştirmektedir. İkinci senaryoda, A devleti yargı yetkisi altındaki yabancı gerçek kişilerin insan haklarına müdahale eden bir siber saldırıyı başka bir devlete karşı icra etmektedir. Üçüncü senaryoda ise, A devleti hem kendi ülkesi dışında bulunan hem de yargı yetkisi altında olmayan gerçek kişilerin insan haklarına müdahale eden bir siber saldırıyı başka bir devlete karşı yürütmektedir.[744]

Birinci ve ikinci senaryolar, insan hakları hukukunun bir devletin ülkesinde ve yargı yetkisi altında uygulanabilirliğine işaret etmektedir. Bir devletin, kendi sınırları içinde veya yargı yetkisi altındaki gerçek kişilerin—örneğin başka bir ülkede bulunan vatandaşlarının—insan haklarına saygı gösterme, bu hakları koruma ve güvence altına alma yükümlülüğü bulunmaktadır. Bu durum, insan hakları hukukunun uygulanabilirliğine dair genel bir yaklaşımı

[743] Daniel J. Gervais, ""The Regulation of Inchoate Technologies The Regulation of Inchoate Technologies", 47 *Houston Law Review* (2010) 665.
[744] Delerue, *Cyber Operastions and International Law,* 260.

ortaya koymaktadır.[745] Burada önemli olan husus, "ülke" kavramının tanımının genellikle açık ve net olmasıdır; ancak "yargı yetkisi" kavramı, birden fazla anlam içerebilmekte ve devletlerin sınır ötesi faaliyetlerini de kapsayacak şekilde daha geniş bir anlamda yorumlanabilmektedir.

İnsan hakları bağlamında, bir devletin başka bir devlette bulunan yabancıların insan haklarına saygı gösterme yükümlülüğü ancak bu yabancıların o devletin resmi organlarının "etkin kontrolü" altında olması ve dolayısıyla o devletin yargı yetkisi kapsamına girmesi durumunda söz konusu olur. Benzer şekilde, bir devlet yabancı bir devletin daveti, rızası veya zımni onayıyla o devlete ait bir toprakta bazı "kamu yetkileri" kullanıyorsa, bu durumda sınır ötesi yargı yetkisine sahip olur. [746] Yargı yetkisi kavramının bu tür genişletilmiş anlamlarına ve buna bağlı insan haklarına saygı yükümlülüğüne rağmen, siber saldırılardan etkilenen gerçek kişilerin çoğu, fail devletlerin yargı yetkisi dışında kabul edilmektedir.

İnsan hakları hukukunun uygulanabilirliğine ilişkin bu geleneksel yaklaşım, genellikle siber gözetleme programları yürüten devletler tarafından benimsenmektedir. Bu devletler, insan hakları hukukunun yalnızca kendi ülkesinde bulunan gerçek kişilere—uyruklarına bakılmaksızın—ve yurtdışında bulunan vatandaşlarına ya da daha geniş anlamda kendi yargı yetkisi altındaki gerçek kişilere uygulandığını savunmakta ve dolayısıyla gözetleme kapasitelerinin sınırlandırılması gerektiğini ileri sürmektedirler.[747]

Yargı yetkisinin siber uzaya genişletilmesi açısından karşılaşılan en önemli zorluklardan biri, devletlerin siber saldırılar da dahil olmak üzere, yargı yetkisi dışındaki kişileri hedef alabilecek veya etkileyebilecek sınır ötesi faaliyetleri artırmalarıdır.[748] Daha açık bir ifadeyle, siber saldırıların büyük bir kısmı, saldırıyı gerçekleştiren devletin doğrudan kontrolü veya yargı yetkisi altında olmayan ve aynı zamanda başka bir devlette (saldırıyı gerçekleştiren devletin sınırları dışında) yaşayan gerçek kişilerin insan haklarına zarar verebilir veya bu haklara müdahale edebilir. Bu bağlamda sorgulanması gereken temel husus, bu tür müdahalelerin insan hakları normlarına aykırı olup olmadığıdır. Ancak bu soruya kesin bir yanıt bulunmamaktadır. Özellikle siber saldırılar ve insansız hava araçları saldırılarının yaygınlaştığı günümüzde, insan haklarının uygulanabilirliği konusunda önemli zorluklar ortaya çıkmaktadır. Uluslararası insan

---

[745] Olivier De Schutter, *International Human Rights Law*, 2. bs. (Cambridge: Cambridge University Press, 2014), 147 ve devamı.

[746] Avrupa İnsan Hakları Mahkemesi (AİHM), *Banković ve Diğerleri / Belçika ve Diğerleri*, B. No: 52207/99, Raporlar 2001-XII, para. 71; Avrupa İnsan Hakları Mahkemesi (AİHM), *Al-Skeini ve Diğerleri / Birleşik Krallık*, Karar, B. No: 55721/07, Raporlar 2011-IV, para. 135.

[747] Delerue, *Cyber Operastions and International Law,* 264.

[748] Fons Coomans ve Menno T. Kamminga (ed.), *Extraterritorial Application of Human Rights Treaties* (Antwerp: Intersentia, 2004); Françoise Hampson, "The Scope of the Extra-Territorial Applicability of International Human Rights Law", *The Delivery of Human Rights: Essays in Honour of Professor Sir Nigel Rodley*, ed. Françoise Hampson, Geoff Gilbert ve Clara Sandoval (Londra: Routledge, 2011), 157-182.

hakları hukukunun mevcut yorumuna göre, siber saldırılardan etkilenen gerçek kişiler, saldırıyı gerçekleştiren devletin sınırları içinde yaşamadıkları için "mekânsal model" (*spatial model*) kapsamında değerlendirilmemektedir.[749] Ayrıca, bu gerçek kişiler ne saldırıyı gerçekleştiren devletin vatandaşıdır ne de bu devletin yargı yetkisi ya da etkin kontrolü altındadır. Bu nedenle, söz konusu kişiler uluslararası insan hakları hukukunun "kişisel model" (*personal model*) olarak adlandırılan kapsamı içinde değerlendirilememektedir.[750] Diğer bir ifadeyle, uluslararası insan hakları hukukunun uygulanabilirliği bağlamında, bu gerçek kişiler hem coğrafi hem de kişisel kriterler bakımından saldırıyı gerçekleştiren devletin sorumluluk alanı dışında kalmaktadır.[751]

İnsan haklarının siber uzaya uygulanabilirliği konusunda Peter Margulies tarafından ortaya konan yaklaşım dikkat çekicidir. Margulies, devletlerin *Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşmesi*'den kaynaklanan haklara saygı gösterme yükümlülüğünün sınır ötesi bir kapsamda uygulanması gerektiğini savunmaktadır.[752] Ancak bu sınır ötesi uygulama yalnızca saygı gösterme yükümlülüğünü kapsamakta olup, bu hakları temin etme görevi bu kapsama dahil edilmemektedir. Ayrıca Margulies, siber gözetim bağlamında "etkin kontrol" kavramının yargı yetkisi açısından oldukça dar bir çerçeveye sahip olduğunu vurgulamakta ve bunun yerine "sanal kontrol" kavramının kullanılmasını önermektedir. Margulies'ün geliştirdiği "sanal kontrol" testi, bir devletin gerçek kişilerin iletişimleri üzerinde kontrol sahibi olması durumunda, fiziki ya da coğrafi bir sınır olmaksızın bu kişiler üzerinde yargı yetkisine sahip olacağını ileri sürmektedir.[753]

2.3.2. Dijital Çağda Mahremiyet

Siber saldırılar bağlamında ihlal edilme riski en yüksek olan insan hakkı, mahremiyet hakkıdır. Örneğin, 2013 yılında, ABD Ulusal Güvenlik Ajansı (NSA) ve Birleşik Krallık Hükümet İletişim Merkezi'nin (GCHQ), Avustralya, Kanada ve Yeni Zelanda ile iş birliği

[749]Delerue, *Cyber Operastions and International Law,* 263.
[750] Delerue, *Cyber Operastions and International Law,* 263.
[751] Delerue, *Cyber Operastions and International Law,* 263.
[752] Peter Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism", *Fordham Law Review* 82 (2013), 2137-2149.
[753] Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism", 2150-2152.

içinde gerçekleştirdiği kitlesel gözetim programlarının kamuoyuna ifşa edilmesi, siber uzaydan kaynaklanan casusluk faaliyetlerini gün yüzüne çıkarmıştır.[754]

Siber uzayın kendine özgü yapısından dolayı mahremiyet hakkı özel bir öneme sahiptir.[755] Daha açık bir ifadeyle belirtecek olursak son derece dijitalleşmiş ve internet bağlantılı toplumlarda, giderek daha fazla kişisel veri bilgisayarlarda depolanmakta ve bilgisayar ağları üzerinden değiş tokuş edilmektedir.[756] Böylece bu veriler, sahiplerinin rızası olsun ya da olmasın, devletler, şirketler ve gerçek kişiler de dahil olmak üzere üçüncü taraflarca erişilebilir hale gelmiş ve özellikle gözetleme amacıyla kullanılmıştır. Bu çalışmamız bağlamında veri toplamanın iki ana biçimi birbirinden ayırt edilmelidir. Bunlar: a) kitlesel veri toplama (*mass data collection*) ve b) hedefli veri toplama (*targeted collection of data*)dır.[757]

Gözetleme için kitlesel veri toplama genellikle internet kabloları ve altyapıları üzerinden geçen verilerin toplanmasıyla gerçekleştirilir.[758] Kitlesel veri toplama fiilinde aynı anda çok sayıda kişiden veri toplanması söz konusu olduğundan, özel hayatın gizliliğinin kitlesel olarak ihlal edilmesi ihtimali oldukça yüksektir.[759] Bu uygulamalar, çok sayıda kişinin mahremiyet hakkına ayrım gözetmeksizin müdahale oluşturduğu için önemli endişelere neden olmaktadır.[760] Verilerin hedef gözetilerek toplanması, hedef alınan gerçek kişilerin yanı sıra hedef alınan verilerle birlikte verileri toplanabilecek diğer gerçek kişilerin de mahremiyet hakkını ihlal etmektedir.

Mahremiyet hakkı, gözetleme alanın dışında kalan siber saldırılar yoluyla da ihlal edilebilir. Bu hak, kitlesel gözetleme için yapılan toplu veri toplama ya da belirli bazı gerçek kişileri hedef alan casusluk faaliyetleriyle kolayca ihlal edilebilir. Ancak, siber casusluk, devletler tarafından gerçekleştirilen veya desteklenen ve mahremiyet hakkını veya diğer insan haklarını ihlal edebilecek tek siber faaliyet türü değildir. İnternetin birbirine bağımlı doğası

---

[754] Anne Peters, "Surveillance without Borders? The Unlawfulness of the NSA-Panopticon", *EJIL: Talk!* (Kasım 2013), www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/.

[755] Peter Blume, "Data Protection and Privacy: Basic Concepts in a Changing World", *Scandinavian Studies in Law* 56 (2010), 151-154.

[756] Christoph Sobotta ve Juliane Kokott, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR", *European Data Protection Law Review* 3 (2013).

[757] Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", *UN Doc A/HRC/23/40* (2013), 10-13; Ben Wagner, Joanna Bronowicka ve Thomas Berger, "Surveillance and Censorship: The Impact of Technologies on Human Rights", *European Parliament* (2015), 8.

[758] Peter Malanczuk, "Data, Transboundary Flow, International Protection", *Max Planck Encyclopedia of Public International Law (MPEPIL)*, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e771 (OUP, 2009);

[759] Navi Pillay, "Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age", *UN Doc A/HRC/27/37* (2014), 6-7.

[760] Wagner, Bronowicka ve Berger, "Surveillance and Censorship: The Impact of Technologies on Human Rights", 11-12.

nedeniyle, bir siber saldırının doğrudan hedef almadığı gerçek kişiler ve gruplar da bu saldırının sonucunda insan haklarının ihlaline maruz kalabilir. Sony Pictures Entertainment'ın hacklenmesi olayı, casusluk amacı taşımayan bir siber saldırının mahremiyet hakkını nasıl ihlal edebileceğine dair önemli bir örnek teşkil etmektedir.[761] Bu saldırının failleri, Sony'nin sunucularından ayrım gözetmeksizin veri toplamış ve bu verileri kamuoyuna açık bir şekilde yayımlamıştır. Yayınlanan veriler arasında çalışanlara ait özel e-postalar ve kişisel bilgiler de bulunmaktadır. Bu örnekte, Sony Pictures Entertainment çalışanlarını gözetleme amacı olmamasına rağmen, gerçekleştirilen siber saldırılar yine de onların mahremiyet hakkına müdahalede bulunmuştur. Bu örnek, gözetleme amacı taşımayan bir siber saldırının dahi nasıl veri toplayabileceğini ve mahremiyet hakkında müdahalede bulunabileceğini göstermektedir.

2.3.3. Diğer İnsan Hakları

Siber uzayın kendine özgü doğası nedeniyle bazı siber operasyonlar hiç etki doğurmazken, diğerleri veri hırsızlığı ya da veri imhası gibi yalnızca dijital alanla sınırlı etkiler oluşturabilir; buna karşılık bazıları ise mülkiyetin zarar görmesi veya yok edilmesinin yanı sıra can kaybı ve yaralanma gibi fiziksel sonuçlara kadar varan farklı seviyelerde etkiler doğurabilir. Örneğin, bir siber saldırının bir şehrin veya eyaletin elektrik şebekesini bozması ya da tamamen kapatması sonucunda ulaşım sistemleri, su ve kanalizasyon hizmetleri, gıda tedariki aksayabilir ve elektrik kesintisi yaşanabilir.[762] Bu tür bir durum, kesintiden etkilenen insanların yaşamı ve sağlığı üzerinde ciddi ve hayati sonuçlar doğurabilir. Bu nedenle, ortaya çıkan bu etkiler doğrudan belirli insan hakları normlarına müdahale niteliği taşıyabilir.

Siber saldırılar, nükleer santraldeki santrifüjlerin fiziksel olarak tahrip edilmesi gibi maddi varlıklarda hasar yaratabileceği gibi, sabit diskteki verilerin silinmesi veya bozulması gibi maddi olmayan zararlar da meydana getirebilir. Çalınan, zarar gören ya da yok edilen veriler, hedef devletle ilişkili ya da ilişkili olmayan gerçek veya tüzel kişilere ait olabilir. Benzer şekilde, siber saldırılar sonucunda zarar görebilecek diğer mülkiyet ve varlıklar da bu kapsama dahildir. Bu tür durumlarda, siber saldırılar, mülkiyet sahibi gerçek veya tüzel kişilerin mülkiyet hakkına doğrudan müdahale teşkil edebilir.

Uluslararası hukuk açısından özel mülkiyetin korunması, özellikle yabancıların haklarının korunmasına yönelik örf ve adet hukuku normları ile insan hakları hukuku gibi çeşitli doktrinlere dayanmaktadır. Ancak, bu hakkın siber saldırılar nedeniyle ortaya çıkan zarar ve

[761] Delerue, *Cyber Operastions and International Law,* 266.
[762] Delerue, *Cyber Operastions and International Law,* 269.

tahribat durumlarına uygulanıp uygulanmayacağı, yalnızca gelecekteki devlet uygulamaları ve pratikleriyle kesinlik kazanacaktır. Ayrıca, veri hırsızlığı, verinin bozulması veya yok edilmesi, aynı zamanda bireylerin mahremiyet hakkına yönelik bir müdahale olarak da değerlendirilmektedir.[763]

Ölüm veya yaralanmaya neden olan siber saldırılar, insan hayatını ve güvenliğini düzenleyen insan hakları normlarına müdahale teşkil edebilir. Günümüze kadar hiçbir siber saldırı yaralanmaya veya can kayına sebep olmamışsa da, gelecekteki siber saldırılar bu türden bir sonuç doğurabilir.[764] Sonuç olarak, siber saldırılar sonucunda, yaşam hakkı, güvenlik hakkı ve mülkiyet hakları gibi insan hakları ihlal edilebilmektedir.

2.4. Kuvvet Kullanma Yasağı ve Siber Eylemler

Siber uzaydan kaynaklanan siber saldırıların uluslararası hukukunun yasakladığı kuvvet kullanma yasağını ihlal edip etmediği de literatürde çokça tartışılan konular arasında yer almaktadır.

2.4.1. Uluslararası Hukukta Jus contra Bellum ve Siber Eylemler

Birleşmiş Milletler (BM) Şartı, devletlerin diğer devletlere karşı kuvvet kullanma tehdidinde bulunmalarını veya kuvvet kullanmalarını yasaklamaktadır. Bu yasak, Şart'ın 2. maddesinin 4. paragrafında şu şekilde ifade edilmiştir:

"Bütün üyeler, uluslararası ilişkilerinde, herhangi bir devletin toprak bütünlüğüne veya siyasal bağımsızlığına karşı ya da Birleşmiş Milletler'in Amaçları ile bağdaşmayacak herhangi bir şekilde kuvvet kullanma tehdidine veya kuvvet kullanılmasına başvurmaktan kaçınırlar."[765]

BM Şartı, kuvvet kullanma yasağına iki istisna öngörmektedir. Bunlardan ilki, Şart'ın VII. Bölümü uyarınca BM Güvenlik Konseyi tarafından kuvvet kullanımına izin verilmesidir. İkincisi ise Şart'ın 51. maddesinde düzenlenen meşru müdafaa hakkıdır. Bu bağlamda, kuvvet kullanımıyla ilişkili üç temel kavram öne çıkmaktadır: (1) kuvvet tehdidi veya kuvvet kullanımı, (2) silahlı saldırı ve (3) barışa tehdit, barışın ihlali ve saldırı fiili. Bu kavramlar farklı hukuki bağlamlarda kullanılmakta olup, aralarında kesin bir hiyerarşik ilişki bulunmamaktadır.

---

[763] Delerue, *Cyber Operastions and International Law,* 269.
[764] Lucas Lixinski, *Legal Implications of the Privatization of Cyber Warfare* (EUI Working Papers, Academy of European Law 2010/2, PRIV-WAR Project 2010), 10, http://hdl.handle.net/1814/13577.
[765] Birleşmiş Milletler (BM), *Birleşmiş Milletler Şartı* (San Francisco: Birleşmiş Milletler, 1945), md. 2/4.

Her biri, BM Şartı'nın farklı bölümlerinde yer almakta ve farklı eşiklere işaret etmektedir. Örneğin, "silahlı saldırı" kavramı, meşru müdafaa hakkının doğabilmesi için gerekli olan eşiği ifade ederken; "saldırganlık" kavramı, özellikle BM Genel Kurulu'nun 3314 (XXIX) sayılı Kararı'nda tanımlandığı üzere, daha çok siyasal sorumluluk ve cezai sorumluluk bağlamında değerlendirilir. Her iki kavram da kuvvet kullanımının ağır biçimlerini kapsamakla birlikte, farklı işlevlere sahiptir.[766] Bununla birlikte, söz konusu terimlerin hiçbiri BM Şartı'nda açıkça tanımlanmamıştır.

Yukarıda belirtilen üç kategori aşağıdaki şekilde özetlenebilir: İlk kategori, BM Şartı'nın 2. maddesinin 4. paragrafına dayanmaktadır. Bu hüküm, devletlerin kuvvet tehdidinde bulunmasını veya kuvvet kullanmasını yasaklamakta olup, BM Şartı tarafından belirlenen en geniş ve en düşük eşiği ifade etmektedir. Yalnızca bu eşiğe ulaşan siber saldırılar, *jus contra bellum* kapsamında siber savaş olarak değerlendirilebilir. İkinci kategori ise BM Şartı'nın 51. maddesinden kaynaklanmaktadır. Buna göre, silahlı bir saldırı meydana geldiğinde saldırıyı gerçekleştiren devlete karşı mağdur devletin meşru müdafaa hakkı bulunmaktadır. Bununla birlikte, "silahlı saldırı" kavramı ile "kuvvet kullanımı" arasında fark olup olmadığı hususunda çeşitli tartışmalar mevcuttur. Azınlık bir grup devlet ve akademisyene göre bu iki kavram eşdeğerdir ve dolayısıyla her türlü kuvvet kullanımı mağdur devlete meşru müdafaa hakkı doğurur.[767] Çoğunluk görüşe göre, yalnızca kuvvet kullanımının en ağır biçimleri "silahlı saldırı" olarak nitelendirilebilir. UAD'da Nikaragua Davası'nda bu yaklaşımı benimsemiş ve yalnızca "kuvvet kullanımının en ağır biçimlerinin" silahlı saldırı teşkil edeceğini açıkça ifade etmiştir.[768] Üçüncü kategori ise "saldırganlık" kavramıdır. BM Şartı'nın 39. maddesi uyarınca BM Güvenlik Konseyi, "barışa yönelik herhangi bir tehdit, barışın ihlali veya saldırı fiili"nin varlığını tespit etme yetkisine sahiptir. Bu bağlamda, saldırganlık kavramı, "hukuka aykırı kuvvet kullanımının en ağır ve en tehlikeli biçimlerini" kapsayacak şekilde tanımlanmaktadır.[769] Bununla birlikte, barışın ihlali veya barışa karşı tehdit kavramları Şart'ta tanımlanmamış olup, Güvenlik Konseyi'nin takdirine ve uygulamasına bırakılmıştır.[770] Sonuç

[766] Mikaela Nyman, *Cyber Attacks as Armed Attacks? The Right of Self-Defence When a Cyber Attack Occurs* (Yüksek Lisans Tezi, Stockholm Üniversitesi Hukuk Fakültesi, 2023).
[767] Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 47, para. 7.
[768] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits), [1986] ICJ Reports 14, 101, para. 191.
[769] Birleşmiş Milletler Genel Kurulu (BMGK), *Saldırının Tanımı*, Karar 3314 (XXIX) (14 Aralık 1974).
[770] Michael Wood, "Peace, Breach of", *Max Planck Encyclopedia of Public International Law* (MPEPIL), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e372 (Oxford University Press, 2009); Erika de Wet, "Peace, Threat to", *Max Planck Encyclopedia of Public International Law* (MPEPIL), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e374 (Oxford University Press, 2009).

olarak, kuvvet kullanma yasağına aykırı bir siber eylemin eşiği, BM Şartı m.2/4'te öngörülen "kuvvet tehdidi veya kuvvet kullanımı" eşiğidir. Başka bir ifadeyle, ancak bu eşiğe ulaşan, yani siber kuvvet tehdidi veya siber kuvvet kullanımı olarak nitelendirilebilecek siber saldırılar, *jus contra bellum* kapsamında uluslararası hukuka aykırı kabul edilebilir. Kanaatimizce de siber uzaydan kaynaklanan siber saldırılar bakımından m. 2/4, hem kuvvet tehdidine hem de kuvvet kullanımına yönelik genel bir yasak öngörmektedir.[771]

Mevcut uluslararası hukukta, devletlerin "siber kuvvet" kullanımını açıkça yasaklayan özel bir uluslararası antlaşma bulunmamaktadır. Bu bağlamda, "siber kuvvet" kullanımına ilişkin sınırlamalar, BM Şartı ile uluslararası örf-adet hukukunun öngördüğü genel kuvvet kullanma yasağına dayanmaktadır. Kanaatimizce, kuvvet kullanma tehdidi veya kuvvet kullanma yasağı açısından değerlendirildiğinde, BM Şartı m. 2/4'te yer alan mevcut düzenleme ile uluslararası örf-adet hukukunun siber kuvvet kullanımı bakımından yeterli olduğu söylenebilir. Zira Şart m.2/4'te öngörülen kural, güvenlik tehditlerindeki değişimlere uyum sağlayabilecek ölçüde esnek bir şekilde kaleme alınmıştır. Nitekim BM Şartı'nın kabulünden bu yana, söz konusu örf-adet hukuku kuralının içeriği değişmemiş ve devlet uygulamalarıyla dönüştürülmemiştir.

2.4.2. Kuvvet Kullanma Yasağı Kapsamında Siber Saldırılar

BM Şartı'nda "kuvvet" kavramı tanımlanmamış olmakla birlikte, siber savaşın temel unsurlarından biri olan "savaş" kavramı, yalnızca "kuvvet" kullanımının bir türü olarak değerlendirilmektedir. Bu çerçevede "kuvvet" kavramı, daha geniş bir anlam taşımakta ve daha somut bir olguyu ifade etmektedir.

Yoram Dinstein'ın da belirttiği üzere, BM Şartı m. 2/4'te yer alan "kuvvet" ifadesinin önünde "silahlı" sıfatı bulunmazken, Şart'ın diğer bölümlerinde, örneğin 41. ve 46. maddelerinde "silahlı kuvvet" ifadesi açıkça yer almaktadır.[772] Bazı hukukçular yasaklanan kuvvetin yalnızca silahlı kuvvetle sınırlı olduğunu savunurken, [773] diğerleri bu yasağın daha geniş bir yorumla silahlı kuvvetin ötesini kapsaması gerektiğini öne sürmektedir.[774] UAD,

[771] Christine Gray, *International Law and the Use of Force* (Oxford: Oxford University Press, 2008), 30-33.
[772] Delerue, *Cyber Operastions and International Law,* 283-284.
[773] Tom Ruys, "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?", *American Journal of International Law* 108 (2014), 159-163; Jutta Brunnée, "The Meaning of Armed Conflict and the Jus ad Bellum", *What Is War? An Investigation in the Wake of 9/11*, ed. Mary Ellen O'Connell (Leiden: Martinus Nijhoff Publishers, 2012), 32; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), 40-49.
[774] Olivier Corten, *The Law against War*, çev. Çevirmen Adı Soyadı (Basım Yeri: Yayıncı, Basım Yılı), 52; Yoram Dinstein, *War, Aggression and Self-Defence*, çev. Çevirmen Adı Soyadı (Basım Yeri: Yayıncı, Basım Yılı), 88;

*Nükleer Silahlar Danışma Görüşü'*nde, yasağın "kullanılan silahların türünden bağımsız olarak her türlü kuvvet kullanımını kapsadığını" ifade etmiştir. [775] Bu yaklaşım, Divan'ın kuvvet kullanımını sadece silahlı eylemlerle sınırlandırmayan, daha geniş bir yorumu benimsediğini göstermektedir.[776]

Yeni teknolojik araçların hızla gelişmesi, neyin "silah" olarak nitelendirilebileceğinin belirlenmesini giderek zorlaştırmaktadır. Patlayıcı etkiler doğurmayan kimyasal, bakteriyel ve biyolojik silah türlerinin geliştirilmesi, klasik tanımlamalara meydan okumaktadır. Siber saldırılar ise kuvvet kullanımı kapsamında sınıflandırılması güç eylemler olarak öne çıkmakta ve dolayısıyla bunların silah olarak kullanımı, geleneksel hukuk çerçevesini sorgulatmaktadır.

Ian Brownlie, bu tür silahların kullanımı hususunda hukuka aykırı kuvvet kullanımı oluşturup oluşturmadığını değerlendirmek üzere şu çerçeveyi ortaya koymuştur:

"Bu tür silahların kullanımı iki gerekçeyle kuvvet kullanımı ile eş tutulabilir. Birincisi, ilgili araçların genellikle 'silahlar' ve 'savaş yöntemleri' olarak adlandırılmasıdır. Daha tutarlı olan ikinci görüşe göre ise, bu silahların yaşam ve mülkiyetin tahrip edilmesi amacıyla kullanılması ve çoğunlukla 'kitle imha silahları' olarak tanımlanmasıdır."[777]

Ian Brownlie tarafından yapılan bu tanımın her iki unsuru da siber saldırılara uygulanabilir. Birincisi, bu tür siber saldırılar genellikle "siber savaş" veya "bilgi savaşı" olarak adlandırılmaktadır. İkincisi ise, bu saldırıların yaşam ve mülkiyet hakkını yok etmek amacıyla gerçekleştirilebilmesidir.[778] Brownlie'nin tanımı, kuvvetin "silahlı" ya da "silahlandırılmış" olarak nitelendirilmesi kriterinin önemini yitirdiğine işaret etmektedir; zira günümüzde birçok kuvvet türü, geleneksel silah özelliklerini taşımamaktadır.

Yukarıda açıklananlar doğrultusunda, kuvvet kullanma veya tehdidinin yalnızca silahlı kuvvetle sınırlandırılması artık geçerli bir yaklaşım değildir. Bu çerçevede, gerekli koşulların varlığı halinde siber saldırılar, BM Şartı m. 2/4 kapsamında kuvvet kullanma yasağı ihlali teşkil edecektir.

Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited", *Journal of Conflict and Security Law* 56 (2011).

[775] Uluslararası Adalet Divanı, *Nükleer Silahların Kullanımının veya Kullanım Tehdidinin Hukuka Uygunluğu Hakkında Danışma Görüşü*, 8 Temmuz 1996, I.C.J. Reports 1996, s. 226- 244.

[776] Hans Kelsen, *The Law of the United Nations: A Critical Analysis of Its Fundamental Problems* (London: Stevens and Sons, 1950), 57.

[777] Ian Brownlie, *Principles of Public International Law*, 7. Baskı (Oxford: Oxford University Press, 2008), 362.

[778] Marco Roscini, "World Wide Warfare – Jus ad bellum and the Use of Cyber Force", *Max Planck Yearbook of United Nations Law Online* 14/1 (2010), 85–130.

2.4.3. Siber Saldırıları "Kuvvet Kullanımı" Olarak Nitelendiren Yaklaşımlar

Siber saldırıların kuvvet kullanımı olarak nitelendirildiği yerleşik bir devlet uygulaması henüz bulunmamaktadır. Atfedilebilirlik endişeleri nedeniyle devletlerin bu konudaki tutumları sürekli değişmekte ve büyük çeşitlilik göstermektedir. Bununla birlikte, literatürde siber saldırıları "kuvvet kullanımı" olarak değerlendiren çeşitli yaklaşımlar mevcuttur. Bu yaklaşımlar arasında üç temel model ön plana çıkmaktadır: hedef temelli (*target-based*), araç temelli (*instrument-based*) ve sonuç temelli (*consequence-based*) yaklaşımlar.[779] Literatürde hedef temelli ve araç temelli yaklaşımlara daha az yer verilirken, sonuç temelli yaklaşım en çok tercih edilen model olarak öne çıkmaktadır.

Hedef temelli yaklaşım, siber saldırıların etkileri veya operasyonun niteliği ne olursa olsun, bir devletin ulusal kritik altyapısına (UKA) yönelik gerçekleştiğinde kuvvet kullanımı sınırını aşmış sayılması gerektiğini savunur. [780] Ancak bu yaklaşım, yalnızca hafif rahatsızlık yaratan ya da bilgi toplama amaçlı siber faaliyetleri dahi kuvvet kullanımı kapsamında değerlendirebileceği için kapsam açısından aşırı geniştir. Ayrıca, bu yaklaşımın önemli bir eksikliği olarak, "ulusal kritik altyapı" kavramına ilişkin evrensel ve kabul görmüş bir tanımın bulunmaması gösterilmektedir.[781]

Araç temelli yaklaşım, bir eylemin gerçekleştirilmesinde kullanılan araçlara, yani silahlara odaklanmakta olup, geleneksel olarak silahlı kuvvet ile ekonomik ve siyasi baskı arasındaki ayrımı yapmada kullanılmaktadır. Ancak bu yaklaşım, fiziki özelliklere sahip araçlara odaklanması nedeniyle eleştirilmiştir; bu nedenle siber uzay bağlamında dijital kodlara genişletilmesi uygun görülmemekte ve fiziki zarara yol açan siber saldırıların dahi BM Şartı m. 2/4 kapsamında kuvvet kullanımı olarak değerlendirilemeyeceği sonucuna varacağı ileri sürülmektedir.[782]

Sonuç temelli yaklaşım, siber saldırıların sanal sonuçları, fiziksel yıkım veya can kaybı gibi etkilerine odaklanmaktadır. Bu yaklaşıma göre, fiziksel yıkım veya can kaybına yol açan siber saldırılar her zaman kuvvet kullanımı olarak nitelendirilirken, fiziksel olmayan sonuçlar bu yaklaşımın kapsamı dışında kalabilir. Sonuç temelli yaklaşım, diğer iki yaklaşıma kıyasla

[779] Roscini, "World Wide Warfare – Jus ad bellum and the Use of Cyber Force", 130.
[780] Walter G. Sharp Sr., *Cyberspace and the Use of Force* (Falls Church: Aegis Research Corporation, 1999), 129-132.
[781] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 54.
[782] Stephanie Gosnell Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare", *Stanford Journal of International Law* 48 (2012), 226-227; Matthew C. Waxman, "Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", *International Law Studies* 89 (2013), 111.

literatürde çoğu akademisyen tarafından benimsenmektedir. [783] Kanaatimizce de bu yaklaşım, siber saldırıların BM Şartı m. 2/4'te belirtilen gereklilikleri karşılayıp karşılamadığını analiz etmek için en uygun çerçeveyi sunmaktadır.

Marco Roscini ise, araç temelli ve sonuç temelli yaklaşımların birleştirilmesi gerektiğini savunmaktadır. Roscini'ye göre, sonuçlar önemli olmakla birlikte, kullanılan araç ve hedefin de göz ardı edilmemesi gerekmektedir. Daha açık bir ifadeyle, Roscini'nin görüşünde temel yaklaşım sonuç odaklı kalmakla birlikte, hedef odaklı ve araç odaklı yaklaşımlardan unsurlar eklenerek zenginleştirilmelidir.[784]

Siber saldırılara ilişkin bu yaklaşımlar, kuvvet kullanma yasağını düzenleyen mevcut uluslararası hukuk çerçevesine dayanmaktadır. Ancak burada, mevcut hukuki çerçeveyi uyarlamak yerine, siber saldırılara özgü özel bir hukuki yaklaşım geliştirilip geliştirilemeyeceği sorusu gündeme gelmektedir. [785] Çünkü ilk bakışta, BM Şartı çerçevesinin dışında siber saldırılara yönelik yeni bir hukuki düzenlemenin oluşturulması cazip bir öneri olarak görünmektedir.

Bununla birlikte, kanaatimizce mevcut uluslararası hukuk çerçevesinin kullanılmaya devam edilmesini destekleyen iki temel neden bulunmaktadır. Birincisi, BM Şartı'nın sunduğu hukuki çerçeve oldukça esnek olup, siber saldırıların farklı ve karmaşık yapısına uyum sağlayabilecek niteliktedir. İkincisi ise, bu tür yeni bir hukuki çerçevenin geliştirilmesi için gerekli uluslararası uzlaşının sağlanmasının oldukça zor ve zaman alıcı bir süreç olmasıdır. Bu nedenle, BM Şartı'nın mevcut hukuki çerçevesinin siber saldırıları değerlendirmek için uygun ve yeterli bir araç olduğunu söyleyebiliriz. Bu bağlamda, sonuç temelli yaklaşım, araç temelli ve hedef temelli yaklaşımlardan belirli unsurlarla desteklenerek en uygun yöntem olarak öne çıkmaktadır.[786]

2.4.4. Kuvvet Kullanımı Yasağını Oluşturan Unsurlar ve Siber Eylemler

Yoğunluk ve ağırlık eşiği, "silahlı saldırı" ve "saldırganlık" kavramları bakımından aranan temel kriterler arasında yer almaktadır. Uluslararası Adalet Divanı (UAD), silahlı

[783] Roscini, *Cyber Operations and the Use of Force in International Law*, 54.
[784] Roscini, *Cyber Operations and the Use of Force in International Law*, 50.
[785] Duncan B. Hollis, "Why States Need an International Law for Information Operations", *Lewis and Clark Law Review* 11/4 (2007), 8.
[786] Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfection of International Law* (Leiden: Brill and Martinus Nijhoff Publishers, 2015), 139.

saldırıları "kuvvet kullanımının en ağır biçimleri" olarak nitelendirmektedir.[787] BM Genel Kurulu'nun 3314 (XXIX) sayılı Kararı'nda ise saldırganlık, "hukuka aykırı kuvvet kullanımının en ciddi ve tehlikeli biçimleri" olarak tanımlanmıştır. Burada özellikle vurgulanması gereken husus, ne UAD ne de BM Şartı'nda kuvvet kullanma yasağının ihlaline yol açabilecek bir yoğunluk eşiğinin açıkça belirlenmemiş olmasıdır. Bununla birlikte, bu durum, uygulamada böyle bir eşik bulunmadığı anlamına gelmemektedir.

BM Şartı m.2/4'te düzenlenen kuvvet kullanma yasağı bağlamında bazı uluslararası hukukçular, bu yasağın kapsamına girmeyen bir "ağırlık eşiği" bulunduğu görüşünü ileri sürmektedir. Bu yaklaşıma göre, kuvvet kullanımı ancak belirli bir yoğunluk ve ağırlık seviyesini aştığında kuvvet kullanma yasağının ihlali niteliğini kazanacaktır.[788] Bu yaklaşım, Şart'ın kabulünden bu yana devletler tarafından da desteklenmiştir. Örneğin, düşük yoğunluktaki bazı fiziksel kuvvet kullanımları[789] devletler tarafından kuvvet kullanımı olarak nitelendirilmemiştir. Bu kapsamda Gürcüstan'daki çatışmalara ilişkin Uluslararası Gerçekleri Araştırma Komisyonu (*International Fact-Finding Commission on the Conflict in Georgia*)[790] da bu görüşü benimseyerek, "kuvvet kullanma yasağı, asgari bir yoğunluk eşiğini aşan tüm fiziksel kuvvet kullanımlarını kapsar" ifadesini kullanmıştır. Buna karşılık, bazı uluslararası hukuk uzmanları ise bu türden bir ağırlık eşiğinin varlığını kabul etmemekte ve en düşük kuvvet kullanımlarının bile BM Şartı m. 2/4 kapsamına girdiğini savunmaktadır.[791]

UAD, Şart madde 2/4 için açık bir ciddiyet eşiği belirlememiştir. Bununla birlikte, Divan önüne getirilen bazı davalardan, kuvvet kullanımında asgari bir ağırlık eşiğinin varlığına ilişkin çıkarımlar yapmak mümkündür. Nitekim Korfu Boğazı Davası'nda UAD, İngiliz savaş gemilerinin Arnavutluk karasularına müdahalesinin Arnavutluk'un egemenliğinin ihlali olduğuna hükmetmiş; ancak bu eylemi tehdit veya kuvvet kullanma yasağının ihlali olarak

[787] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, 101, 191.
[788] Mary Ellen O'Connell, "Cyber Security without Cyber War", *Journal of Conflict and Security Law* 17 (2012), 102-105.
[789] Düşük yoğunluklu kuvvet kullanımları; gerçek kişilerin hedef alınarak öldürülmesi, bir devletin başka bir devletteki vatandaşlarını kurtarmaya yönelik operasyonları, başka bir devletin topraklarında gerçekleştirilen sınırlı çaplı terörle mücadele operasyonları, kolluk kuvvetleri tarafından icra edilen operasyonlar, "sıcak takip" girişimleri ve sınır çatışmaları gibi durumları kapsamaktadır.
[790] Independent International Fact-Finding Mission on the Conflict in Georgia (IIFFMCG), *Report of the International Fact-Finding Commission on the Conflict in Georgia*, Vol. 2 (2009), 242, https://www.ceiig.ch/Report.html.
[791] André de Hoogh, "Georgia's Short-Lived Military Excursion into South Ossetia: The Use of Armed Force and Self-Defence", *EJIL: Talk!*, 9 Aralık 2009, https://www.ejiltalk.org/georgia's-short-lived-military-excursion-into-south-ossetia-the-use-of-armed-force-and-self-defence/.

nitelendirmemiştir. [792] UAD'nin bu yaklaşımı, bazı akademisyenler tarafından ciddiyet eşiğinin varlığına işaret eden bir argüman olarak değerlendirilmektedir.[793]

Mary Ellen O'Connel, kuvvet kullanımı yasağının ihlalinde asgari bir ağırlık eşiğinin bulunması gerektiğini savunmakta ve bu görüşünü siber saldırılar bağlamında şöyle ifade etmektedir:

"Siber uzay, bazı yazarların suç oluşturan fiilleri, 51. madde uyarınca kuvvet kullanma hakkını tetiklemek amacıyla silahlı saldırıyla eşitlemeye çalıştıkları başka bir alandır. İnternet, iletişim ve ticaretin yanı sıra önemli ölçüde suç faaliyetlerinin gerçekleştiği bir alan olmakla birlikte, siber güvenliğin artırılması askeriye yerine kolluk kuvvetlerinin görevidir." [794]

Bir siber saldırının kuvvet kullanma yasağını ihlal edebilmesi için, bu saldırının ya doğrudan bir devlet tarafından ya da devletin desteklediği devlet dışı aktörler aracılığıyla gerçekleştirilmiş olması gerekmektedir. Daha açık bir ifadeyle, yalnızca devlet destekli devlet dışı aktörler tarafından yapılan siber saldırılar, BM Şartı m. 2/4 kapsamında kuvvet kullanma yasağının ihlali olarak değerlendirilecektir. Diğer tüm siber saldırılar ise, ceza hukuku çerçevesinde ele alınmalıdır. Bununla birlikte, devletler tarafından veya onların etkin kontrolü altında gerçekleştirilen siber saldırılar arasında yalnızca BM Şartı m. 2/4'te belirtilen ağırlık eşiğini aşanlar kuvvet kullanımı olarak kabul edilebilir.

Siber saldırılar, ölçek açısından oldukça çeşitli ve heterojen bir kategori teşkil etmekte olup, veri yok edilmesi, maddi zarar ve can kaybı gibi farklı sonuçlar doğurabilmektedir. Bazı yazarlar, ağırlık (*gravity*) eşiğini ciddiyet (*severity*) unsuru ile tanımlamakta; yani bir devletin başka bir devlete karşı gerçekleştirdiği siber saldırının kuvvet kullanımı olarak değerlendirilebilmesi için ulaşması gereken eşik seviyesi olarak ciddiyet eşiğini benimsemektedirler. Ciddiyet eşiğine başvurulması, farklı siber saldırı türlerinin ayrımını yapmayı ve kuvvet kullanma yasağını ihlal eden eylemleri belirlemeyi mümkün kılmaktadır.[795] Bununla birlikte, şimdiye kadar ortaya koyduklarımız ışığında, siber saldırıların kuvvet kullanımı olarak nitelendirilmesine ilişkin net bir eşik belirlemenin oldukça zor olduğu söylenebilir. Böyle bir eşik, her somut olayın özel koşulları çerçevesinde, duruma özgü çeşitli kriterler ve deliller dikkate alınarak tespit edilmelidir.[796]

---

[792] International Court of Justice (ICJ), *Corfu Channel Case (United Kingdom v. Albania), Merits*, Judgment of 9 April 1949, ICJ Reports 1949, 4-35.
[793] Olivier Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law*, trans. Christopher Sutcliffe (Oxford: Hart Publishing, 2010), 69-70.
[794] Mary Ellen O'Connell, "Cyber Security without Cyber War", *Journal of Conflict and Security Law* 17 (2012), 187.
[795] Delerue, *Cyber Operastions and International Law,* 294.
[796] Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", *Yale Journal of International Law* 36 (2011), 421-443.

2.4.5. Fiziksel Etki Doğuran Siber Saldırılar ile Siber Etkiler Doğuran Saldırılar

Gerçek dünyada fiziksel etkiler doğuran siber saldırılar ile yalnızca fiziksel olmayan etkiler (örneğin veri yok edilmesi, bilgisayar programlarının kesintiye uğratılması veya dağıtılmış hizmet engelleme saldırısı - DDoS gibi) doğuran siber saldırılar arasında ayrım yapılması gerekmektedir. Literatürde, fiziksel zarar veya yaralanmaya yol açan siber saldırılar genellikle kuvvet kullanımı kapsamında değerlendirilirken, gerçek dünyada herhangi bir somut fiziksel etki doğurmayan siber saldırıların kuvvet kullanımı olarak nitelendirilmesi hâlâ önemli ölçüde tartışmalıdır.[797] Buna karşılık, gerçek dünyada somut bir fiziksel etki yaratmayan siber saldırıların kuvvet kullanımı kapsamında değerlendirilmesi ise ciddi bir tartışma konusudur.[798]

Literatürdeki yaygın görüşe göre, ister fiziksel zarar, ister yaralanma, ister can kaybı doğursun, herhangi bir fiziksel etki doğuran siber saldırı kuvvet kullanımı olarak kabul edilmeye yeterlidir. Düşük yoğunlukta zarar oluşturan, örneğin yalnızca bir bilgisayara zarar verip başka etkiler doğurmayan siber saldırılar da kuvvet kullanımı kapsamında değerlendirilebilir; ancak saldırıya maruz kalan devlet, bu durumu kuvvet kullanımı olarak nitelendirmemeyi tercih edebilir. Bu bağlamda, örneğin bir devletin başka bir devlete karşı hükümet üyelerinin akıllı telefonlarına fiziksel zarar vermeyi amaçlayan bir siber saldırı gerçekleştirmesi durumunda, bu eylem kuvvet kullanımı olarak nitelendirilebilir; ancak düşük yoğunluklu etkileri nedeniyle böyle bir devletin saldırıyı bu şekilde tanımlaması muhtemel görünmemektedir. Bu bağlama *Stuxnet* saldırısı örnek olarak verilebilir. Stuxnet virüsü, İran'ın nükleer programına ait santrifüjlere fiziksel zarar vermiş ve bu nedenle söz konusu siber saldırı kuvvet kullanımı olarak değerlendirilmiştir.[799] Literatürde çoğunluk görüşü, bu saldırıyı kuvvet kullanımı olarak kabul etse de, ne İran ne de başka herhangi bir devlet tarafından resmi olarak bu şekilde nitelendirilmemiştir. Stuxnet virüsünün yalnızca birkaç santrifüjü tahrip edip tüm nükleer tesisi yok etmemesi, bu operasyonun devletler tarafından kuvvet kullanımı olarak tanımlanmamasının sebeplerinden biri olabilir. Diğer bir olası neden ise, İran'ın durumu tırmandırmamak amacıyla saldırıyı kuvvet kullanımı olarak nitelendirmemeyi tercih etmiş olmasıdır. Kanaatimizce, Stuxnet'in objektif olarak kuvvet kullanımı yasağının ihlalini teşkil edip etmediği ile bir devletin bunu resmî olarak kuvvet kullanımı olarak nitelendirme kararı

[797] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited", *Villanova Law Review* 56/3 (2011), 569-606.
[798] Christopher C. Joyner ve Catherine Lotrionte, "Information Warfare as International Coercion: Elements of a Legal Framework", *European Journal of International Law* 12 (2001), 825-850.
[799] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), 37-75.

arasında ayrım yapmak önem taşımaktadır. Zira ilki esasen uluslararası hukuk kapsamında değerlendirilen bir konuyken, ikincisi daha çok siyasi ve stratejik bir meseledir.[800]

Gerçek dünyada somut fiziksel etkiler doğurmayan siber saldırıların kuvvet kullanımı olarak değerlendirilmesine ilişkin literatürde yeknesak bir görüş bulunmamaktadır. Bazı yazarlar bu tür saldırıların kuvvet kullanımı kapsamında değerlendirilmesine açıkça karşı çıkarken, diğerleri belirli koşulların varlığı halinde böyle bir değerlendirmeyi desteklemektedir.[801] Bu durumda iki temel soru ortaya çıkmaktadır: Birincisi, fiziksel etkilerin varlığı tek başına bir eşik oluşturur mu? İkincisi ise, fiziksel etkiler her zaman fiziksel olmayan etkilerden daha ağır kabul edilir mi? Fiziksel etki doğuran siber saldırıların daha görünür ve somut olduğu, dolayısıyla kuvvet kullanımı olarak nitelendirilmeye daha uygun olduğu doğrudur. Ancak, yalnızca fiziksel olmayan etkiler yaratan siber saldırılar da geniş çaplı sonuçlar doğurma kapasitesine sahiptir. Bu kapsamda, hedef devletin varlığına karşı doğrudan veya dolaylı sonuçlar doğuran siber saldırıların kuvvet kullanımı olarak nitelendirilmemesi mantıksız görünmektedir.[802]

2.4.6. Kuvvet Kullanımı Niteliğindeki Siber Saldırıların Atfedilmesi Sorunu

Siber saldırıların çoğu yeni devlet dışı aktörler tarafından gerçekleştirilmektedir. Bu durum, bu tür fiillerin devletler tarafından üstlenilmesi meselesini gündeme getirmektedir. Bir devletin uluslararası hukuk bağlamında sorumluluğunun doğabilmesi için, ilgili fiilin o devlete atfedilmesi gerekmektedir. Atfedilebilirlik açısından dikkat edilmesi gereken en önemli hususlardan biri, devletin soyut bir varlık olmasıdır. Bu bağlamda, bir devlet ancak bir veya birden fazla gerçek kişi aracılığıyla hareket edebilir ve bu kişilerin fiilleri devlete atfedilebilir. Daha açık bir ifadeyle, Dionisio Anzilotti'nin de vurguladığı üzere, atfetmek amacıyla "bir devletin faaliyeti, hukukun devlete yüklediği gerçek kişilerin faaliyetinden başka bir şey değildir."[803]

BM Şartı m. 2/4'te yer alan kuvvet kullanma yasağı yalnızca devletler bakımından geçerlidir. Ancak, bir devlet bu yasağı, devlet dışı aktörleri yönlendirerek veya onlara destek

[800] Delerue, *Cyber Operastions and International Law,* 297.
[801] Delerue, *Cyber Operastions and International Law,* 297.
[802] Delerue, *Cyber Operastions and International Law,* 298.
[803] Dionisio Anzilotti, *Cours de droit international* (Recueil Sirey 1929), 469 ("Nous savons que l'activité de l'Etat n'est autre que l'activité d'individus que le droit international impute à l'Etat"); İngilizce çeviri için bkz. Djamchid Momtaz, "Attribution of Conduct to the State: State Organs and Entities Empowered to Exercise Elements of Governmental Authority", in James Crawford, Alain Pellet ve Simon Olleson (eds), *The Law of International Responsibility* (Oxford: Oxford University Press, 2010), 237.

vererek ihlal etmiş olabilir. Bu bağlamda, devletler tarafından gerçekleştirildiği iddia edilen siber saldırıların büyük bir kısmı, aslında kısmen veya tamamen devlet dışı aktörler tarafından gerçekleştirilmekte bulunmaktadır.[804] Bu bağlamda devletler tarafından gerçekleştirildiği iddia edilen siber saldırıların çoğu aslında kısmen ya da tamamen devlet dışı aktörler tarafından gerçekleştirilmektedir.[805] Örneğin, 2007'de Estonya'ya karşı gerçekleştirilen siber saldırıların ardından Estonya bu saldırıların Rusya tarafından gerçekleştirildiği iddia etmiş, ancak bu iddiayı destekleyecek kanıtları olmadığını kabul etmiştir.[806] Buna karşın, Rus gençlik grubu "Nashi" üyeleri söz konusu siber saldırılarda yer aldıklarını kabul etmiş; ayrıca Rusya parlamentosunun bir üyesi de yardımcısının Estonya'ya yönelik siber saldırılar gerçekleştirdiğini doğrulamıştır.[807] Anonymous ve Rus İş Ağı (*Russian Business Network*-RBN) gibi farklı bilgisayar korsanlarının devletler adına siber saldırılar gerçekleştirdiği bilinmektedir.[808] Bu kapsamda örneğin RBN, Rusya-Gürcistan Savaşı sırasında Gürcistan'a karşı siber saldırılar gerçekleştirmiştir.[809] Yeni devlet dışı aktörler tarafından gerçekleştirilen bu tür siber saldırılar, saldırıların devletlere atfedilmesini ve uluslararası hukukun uygulanmasını zorlaştırmaktadır. Ancak, yeni devlet dışı aktörler tarafından gerçekleştirilen bu siber saldırılar, ulusal hukuk tarafından devleti temsil etmeye yetkilendirilen devlet organları veya belirli devlet yetkilerini kullanma hakkına sahip kurumlara atfedilebiliyorsa, bu durumda devletin uluslararası hukuk bakımından sorumluluğu doğacaktır.

2.5. Özen Yükümlülüğü ve Siber Eylemler

Özen yükümlülüğü ilkesi, bir devletin topraklarının diğer devletlerin haklarını ihlal eden fiiller için bilerek kullanılmasına izin vermeme yükümlülüğünü ifade etmektedir.[810] İlke, UAD tarafından verilen Korfu Kanalı Davası kararında şu şekilde tanımlanmıştır: "Her devlet,

[804] Michael C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", *Yale Journal of International Law* 36 (2011), 446.
[805] Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), 140.
[806] "Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks", *RIA Novosti*, 9 June 2007, https://en.ria.ru/world/20070906/76959190.html.
[807] Charles Clover, "Kremlin-Backed Group behind Estonia Cyber Blitz", *Financial Times*, 11 March 2009, https://www.ft.com/content/57536d5a-0ddc-11de-8ea3-0000779fd2ac.
[808] John Leyden, 'Russian Politician: "My Assistant Started Estonian Cyberwar" – Dubious DDoS Lols', *The Register*, 10 March 2009, https://www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/; 'Behind The Estonia Cyberattacks', *Radio Free Europe/Radio Liberty*, 6 March 2009, https://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.
[809] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014) 90–93.
[810] Joanna Kulesza, *Due Diligence in International Law* (Leiden: Brill & Martinus Nijhoff Publishers, 2016).

ülkesinin diğer devletlerin haklarına aykırı biçimde kullanılmasına bilerek izin vermeme yükümlülüğü altındadır." [811]

Özen yükümlülüğü ilkesi, devletlerin egemen eşitliği ilkesinde doğmaktadır.[812] Bunu Max Huber'in Palmas Adası Tahkim davasında ifade ettiği cümlelerden açık bir şekilde görmek mümkündür: "*Egemenlik bir devletin kendi ülkesinde münhasıran faaliyet yürütme hakkı anlamına gelir. Ancak bu hakla birlikte bir yükümlülük de doğar: Devlet, ülkesinde diğer devletlerin haklarını, özellikle barış ve savaş zamanında bütünlük ve dokunulmazlık haklarını korumakla ve ayrıca vatandaşları için diğer devletlerde talep edebileceği hakları güven altına almakla yükümlüdür."* [813]

Özen yükümlülüğü ilkesi bir sonuç yükümlülüğü olmayıp, bir davranış yükümlülüğüdür. Daha açık bir ifadeyle, bir devletin sorumluluğu, öngördüğü sonucu gerçekleştirememesinden değil, gerekli önlemleri almakla yükümlü olmasına rağmen bu önlemleri açıkça ihmal etmesinden kaynaklanır. Bu bağlamda, haksız fiilin kime atfedildiği önem taşımamaktadır; fiil devlet tarafından ya da devlet dışı bir aktör tarafından gerçekleştirilmiş olabilir. Özen yükümlülüğü açısından esas olan, ilgili devletin topraklarının diğer bir devletin haklarına aykırı fiiller için kullanılmasına izin vermesidir.[814]

Uluslararası hukuktaki özen yükümlülüğü (*due diligence*), devletlerin ve uluslararası örgütler gibi diğer uluslararası hukuk kişiliklerinin davranışlarını değerlendiren bir standarttır. Bu kavram genellikle davranış yükümlülüğüne dayalı olarak yorumlanmakta olup, çoğunlukla pozitif önleme, koruma veya telafi etme yükümlülüğünü içermektedir. Ancak, dilsel belirsizlikler nedeniyle bazen doğrudan bir davranış yükümlülüğü olarak da ele alınmakta ve bu bağlamda özen standardı (*standard of care*) veya özen yükümlülüğü (*duty of care*) olarak adlandırılmaktadır.

Buna karşılık, özen yükümlülüğü zarar vermeme yükümlülüğü (*no harm rule*) veya zarar vermeme ödevi (*duty not to harm*) kapsamında da değerlendirilebilir; bu anlamda diğer devletlerin, uluslararası örgütlerin veya ulusal ve yabancı bireylerin çıkarlarını ya da haklarını, makul önlemler alarak üçüncü tarafların (vatandaşlar, yabancılar, diğer devletler, uluslararası

---

[811] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, Judgment on the Merits, [1949] ICJ Reports 4, 22.

[812] Karine Bannelier ve Théodore Christakis, *Cyber-Attacks–Prevention-Reactions: The Role of States and Private Actors [Cyberattaques–Prévention-Réactions: Rôles Des Etats et Des Acteurs Privés]* (Les Cahiers de la Revue Défense Nationale, 2017), 16–17, https://ssrn.com/abstract=2941988.

[813] *The Island of Palmas (or Miangas)*, (1928) 11 RIAA 831, 839; ayrıca bkz. *Affaire des biens britanniques au Maroc espagnol (Espagne contre Royaume-Uni)*, (1925) 2 RIAA 615, 649.

[814] Karine Bannelier-Christakis, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?", *Baltic Yearbook of International Law* 14 (2015), 23-25.

örgütler veya doğal afetler gibi) neden olabileceği önemli zararlara karşı koruma gerekliliğini ifade etmektedir.

Bu yükümlülüğün kapsamına, ilgili zararın riskinin öngörülmüş veya makul olarak öngörülebilir olması ve müdahale kapasitesinin bulunması şartları da dahildir. Özen yükümlülüğünün ihlali ise hukuken uygunsuz veya haksız ihmal (*undue or wrongful negligence*) olarak değerlendirilir.[815]

Özen yükümlülüğü, geleneksel çevre sorunlarından siber uzay gibi birçok yeni alanı da kapsamaktadır.[816] Genellikle, özen yükümlülüğü sorumlu devletin belirli yükümlülüklere ve standartlara uyup uymadığı temelinde değerlendirilir.[817] Ancak, bu ilkeye ilişkin "belirli yükümlülükler ve standartlar" uluslararası alanda henüz net bir şekilde tanımlanmamış olup, esnek bir yapıya sahiptir. Bu durum, özen yükümlülüğü ilkesinin her somut olayın koşullarına bağlı olarak değişiklik gösterebileceği anlamına gelmektedir.

Özen yükümlülüğü ilkesine ilişkin yükümlülükler "birleşik bir içeriğe" sahip olmayabilir; bu nedenle, ilkeye ait yükümlülüklerin temel özelliklerini belirlemek güçleşmektedir. Ancak, siber uzay bağlamında, devletlerin siber altyapılarının devlet dışı aktörler tarafından kötü niyetli sınır ötesi faaliyetler için kullanılmasını önlemek amacıyla kapasitelerini kullanmaları durumunda, özen yükümlülüğünün maddi içeriği özellikle yapılageliş hukuku (*lex ferenda*) esas alınarak tanımlanabilir.[818]

2.5.1. Siber Uzaydaki Devlet Dışı Aktörler ve Özen Yükümlülüğü

Birleşmiş Milletler Hükümetlerarası Uzmanlar Grubu tarafından hazırlanan Tallinn El Kitabı 2.0'de yer alan 16. Kural, özen yükümlülüğünü düzenlemektedir. Söz konusu kural, metinde şu şekilde ele alınmıştır:

"Devlet, ülkesinin veya kontrolü altındaki alanların ya da siber altyapının, diğer devletlerin haklarını etkileyen ve bu devletler için ağır sonuçlar doğuran siber saldırılar için kullanılmasına izin vermemek üzere gerekli özeni gösterme yükümlülüğü altındadır." [819]

---

[815] Samantha Besson, *Due Diligence in International Law*, çev. Sevrine Knuchel (The Hague: Academie De Droit International De La Haye / The Hague Academy of International Law, 2023), 58-59.

[816] Akiko Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", *Laws* 7/4 (2018), 2.

[817] Timo Koivurova, "Due Diligence", *Max Planck Encyclopedia of Public International Law (MPEPIL)* (Şubat 2010). Erişim: http://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL (erişim 16 Aralık 2024).

[818] Russell Buchan, "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm", *Journal of Conflict and Security Law* 21 (2016), 429–53.

[819] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2. baskı, (Cambridge: Cambridge University Press, 2017), 30.

Bu düzenlemeden anlaşılacağı üzere, özen yükümlülüğü devletlerin uyması beklenen davranış standardını ifade etmektedir. Kural 16, en az üç tarafın dahil olduğu bir durumu esas almaktadır: (1) siber saldırının hedef aldığı devlet; (2) kuralın bağlayıcı olduğu ülke devleti; ve (3) siber saldırının faili olan üçüncü taraf. Kural 16, üçüncü taraflarca gerçekleştirilen tüm siber saldırılar için geçerlidir; bu tarafın bir birey, şirket, devlet dışı bir grup veya bir devlet olup olmadığına bakılmaksızın uygulanmaktadır.

Özen yükümlülüğü ilkesi, devletlerin egemenlik sınırları içinde bulunan tüm alanlarda geçerlidir. Daha açık bir ifadeyle, bu yükümlülük devletin egemenlik sınırları içindeki tüm alanlarda gerçekleştirilen siber saldırıları gerçekleştiren gerçek kişileri ve saldırılar için kullanılan siber altyapıyı kapsamaktadır. Ancak, siber saldırıyı başlatan tarafın üçüncü bir devlette yerleşik olup uzaktan faaliyet gösteriyor olabileceği unutulmamalıdır. Bu bağlamda, örneğin A devletinde bulunan bir bilgisayar korsanı grubu, B devletine yönelik yıkıcı bir siber saldırıyı C devletinde bulunan siber altyapıyı kullanarak gerçekleştirdiğinde; eğer C devleti bu kullanımı fark eder ve saldırıyı önlemek için gerekli tedbirleri almazsa, özen yükümlülüğünü ihlal etmiş sayılır.

Hükümetlerarası Uzmanlar Grubu, Tallinn El Kitabı 2.0'nin 16. Kuralı kapsamında, özen yükümlülüğünün sınır ötesinde de iki durumda geçerli olduğunu kabul etmiştir. Birinci durumda, bir devlet egemenlik hakkı olmaksızın yabancı bir toprak üzerinde fiili kontrol sahibi olabilir; örneğin, ilhak veya askeri işgal gibi durumlarda olduğu gibi. Bu durumda, söz konusu devletin, kontrolü altındaki topraklardaki siber altyapı ve faaliyetlere karşı gerekli özeni göstermesi gerekmektedir.

İkinci olarak, bir devlet ülkesi dışında bulunan ve kendi kontrolü altındaki devlet siber altyapıları üzerinde de gerekli özen yükümlülüğünü yerine getirmelidir. Burada "devlet kontrolü" (*governmental control*) terimi, ilgili altyapının kullanımının özel bir kuruluş tarafından değil, doğrudan devlet tarafından kontrol edildiğini ifade etmektedir. Devlete ait siber altyapıya ilişkin özen yükümlülüğünün doğduğu durumlara örnek olarak, diğer bir ülkedeki askeri tesiste bulunan ulusal görev ağı, açık denizlerde veya uluslararası hava sahasında bulunan egemen platformlardaki siber altyapısı ve diplomatik temsilciliklerdeki siber altyapısı gösterilebilir.[820]

Hükümetlerarası Uzmanlar Grubu, Tallinn El Kitabı 2.0'nin 16. Kuralı kapsamında "kontrol" (*control*) kavramının her zaman "yetki" (*jurisdiction*) kavramıyla eş anlamlı olmadığını vurgulamaktadır. Buna göre, bir devletin başka bir devlette faaliyet gösteren

[820] Schmitt, *Tallinn Manual 2.0*, 33.

şirketler üzerinde düzenleyici yetkiye (*prescriptive jurisdiction*) sahip olması, bu şirketlerin işlettiği siber altyapıyı fiilen kontrol edebildiği anlamına gelmemektedir.

Özen yükümlülüğünün sınır ötesi (*extraterritorial*) bağlamda devreye girmesi için temel koşul, devletin ilgili siber altyapıyı fiilen kontrol etmesidir. Bu kontrol, altyapının doğrudan devlet tarafından işletilmesi veya altyapının yer aldığı toprak, bina ya da nesne üzerinde devletin fiili hakimiyetinin bulunması ile sağlanır. Özen yükümlülüğünün sınır ötesi kapsamda ortaya çıkması, devletin münhasır kontrol uyguladığı siber altyapı veya faaliyetlere bağlıdır. Bununla birlikte, birden fazla devletin eşzamanlı (*concurrent*) kontrol uyguladığı durumlarda, her bir devlet ayrı ayrı gerekli özeni göstermekle yükümlüdür.

Grubun tartıştığı önemli bir husus da, bir devletin rolünün yalnızca veri aktarımına aracılık eden "transit devlet" olması durumunda özen yükümlülüğünün uygulanıp uygulanmayacağıdır. Örneğin, bir devletin sınırları içinde bulunan fiber optik kablolar üzerinden geçen veri trafiğinin kötü niyetli amaçlarla kullanılması söz konusu olabilir. Uzmanlar, transit devletin, ülkesinde botnet ağı gibi kötü niyetli bir siber altyapının barındırıldığı durumdan ayırt edilmesi gerektiğini belirtmiştir.

Bu kapsamda, Grup transit devletlerin özen yükümlülüğünü yerine getirmesi için iki temel koşulda hareket etmesi gerektiği konusunda mutabakata varmıştır: (1) Devletin, belirli bir zarar eşiğini aşan saldırgan faaliyet hakkında ya fiili (*actual*) ya da varsayılan (*constructive*) bilgiye sahip olması; (2) Bu faaliyeti etkili biçimde durdurmak için uygulanabilir ve etkili önlemleri alma kapasitesine sahip olması.

Bu çerçevede, özen yükümlülüğünün sınır ötesi uygulanabilirliği, hem fiili kontrol hem de bilgi ve müdahale kapasitesi ölçütleriyle sınırlandırılmaktadır.[821]

Bununla birlikte, Hükümetlerarası Uzmanlar Grubu, siber uzaydaki gelişmiş iletişim teknolojilerinin doğası gereği, "transit devletin" kötü niyetli trafiği tespit etmesinin ve bu trafiğin kendi siber altyapısından geçtiğinin farkında olmasının büyük ölçüde güç olduğunu kabul etmiştir. Zararlı yazılımın imzası bilinmeyebilir, bu nedenle antivirüs programları tarafından tespit edilmesi mümkün olmayabilir veya zararlı yazılımlar gelişmiş şifreleme teknikleri kullanabilir. Ayrıca, internet trafiğinin önemli bir bölümü genellikle internet servis sağlayıcılarının (ISP) özel siber altyapıları üzerinden aktığından, zararlı yazılım tespit edilse dahi ISP'nin bu durumu devlet yetkililerine bildirme yükümlülüğü iç hukuk normlarına bağlıdır.

[821] Schmitt, *Tallinn Manual 2.0*, 33.

Buna rağmen, Uzmanlar Grubu, daha önce değinilen özen yükümlülüğü ilkesinin transit devletlerin taşıdığı hukuki sorumluluğu doğru şekilde yansıttığı hususunda görüş birliğine varmıştır. Bu çerçevede, esas sorun ilkenin uygulanabilirliği değil, transit devletin zararlı faaliyetlerden haberdar olup olmadığıdır.[822]

Siber saldırıya uğrayan devletin maruz kalması gereken maddi zarar hususunda, Hükümetlerarası Uzmanlar Grubu, Tallinn El Kitabı 2.0'nin 16. Kuralı kapsamında değerlendirilen siber saldırıların, etkilenen devletin uluslararası hukuk çerçevesinde sahip olduğu haklara "aykırı" ve "ciddi olumsuz sonuçlar" doğuran tüm siber faaliyetleri kapsadığı konusunda mutabakata varmıştır. Dolayısıyla, bu iki şartın birlikte gerçekleşmesi gerekmektedir.

Burada geçen "haklara aykırı" ifadesi yalnızca iç hukuk ihlallerini değil; aynı zamanda siber saldırıya maruz kalan devlete karşı uluslararası hukuk kapsamında doğan yükümlülüklerin ihlalini de kapsamaktadır. Bu bağlamda bir örnek vermek gerekirse; A devletinin kontrolündeki ve komuta-kontrol altyapısı aracılığıyla B devletine bilgi gönderen kötü amaçlı bir yazılımı devreye soktuğu bir durumu ele alalım. B devleti bu operasyonun farkındadır. Söz konusu kötü amaçlı yazılım, C devletindeki bir gaz boru hattı kontrol sisteminin işleyişini manipüle ederek patlamaya yol açmaktadır.

A devletinin B devletine karşı işlediği bu fiil, BM Şartı m. 2/4 kapsamında kuvvet kullanma yasağının ihlali niteliğinde olduğundan, B devleti, saldırıya müdahale edebilecek durumda ise, saldırıyı sona erdirmek için gerekli önlemleri almakla yükümlüdür.[823]

Hükümetlerarası Uzmanlar Grubu, bir devlet tarafından gerçekleştirilen siber saldırının hedef devletin uluslararası hukuktan kaynaklanan tüm haklarına aykırı olmaması halinde, saldırının gerçekleştiği devletin bu saldırıyı sona erdirmekle yükümlü tutulmasının tutarsız olacağı konusunda görüş birliğine varmıştır. Bu nedenle, Grup, özen yükümlülüğünün yalnızca söz konusu siber saldırının uluslararası hukuka aykırı bir devlet fiili teşkil ettiği durumlarda geçerli olduğunu kabul etmiştir.

Bu bağlamda bir örnek vermek gerekirse; A devleti, C devletinin siber altyapısını kullanarak B devletinin devlet veritabanlarını siber casusluk amacıyla izliyorsa, casusluğun uluslararası hukukta doğrudan haksız fiil teşkil etmemesi nedeniyle, C devletinin A devletinin saldırılarını sona erdirmek için herhangi bir özen yükümlülüğü bulunmamaktadır.[824]

[822] Schmitt, *Tallinn Manual 2.0*, 34.
[823] Schmitt, *Tallinn Manual 2.0*, 34.
[824] Schmitt, *Tallinn Manual 2.0*, 35.

Hükümetlerarası Uzmanlar Grubu, klasik görüşü benimseyerek, uluslararası hukuku ihlal edebilecek tarafın yalnızca devletler olduğunu savunmuştur. Bu bağlamda, Uzmanlar Grubu arasında özellikle, siber saldırıların yalnızca devletler tarafından gerçekleştirildiği veya devletlere isnat edilebildiği durumlarda, söz konusu saldırıların bir devletin egemenlik hakkını ihlal ettiği veya kuvvet kullanma yasağını ihlal ettiği konusunda mutabakat sağlanmıştır.[825]

Bununla birlikte, Hükümetlerarası Uzmanlar Grubu, özen yükümlülüğü ilkesinin kapsamının, uluslararası hukuka doğrudan aykırı olmamakla birlikte ciddi olumsuz sonuçlar doğuran ve hedef devletin uluslararası hukuktan kaynaklanan haklarını etkileyen devlet dışı aktörler tarafından gerçekleştirilen siber saldırıları da içerdiği konusunda görüş birliğine varmıştır.[826] Hükümetlerarası Uzmanlar Grubu, uluslararası hukukun çeşitli alanlarında, devlet dışı aktörlerin devletlere yönelik artan tehditlerinin dikkate alınmasıyla, özen yükümlülüğü ilkesinin açık ve net biçimde şekillendiğine işaret etmiştir. Bu durum, özellikle özel şirketlerin faaliyetleri sonucunda sınır ötesi çevresel zararların ortaya çıkması bağlamında uluslararası çevre hukukunda somutlaşmıştır. Grup, ciddi ve sınır ötesi olumsuz sonuçlar doğuran devlet dışı aktörlerin siber saldırılarının, devletin özen yükümlülüğü kapsamından çıkarılması için ikna edici bir gerekçe teşkil etmediğini vurgulamıştır. Özellikle, siber saldırıların diğer devletlere zarar verme potansiyeli bakımından taşıdığı yüksek risk unsuruna özel bir önem atfetmiştir.[827]

Özel şirketlerin fiilleri bağlamında devletin özen yükümlülüğünün ihlalini somutlaştırmak amacıyla kurgusal bir örnek vermek gerekirse; büyük bir teknoloji şirketi olan "T", Z devletinin kritik iletişim altyapısına yönelik siber saldırılar gerçekleştirmiş ve bu saldırılar neticesinde Z devletinde geniş çaplı internet kesintileri meydana gelmiştir. Bu kesintiler, Z devletinde kamu hizmetlerinin aksamasına, ekonomik faaliyetlerin durmasına ve halkın bilgiye erişim hakkının ihlaline yol açmıştır. "T" şirketinin merkezi A devletinde bulunmakta olup, A devleti makamları siber saldırıların farkında olmalarına rağmen gerekli önlemleri almamıştır. Bu durum, A devletinin özen yükümlülüğünü ihlal ettiğini göstermektedir.

Söz konusu kurgusal olay, devlet dışı aktörler tarafından gerçekleştirilen siber saldırıların ciddi ve sınır ötesi olumsuz sonuçlar doğurabileceğini ve dolayısıyla özen yükümlülüğü ilkesinin bu tür durumları da kapsaması gerektiğini açık biçimde ortaya koymaktadır.

---

[825] Schmitt, *Tallinn Manual 2.0*, 34.
[826] Schmitt, *Tallinn Manual 2.0*, 35.
[827] Schmitt, *Tallinn Manual 2.0*, 35-36.

Özel şirketlerin fiilleri nedeniyle devletin özen yükümlülüğünün ihlalini farklı bir kurgusal vaka üzerinden değerlendirecek olursak; büyük teknoloji şirketi "BigWorld", B devletinde yaklaşan devlet başkanlığı seçimlerine müdahale amacıyla sosyal medya platformları ve yapay zeka destekli algoritmalar aracılığıyla dezenformasyon kampanyaları yürütmüş, seçmenlerin bilgiye erişimini manipüle etmiş ve kamuoyunu yanıltıcı bilgilerle etkilemiştir. Bu müdahale neticesinde, B devletindeki demokratik seçim süreci zedelenmiş ve vatandaşların özgür, adil ve şeffaf seçim hakları ihlal edilmiştir.

BigWorld şirketinin merkezi E devletinde bulunmakta olup, E devleti makamları söz konusu siber faaliyetlerin farkında olmalarına rağmen, uluslararası hukuktan doğan özen yükümlülüğüne aykırı şekilde gerekli önlemleri almamış ve şirketin faaliyetlerini engellemek için makul tedbirleri uygulamamıştır. Bu durum, uluslararası hukukun temel ilkelerinden olan egemenlik ve müdahale yasağının ihlalini teşkil etmektedir. Dolayısıyla, E devleti uluslararası hukuktan kaynaklanan yükümlülüklerini ihlal ederek, şirketin faaliyetlerini engellemek için gerekli önlemleri almamış; bu durum ise uluslararası sorumluluk doğuran ciddi bir ihmal olarak kabul edilmelidir.

Sonuç olarak, devletlerin uluslararası hukuk kapsamında, kendi egemenlik alanları içerisinde diğer devletlere yönelik gerçekleşen siber müdahaleleri engellemek için makul ve orantılı önlemler alma yükümlülüğü bulunduğu açıktır. Bu nedenle, özen yükümlülüğü ilkesinin yalnızca hukuka aykırı devlet fiillerini değil, aynı zamanda devlet dışı aktörlerin neden olduğu ciddi ve nitelikli zararları da kapsaması gerektiği kanaatindeyiz.

Hükümetlerarası Uzmanlar Grubu ise, bir devletin egemenliğinden kaynaklanan ve başka bir devlette "ciddi olumsuz sonuçlar" doğuran tüm zararlı devlet dışı siber saldırıların özen yükümlülüğü kapsamına girmediğini belirtmiştir. Özen yükümlülüğü ilkesi, devletler tarafından gerçekleştirilen siber saldırılarla benzer şekilde, yalnızca devlet dışı aktörlerin hedef devletin uluslararası hukuktan doğan haklarını etkileyen fiillerinde devreye girmektedir.

Konunun daha iyi anlaşılması için iki kurgusal örnek sunulabilir. Birinci vakada, D devletinde faaliyet gösteren bağımsız bir bilgisayar korsanı grubu, F devletinin merkez bankasının finansal sistemine yönelik sistematik siber saldırılar düzenlemiştir. Bu saldırılar sonucunda F devletinin para piyasalarında ciddi aksaklıklar meydana gelmiş, ekonomik istikrar sarsılmış ve halkın temel finansal hakları zarar görmüştür. D devleti, bu bilgisayar korsanı grubunun faaliyetlerinden önceden haberdar olmasına rağmen gerekli önlemleri almamış ve saldırıların devam etmesine göz yummuştur. Söz konusu durum, D devletinin kendi egemenlik alanından kaynaklanan zararlı siber faaliyetlere karşı yeterli koruma sağlamayarak F devletinin egemenlik haklarını ihlal ettiğini göstermektedir. Zira D devleti, ülkesinden kaynaklanan ancak

F devletine zarar veren siber saldırıları engellemek için makul ve orantılı önlemler alma yükümlülüğüne sahiptir. Bu yükümlülüğün yerine getirilmemesi, D devletinin uluslararası sorumluluğunu doğurur.

İkinci kurgusal örnekte ise, "XxNet" adlı büyük bir teknoloji şirketi, C devletindeki mevcut iktidarı devirmek amacıyla sosyal medya platformları üzerinden organize dezenformasyon kampanyaları ve provokatif içerikler yaymıştır. Bu faaliyetler, toplumda istikrarsızlık ve çatışmaların artmasına yol açarak C devletinin kamu düzenini ciddi şekilde zedelemiştir. Şirketin merkezi D devletinde bulunmakta olup, D devleti makamları bu müdahalelerden haberdar olmalarına rağmen şirketin faaliyetlerini engellemek için gerekli önlemleri almamıştır. Buna ek olarak, E devleti de XxNet'in kullandığı bazı sunucu ve altyapı hizmetlerini sağlayarak dolaylı yoldan müdahaleyi kolaylaştırmıştır. Bu durumda, egemenlik ve iç işlerine müdahale yasağı ilkeleri hem D hem de E devletleri tarafından ihlal edilmiştir. Her iki devlet de kendi topraklarından kaynaklanan bu zararlı faaliyetlere karşı özen yükümlülüğünü yerine getirmeyerek uluslararası sorumluluklarını gündeme getirmiştir.

Müdahale yasağı bağlamında özen yükümlülüğüne bakıldığında, bir devlet tarafından gerçekleştirildiğinde müdahale yasağını ihlal edecek nitelikteki siber saldırıların, devlet dışı aktörler tarafından başlatılması halinde dahi ilgili ülke devleti bu saldırılar karşısında özen yükümlülüğü altındadır. Benzer şekilde, devlet tarafından gerçekleştirildiğinde egemenlik ilkesinin ihlalini oluşturacak siber saldırılar bakımından da aynı yaklaşım geçerlidir.

Bu kapsamda bir örnek olay olarak, uluslararası alanda faaliyet gösteren ve merkezi A ülkesinde bulunan büyük teknoloji şirketi TechPo ele alınabilir. A ülkesi, gelişmiş siber altyapısı ve inovasyon ortamıyla bilinen bir devlettir. Ancak TechPo, rakip devlet B ülkesindeki kritik enerji altyapısına yönelik, devlet tarafından yapılması halinde müdahale yasağı teşkil edecek karmaşık bir siber saldırı planlamış ve uygulamıştır. TechPo'nun gerçekleştirdiği bu saldırı, B ülkesinin enerji santrallerinin kontrol sistemlerine sızarak uzun süreli enerji kesintilerine yol açmış ve B ülkesinin iç güvenliği ile ekonomik istikrarını ciddi şekilde tehdit etmiştir. Eğer bu saldırı doğrudan A devleti tarafından gerçekleştirilmiş olsaydı, B ülkesinin egemenliğine yönelik müdahale olarak kabul edilip müdahale yasağı çerçevesinde A devletinin uluslararası sorumluluğunu doğuracaktı.

Ancak mevcut durumda saldırı doğrudan TechPo tarafından yapılmıştır. Bu nedenle B ülkesi, A devletinden TechPo'nun saldırılarını derhal durdurmasını ve gerekli önlemleri almasını talep etmiştir. Uluslararası hukuk bağlamında, A devleti, kendi sınırları içerisinde faaliyet gösteren TechPo'nun bu tür hukuka aykırı siber saldırılarını engellemek için özen

yükümlülüğünü taşımaktadır. Aksi takdirde, A devleti B ülkesine yönelik uluslararası sorumlulukla karşı karşıya kalacaktır.

Özen yükümlülüğü bağlamında, ApSo adlı özel bir şirketin B devletine ait son derece gizli belgeleri ele geçirerek C devletinde çevrim içi olarak yayımlaması örneğini ele alalım. Bu durumda, ApSo'nun gerçekleştirdiği ifşa, belgeleri yayımlanan B devleti açısından ciddi olumsuz sonuçlar doğurabilir. Ancak belgelerin yayımlandığı C devleti, söz konusu belgelerin internetten kaldırılmasını sağlamakla yükümlü değildir. Zira bu olayda, B devletinin uluslararası hukuk tarafından korunan herhangi bir hakkı ihlal edilmemiştir.

Uluslararası hukukta özen yükümlülüğü ilkesinin ne zaman uygulanacağı hususunda zararın kesin sınırları henüz netleşmemiştir. Hükümetlerarası Uzmanlar Grubu, bu ilkenin yalnızca "ciddi olumsuz sonuçlar" (*serious adverse consequences*) doğuran siber saldırılar bakımından uygulanabileceği konusunda mutabık kalmıştır. Bununla birlikte, Grup, hangi durumların "ciddi" olarak nitelendirilebileceğine ilişkin somut bir ölçüt belirlememiştir. Bu yaklaşım, uluslararası çevre hukukundaki benzer uygulamalardan esinlenerek geliştirilmiştir.

Bununla birlikte, bazı uzmanlar bu eşiğin daha düşük tutulması gerektiğini savunmuş; "ciddi" (*serious*) yerine "önemli" (*significant*) veya "kayda değer" (*substantial*) gibi daha düşük yoğunlukta sonuçları ifade eden terimlerin kullanılmasını önermiştir.[828]

Hükümetlerarası Uzmanlar Grubu, bir devletin ulusal çıkarlarını etkilemenin, tek başına uluslararası hukuku ihlal eden bir zarar türü olarak değerlendirilemeyeceği görüşündedir. Bu çerçevede, yalnızca rahatsızlık vermek, küçük çaplı kesintilere yol açmak veya önemsiz bir maliyete sebep olmak gibi sonuçlar, özen yükümlülüğünün ihlalini doğuracak düzeyde zarar olarak kabul edilmemektedir. Dolayısıyla, bir devletin ülkesinin kullanılması sonucunda başka bir devlette olumsuz etkiler doğuran her fiil, kendiliğinden özen yükümlülüğü ilkesinin ihlali anlamına gelmez.

Bu duruma örnek olarak, bir devletin Spor Bakanlığı'na ait ve yalnızca ulusal takımlar hakkında bilgi sağlayan resmi internet sitesinin, başka bir devlette bulunan bilgisayar korsanları tarafından sınırlı ölçüde tahrif edilmesi verilebilir. Böyle bir siber saldırı, hedef devlete yeterli düzeyde zarar vermediğinden, ülke devletinin bu faaliyeti sona erdirmek amacıyla önlem almaması özen yükümlülüğünün ihlali olarak değerlendirilmeyecektir.

Benzer şekilde, bir devlette yerleşik bir medya kuruluşu ya da blog yazarının, başka bir devlet hakkında olumsuz içerikli bilgi yayımlaması halinde de özen yükümlülüğü gündeme gelmez. Zira bu tür bir durum, hedef devletin uluslararası hukuk tarafından korunan herhangi

[828] Schmitt, *Tallinn Manual 2.0*, 36-37.

bir hakkını ihlal etmemektedir. Örneğin, V devletinde merkezî bulunan "BigCorp" adlı büyük bir teknoloji şirketi, dünya çapında kullanılan bir sosyal medya platformu işletmektedir. Bu platformda bazı kullanıcılar, T devletinin hükümet politikalarını eleştiren ve olumsuz yorumlar içeren paylaşımlar yapmaktadır. Söz konusu içerikler T devleti vatandaşları tarafından da erişilebilir olsa da, bu durum T devletinin uluslararası hukuk kapsamındaki haklarını ihlal etmemektedir. Dolayısıyla T devletinin, V devletinden BigCorp'a müdahale etmesini talep etmesi veya V devletinin böyle bir yükümlülüğü bulunmamaktadır.

Bununla birlikte, eğer bir siber saldırı, vergi ödemeleri, oy kullanma işlemleri veya afet yardımı rehberliği gibi kritik devlet hizmetlerini engelleyecek şekilde gerçekleştirilirse, ilgili devlete bu faaliyetleri durdurma yönünde özen yükümlülüğü doğar. Kurgusal bir örnek olarak, BigCorp'un T devletinin resmi vergi ödeme portalı ve afet yardımı rehberliği hizmetlerini barındıran bulut sunucularını işletmesi düşünülebilir. Bir bilgisayar korsanı grubu, BigCorp'un sunucularına sızarak bu hizmetlerin işlevini engelleyecek şekilde siteleri tahrif eder. Bu saldırı sonucunda, T devleti vatandaşları vergi ödemelerini yapamaz ve afet yardımı hakkında kritik bilgilere ulaşamaz hale gelir. Bu fiil, T devletinin kritik kamu hizmetlerine doğrudan zarar verdiğinden, hukuka aykırı bir eylem niteliğindedir. Dolayısıyla BigCorp'un faaliyet gösterdiği devlet, T devletine karşı özen yükümlülüğünü yerine getirmek, saldırıya son vermek ve ortaya çıkan zararların giderilmesi için gerekli tedbirleri almakla yükümlüdür.

Hükümetlerarası Uzmanlar Grubu, siber saldırıların uluslararası hukuk kapsamında haksız fiil olarak nitelendirilebilmesi için fiziksel nesnelere zarar verilmesi veya gerçek kişilerin yaralanması gibi sonuçların ortaya çıkmasının zorunlu olmadığı hususunda görüş birliğine varmıştır. Gruba göre, bir siber saldırının haksız fiil teşkil edebilmesi için, kritik altyapının işleyişine müdahale edilmesi ya da ekonomik düzende ciddi bozulmalara yol açması gibi sonuçların meydana gelmesi yeterlidir.[829] Bu çerçevede, örneğin başka bir devlette bulunan devlet dışı aktör niteliğindeki bilgisayar korsanları tarafından bir devleti hedef alarak gerçekleştirilen ve çevrimiçi bankacılık, medya, kamu hizmetleri ile ticari faaliyetlerde ağır aksamalara sebep olan siber saldırılar; fiziksel zarar veya yaralanma meydana gelmese dahi, yarattıkları etki bakımından ağır olarak değerlendirilmektedir. Bu nedenle, söz konusu saldırılar açısından özen yükümlülüğü ilkesinin uygulanması gerektiği kabul edilmektedir.[830]

Siber uzay bağlamında devlet sorumluluğunun tespitinde en güç alanlardan biri, botnetler aracılığıyla gerçekleştirilen saldırılardır. Botnetler özelinde, zararın ciddi ve olumsuz sonuçlar doğurup doğurmadığının belirlenmesi, son derece karmaşık bir değerlendirme

[829] Schmitt, *Tallinn Manual 2.0*, 37-38.
[830] Schmitt, *Tallinn Manual 2.0*, 37-38.

gerektirir. Örneğin, bir devlette bulunan bir bilgisayar grubunun, çeşitli devletlerde konuşlanmış botnetleri kullanarak başka bir devlete yönelik siber saldırılar gerçekleştirdiği varsayılsın. Bu saldırılar, hedef devlet açısından son derece ağır sonuçlar doğurabilir. Ancak botnetlerin, bulundukları devletlerin sınırları içinde münferit olarak kullanılması, tek başına benzer ölçüde ciddi sonuçlar yaratmayabilir. Bu durum, botnetlerin bulunduğu devletlerin, söz konusu kullanımı durdurmaya yönelik gerekli önlemleri almamaları hâlinde, özen yükümlülüğü ilkesini ihlal edip etmedikleri sorusunu gündeme getirmektedir.

Hükümetlerarası Uzmanlar Grubu, bir siber saldırı sonucunda bir devletin maruz kaldığı zararın, özen yükümlülüğü kapsamında belirlenen eşik düzeyini karşılaması hâlinde, bu zararın kaynağının veya ortaya çıktığı yerin önem taşımadığını vurgulamaktadır.[831] Örneğin, A Devleti'nin, devlet faaliyetlerinin yürütülmesi için kritik öneme sahip verilerini, B Devleti sınırları içerisindeki sunuculardа depoladığını varsayalım. C Devleti'nde faaliyet gösteren devlet dışı bir aktör, bu sunuculara yönelik bir siber saldırı gerçekleştirerek söz konusu verileri bozmuş olsun. Bu senaryoda, C Devleti topraklarının başka bir devlete zarar vermek amacıyla kullanılması nedeniyle, C Devleti'nin A Devleti'ne karşı özen yükümlülüğü kapsamında sorumluluğu doğacaktır. Bu yaklaşım, uluslararası hukukta devletin sorumluluğunun tespitinde esas alınması gereken ölçütün, zararın meydana geldiği yerden ziyade, zararın ağırlığı ve etkisi olduğunu göstermektedir. Daha açık bir ifadeyle, bir devletin ülkesi, başka bir devlete yönelik zararlı siber faaliyetlerin icrasına aracılık ediyorsa, o devletin bu faaliyetleri önlemek ve durdurmak yönündeki uluslararası yükümlülüklerini yerine getirmesi gerekir.[832]

Özen yükümlülüğü ilkesi, hedef alınan siber altyapının devlet kurumlarına mı yoksa özel sektöre mi ait olduğu hususunda herhangi bir ayrım gözetmez. Bu çerçevede, A Devleti'nde faaliyet gösteren bir petrol şirketinin, B Devleti'nde bulunan rakip özel bir şirkete yönelik yıkıcı bir siber saldırı gerçekleştirmesi durumunu ele alalım. Eğer A Devleti, söz konusu saldırıdan haberdar olmasına rağmen makul ve uygulanabilir önlemleri almazsa ve ortaya çıkan zarar, gerekli ciddiyet eşiğini aşarsa, A Devleti özen yükümlülüğü ilkesini ihlal etmiş sayılır.

Bu ilkenin uygulanmasında bilgi unsuru belirleyici niteliktedir. Bir devletin kendi ülkesinin başka bir devlete karşı düşmanca siber saldırılar için kullanıldığına ilişkin açık ve somut bilgiye sahip olması hâlinde, özen yükümlülüğü ilkesi devreye girer. Bu bağlamda, bir devletin somut bilgiye sahip olduğunun kabul edilebilmesi için, istihbarat teşkilatları gibi

[831] Schmitt, *Tallinn Manual 2.0*, 37-38.
[832] Schmitt, *Tallinn Manual 2.0*, 37-38.

yetkili devlet organlarının ülkesinden kaynaklanan bir siber saldırıyı tespit etmesi veya bu yönde güvenilir bilgiler elde etmesi gerekir.

Hükümetlerarası Uzmanlar Grubu, özen yükümlülüğü ilkesinin uygulanmasında "yapıcı bilgi"nin (*constructive knowledge*) de dikkate alınması gerektiği hususunda mutabakata varmıştır. Bu çerçevede, somut koşulların bir devletin olağan süreçler içinde belirli bir siber saldırıyı fark etmesini gerektirmesi halinde, bu durum devlet açısından yapıcı bilgi olarak değerlendirilmelidir. Başka bir ifadeyle, bir devletin söz konusu siber saldırılardan fiilen haberdar olmaması, eğer ülkesinin bu saldırılar için kullanıldığını bilmesi bekleniyorsa, özen yükümlülüğü ilkesini ihlal ettiği gerçeğini ortadan kaldırmaz.[833]

Özen yükümlülüğünün doğup doğmadığının tespitinde, birçok unsur devletin söz konusu siber saldırılardan haberdar olması gerektiği yönündeki değerlendirmeyi etkileyebilir. Bu çerçevede, örneğin S devletinin kamuya ait siber altyapısının Z devleti veya devlet dışı bir aktör tarafından kullanılması halinde, S devletinin bu durumu fark etmesinin beklenmesi olağandır.

Özen yükümlülüğü ilkesi, ihmal yoluyla ihlal edilebilen bir hukuki yükümlülüktür. İhmal, yalnızca hiçbir eylemde bulunmamayı değil; aynı zamanda, mevcut koşullarda daha uygun, makul ve uygulanabilir tedbirler alınabilecekken etkisiz veya yetersiz önlemlerle yetinilmesini de kapsar. Bu bağlamda, bir devletin ülkesindeki siber altyapının bir teknoloji şirketi tarafından başka bir devlete karşı siber saldırı amacıyla kullanılmasına kayıtsız kalması, özen yükümlülüğünün ihlali anlamına gelir. Benzer şekilde, başka bir devletin bu tür faaliyetlerin yürütüldüğüne dair güvenilir bir bildirimde bulunmasına rağmen, makul tedbirleri almayan ve bu faaliyetlerin sona erdirilmesini sağlamayan devlet de özen yükümlülüğünü ihlal etmiş sayılır.

Hükümetlerarası Uzmanlar Grubu, bir devletin uluslararası haksız fiil teşkil eden siber saldırıyı sona erdirmek amacıyla harekete geçmesi gerektiğini, ancak özen yükümlülüğüne uyma bakımından kullanılacak araçları seçme konusunda takdir yetkisinin ilgili devlete ait olduğunu kabul etmiştir. Bu bağlamda, devletin; saldırıyı gerçekleştiren özel şirkete ait bilgisayarlara sızarak ve kötü amaçlı yazılımı kaldırmaya zorlayarak, devlet dışı aktörleri tutuklayarak veya hedef devleti isimsiz ya da üçüncü bir taraf aracılığıyla belirli bir siber saldırı hakkında bilgilendirerek, böylece önleyici tedbirler alınmasını sağlayarak haksız fiil teşkil eden siber saldırıları durdurabilmesi hâlinde, özen yükümlülüğünü yerine getirmiş olacağı belirtilmiştir. Ayrıca Uzmanlar Grubu, bir devletin iç hukukunun diğer devletlere istihbarat

[833] Schmitt, *Tallinn Manual 2.0*, 40.

paylaşımına sınırlamalar getirmesinin, kendi ülkesinden kaynaklanan zararlı siber saldırıları durdurmadaki ihmalini mazur göstermeyeceğini ifade etmiştir.[834]

Hükümetler Arası Uzmanlar Grubu, bir devletin kendi ülkesinden başka bir devlete karşı gerçekleştirilen ve uluslararası haksız fiil niteliği taşıyan bir siber saldırı hakkında yeterli düzeyde bilgi sahibi olduğu, ancak hedef devletin bu saldırıdan haberdar olmadığı bir senaryoyu ele almıştır. Zira bu tür bir senaryo, istihbarat paylaşımına ilişkin hassas konuları gündeme getirmektedir. Grup, söz konusu devletin, saldırının ayrıntılarını hedef devlete bildirme konusunda tereddüt yaşayabileceğini; zira böyle bir bilgilendirmenin, kendi siber ve istihbarat yeteneklerini açığa çıkarma riskini barındırabileceğini kabul etmiştir.[835]

Devlet veya devlet dışı aktörler tarafından gerçekleştirilen uluslararası haksız fiil niteliğindeki siber saldırılar için kullanılan siber altyapıyı kontrol eden özel kişi veya kuruluş, ülke devletiyle işbirliğini tamamen reddedebilir. Hükümetler Arası Uzmanlar Grubu, bu tür işbirliği eksikliğinin, ülke devletinin özen yükümlülüğünü ihlal etmediği anlamına gelmediği görüşündedir. Grup, ülke devletinin, uluslararası hukuka uygunluk çerçevesinde, ilgili kişi veya kuruluşun işbirliğini sağlamak amacıyla mevcut tüm makul ve etkili araçları kullanmakla yükümlü olduğunu belirtmektedir. Ancak, devlet tüm makul çabalarını göstermesine rağmen hâlâ haksız fiil teşkil eden siber saldırıların sona erdirilmesi için gerekli işbirliğini temin edemiyorsa, bu durumda özen yükümlülüğü ilkesinin ihlalinden kaynaklanan sorumluluk doğmayacaktır.[836]

Bir devlet, ülkesinden kaynaklanan haksız fiil teşkil eden siber saldırıları önlemek amacıyla gerekli ve makul tüm tedbirleri özenle almış; ancak tüm bu çabalara rağmen hedef devlet zarar görmüşse, ilgili devlet özen yükümlülüğünü ihlal etmiş sayılmaz. Çünkü özen yükümlülüğü ilkesi, bir sonuç yükümlülüğü değil, davranış yükümlülüğü niteliğindedir. Bu bağlamda, devletin haksız fiil teşkil eden faaliyetleri her zaman başarıyla sona erdirmesi değil, yalnızca makul ve titiz çabalar göstermesi beklenmektedir.

2.5.2. Somut Bir Vakıa Olarak Google

Özen yükümlülüğü kapsamında, devlet dışı yeni aktörler olarak özel şirketlerin fiilleri nedeniyle devletlerin sorumluluğunu gündeme getiren en somut örneklerden biri, 2011 Mısır Devrimi sırasında Amerika merkezli Google şirketinin eylemleridir. 11 Şubat 2011 tarihinde,

[834] Schmitt, *Tallinn Manual 2.0*, 44.
[835] Schmitt, *Tallinn Manual 2.0*, 44.
[836] Schmitt, *Tallinn Manual 2.0*, 48.

Mısır'daki meşru iktidara karşı süren isyanlar sırasında, yetkililer ülke genelinde internet erişimini tamamen kesme kararı almıştır. Bu internet kesintisi, daha önce benzeri görülmemiş bir yöntemle, ülkedeki tüm İnternet Servis Sağlayıcıları (İSS) hizmet vermekten alıkoyan bir emir aracılığıyla uygulanmıştır.[837] Karartmanın devam ettiği günlerde ise Google, Mısır yetkililerinin bu engellemesini sona erdirmiştir.

21 Ocak 2010 tarihinde, dönemin ABD Dışişleri Bakanı Hillary Clinton, Chicago'daki İfade Özgürlüğü Müzesi'nde gerçekleştirdiği konuşmada, özel şirketlerin faaliyetleri nedeniyle bir devletin egemenliğine getirilebilecek sınırlamalara dikkat çekmiştir.[838] Clinton, ABD'nin ifade özgürlüğü, bilgiye erişim hakkı, toplanma hakkı ve internet üzerinden ifade edilen din özgürlüğünü koruma amacını vurgulamıştır. Konuşmasında ayrıca, Çin, Kuzey Kore, Mısır, Vietnam, Tunus, Özbekistan ve Suudi Arabistan gibi ülkeleri, kendi topraklarında ifade özgürlüğü ve çevrimiçi bilgi akışına getirdikleri kısıtlamalar nedeniyle açıkça eleştirmiştir.

Clinton, daha da ileri giderek, ifade özgürlüğüne ilişkin mevcut Birleşmiş Milletler insan hakları koruma sistemini göz ardı ederek, internet filtrelemesi yoluyla bilgiye erişimi kısıtlayan devletlerin vatandaşlarının bireysel bilgi edinme hakkını kullanabilmeleri için ABD'nin destek sağlayacağını belirtmiştir. Dışişleri Bakanı, devletlerin uyguladığı bu tür engelleri aşmaya yönelik teknolojilerin geliştirilmesi ve uygulanmasının planlandığını açıklamıştır. Bu açıklama, o döneme kadar devletler arasında zımni olarak kabul edilen; çevrimiçi filtrelemenin her devletin münhasır yetkisi kapsamında olduğu anlayışından farklı bir yaklaşımı yansıtmaktadır.

Clinton, bu meşhur konuşmasından bir yıl sonra, bilgiye özgürce erişim hakkından mahrum bırakılan bireylere destek sağlamak amacıyla "İnternet Özgürlüğü" (*Internet Freedom*) programını başlattı.[839] Bu program, Mısır'da nihai hedefine ulaşmadan önce dahi, uluslararası hukuk açısından eleştirel bir incelemeye tabi tutulabilirdi. Zira, dünyanın en güçlü devletlerinden biri adına konuşan Clinton, yabancı devletlerin vatandaşlarının iç hukuklarını ihlal etmelerini teşvik etme niyetinde olduğunu açıkça ifade etmişti.

Clinton tarafından yapılan bu açıklamalar, insan hakları ilkeleri ile devletlerin egemen eşitliği ilkesi arasındaki hiyerarşi sorununu gündeme getirmektedir. Somut olay bağlamında

---

[837] Joanna Kulesza, "Social Media Censorship vs. State Responsibility for Human Rights Violations Case Study of the Arab Spring Uprising in Egypt", *Social Media in Politics Case Studies on the Political Power of Social Media*, ed. Bogdan Pa˘trut ve Monica Pa˘trut (London: Springer Cham Heidelberg New York Dordrecht London, 2014), 265.

[838] Hillary Rodham Clinton, "Remarks on Internet Freedom", U.S. Department of State, erişim 14 Haziran 2025, http://www.state.gov/secretary/rm/2010/01/135519.htm.

[839] Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World, Remarks", U.S. Department of State, erişim 14 Haziran 2025, http://www.state.gov/secretary/rm/2011/02/156619.htm.

yenilik arz eden tek unsur, tartışılan insan hakkının çevrimiçi ortamda kullanılacak olmasıdır. Bu bağlamda, Mısır'daki İnternet Servis Sağlayıcısı (ISS) tarafından işletilen kritik internet altyapısının günlük işleyişine devlet müdahalesinin sınırları sorusu, devletin bireysel haklara müdahale sınırları meselesinin doğrudan bir yansımasıdır. Bu sorunun cevaplanmasındaki zorluk ise, öncelikle Mısır'ın yargı yetkisinin ulusal nitelikte olması ile siber uzayın ulusal sınırlarla sınırlanmayan ulusötesi karakterinin çelişmesinden kaynaklanmaktadır.[840]

Clinton tarafından yapılan açıklamalar, ABD'nin Mısır'daki Google hizmetlerine zımni onay vermesi anlamına gelmekte olup, bu durum insan hakları doktrini çerçevesinde meşruiyet bulmamaktadır. Ayrıca, ABD'nin, yabancı bir devletin egemenliğine yönelik özel bir şirket tarafından gerçekleştirilen müdahaleyi önlemek amacıyla gerekli önlemleri almaması, uluslararası hukukta kabul edilen özen yükümlülüğüne aykırı olarak değerlendirilebilir. Uluslararası hukukta benimsenen özen yükümlülüğü ilkesi gereğince, ABD, Google'ın başka devletlerin egemenlik alanına müdahalesini engellemek konusunda yetkililerinin gerekli özeni göstermemesi nedeniyle uluslararası hukuk bakımından sorumluluk taşımaktadır.[841]

Mısır'ın devlet egemenliğine aykırı olarak Google tarafından gerçekleştirilen fiillerin, Clinton'ın açıklamaları hariç tutulduğunda, herhangi bir ABD devlet politikasının doğrudan sonucu olduğunu söylemek güçtür. Zira Clinton'ın yaptığı açıklamaların hiçbiri, herhangi bir kuruluşun ABD adına hareket etmesi için doğrudan bir devlet yetkisi vermemektedir. Bu bağlamda, ABD doğrudan Google'ın Mısır'daki eylemlerinden sorumlu tutulamaz. Çünkü Google, ABD makamları adına ya da bu makamların verdiği yetkiye dayanarak hareket etmemiştir. Ancak bu durum, ABD'nin Google'ın fiillerinin sonuçlarından sorumluluğunu ortadan kaldırmamaktadır.

Devletlerin egemen eşitliği prensibi gereğince, Mısır'daki meşru iktidar tarafından alınan kararlara ABD dâhil tüm diğer devletlerin saygı göstermesi zorunludur. Devletlerin egemen eşitliğine saygı yükümlülüğü, devletlerin kendi topraklarından kaynaklanan ve başka devletlere zarar verebilecek fiilleri önleme sorumluluğunu da içermektedir. Bu sorumluluk, zararlı müdahalenin etkilerini ortadan kaldırmak amacıyla potansiyel mağdur devletle her türlü işbirliğini gerçekleştirmeyi de kapsar. Dolayısıyla, bir devlet, başka bir devletin meşru çıkarlarını etkili şekilde koruyamadığı durumlarda dahi, Google gibi özel şirketlerin kendi

[840] Joanna Kulesza, *International Internet Law* (Oxon ve New York: Routledge, 2012), 1-10.
[841] Riccardo Pisillo-Mazzeschi, "The Due Diligence Rule and the Nature of International Responsibility of States", *German Yearbook of International Law* 35 (1992), 9-51.

ülkesini veya yetki alanındaki diğer kaynakları kullanarak bu çıkarlar üzerinde müdahalede bulunmasına pasif biçimde izin veremez.[842]

Somut olayda, ABD, meşru Mısır hükümeti tarafından yürütülen süreci işlevsiz kılmayı amaçlayan Google'ın gerçekleştirdiği eylemlerin farkındaydı. Ancak ABD, Google'ın bu fiillerini önlemeye yönelik herhangi bir tedbir almamıştır. Sonuç olarak, ABD, Google'ın Mısır'ın iç politikasına yönelik zararlı etkilerini durdurmayarak uluslararası hukukta öngörülen özen yükümlülüğünü ihlal etmiştir.

2.5.3. Özen Yükümlülüğü Bağlamında Tahran Rehineler Davası

Devlet kaynaklarının hukuka aykırı şekilde kullanılmasının önlenmesinde özen yükümlülüğü ilkesi, Tahran Rehineler Davası'nda ayrıntılı olarak incelenmiştir.[843] Uluslararası Adalet Divanı (UAD), kararında İran'ın, bölgedeki ABD müdahalesini protesto eden İranlı öğrenciler tarafından saldırıya uğrayan Tahran'daki ABD diplomatik misyonunu korumakla yükümlü yetkililerin gerekli önlemleri almamasından dolayı sorumlu olduğunu teyit etmiştir. Divan'a göre, İranlı öğrencilerin eylemleri doğrudan İran devletine atfedilmese de, Tahran'daki diplomatik misyonu korumakla yükümlü İranlı yetkililerin önleyici tedbirler almaması nedeniyle İran sorumludur. Divan'ın da belirttiği üzere, İranlı öğrencilerin fiillerinin doğrudan yetkililere atfedilmemesi, İran'ın bu saldırılarla ilgili sorumluluktan muaf olduğu anlamına gelmemektedir; zira bu durum, İran'ın diplomatik misyonları ve personelini koruma yönündeki uluslararası yükümlülükleriyle çelişmektedir. Divan, İran'ın ABD diplomatları ve misyonlarının korunmasını sağlamak için gerekli adımları atmadığını ve İranlı yetkililerin tamamen hareketsiz kalmasının uluslararası yükümlülüklerine aykırı olduğunu özellikle vurgulamıştır.[844]

Divan, bu kararıyla bir devletin uluslararası hukuktan doğan yükümlülüklerini yerine getirirken özen yükümlülüğüne uygun davranması gerektiğini teyit etmiş ve devlet organlarının özeni göstermemesi halinde, özel kişilerin fiillerinden kaynaklanan zararlı sonuçların devlete atfedilebileceği ihtimalini vurgulamıştır.[845] Bir devletin, yargı yetkisinin geçerli olduğu alanlarda, ülkesini sınır ötesi zarara yol açmaya çalışan gerçek kişiler veya bireyler için

[842] Kulesza, "Social Media Censorship vs. State Responsibility for Human Rights Violations Case Study of the Arab Spring Uprising in Egypt", 265.
[843] Uluslararası Adalet Divanı (UAD), K. United States Diplomatic and Consular Staff in Tehran (ABD v. İran) (24 Mayıs 1980).
[844] UAD, United States Diplomatic and Consular Staff in Tehran, Par. 32.
[845] UAD, United States Diplomatic and Consular Staff in Tehran, Par. 32.

kullanılabilir hâle getirmesi, uluslararası hukuka aykırı bir eylem olarak nitelendirilebilir. Bu durum, devlet organlarının söz konusu sınır ötesi zararı önleme yönündeki özen yükümlülüğünü ihmal etmesi nedeniyle devlet sorumluluğunun doğmasına zemin hazırlayabilir. Bu sonuca, 1992 tarihli Uluslararası Hukuk Komisyonu'nun (UHK) Devlet Sorumluluğu Taslak Maddeleri'nin 14. maddesinin 3. fıkrası temel teşkil etmektedir. Taslağın baş editörü ve devlet sorumluluğu Özel Raportörü James Crawford'a göre, söz konusu kurallar "belirli bir olayın önlenmesi yükümlülüğünün ihlaline" ilişkindir.[846] Bu yükümlülük, devletlerin zararın önlenmesi için makul ve gerekli tüm tedbirleri almasını zorunlu kılmakla birlikte, bu tedbirlerin zararın mutlak surette engelleneceğine dair bir garanti sağlamasını şart koşmamaktadır.[847]

Özen yükümlülüğü standardı, her somut olayın koşullarına göre tayin edilmektedir. Birleşmiş Milletler sınır ötesi zararlar konusunda Özel Raportörü P.S. Rao'ya göre, "gerekli özen yükümlülüğünün ihlali," ayrıca "bir devletin, söz konusu zarara yol açan olayı kasıtlı veya ihmalkar şekilde gerçekleştirmesi; ya da kendi topraklarında başkalarının bu zararı vermesini kasıtlı veya ihmalkar tutumla engellememesi ya da zararın giderilmesinden kaçınması durumlarında da kabul edilebilir." [848] Bu bağlamda, bir devlet uygun mevzuatı düzenlememesi, iç hukuku uygulamaması ya da yargı yetkisi veya kontrolü altındaki alanlarda hukuka aykırı faaliyetleri önlememesi nedeniyle sorumluluğa tabi tutulabilir. Özen yükümlülüğünün ihlali, ayrıca devlet makamlarının, ilgili koşullar çerçevesinde, belirli bir faaliyetin sınır ötesi zarara yol açabileceğini bilmesi veya bilmesi gerekmesi halinde de söz konusu olmaktadır.[849]

2.6. Devlet Dışı Aktörlerin Doğrudan Sorumluluğu

Buraya kadar aktardıklarımızdan hareketle, siber uzaydan kaynaklanan saldırıların yalnızca devlet kaynaklı tehditlerle açıklanamayacak kadar karmaşık bir yapıya sahip olduğu açıktır. Günümüzde, büyük teknoloji şirketleri, organize bilgisayar korsanı grupları, siber paralı askerler ve veri trafiğini kontrol eden özel platformlar gibi yeni devlet dışı aktörler, küresel

[846] Kulesza, "Social Media Censorship vs. State Responsibility for Human Rights Violations Case Study of the Arab Spring Uprising in Egypt", 273.
[847] Kulesza, "Social Media Censorship vs. State Responsibility for Human Rights Violations Case Study of the Arab Spring Uprising in Egypt", 273.
[848] Kulesza, "Social Media Censorship vs. State Responsibility for Human Rights Violations Case Study of the Arab Spring Uprising in Egypt", 273.
[849] Kulesza, "Social Media Censorship vs. State Responsibility for Human Rights Violations Case Study of the Arab Spring Uprising in Egypt", 274.

güvenlik ve insan hakları üzerinde doğrudan etkili siber eylemler gerçekleştirmektedir. Bu tür aktörler tarafından gerçekleştirilen ve herhangi bir devletle doğal bağları bulunmayan siber saldırıların uluslararası hukuk çerçevesinde nasıl sorumluluk doğuracağı sorusu ise henüz yeterince yanıtlanmamıştır. Bu bağlamda, sorumluluğa ilişkin klasik atıf çerçevesinin yetersiz kaldığı durumlarda, uluslararası hukukta yeni bir sorumluluk teorisi olarak önerdiğimiz "*siber uzaydaki fonksiyonel egemenlik yaklaşımı*" aşağıda ele alınacaktır.

Mevcut uluslararası hukukta yalnızca devletlerin doğrudan uluslararası sorumluluğu öngörülmekte; bireyler veya şirketler gibi devlet dışı aktörlerin fiilleri ise çoğunlukla bir devlete atfedilmek suretiyle değerlendirilmektedir. Ancak bu yaklaşım, özellikle siber uzayda anonimlik, çoklu vatandaşlık, sınır aşan teknolojik yapılar ve özel sektörün kontrol kapasitesi gibi özellikler nedeniyle yetersiz kalmaktadır. 2001 tarihli Taslak Maddeler, devlet dışı bir aktör tarafından gerçekleştirilen bir fiilin yalnızca devlete atfedilmesi halinde sorumluluğun doğacağını düzenlemektedir. Ancak Taslak Maddeler, failin hiçbir devletle doğrudan ilişkisi bulunmadığı durumlarda sorumluluğun nasıl düzenleneceğine dair bir hüküm içermemektedir.

Kanaatimizce, bu boşluğun giderilebilmesi için devlet dışı aktörün fiilen egemenliğe benzer bir güç kullanıp kullanmadığı esas alınmalıdır. Daha açık bir ifadeyle, siber uzaydaki bir devlet dışı aktörün belirli bir dijital alanı kontrol etmesi, normlar koyması, veri erişimini sınırlandırması, bireylerin haklarına doğrudan müdahale etmesi ve teknik yeteneklerle zorlayıcılık oluşturması durumunda, bu aktör fiilen bir "egemen" gibi davranmaktadır. Bu durumda, kişinin gerçek ya da tüzel olması değil, hangi fonksiyonları yerine getirdiği dikkate alınmalıdır. Örneğin, veri güvenliğini ihlal eden büyük bir sosyal medya şirketi ya da kritik altyapıya saldıran bir bilgisayar korsanı kolektifi, egemenliğin belirli işlevlerini fiilen üstlenmiş sayılabilir.

Bu tür bir egemenlik anlayışı, klasik devlet sorumluluğu yaklaşımının ötesine geçerek, doğrudan birey veya özel tüzel kişinin uluslararası hukuka aykırı fiillerinden dolayı sorumluluğunu gündeme getirebilir. Bu sorumluluk, özellikle uluslararası toplumun tamamını ilgilendiren çevrimiçi özgürlükler, özel hayatın gizliliği, sağlık sistemlerine yönelik saldırılar veya altyapı tehditleri gibi alanlarda meşru ve gereklidir.

Bu yaklaşımın üç temel hukuki dayanağı bulunmaktadır. Birincisi, Uluslararası Ceza Mahkemesi'ni (UCM) kuran Roma Statüsü'dür. Roma Statüsü, bireylerin doğrudan uluslararası hukuk kapsamında sorumluluğunu açıkça kabul eden ilk bağlayıcı metinlerden biri olmuştur. Devlet dışı aktörler olarak bireyler, savaş suçları, insanlığa karşı suçlar ve soykırım gibi eylemlerden dolayı bireysel olarak yargılanabilmekte ve mahkûm edilebilmektedir. Bu durum, uluslararası hukukta sorumluluğun yalnızca devletlere özgü olmadığını ortaya koymuş ve

özellikle devlet dışı silahlı grupların liderlerinin yargılandığı *Lubanga, Katanga* ve *Al Mahdi* davalarında fiilen uygulanmıştır. [850] Bu çerçevede, savaş hukukunda bireysel sorumluluk kabul ediliyorsa, benzer şekilde siber savaşlarda da bireylerin ya da özel bilgisayar korsanı gruplarının sorumluluğu ilkesel olarak mümkündür.

İkincisi, Birleşmiş Milletler İş Dünyası ve İnsan Haklarına Dair Rehber İlkeler (UNGPs), özellikle çok uluslu şirketlerin insan hakları ihlallerinden doğan sorumluluklarını tanımlayan önemli bir normatif çerçeve sunmuştur. Bu ilkeler bağlayıcı olmamakla birlikte, hem uluslararası hukuk tartışmalarında hem de birçok devletin iç hukukunda referans olarak kabul edilmektedir. Örneğin, Facebook'un Myanmar'da Rohingya halkına yönelik şiddeti körükleyen içeriklerin yayılmasına izin vermesi ve gerekli önlemleri almaması, uluslararası düzeyde hem hukuki hem de etik sorumluluk tartışmalarına konu olmuş; bu durum, UNGPs'nin pratikteki önemini ortaya koymuştur. Benzer şekilde, İsrailli NSO Group adlı şirketin Pegasus casus yazılımını hükümetlere satarak insan hakları ihlallerine yol açması, özel bir şirketin uluslararası sorumluluğunu gündeme getiren önemli bir örnektir.[851] Bu vakalar, devlet dışı aktörlerin siber eylemler yoluyla uluslararası düzeyde sonuçlar doğurabileceğini göstererek, UNGPs çerçevesinde sorumluluklarının hukuken tartışılmasını meşrulaştırmaktadır.

Üçüncüsü ise, uluslararası hukukta giderek güçlenen özen yükümlülüğü anlayışıdır. Geleneksel olarak yalnızca devletlere yüklenen bu sorumluluk, siber uzayda özel aktörlerin faaliyetlerinin etkisi arttıkça daha kapsamlı şekilde yorumlanmaya başlanmıştır. Özellikle uluslararası çevre hukuku, deniz hukuku ve siber güvenlik gibi alanlarda, özel sektörün de özen yükümlülüğü kapsamında belirli sorumluluklar üstlenmesi gerektiği yönünde güçlü görüşler gelişmiştir. Örneğin, 2020 tarihli Uluslararası Kızılhaç Komitesi'nin "Siber Uzayda Silahlı Çatışmalar ve Hukuki Sorumluluk" raporu, siber altyapının büyük ölçüde özel sektöre ait olması sebebiyle, bu aktörlerin çatışma dönemlerinde de insan haklarına ve uluslararası insancıl hukuka uygun davranmakla yükümlü olduğunu savunmuştur. [852] Ayrıca, Tallinn El Kitabı 2.0'da, özel aktörlerin devlet talimatı olmaksızın gerçekleştirdikleri siber faaliyetlerin dahi

[850] *Prosecutor v. Thomas Lubanga Dyilo*, ICC-01/04-01/06, *Judgment*, 14 March 2012; *Sentence*, 10 July 2012; CC, *Decision Establishing Principles and Procedures for Reparations* (7 March 2015); *Trial Chamber II, Tazminat Kararı*, December 2017; *Prosecutor v. Germain Katanga*, ICC-01/04-01/07, *Judgment*, 7 March 2014; *Prosecutor v. Ahmad Al Faqi Al Mahdi*, ICC-01/12-01/15, *Judgment*, 27 September 2016.

[851] Amnesty International (Amnesty International Security Lab and Forbidden Stories), *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector* (Pegasus Project briefing), July 2021.

[852] International Committee of the Red Cross, "Malicious use of cyber technology can cause suffering during armed conflicts," Statement to UN Security Council Arria-Formula Meeting, 22 May 2020; and *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC position paper* (2019).

uluslararası barış ve güvenliği tehdit edebileceği belirtilmiş ve bu tür durumlara uygulanabilecek hukukî rejimin geliştirilmesi gerekliliği vurgulanmıştır.[853]

Bu üç temel hukuki zemin birlikte değerlendirildiğinde, devlet dışı bir aktörün siber uzayda fiilen egemenliğe benzer fonksiyonlar üstlenmesi durumunda, sorumluluğun yalnızca devlete atfedilmesi yoluyla değil, doğrudan bu aktörün uluslararası hukuki sorumluluğu aracılığıyla hesap verebilirliğin sağlanması mümkün olacaktır. Böylelikle mevcut sorumluluk boşlukları, çağdaş hukuk ilkeleriyle uyumlu bir şekilde kapatılmış olur.

Dolayısıyla, mevcut düzenlemeler, teoriler ve içtihatlar ışığında, bir devlete atfedilemeyen ancak uluslararası hukukta açık bir ihlal teşkil eden siber saldırılar karşısında, bu eylemi gerçekleştiren devlet dışı aktörün "egemenliğe benzer fonksiyonlar" icra edip etmediği tespit edilerek doğrudan uluslararası hukuki sorumluluğu tesis edilmelidir. Bu sayede yalnızca devletler değil, dijital alanda fiilen yetki kullanan özel aktörler de uluslararası toplum nezdinde sorumlu tutulacaktır. Bu yaklaşım, özellikle siber güvenlik ve insan hakları alanındaki normatif boşlukların doldurulması bakımından önemli bir katkı sağlayacaktır.

[853] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 17, Rule 33.

SONUÇ

Siber uzay, oldukça geniş ve soyut bir alan olup, dijital etkileşimlerin geleneksel fiziksel sınırları aşması ve bilgi akış hızının klasik yönetişim anlayışlarını zorlaması nedeniyle, bu alanda faaliyet gösteren yeni devlet dışı aktörlerin hukuka aykırı fiillerinden dolayı sorumluluğu, uluslararası hukuk alanında en önemli sorunlardan biri haline gelmiştir. Her ne kadar siber uzayın sınırlarının belirsiz olduğu ifade edilse de bu alanın altyapısı—sunucular, kablolar ve veri merkezleri gibi—egemen devletlerin topraklarında bulunmakta olup, çok katmanlı ve örtüşen yetki alanları ile kontrol iddialarına tabi bulunmaktadır. Siber uzayın bu karmaşık yapısı, özellikle büyük teknoloji şirketleri gibi özel aktörlerin ve bilgisayar korsanlarının yükselişiyle birlikte, uluslararası hukukun dijital çağda sorumluluk ve hesap verebilirlik kavramlarını nasıl şekillendireceğine dair daha incelikli ve bütüncül bir yaklaşımı zorunlu kılmaktadır.

Siber uzaya ilişkin yürütülen en önemli tartışmalardan biri, bu alana uluslararası hukuk kurallarının uygulanabilir olup olmadığı meselesidir. Kanaatimizce, uluslararası hukuk kurallarının siber uzaya uygulanabilirliğine dair herhangi bir hukuki engel bulunmamaktadır. Her ne kadar uluslararası hukuk kurallarının büyük bir kısmı, modern bilgisayar teknolojilerinin icadından çok önce gerek antlaşmalar gerekse uluslararası örf ve adet hukuku çerçevesinde geliştirilmiş olsa da, bu kurallar yalnızca kabul edildikleri dönemin koşullarıyla sınırlı değildir; aksine, zaman ve mekân bakımından genel geçer nitelikte olup devletlerin tüm faaliyet alanlarına uygulanabilir durumdadır.

Bu bağlamda, 1945 tarihli BM Şartı, 1949 tarihli Cenevre Sözleşmeleri ve Ek Protokolleri ile 2001 tarihli Taslak Maddeler gibi temel belgelerde yer alan ilkeler, yalnızca kabul edildikleri dönemin somut olaylarına değil, aynı zamanda uluslararası toplumun karşı karşıya kaldığı yeni meydan okumalar da dâhil olmak üzere, tüm devlet eylemlerine uygulanabilecek niteliktedir. Dolayısıyla, mevcut uluslararası hukuk kurallarının siber uzay bağlamında da geçerliliğini koruduğu hususunda herhangi bir tereddüt bulunmamaktadır.

Mevcut uluslararası hukuk çerçevesi esasen devletlerin ulusal sınırlarıyla sınırlı olduğu bir dünya düzenine uygun biçimde kurgulanmıştır. Bu nedenle, siber uzayın dinamik ve sınırları aşan gerçeklikleriyle uyum sağlamakta önemli güçlüklerle karşılaşılmaktadır. Çok uluslu büyük teknoloji şirketleri ve merkezi olmayan bilgisayar korsanları kolektifleri gibi yeni devlet

dışı aktörler, genellikle doğrudan devlet kontrolünün ötesinde faaliyet göstermelerine rağmen, uluslararası alanda kayda değer sonuçlar doğurabilmektedir. Bununla birlikte, siber uzaya ilişkin küresel ölçekte yeni normlar ve düzenlemelerin oluşturulması günümüz koşullarında oldukça düşük bir ihtimal olarak değerlendirilmektedir. Bu alanda bağlayıcı bir uluslararası hukuk belgesinin müzakere edilmesi yıllar sürebileceği gibi, böyle bir belgenin muhtemelen en düşük ortak paydada uzlaşılarak hazırlanacağı ve mevcut uluslararası hukuk kurallarına kıyasla daha zayıf koruma mekanizmaları içereceği öngörülmektedir. Ayrıca, bir antlaşmanın varlığı, onun yorumlanmasına ilişkin sorunları tamamen ortadan kaldırmamaktadır; uygulama mekanizmaları ve usulleri belirsiz kalabilir.

Siber uzaya ilişkin örf-adet hukukunun oluşumu da şu an için pek mümkün değildir. Bu alanda örf-adet hukukunun oluşabilmesi için yeterli düzeyde devlet uygulaması ve bu uygulamaların zorunluluk bilinciyle (*opinio juris*) gerçekleştirilmesi gerekmektedir. Siber saldırılar bağlamında bu koşulların yakın gelecekte sağlanması oldukça zordur. Bunun temel nedeni, birçok devletin siber saldırılarının yüksek seviyede gizlilikle yürütülmesi ve dolayısıyla diğer devletlerin gözleminden uzak olmasıdır. Bu bakımdan, görünmeyen veya tespit edilemeyen devlet uygulamalarının, yeni bir örf-adet hukukunun oluşumuna katkıda bulunması mümkün değildir. Ayrıca, devletler, diğer devletlerin gerçekleştirdiği siber saldırıları uluslararası hukuka aykırı olarak kınama konusunda genel bir isteksizlik sergilemektedir. Bu durum, örf-adet hukukunun oluşum sürecini daha da zorlaştırmaktadır.

Devletlerin siber uzaya ilişkin uluslararası hukuka dair pozisyonlarını netleştirmekte isteksiz olmalarının temel nedenlerinden biri, egemen eşitlik ilkesidir. Bu ilkeye göre, ortaya çıkan herhangi bir örf-adet kuralı tüm devletler açısından bağlayıcı olacaktır. Dolayısıyla devletler, diğer devletlerin hareketlerini kısıtlayan yeni bir normu kabul etmekle, kendi siber saldırılarına getirilecek kısıtlamalara razı olmak arasında kalmaktadır. Buna ek olarak, siber teknolojideki hızlı gelişmeler ve bu teknolojilerin gelecekte nasıl kullanılacağına dair belirsizlikler, devletlerin tereddütlerini artırmaktadır. Devletler, ileride daha faydalı olabilecek siber yeteneklere getirilecek kısıtlamalardan kazanç sağlayıp sağlamayacaklarını öngörememektedir. Bu durum, ulusal çıkarlar doğrultusunda diğer devletlerin siber saldırılarına karşı savunma ile kendi siber saldırılarını yürütme görevleri arasında kalan devlet kurumları arasında görüş ayrılıklarına yol açmaktadır. Tüm bu engeller ışığında, yeni uluslararası normların oluşması için gerekli hukuki görüşlerin yakın gelecekte netleşmesi beklenmemektedir.

Bu çalışma kapsamında tartışılan önemli hususlardan biri, yeni devlet dışı aktörlerin uluslararası hukuk kişiliğine sahip olup olmadıkları meselesidir. Zira bu aktörlerin fiillerinden

dolayı uluslararası hukuk bakımından sorumlu tutulabilmeleri, öncelikle onların uluslararası hukukun özneleri olarak kabul edilip edilmediklerine bağlıdır. Bu durum ise mevcut uluslararası hukuk literatüründe oldukça karmaşık ve yoğun tartışmalara konu olan bir mesele olarak öne çıkmaktadır. Çünkü geleneksel uluslararası hukuk, esas itibarıyla devlet merkezlidir ve devletleri uluslararası hukukun asli hak ve yükümlülüklerine sahip birincil özne olarak kabul etmektedir.

Bununla birlikte kanaatimizce, uluslararası hukuk kişiliği sabit ve değişmez bir statü değildir. Uluslararası hukukun özneleri, zaman içerisinde toplumun değişen ihtiyaçları ve uluslararası ilişkilerdeki dönüşümlere paralel olarak yeniden şekillenmektedir. Nitekim UAD'ye göre, bir varlığın uluslararası hukuk kişiliğine sahip olup olmadığının belirlenmesi yalnızca kurucu belgelerde açıkça belirtilip belirtilmediğine değil, aynı zamanda uluslararası toplumun işlevsel ihtiyaçlarına da bağlıdır. Bu bağlamda, İkinci Dünya Savaşı sırasında ve sonrasında yaşanan ağır insan hakları ihlalleri sonucunda gerçek kişilere doğrudan hakların tanınması, bu dönüşümün en çarpıcı örneklerinden biridir.

AİHS kapsamında bireylere tanınan bireysel başvuru hakkı ile Roma Statüsü çerçevesinde bireylerin uluslararası cezai sorumluluklarının tanınması, bireylerin uluslararası hukukun aktif özneleri haline geldiğini göstermektedir. Benzer şekilde, özel şirketler de özellikle devletlerle yapılan yatırım anlaşmaları ve *Birleşmiş Milletler İş Dünyası ve İnsan Hakları Rehber İlkeleri* çerçevesinde doğrudan hak ve yükümlülüklere sahip hale gelmişlerdir. Her ne kadar bu aktörlerin kişiliği devletlerinki kadar tam olmasa da, fiilen uluslararası hukuk kişiliğinin birçok unsurunu taşıdıkları açıktır.

Günümüzde bu şirketler yalnızca devletlerle değil, aynı zamanda uluslararası örgütler ve diğer özel aktörlerle de çeşitli düzeylerde uluslararası ilişkiler kurabilmektedir. Bu durum, 1933 tarihli Montevideo Sözleşmesi'nde devletlerin sahip olması gereken özelliklerden biri olarak belirtilen "diğer devletlerle ilişkiye girme yeteneği" ölçütünün artık yalnızca devletlerle sınırlı kalmayıp, uluslararası alanda faaliyet gösteren tüm aktörler için geçerli hale geldiğini göstermektedir. Bu bağlamda şirketler hem ulusal hem de uluslararası düzeyde sorumluluklar üstlenmekte ve giderek daha fazla uluslararası toplumun bir parçası olarak kabul edilmektedirler. Özellikle çevre hukuku ve insan hakları alanlarında çok uluslu şirketlerin doğrudan sorumluluğa tabi tutulmaları, bu gelişmenin somut bir yansımasıdır.

Sonuç olarak, uluslararası hukuk kişiliği artık sadece egemenliğe değil; bir varlığın uluslararası toplumla işlevsel düzeyde ilişki kurabilme yeteneğine göre değerlendirilmektedir. Bu çerçevede bireyler uluslararası mahkemelere başvurabilmekte, şirketler ise devletlerle sözleşmeler yaparak ve uluslararası normlara uyarak bu ilişkileri sürdürebilmektedir.

Dolayısıyla bu tür aktörler artık yalnızca pasif konumda yer alan nesneler değil, aksine uluslararası hukukta aktif roller üstlenen özneler olarak kabul edilmektedir.

Büyük teknoloji şirketleri küresel dijital altyapıdaki kritik rolleri nedeniyle uluslararası barış, güvenlik ve insan hakları üzerinde doğrudan kritik etkiye sahiptir. Bu aktörlerin hukuki kişiliklerinin tanınması, hesap verebilirliğin netleşmesini ve uluslararası toplumun bu aktörlere doğrudan yükümlülükler getirebilmesini kolaylaştıracaktır. Ayrıca, uluslararası örgütler, kurtuluş hareketleri ve bazı sivil toplum kuruluşları gibi devlet dışı aktörler, belirli antlaşmalar veya örf-adet kuralları çerçevesinde sınırlı da olsa uluslararası hukuk kişiliğine sahiptir. Bu kapsamda, büyük teknoloji şirketleri gibi özel şirketlere de benzer bir statü tanınması oldukça mantıklı bir gelişme olarak görülecektir. Ayrıca *BM İş ve İnsan Hakları Rehber İlkeleri*'ne baktığımızda bu İlkeler şirketlerin insan haklarına saygı gösterme sorumluluğunu vurgulamaktadır. Her ne kadar bu ilkeler bağlayıcı olmasa da özel aktörlerin uluslararası sorumluluklarının giderek kabul gördüğünü göstermektedir. Bunların yanı sıra, büyük teknoloji şirketlerinin doğrudan uluslararası yükümlülüklere tabi olmaması, düzenleme ve yaptırım açısından boşluklara neden olmakta, özellikle veri koruma, içerik denetimi ve siber güvenlik alanlarında zorluklara yol açmaktadır. Ayrıca bu şirketlerin jeopolitik etkisi, çoğu devletin gücünü aşmakta olup, bu aktörlerin uluslararası ilişkilerdeki rolünün hukuki olarak da tanınmasını gerektirmektedir.

Bu tez çalışması kapsamında tespit edilen hususlardan biri de siber suç, siber savaş ve siber saldırı kavramları arasındaki farklılıklardır. Bu üç kavram arasında açık bir ayrım yapılmaksızın gerçekleştirilecek değerlendirmeler, yeni devlet dışı aktörlerin fiillerine uygulanacak hukuk kurallarının belirlenmesini zorlaştıracaktır.

Bu bağlamda, siber saldırı, siyasi ya da ulusal güvenlik amacıyla bir bilgisayar ağının işlevini zayıflatmak amacıyla gerçekleştirilen aktif bir eylemdir. Siber savaş, siber saldırı unsurlarını taşımakla birlikte, devlet aktörleri tarafından gerçekleştirilen; konvansiyonel silahlı saldırıya eşdeğer etki doğuran ve silahlı çatışma bağlamında meydana gelen bir durumdur. Siber suç ise, genellikle devlet dışı aktörler tarafından işlenen ve ceza hukuku kurallarını ihlal eden fiillerden oluşur. Siber suç, siber saldırıdan farklı olarak her zaman ağ sistemine zarar verme amacı taşımaz; siyasi ya da ulusal güvenlik amacı gütmez ve daha çok ekonomik kazanç ya da kişisel çıkar sağlama amacına yöneliktir.

Siber uzaydaki yeni devlet dışı aktörlerin uluslararası hukuk kişisi olduklarına ilişkin bir düzenleme ya da yaygın bir kanaat olmasa da 2001 tarihli Taslak Maddelerin 5, 8 ve 11. maddeleri devlet dışı aktörlerin fiillerinin dolaylı da olsa sorumluluk oluşturduğunu kabul etmekte ancak sorumluluğu devlete atfetmektedir. Diğer bir ifadeyle Taslak Maddeler devlet

sorumluluğunun önceliğini korurken, devlet dışı aktörlerin karmaşık rolünü de yansıtmaktadır. Taslak Maddelerinin yeterli olmaması halinde özen yükümlülüğü ilkesi devreye girerek devletin sorumluluğunun göz ardı edilmesinin önüne geçmektedir. Aynı zamanda, BM Rehber İlkeleri ve Tallin Manual gibi yumuşak hukuk metinleri özel aktörlerin siber uzaydaki rollerine ve sorumluluklarına ilişkin gelişen yaklaşımı ortaya koymaktadır.

Siber uzayın karmaşık yapısı ve genellikle izlenebilirliğinin sınırlı olması nedeniyle, fiilleri doğrudan herhangi bir devlete atfedilemeyen yeni devlet dışı aktörler tarafından gerçekleştirilen haksız fiiller, uluslararası sorumluluk açısından önemli bir güçlük teşkil etmektedir. Daha açık bir ifadeyle, bu durum uluslararası hukuk ve devlet sorumluluğu bağlamında ciddi bir ikilem yaratmaktadır; çünkü açık bir atıf olmaksızın, zarar gören devletler karşı önlemler alma, meşru müdafaa hakkını kullanma veya egemenlik ihlalleri ve diğer uluslararası yükümlülükler için herhangi bir devleti sorumlu tutma konusunda sınırlı kalmaktadır. Buna karşın, mevcut uluslararası hukuk doktrini ve uygulaması, devlet dışı aktörlerin haksız fiillerinin doğrudan devlete atfedilememesi durumunda dahi, devletlerin sorumluluğunun veya en azından belirli yükümlülüklerinin ortaya çıkabileceği çeşitli mekanizmalar sunmaktadır.

Yukarıda da ifade edildiği üzere, bu tez çalışmasının araştırma sorusunun ilk aşaması; devlet dışı aktörlerin fiillerinin, Taslak Maddeler'in 4, 5, 8 ve 11. maddeleri ile "etkin kontrol" ve "genel kontrol" testleri kapsamında doğrudan devlete atfedilemediği durumlarda, ortaya çıkan devlet sorumluluğu boşluğunun nasıl doldurulacağıdır. Bu boşluğu gidermek amacıyla, çalışmamızda "özel yükümlülük ilkesi"ne başvurulmuştur. Bu ilke; doğrudan atfın mümkün olmadığı hâllerde, devletlerin kendi ülkelerinde gerçekleşen haksız fiillerin faillerinin doğrudan kontrolü veya yönlendirmesi altında olup olmadığına bakılmaksızın, bu fiilleri engellemeye yönelik makul ve etkili önlemleri alma yükümlülüğünü ifade etmektedir. Söz konusu fiillerin kapsamına, uluslararası hukuka aykırı siber saldırılar da dâhildir.

Bu çerçevede, siber uzayda devlet dışı aktörler tarafından başka bir devlete yönelik olarak gerçekleştirilen zararlı eylemler karşısında, söz konusu faaliyetin kaynağının devlet tarafından bilinebilir nitelikte olması ve devletin bu faaliyetleri engelleme kapasitesine sahip bulunması hâlinde özen yükümlülüğü doğmaktadır. Eğer devlet, bu tür siber eylemlere bilerek sessiz kalır ya da etkili önlemler almazsa, uluslararası sorumluluğu gündeme gelebilir.

Bu bağlamda, daha önce belirtilen Google vakası örnek olarak gösterilebilir. Dönemin ABD Dışişleri Bakanı Hillary Clinton tarafından yapılan açıklamalar, Google'ın Mısır'daki faaliyetlerine göz yumulduğunu ve bu faaliyetlerin olumlu karşılandığını göstermektedir. Bu durum, ABD'nin sorumluluğunu gündeme getirmiştir.

Araştırma sorusunun ikinci aşaması ise "Devlet dışı aktörlerin doğrudan sorumluluğu mümkün müdür?" sorusuna odaklanmaktadır. Zira mevcut uluslararası hukuk kuralları, devlet dışı aktörlerin sorumluluğunu açıkça düzenlememektedir. Ancak kanaatimizce, devlet dışı aktörlerin doğrudan sorumluluğu mümkündür. Bu çalışmada önerdiğimiz "fonksiyonel egemenlik" yaklaşımı, söz konusu boşluğun giderilmesi bakımından bir çözüm sunmaktadır. Bu yaklaşıma göre, bir devlet dışı aktör siber uzayda egemen bir devlet gibi hareket ediyorsa, daha açık bir ifadeyle veri erişimini kontrol ediyor, haklara müdahale ediyor, norm koyuyor veya zorlayıcı güç kullanıyorsa, bu aktör artık doğrudan sorumlu tutulmalıdır. Roma Statüsü'ndeki bireysel sorumluluk anlayışı, Birleşmiş Milletler İş Dünyası ve İnsan Hakları Rehber İlkeleri ile özel sektöre yönelik özen yükümlülüğü örnekleri bu yaklaşımın hukuki temelini oluşturmaktadır. Böylece yalnızca devletlere değil, dijital alanda fiilen güç kullanan özel aktörlere de uluslararası hukuk çerçevesinde sorumluluk yüklenebilmesi mümkün hâle gelmektedir.

Sonuç olarak, burada ele alınan kural ve ilkeler, siber uzay gibi yeni ve dinamik bir alanda dahi, özel bir düzenleme yapılmaksızın mevcut uluslararası hukuk normlarının uygulanarak devlet sorumluluğunun tesis edilebileceğini ortaya koymaktadır. Mevcut uluslararası hukuk, devletlerin kendi yetki alanlarında bulunan veya faaliyet gösteren devlet dışı aktörler üzerinde doğrudan kontrol sahibi olmadıkları iddiasıyla sorumluluktan kaçamayacaklarını açıkça hükme bağlamaktadır. Bu bağlamda, doğrudan atıf mekanizması devletin uluslararası haksız fiillerden doğan sorumluluğunun "altın standardı" olmaya devam etmekle birlikte, özen yükümlülüğü ilkesi ve ilgili diğer kurallar, modern siber çatışmaların karmaşık yapısı içinde uluslararası hukuk düzeninin sürekliliğinin sağlanmasında temel araçlar olarak işlev görmektedir.

KAYNAKLAR

Acer, Yücel – Kaya, İbrahim, *Uluslararası Hukuk: Temel Ders Kitabı İngilizce Özetli*, 10. Baskı, Ankara: Seçkin Yayınevi, 2013.

Aksar, Yusuf. *Temel Metin ve Davalarla Uluslararası Hukuk.* Ankara: Seçkin Yayınevi, 2017.

Addo, Michael K. (ed.), *Human Rights Standards and the Responsibility of Transnational Corporations*, Netherlands: Kluwer Law International, 1999.

Ago, Roberto, "Fourth Report on State Responsibility", *Yearbook of the International Law Commission* 2 (1972), 99, UN Doc A/CN.4/264 ve Ek.

Ago, Roberto, "Third Report on State Responsibility by Special Rapporteur", *Yearbook of the International Law Commission*, 1971, Cilt 2, Bölüm 1.

Akande, Dapo, "Classification of Armed Conflicts: Relevant Legal Concepts", *International Law and the Classification of Conflicts*, ed. Christine Chinkin – Mary Kaldor, Oxford: Oxford University Press, 2012.

Aksar, Yusuf, *Teoride ve Uygulamada Uluslararası Hukuk II*, 2. Baskı, Ankara: Seçkin Yayınevi, 2013.

Andress, Jason, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2. Baskı, Syngress, 2013.

Anzilotti, Dionisio, *Cours de droit international*, traduction française d'après la troisième édition italienne par Gilbert Gidel, Paris: Recueil Sirey, 1929.

Armağan, Merve İ., *Uluslararası Hukukta Çok Uluslu Şirketler ve İnsan Hakları Yükümlülükleri*, İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2019.

Arora, Prachi – Poojary, Mishita – Patel, Ishita, "A Review Paper on White Hat Hackers". *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* 12/1 (Aralık 2021), 283-290.

Arora, Ritika – Behal, Sunny, "IP Spoofing". *Shaheed Bhagat Singh College of Engineering,* (Ocak 2010), 2-15.

ARS, Responsibility of States for Internationally Wrongful Acts. Birleşmiş Milletler: Genel Kurul, 2001.

Arthur Young and Co. v. Islamic Republic of Iran (Arthur Young), K. 338-484-1 (1 Aralık 1987), *Iran–United States Claims Tribunal Reports* 17 (1987), 245-270.

Aslan, Ömer, "A Methodology to Detect Distributed Denial of Service Attacks". *Bilişim Teknolojileri Dergisi* 15/2 (Nisan 2022), 150-160.

Aslay, Fulya, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi". *International Journal of Multidisciplinary Studies and Innovative Technologies* 1/1 (2017), 26-35.

Avrupa İnsan Hakları Mahkemesi (AİHM), *Al-Skeini ve Diğerleri / Birleşik Krallık*, Karar, B. No: 55721/07, *Raporlar* 2011-IV, para. 135.

Avrupa İnsan Hakları Mahkemesi (AİHM), *Banković ve Diğerleri / Belçika ve Diğerleri*, B. No: 52207/99.

Babacan, Kazım – Tam, Mehmet Sinan, "The Information Warfare Role of Social Media: Fake News in the Russia - Ukraine War". *Erciyes İletişim Dergisi* 3 (Ekim 2022), 77-89.

Bakshi, Bipin, "Information Warfare: Concepts and Components". *International Journal of Research and Analytical Reviews* 5/4 (Kasım 2022), 178-185.

Banks, William C., "Cyber Espionage And Electronic Surveillance: Beyond The Media Coverage". *Emory Law Journal* 66/513 (2017), 513-550.

Bannelier, Karine – Christakis, Théodore, *"Cyber-Attacks–Prevention-Reactions: The Role of States and Private Actors". Les Cahiers de la Revue Défense Nationale* (2017), 1-86.

Bannelier-Christakis, Karine, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?". *Baltic Yearbook of International Law* 14 (2015), 23-40.

Barata, N. J., *Patriotic Hackers: Non-State Actors Fighting Wars for States*, Aveiro: University of Aveiro, 2015.

Barlow, John Perry, "A Declaration of the Independence of Cyberspace". *Electronic Frontier Foundation (EFF)*, (1996).

Barrett, Brian, "America's Electronic Voting Machines Are Scarily Easy Targets". *WIRED*, (2016).

Basharat, Asma - Sirhindi, Rabia - Cheema, Ahmad Raza Khokhar, Imtiaz, "A Novel Solution for IP Spoofing Attacks". *6th WSEAS International Conference on Information Security and Privacy,* 100-109.

Becker, Tal, *Terrorism and the State: Rethinking the Rules of State Responsibility*, Kuzey Amerika: Hart Publishing, 2017.

Bhavsar, Vaishnavi Kadlak - Aditya Sharma, Shabnam, "Study on Phishing Attacks", *International Journal of Computer Applications* 182/33 (Aralık 2018), 27-33.

Bianchi, Andrea (ed.), *Non-State Actors and International Law*, İngiltere: The Library of Essays in International Law, 2009.

Bidgoli, Hossein (ed.), *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications*, New Jersey–Canada: John Wiley and Sons, 2008.

Birleşmiş Milletler (BM), *Report of the Sub-Committee on State Responsibility (1963). Yearbook of the International Law Commission*, Cilt 2, 227. UN Doc A/CN.4/152.

Birleşmiş Milletler (BM), *Case Concerning the Differences between New Zealand and France Arising from the Rainbow Warrior Affair* (1990), 19 *Reports of International Arbitral Awards*, 199–201.

Birleşmiş Milletler Genel Kurulu, Genel Kurul Kararı 799 (VIII), 8. Sessiyon, Ek No 17, Birleşmiş Milletler Belgesi A/799 (1953).

Birleşmiş Milletler Güvenlik Konseyi (BMGK), Letter Dated 15 June 1960 from the Representative of Argentina Addressed to the President of the Security Council, UN Doc S/4336 (1960).

Birleşmiş Milletler Güvenlik Konseyi (BMGK), Question Relating to the Case of Adolf Eichmann, UNSC Resolution S/RES/138 (1960).

Birleşmiş Milletler Uluslararası Hukuk Komisyonu (BMUHK), *Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Sorumluluğuna İlişkin Taslak Maddeler*, 2001.

Birleşmiş Milletler, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", A/RES/73/266, 2 Ocak 2019.

Blackstone, William, *Commentaries on the Laws of England*, cilt 4, der. W. Morrison, London: Cavendish, 2001.

Blume, Peter, "Data Protection and Privacy: Basic Concepts in a Changing World". *Scandinavian Studies in Law* 56 (2010), 151-154.

BM-UAM, Birleşmiş Milletler Uluslararası Adalet Mekanizması. *Poglioli Davası (İtalya / Venezuela). Reports of International Arbitral Awards*, Cilt 10, 669, 689.

BM-UHK, Birleşmiş Milletler – Uluslararası Hukuk Komisyonu. F. V. García Amador, "First Report on State Responsibility", *Yearbook of the International Law Commission*, Cilt 2 (1956), Belge A/CN.4/96.

Bodansky, Daniel M. - Cook, John R., "Symposium: The ILC's State Responsibility Articles". *American Journal of International Law* 96/4 (2002), 780-790.
Borchard, Edwin. *The Diplomatic Protection of Citizens Abroad*. New York: Banks Law Publishing, 1915.
Borchard, Edwin. The Diplomatic Protection of Citizens Abroad. New York: Banks Law Publishing, 1915.
Bozkurt, Enver – Poyraz, Yasin – Erdal, Selcen, *Devletler Hukuku*, 11. Baskı, Ankara: Yetkin Yayınları, 2021.
Brenner, Susan W. - Carrier, Brian - Henninger, Jef, "The Trojan Horse Defense in Cybercrime Cases". *The Santa Clara High Technology Law Journal* 21/1 (2004), 5-30.
Brower, Charles Nelson - Brueschke, Jason D., *The Iran–United States Claims Tribunal*, The Hague: Nijhoff, 1998.
Brownlie, Ian, "The Responsibility of States for the Acts of International Organizations". In *International Responsibility Today: Essays in Memory of Oscar Schachter*, ed. Maurizio Ragazzi, Leiden/Boston: Martinus Nijhoff Publishers, 2005.
Brownlie, Ian, *Brownlie's Principles of Public International Law*, edited by James Crawford, 8th ed., Oxford: Oxford University Press, 2012.
Brownlie, Ian, *Principles of Public International Law*, 7. Baskı, Oxford: Oxford University Press, 2008.
Brownlie, Ian, *System of the Law of Nations: State Responsibility Part I*, Oxford: Clarendon Press, 1983.
Brunnée, Jutta, "The Meaning of Armed Conflict and the Jus ad Bellum". In *What Is War? An Investigation in the Wake of 9/11*, edited by Mary Ellen O'Connell, Leiden: Martinus Nijhoff Publishers, 2012.
Brunnée, Jutta, "The Meaning of Armed Conflict and the Jus ad Bellum". In *What Is War? An*
Buchan, Russell, "Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm". *Journal of Conflict and Security Law* 21 (2016), 429–453.
Burgess, Jean - Marwick, Alice - Poell, Thomas, *The SAGE Handbook of Social Media*, London, 2020.
Burgess, Jean Marwick, Alice Poell, Thomas, "Regulation of and by Platforms". *The SAGE Handbook of Social Media*, London, 254–278.
Caron, David D., "Attribution Amidst Revolution: The Experience of the Iran–United States Claims Tribunal". *American Society of International Law Proceedings* 84 (1990).
Castells, Manuel, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, New York: Oxford University Press, 2001.
Cerone, John, "Out of Bounds? Considering the Reach of International Human Rights Law". *Center for Human Rights and Global Justice Working Paper* 5 (2006).
Chalmers, J., "State Responsibility for Acts of Parastatals Organized in Corporate Form". *American Society of International Law Proceedings* 84 (1990).
Cheng, Bin, *General Principles of Law as Applied by International Courts and Tribunals*, London: Cambridge, 1953.
Chirwa, Danwood Mzikenge, "The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights". *Melbourne Journal of International Law* 5 (2004).
Civuli, Abdulla - Luma-Osmani, Shkurte - Rufati, Eip - Arifi, Gjulie, "Cyber Espionage Consequences As A Growing Threat". *Journal of Natural Sciences and Mathematics of UT* 7/13-14 (2022).
Clapham, Andrew, *Human Rights in Private Sphere*, Oxford: Clarendon Press, 1999.
Clausewitz, Carl von, *On War*, çev. Michael Howard – Peter Paret, New Jersey: Princeton University Press, 1989.

Cohen, Alexander F. "Cosmos 954: The International Law of Satellite Accidents". *International Incidents: The Law That Counts in World Politics*. Ed. W. Michael Reisman ve Andrew R. Willard. 68–84. Princeton: Princeton University Press, 1. Basım, 1988.

Cohen, Daniel - Bar'el, Ofir, "The Use of Cyberwarfare in Influence Operations". *Yuval Ne'eman Workshop for Science, Technology and Security,* 7-15.

Cohen-Almagor, Raphael, "Internet History". *International Journal of Technoethics* 2/2 (Nisan–Haziran 2011).

Coleman, Gabriella, "The Anthropology of Hackers". *The Atlantic*. 21 Eylül 2010.

Commission of the European Communities, "Critical Infrastructure Protection in the fight against terrorism". COM (2004) 702 final, Brüksel, 20 Ekim 2004.

Comninos, Alex, "Twitter revolutions and cyber crackdowns: User-generated content and social networking in the Arab spring and beyond". Association for Progressive Communications (APC), Haziran 2011.

Confessore, Nicholas, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far". *The New York Times*, (2018).

Coomans, Fons – Kamminga, Menno T. (eds.), *Extraterritorial Application of Human Rights Treaties*, Antwerp: Intersentia, 2004.

Cordey, Sean, "Cyber Influence Operations: An Overview and Comparative Analysis". *Center for Security Studies (CSS),* (Ekim 2019), 4-10.

Corn, Gary P. – Taylor, Robert, "Sovereignty in the Age of Cyber". *AJIL Unbound* 111 (2017), 207–212.

Corten, Olivier, *The Law against War: The Prohibition on the Use of Force in Contemporary International Law*, Oxford: Hart Publishing, 2010.

Council of the European Union (AB Konseyi), *Independent International Fact-Finding Mission on the Conflict in Georgia* (Brüksel: Council of the European Union, 2009), 1-439.

Crawford, James, "First Report on State Responsibility". BM Dokümanı A/CN.4/490/Add.5, 1998.

Crawford, James, *Les Articles de la C.D.I. sur la Responsabilité de l'État*, Paris: Pédone, 2004.

Crawford, James, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*, Cambridge: Cambridge University Press, 2002.

Curran, James-Seaton, Jean, *Power Without Responsibility: Press, Broadcasting and the Internet in Britain*, London: Routledge, 2009.

Cylinder, Harry, "A Brief History of Cyber-Espionage". *The Baecon Group of Companies*, (Ocak 2021).

Czosseck, Christian – Geers, Kenneth, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam: IOS Press, 2009.

Çatlı, Mehmet. *Dijital Devlet Teorisi.* Ankara: Adalet Yayınevi, 2.Basım, 2021.

Daimî Adalet Divanı (PCIJ), *Home Frontier and Foreign Missionary Society of the United Brethren in Christ v. United Kingdom*, K. Yok (1920), *Reports of International Arbitral Awards* 6, 44.

Darıcılı, Ali Burak – Özdal, Barış, "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi". *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi* 4/1 (Şubat 2017), 20-40.

Deva, Surya. "Treating Human Rights Lightly: A Critique of the Consensus Rhetoric and The Language Employed by the Guiding Principles". *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?*. ed. Surya Deva ve David Bilchitz. 78-94. Cambridge: Cambridge University Press, 2013.

de Aréchaga, E. J., "International Responsibility". In *Manual of Public International Law*, edited by M. Sørensen, 531-558, New York, NY: St Martin's Press, 1968.
de Hoogh, A. J. J., "Articles 4 and 8 of the 2001 ILC Articles on State Responsibility, The Tadić Case and Attribution of Acts of Bosnian Serb Authorities to the Federal Republic of Yugoslavia". *British Yearbook of International Law* 72 (2001), 255-271.
de Hoogh, André, "Georgia's Short-Lived Military Excursion into South Ossetia: The Use of Armed Force and Self-Defence". *EJIL: Talk!*, (Aralık 2009).
Delerue, François, *Cyber Operations and International Law*, Cambridge: Cambridge University Press, 2020.
Denning, Dorothy E., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", In *Networks and Netwars*, ed. John Arquilla - David Ronfeldt, Santa Monica, California: RAND Corporation, 1999.
Denning, Dorothy E. "The Ethics of Cyber Conflict". The Handbook of Information and Computer Ethics, ed. Kenneth Einar Himma ve Herman T. Tavani (Hoboken, NJ: John Wiley & Sons, 2008)
Developments in the Field of Information and Telecommunications in the Context of International Security, *United Nations General Assembly A/RES/73/27*, 11 Aralık 2018.
Dilek, Esma - Talih, Özgür - Bensghir, Türksel Kaya, "Estonya 2007 Siber Saldırılarının İncelenmesi ve Ülkelerin Ulusal Siber Güvenlik Politikalarına Etkileri", *Bilgi Yönetimi Dergisi* 6/2 (Aralık 2023).
Dinniss, Heather Harrison, *Cyber Warfare and the Laws of War*, Cambridge: Cambridge University Press, 2012, 37-75.
Dinstein, Yoram, *War, Aggression and Self-Defence*, 5. Baskı, Cambridge: Cambridge University Press, 2011.
DoD, Department of Defense. *The National Military Strategy for Cyber Operations*. Washington, D.C.: Chairman of the Joint Chiefs of Staff, [Basım Yılı Yok]. Erişim 7 Haziran 2023. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.
Dugard, John (ed.), *International Law – A South African Perspective*, Lansdowne: Juta Law, 2001.
Dülger, Kenan, *Devletin Uluslararası İnsancıl Hukukun İhlalinden Doğan Sorumluluğu*, İstanbul: İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, 2014.
Eagleton, Clyde, "Measure of Damages in International Law". *Yale Law Journal* 39 (1929-30).
Eagleton, Clyde, *The Responsibility of States in International Law*, New York: NYU Press, 1928.
Eckert, Amy, "The Nonintervention Principle and International Humanitarian Interventions". *International Legal Studies* 7 (2001).
Economist, The, "Cyberwar: War in the Fifth Domain". 1 Temmuz 2010.
Egan, Brian J., "International Law and Stability in Cyberspace". *Berkeley Journal of International Law* 35/1 (2017), 169-180.
Elleithy, Khaled M. - Blagovic, Drazen - Cheng, Wang - Sideleau, Paul, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", *Journal of Systemics Cybernetics and Informatics* 3/1 (Ocak 2006).
Eriksson, E. Anders, "Information Warfare: Hype Or Reality?". *The Nonproliferation Review* 6/63 (Spring-Summer 1999), 60-61.
Evans, Malcolm D. (ed.), *International Law*, Oxford: Oxford University Press, 2006.
Faesen, Louk – Sweijs, Tim – Klimburg, Alexander – Tesauro, Giulia, "The Promises and Perils of a Minimum Cyber Deterrence Posture". Hague Centre for Strategic Studies, 2022.

Feng, Shuai, "The Principle of Sovereignty and Its Competitors: Order Construction and Evolutionary Logic of Digital Space". *Russian, East European and Central Asian Studies* 04 (2022), 96–119.
Fischerkeller, Michael P., "Current International Law Is Not an Adequate Regime for Cyberspace". *Lawfare*, (22 Nisan 2021).
Frank, Tenney, "The Status of Actors at Rome". *The University of Chicago Press* 26/1 (Mart 2024), 12-16.
Fuchs, Christian, "The Digital Labour Theory of Value and Karl Marx in the Age of Facebook, YouTube, Twitter, and Weibo". *Reconsidering Value and Labour in the Digital Age* (2015), 26-27.
Fukuyama, Francis, *The Origins of Political Order: From Prehuman Times to the French Revolution*, Farrar, Straus and Giroux, Kindle Edition, chapter 18.
Gervais, Daniel J. "The Regulation of Inchoate Technologies". Houston Law Review 47 (2010), 665-705.
Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, 25 September 1997, ICJ Reports 1997, No. 7.
Gabriel, Rachel A. - Koven, Barnett S., *Malicious Non-State Actors and Contested Space Operations*, Office of University Programs and DoD Strategic Multilayer Assessment Branch, 2018.
Gallais, C. - Filiol, E., "Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure". *Journal of Information Warfare* 16/1 (2017).
García Amador, FV, First Report on State Responsibility (1956), *Yearbook of the International Law Commission* 2, 104, 182, UN Doc A/CN.4/96.
García Amador, FV, Second Report on State Responsibility (1957), *Yearbook of the International Law Commission* 2, 104, 121, UN Doc A/CN.4/106.
Geneva Conventions I to IV, Protocol Additional to the Geneva Conventions.
Ghappour, Ahmed, "Tallinn, Hacking, and Customary International Law". *AJIL Unbound* 111 (2017), 224–228.
Gibson, William, *Burning Chrome*, New York: Omni Publications International Ltd., 1982.
Gibson, William, *Neuromancer*, Londra: Gollancz, 2016.
Gill, Terry D. and Kinga Tibori-Szabó, *The Use of Force and the International Legal System*, Cambridge: Cambridge University Press, 2023.
Ginsburg, Tom, "Introduction to Symposium on Sovereignty, Cyberspace - Tallinn Manual 2.0". *AJIL Unbound* 111 (2017).
Goldsmith, Jack, "Yet More Thoughts on the DNC Hack: Attribution and Precedent". *Lawfare*, (Temmuz 2016).
Gray, Christine, "The International Court of Justice". *British Yearbook of International Law* 59, 1 (1988).
Gray, Christine, *International Law and the Use of Force*, Oxford: Oxford University Press, 2008.
Greenberg, Andy, "Hackers Remotely Kill a Jeep on the Highway – With Me in It". *WIRED*, 21 Temmuz 2015.
Greitzer, Frank L. - Moore, Andrew P. - Cappelli, Dawn M. - Andrews, Dee H. - Carroll, Lynn A. - Hull, Thomas D., "Combating the Insider Cyber Threat", *IEEE Security and Privacy* 6/1 (Ocak-Şubat 2008).
Griebel, Jorn - Plücken, Milan, "New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia". *Leiden Journal of International Law* 21 (2008).

Griebel, Jorn - Plücken, Milan, "New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia". *Leiden Journal of International Law* 21 (2008).
Greenwood, Christopher. "State Responsibility and Civil Liability for Environmental Damage Caused by Military Operations." *International Law Studies* 69 (1993), 397-415. Erişim 14 Temmuz 2025. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1521&context=ils
Grotius, Hugo, *De Jure Belli Ac Pacis*, c. 2, çev. JB Scott (1646).
Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, *United Nations General Assembly A/76/135*, 14 Temmuz 2021.
Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *United Nations General Assembly A/65/201*, 30 Temmuz 2010.
Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *United Nations General Assembly A/68/98*, 24 Haziran 2023.
Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly A/70/174, 22 Temmuz 2015.
Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly A/70/174, 22 Temmuz 2015.
Gu, Hongfei. "Data, Big Tech, and the New Concept of Sovereignty". *Journal of Chinese Political Science,* 1-22.
Gu, Hongfei. "Data, Big Tech, and the New Concept of Sovereignty". *Journal of Chinese Political Science,* 1-22.
Hacquebord, Feike, "Two Years of Pawn Storm: Examining an Increasingly Relevant Threat". *Cyentia Cybersecurity Research Library*. Erişim 11 Şubat 024. https://www.isnadsistemi.org/guide/isnad2/isnad-dipnotlu/14-makale/14-5-makale-internette/
Hacquebord, Feike. "Void Balaur: Tracking a Cybermercenary's Activities". Texas: Trend Micro Research, 2021.
Hacquebord, Feike. *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat*, A Trend Micro Research Paper, 2017.
Hacquebord, Feike. Two Years of Pawn Storm: Examining an Increasingly Relevant Threat. A Trend Micro Research Paper, 2017.
Hacquebord, Feike. *Void Balaur: Tracking a Cybermercenary's Activities,* Texas: Trend Micro Research, 2021.
Hakım, Danny - Rosenberg, Matthew, "Data Firm Tied to Trump Campaign Talked Business With Russians", *The New York Times*. Erişim 18 Şubat 2024. https://www.isnadsistemi.org/guide/isnad2/isnad-dipnotlu/14-makale/14-5-makale-internette/
Hakım, Danny - Rosenberg, Matthew. "Data Firm Tied to Trump Campaign Talked Business With Russians". *The New York Times,* (Mart 2018).
Hakım, Danny-Rosenberg, Matthew. "Data Firm Tied to Trump Campaign Talked Business With Russians". *The New York Times,* (18 Mart 2018).
Hall, W. *A Treatise on International Law,* 2. baskı. Oxford: Clarendon Press, 1884.
Hall, W. A Treatise on International Law. Oxford: Clarendon Press, 1884.

Hampson, Françoise. "The Scope of the Extra-Territorial Applicability of International Human Rights Law." *The Delivery of Human Rights: Essays in Honour of Professor Sir Nigel Rodley*. ed. Françoise Hampson, Geoff Gilbert ve Clara Sandoval, 157-182. Londra: Routledge, 2011.

Hampson, Françoise. *The Scope of the Extra-Territorial Applicability of International Human Rights Law,* 1.baskı, İngiltere: Routladge, 2014.

Handler, Stephanie Gosnell, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare". *Stanford Journal of International Law* 48/1 (2012), 209-237. https://www.researchgate.net/publication/297562769_The_new_cyber_face_of_battle_Developing_a_legal_approach_to_accommodate_emerging_trends_in_warfare

Handler, Stephanie Gosnell. "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare." *Stanford Journal of International Law* 48 (2012), 226-227.

Handler, Stephanie Gosnell. "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare". *Stanford Journal of International Law.* 48 (2012), 209-237.

Harris, Shane - Nancy A. Youssef, "FBI Suspects Russia Hacked DNC; U.S. Officials Say It Was to Elect Donald Trump". *The Daily Beast*. Erişim 10 Mart 2024. https://www.thedailybeast.com/fbi-suspects-russia-hacked-dnc-us-officials-say-it-was-to-elect-donald-trump/

Harris, Shane and Nancy A. Youssef. "FBI Suspects Russia Hacked DNC; U.S. Officials Say It Was to Elect Donald Trump." *The Daily Beast,* (Temmuz 2016).

Harris, Shane and Nancy A. Youssef. "FBI Suspects Russia Hacked DNC; U.S. Officials Say It Was to Elect Donald Trump". *The Daily Beast.* (Temmuz 2016).

Holt, Thomas J. - Schell, Brent H., "Patriotic Hackers: Cyber Warriors Defending Their Homeland". *Journal of Cybersecurity Studies* (2015), Erişim 13 Temmuz 2025.

Hathaway, Oona A. - Crootof, Rebecca - Levitz, Philip - Nix, Haley - Nowlan, Aileen - Perdue, William – Spiegel, Julia. "The Law of Cyber-Attack". *California Law Review* 100/4 (Ağustos 2012), 817-886.

Hathaway, Oona A. - Crootof, Rebecca - Levitz, Philip - Nix, Haley - Nowlan, Aileen - Perdue, William – Spiegel, Julia. "The Law of Cyber-Attack". *California Law Review*. 100/4 (Ağustos 2012), 817-886.

Hathaway, Oona A. – Crootof, Rebecca – Levitz, Philip – Nix, Haley – Nowlan, Aileen – Perdue, William – Spiegel, Julia, "The Law of Cyber-Attack". *California Law Review* 100/4 (Ağustos 2012), 817-886. https://openyls.law.yale.edu/server/api/core/bitstreams/a060f74f-2469-4435-bada-cebc181ea9c4/content.

Heintschel von Heinegg, Wolff, "Chapter 1: The Tallinn Manual and International Cyber Security Law". *Yearbook of International Humanitarian Law* 15 (2012), 13-14.

Heintschel von Heinegg, Wolff, "Territorial Sovereignty and Neutrality in Cyberspace". *International Law Studies* 89 (2013), 123-156. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1027&context=ils

Heintschel von Heinegg, Wolff. "Chapter 1: The Tallinn Manual and International Cyber Security Law." *Yearbook of International Humanitarian Law* 15 (2012).

Heintschel von Heinegg, Wolff. "Chapter 1: The Tallinn Manual and International Cyber Security Law". *Yearbook of International Humanitarian Law*. 15 (2012), 3-18.

Heintschel von Heinegg, Wolff. "Territorial Sovereignty and Neutrality in Cyberspace". *International Law Studies* 89 (2013).

Heintschel von Heinegg, Wolff. "Territorial Sovereignty and Neutrality in Cyberspace". *International Law Studies*. 89 (2013), 123-156.
Hennessey, Susan, "What Does the US Government Know about Russia and the DNC Hack?". *Brookings*. Erişim 10 Ocak 2024. https://www.brookings.edu/articles/what-does-the-u-s-government-know-about-russia-and-the-dnc-hack/
Hennessey, Susan. "What Does the US Government Know about Russia and the DNC Hack?" *Lawfare,* (Temmuz 2016).
Hennessey, Susan. "What Does the US Government Know about Russia and the DNC Hack?" *Lawfare.* (Temmuz 2016).
Henych, Mark – Holmes, Stephen – Mesloh, Charles, "Cyber Terrorism: An Examination of the Critical Issues". *Journal of Information Warfare* 2/2 (2003), 1-14. https://www.jstor.org/stable/26502764?seq=1
Henych, Mark - Holmes, Stephen - Mesloh, Charles. "Cyber Terrorism: An Examination of the Critical Issues". *Journal of Information Warfare* 2/2 (2003).
Henych, Mark-Holmes, Stephen-Mesloh, Charles. "Cyber Terrorism: An Examination of the Critical Issues". *Journal of Information Warfare*. 2/2 (2003), 1-14.
Hersch Lauterpacht, "The Subjects of International Law", *International Law. Being the Collected Papers of Hersch Lauterpacht, Volume I: The General Works*, ed. E. Lauterpacht (Cambridge: Cambridge University Press, 1970), 136–150; aktaran Andrea Bianchi (ed.), *Non-State Actors and International Law* (Londra: Routledge, 2009).
Hessbruegge, Jan, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law". *New York University Journal of International Law and Politics* 36/4 (2004), 1-33. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2408953
Hessbruegge, Jan. "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law". *New York University Journal of International Law and Politics* 36/4 (2004), 276-79.
Hessbruegge, Jan. "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law". *New York University Journal of International Law and Politics*. 36/4 (2004), 1-32.
Higgins, Rosalyn. Problems and Process: International Law and How We Use It. Oxford: Oxford University Press, 1995.
Higgins, Rosalyn. Problems and Process: International Law and How We Use It. Oxford: Oxford University Press, 1995.
Higgins, Rosalyn. *Problems and Process: International Law and How We Use It*. Oxford: Oxford University Press, 1995.
Hilt v. Islamic Republic of Iran (Hilt), K. 354-10427-2 (16 Mart 1988), Iran–United States Claims Tribunal Reports 18 (1988).
Hochwald, Thorsten. "How Do Social Media Affect Intra-State Conflicts other than War?". *Connections* 12/3 (2013).
Hochwald, Thorsten. "How Do Social Media Affect Intra-State Conflicts other than War?". *Connections*.12/3 (2013), 9-38.
Hollis, Duncan B. "Russia and the DNC Hack: What Future for a Duty of Non-intervention?". *Opinio Juris,* (Temmuz 2016).
Hollis, Duncan B. "Russia and the DNC Hack: What Future for a Duty of Non-intervention?". *Opinio Juris,* (Temmuz 2016).
Hollis, Duncan B. "Why States Need an International Law for Information Operations". *Lewis and Clark Law Review* 11/4 (2007), 1023-1061.
Hollis, Duncan B. "Why States Need an International Law for Information Operations". *Lewis and Clark Law Review*. 11/4 (2007), 1023-1061.

Hollis, Duncan B., "Russia and the DNC Hack: What Future for a Duty of Non-intervention?". *Opinio Juris*. Erişim 20 Nisan 2024. https://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention/
Hollis, Duncan B., "Why States Need an International Law for Information Operations". *Lewis and Clark Law Review* 11/4 (2007), 1023-1061. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1083889
Holmes, David, *Virtual Globalization: Virtual Spaces/Tourists Spaces*, London: Routledge, 2001.
Holmes, David. Virtual Globalization: Virtual Spaces/Tourists Spaces. London: Routledge, 2001.
Holmes, David. Virtual Globalization: Virtual Spaces/Tourists Spaces. London: Routledge, 2001.
Home Frontier and Foreign Missionary Society of the United Brethren in Christ v. United Kingdom (1920), R. Intl Arb. Awards 6, 44.
Human Rights Watch. "Video Unavailable – Social Media Platforms Remove Evidence of War Crimes." Erişim 13 Şubat 2024.
Hunker, Jeffrey – Margulies, Joseph – Hutchinson, Bonnie, *Role and Challenges for Sufficient Cyber-Attack Attribution* (2008). https://www.osti.gov/servlets/purl/1140596
Hunker, Jeffrey - Margulies, Joseph - Hutchinson, Bonnie. Role and Challenges for Sufficient Cyber-Attack Attribution, *Sandia National Laboratories*. 2008, 1-12.
Hunker, Jeffrey, Joseph Margulies ve Bonnie Hutchinson, "Role and Challenges for Sufficient Cyber-Attack Attribution," Sandia National Laboratories, SAND2011-0070C, 2008.
Hyatt International Corporation v. The Government of the Islamic Republic of Iran, Iran-U.S. C.T.R., c. 9, 1985.
Hyde, Charles. "Concerning Damages Arising From Neglect to Prosecute". *American Journal of International Law*. 22/1 (1928), 140-142.
Hyde, Charles. "Concerning Damages Arising From Neglect to Prosecute". *American Journal of International Law*. 22/1 (1928), 140-142.
ICJ AO 1956, Advisory Opinion of 23 October 1956, Judgments of the Administrative Tribunal of the ILO upon Complaints made against UNESCO. Hollanda: Uluslararası Adalet Divanı, 1956. Erişim 13 Temmuz 2025. https://www.icj-cij.org/public/files/case-related/17/017-19561023-ADV-01-00-EN.pdf.
ICJ, International Court of Justice. *Case Concerning Application of Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, 26 February 2007, [2007] ICJ 2. Erişim adresi: https://www.icj-cij.org/case/91/judgments.
ICJ, International Court of Justice. *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, 25 September 1997, ICJ Reports, No. 7, p. 54, para. 79. Erişim adresi: https://www.icj-cij.org/case/92.
ICJ, International Court of Justice. *United States Diplomatic and Consular Staff in Tehran (Tehran Hostages)*, Judgment, 24 May 1980, ICJ Reports 1980, No. 3, para. 59. Erişim adresi: https://www.icj-cij.org/case/64.
ICRC, *The Geneva Conventions and their Commentaries* (12 Ağustos 1949). Erişim: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf.
ICTY, Uluslararası Ceza Mahkemesi Eski Yugoslavya için Uluslararası Ceza Mahkemesi. K. IT-94-1-A (15 Temmuz 1999).

IIFFMCG, Independent International Fact-Finding Mission on the Conflict in Georgia. *Report of the International Fact-Finding Commission on the Conflict in Georgia, Vol. II*. 1. Basım, 2009.
IIFFMCG, Independent International Fact-Finding Mission on the Conflict in Georgia. *Report of the International Fact-Finding Commission on the Conflict in Georgia*, Vol. II. 2009.
Illing, Sean, "Cambridge Analytica, the Shady Data Firm That Might Be A Key Trump-Russia Link, Explained". *Vox*. Erişim 10 Mart 2024. https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie
Illing, Sean. "Cambridge Analytica, The Shady Data Firm That Might Be A Key Trump-Russia Link, Explained". *Vox.* (Nisan 2018).
Illing, Sean. "Cambridge Analytica, The Shady Data Firm That Might Be A Key Trump-Russia Link, Explained". *Vox*. (Nisan 2018).
International Law Commission (ILC), *Commentary to the Articles on State Responsibility*, Yearbook of the International Law Commission, 2. Cilt (Part II), 2001, 43-439. Birleşmiş Milletler Genel Kurulu Kararı No: A/RES/56/83 (12 Aralık 2001).
Investigation in the Wake of 9/11, edited by Mary Ellen O'Connell, 32, Leiden: Martinus Nijhoff Publishers, 2012.
Iran-U.S. C.T.R., Hyatt International Corporation v. The Government of the Islamic Republic of Iran, K. c. 9 (1985).
Iran–United States Claims Tribunal (Iran–U.S. Claims Tribunal), K. 397-195-1 (15 Kasım 1989).
Iran–United States Claims Tribunal (IUSCT), K. 354-10427-2 (16 Mart 1988), *Iran–United States Claims Tribunal Reports* 18 (1988).
Isnarti, Rika. "The Role of China's Patriotic Hackers and Their Relationship to the Government". *Andalas Journal of International Studies*. 4/2 (Kasım 2015), 161-180.
Isnarti, Rika. "The Role of China's Patriotic Hackers and Their Relationship to the Government". Andalas Journal of International Studies 4/2 (Kasım 2015), 161-180.
IUSCT, Iran–United States Claims Tribunal. K. 326-10913-2 (3 Kasım 1987).
IUSCT, Iran–United States Claims Tribunal. K. 326-10913-2 (3 Kasım 1987).
İran-ABD Talepler Mahkemesi (İran-ABD TM), K. 17 (1987), Iran–US Cl. Trib. Rep., 92-105.
İran-ABD TM, İran-ABD Talepler Mahkemesi. K. 17 (1987).
İran-ABD TM, İran-ABD Talepler Mahkemesi. K. 17 (1987).
İsveç, *Submission by Sweden to UNGA Resolution 68/243 Entitled "Developments in the Field of Information and Telecommunications in the Context of International Security"*, 12 Eylül 2014.
Jamnejad, Maziar and Michael Wood, "The Principle of Non-intervention". *Leiden Journal of International Law* 22/2 (2009), 345-381.
Jamnejad, Maziar and Michael Wood. "The Principle of Non-intervention". *Leiden Journal of International Law.* 22/2 (2009), 345-381.
Jamnejad, Maziar ve Michael Wood. "The Principle of Non-Intervention". *Leiden Journal of International Law*. 22/2 (2009), 363-388.
Jeangène Vilmer, Jean-Baptiste – Escorcia, Alexandre – Guillaume, Marine – Herrera, Janaina. *Information Manipulation: A Challenge for Our Democracies*. Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) ve Institute for Strategic Research (IRSEM, Ministry for the Armed Forces), 2018. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.
Jeangène Vilmer, Jean-Baptiste, Alexandre Escorcia, Marine Guillaume ve Janaina Herrera. "Information Manipulation: A Challenge for Our Democracies." *Policy Planning Staff*

(CAPS, Ministry for Europe and Foreign Affairs) ve Institute for Strategic Research (IRSEM, Ministry for the Armed Forces), Paris, Ağustos 2018. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf.

Jeangène Vilmer, Jean-Baptiste, Escorcia, Alexandre, Guillaume, Marine, Herrera, Janaina. *Information Manipulation: A Challenge for Our Democracies.* Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) ve the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces), Paris, 2018. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Jennings, Robert – Watts, Arthur (ed.). *Oppenheim's International Law*, 1 Cilt. Essex: Longman, 9. Basım, 1992.

Jennings, Robert ve Arthur Watts (eds.). *Oppenheim's International Law*. Cilt 1, 9. Basım. Essex: Longman, 1992.

Jennings, Robert, Watts, Arthur (eds.). *Oppenheim's International Law: Volume 1 Peace.* 1 Cilt. Essex: Longman, 4. Basım, 1992.

Jensen, Eric Talbot, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense". *BYU Law Digital Commons* 207 (2002), 207-240. https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1212&context=faculty_scholarship

Jensen, Eric Talbot. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense". *BYU Law Digital Commons*. (Aralık 2002).

Jensen, Eric Talbot. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense". *BYU Law Digital Commons*. (Aralık 2002), 207-240.

Jin, Dal Yong, "The Construction of Platform Imperialism in the Globalization Era". *Journal for a Global Sustainable Information Society* 11/1 (2013), 145-172. https://www.triple-c.at/index.php/tripleC/article/view/458

Jin, Dal Yong. *Digital Platforms, Imperialism and Political Culture*. Birleşik Krallık: Routledge, 1. Basım, 2017.

Jinks, Derek, "State Responsibility for the Acts of Private Armed Groups". *Chicago Journal of International Law* 4/1 (2003), 83-95.

Jordan, Tim. *Information Politics*. Londra: Pluto Press, 2015.

Jordan, Tim. *Information Politics*. Londra: Pluto Press, 2015. https://www.jstor.org/stable/j.ctv11sn2g6

Joyner, Christopher C. – Lotrionte, Catherine, "Information Warfare as International Coercion: Elements of a Legal Framework". *European Journal of International Law* 12 (2001), 825-850. https://academic.oup.com/ejil/article/12/5/825/422265

Kapossy, Béla – Whatmore, Richard (eds.). The Law of Nations. Indianapolis: Liberty Fund, 2008.

Kelsen, Hans. *The Law of the United Nations: A Critical Analysis of Its Fundamental Problems*. New York: Frederick A. Praeger, 1950.

Kinley, David – Tadaki, Junko, "From Talk to Walk: The Emergence of Human Rights Responsibility for Corporations at International Law". *Virginia Journal of International Law* 44/4 (2003-2004), 931-1023.

Kirchner, Stefan, "The Subjects of Public International Law in a Globalized World". *Baltic Journal of Law and Politics* 2/1 (2009), 86.

Kozik, Andrey L., "The Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace". *Baltic Yearbook of International Law* 14 (2015), 93- 103. https://brill.com/view/journals/byio/14/1/article-

p93_7.xml?srsltid=AfmBOor7Pu0idUzUT2HSCktLko-yBaxM2drDYxxfLSpWkG-_rztV37fQ
Kulesza, Joanna. *Due Diligence in International Law*. Leiden: Brill & Martinus Nijhoff Publishers, 2016.
Kulesza, Joanna. *International Internet Law*. New York: Routledge, 2012.
Kunig, Philip. "Intervention, Prohibition of". *Max Planck Encyclopedia of Public International Law (MPEPIL)*. 2008. Erişim 12 Nisan 2024. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434.
Kurtdarcan, Bleda Rıza, "Uluslararası Sorumluluk Hukuku Kapsamında Devletin De Facto Organı Kavramı Üzerine Kısa Bir Değerlendirme". *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi* 11/143-144 (2016). https://www.jurix.com.tr/article/5424
Küzeci, Elif. *Sayısal Fil: Bilişim Teknolojileri, Devlet ve Hukuk Kesişiminde Bir İnceleme*. İstanbul: İnkılap Yayınevi, 2021.
La Rue, Frank, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression". *UN Doc* A/HRC/23/40. Erişim 12 Şubat 2024. https://digitallibrary.un.org/record/1304394?v=pdf
Lakier, Genevieve, "Informal Government Coercion and The Problem of "Jawboning" *Lawfare*. Erişim 13 Şubat 2024. https://www.lawfaremedia.org/article/informal-government-coercion-and-problem-jawboning
Larson, Eric V. - Darilek, Richard E. - Gibran, Daniel - Nichiporuk, Brian - Richardson, Amy - Schwartz, Lowell H. - Thurston, Cathryn Quantic. *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. ABD: RAND Corporation, 2009. https://www.rand.org/pubs/monographs/MG654.html
Lau, Felix – Rubin, Stuart H. – Smith, Michael H. – Trajkovic, Ljiljana, "Distributed Denial of Service Attacks". *Advancing Technology for Humanity* (Aralık 2024).
Lewis, James A. – Lonergan, Erica D. – Voo, Julia – Garson, Melanie – Ertan, Amy, "Evolving Cyber Operations and Capabilities". *Center for Strategic and International Studies (CSIS)*, (2023). https://www.csis.org/analysis/evolving-cyber-operations-and-capabilities
Lewis, James A., "Cyber Threats to Our Nation's Critical Infrastructure". *Center for Strategic and International Studies (CSIS)* 18/1-7 (Ağustos 2018), 2-10. https://ccdcoe.org/uploads/2018/10/Geers2009_The-Cyber-Threat-to-National-Critical-Infrastructures.pdf
Leyden, John, 'Russian Politician: "My Assistant Started Estonian Cyberwar" – Dubious DDoS Lols". *The Register*. Erişim 10 Mart 2024. https://www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/
Lixinski, Lucas. *Legal Implications of the Privatization of Cyber Warfare*. Academy of European Law, 2010. http://hdl.handle.net/1814/13577.
Longley, Robert, "What Are Non-State Actors?". *ThoughtCo*. Erişim 3 Mart 2024. https://www.ebsco.com/research-starters/politics-and-government/non-state-actor-nsa.Moore, J. B. *History and Digest of International Arbitrations to Which the United States Has Been a Party*. 3 Cilt. Washington: Government Printing Office, 1898.
Luiijf, Eric. *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers*. Global Forum on Cyber Expertise (GFCE).
Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89 (2010). Erişim Mart 2024.
Mačák, Kubo, "Decoding Article 8 of the International Law Commission's Articles on State Responsibility". *Journal of Conflict and Security Law* 21/3 (2016), 420-450.

https://academic.oup.com/jcsl/article-abstract/21/3/405/2525375?redirectedFrom=fulltext
Malanczuk, Peter, "Data, Transboundary Flow, International Protection". *Max Planck Encyclopedia of Public International Law (MPEPIL)*, 2009. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e771. Erişim 14 Mart 2024.
Margulies, Peter, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism". *Fordham Law Review* 82/5 (2013), 2137-2149. Erişim 12 Nisan 2024. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4980&context=flr
Martins, Ralph, "Anonymous' Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts". *The Cyber Defense Review* 2/3 (2017), 95-106. Erişim 17 Aralık 2024. https://www.jstor.org/stable/26267388?seq=1
Mbanaso, Uche – Dandaura, E. S., "The Cyberspace: Redefining A New World". *IOSR Journal of Computer Engineering (IOSR-JCE)* 17/3 (Haziran 2015), 17-24. Erişim 12 Kasım 2024. C017361724-cyberspaceredefiningtheworld.pdf
Masters, Jonathan. *Russia, Trump, and the 2016 U.S. Election*. Council on Foreign Relations. Erişim 13 Temmuz 2025. https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.
Maf, Homayoun. "A Review of the Iran-United States Claims Tribunal". *Mision Juridica* 13/19 (Aralık 2020), 98-119. https://doi.org/10.25058/1794600X.1789.
MC, Milletler Cemiyeti. *Questionnaire No. 4, on Responsibility of States for Damage Done in their Territories to the Person or Property of Foreigners*. Cenevre: Milletler Cemiyeti, 1926.
McCorquodale, Robert – Simons, Penelope, "Responsibility Beyond Borders: State Responsibility for Extraterritorial Violations by Corporations of International Human Rights Law". *The Modern Law Review* 70/4 (2007), 598-625. Erişim 11 Kasım 2023. https://www.jstor.org/stable/pdf/4543156.pdf
Melzer, Nils, "Cyberwarfare and International Law". *UNIDIR Resources* (2011), 2-38. Erişim Tarihi 12 Ocak 2023. https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf
Meray, Seha L. *Devletler Hukukuna Giriş*. Ankara: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1. Baskı, 1959.
Mete, Murat – Balta Peltekoğlu, Filiz, "Sosyal Medyada Enformasyon Savaşı: Kurumsal Güvenlik Bağlamında Bireysel Sosyal Medya Kullanımı". *International Social Sciences Studies Journal* 7/86 (Ağustos 2021), 3328-3338. Erişim 15 Ocak 2023. https://sssjournal.com/?mod=makale_tr_ozet&makale_id=60380
Milanovic, Marko, "State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plücken". *Leiden Journal of International Law* 22 (2009), 307-324, Erişim 11 Şubat 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1307093
Milanović, Marko, "State Responsibility for Genocide". *European Journal of International Law* 17/3 (2006), 553-604. Erişim 12 Kasım2023. https://doi.org/10.1093/ejil/chl019
Miller, Michael L. – Vaccari, Cristian, "Digital Threats to Democracy: Comparative Lessons and Possible Remedies". *Sage Journals* 25/3 (11 Mayıs 2020), 333-356. Erişim 12 Haziran 2023. https://doi.org/10.1177/1940161220922323
Milletler Cemiyeti (MC), *Bases of Discussion*. Cenevre: Milletler Cemiyeti, 1929.
Mitchell, Russ, "How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia" *The Seattle Times*, Erişim 15 Şubat 2024. https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data

Momtaz, Djamchid. "Attribution of Conduct to the State: State Organs and Entities Empowered to Exercise Elements of Governmental Authority." In *The Law of International Responsibility*, ed. James Crawford, Alain Pellet ve Simon Olleson, 237. Oxford: Oxford University Press, 2010.Montijo Davası (ABD / Kolombiya), 1875.

Moore, J. B. *History and Digest of International Arbitrations to Which the United States Has Been a Party*. Cilt 2. Washington: Government Printing Office, 1898.

Moore, J. B. *History and Digest of International Arbitrations to Which the United States Has Been a Party*. Cilt 3. Washington: Government Printing Office, 1898.NATO. "Operation Allied Force." Erişim 10 Haziran 1999. https://www.nato.int/kosovo/all-frce.htm.

Moore, Martin. *Tech Giants and Civic Power*. Kings College London, 2016. https://core.ac.uk/download/pdf/51344227.pdf.

Morozov, Evgeny. "Moldova's Twitter Revolution". *Foreign Policy*. Erişim 7 Nisan 2023. https://www.journalofdemocracy.org/articles/moldovas-twitter-revolution/

Mouri, Akira, "The International Law of Expropriation as Reflected in the Work of the Iran–US Claims Tribunal". *Dordrecht: Nijhoff* (1994), 177-191. Erişim Tarihi 12 Mart 2023. https://brill.com/display/title/9354?srsltid=AfmBOoq4PM9k3vkyAQ4jy5LN8E7tsgl-g3aVv7PA44QK_wqfEPuIG-Rr

Mulford, Joshua P. "Non-State Actors in the Russo-Ukrainian War". *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes* 15/2 (2016), 90-105.

Musk, Elon. "Starlink service is now active in Ukraine. More terminals en route." Twitter. 3 Şubat 2022, 14:15. Erişim 27 Şubat 2023. https://twitter.com/elonmusk/status/149754123456789.

Nakashima, Ellen. "Cyber-Intruder Sparks Response, Debate". *The Washington Post*. Erişim 6 Aralık 2024. https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

Nakashima, Ellen. "National Intelligence Director: Hackers Have Targeted 2016 Presidential Campaigns." *The Washington Post*. Erişim 18 Mayıs 2024. https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html.

Nanda, Sanchit. "World of White Hat Hackers". *International Journal of Scientific & Engineering Research* 10/5 (Mayıs 2019), 285-289. Erişim 12 Aralık 2024. https://www.researchgate.net/publication/334045400_World_of_White_Hat_Hackers

Newman, Lily Hay. "Voting Machines Are Still Absurdly Vulnerable to Attacks." *WIRED*. Erişim 28 Eylül 2023. https://www.wired.com/story/voting-machine-vulnerabilities-defcon-voting-village/.

Nickolov, Eugene. "Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations". *Information & Security: An International Journal* 17 (Ocak 2005), 107-120.

Nieto-Navia, Rafael. "State Responsibility in Respect of International Wrongful Acts of Third Persons: The Theory of Control". *International Law Studies* 69 (1993), 1-45.

Nolte, Georg. "Article 2 (7)." *The Charter of the United Nations: A Commentary*. ed. Bruno Simma vd. Oxford: Oxford University Press, 2012, 284-285.

Nørgaard, Carl Aage. "The Position of the Individual in International Law". *The American Journal of International Law* 58/1 (Ocak 1964), 204-211.

Nye, Joseph S. "After the Liberal International Order." *Project Syndicate*. Erişim 16 Şubat 2024. https://www.project-syndicate.org/commentary/biden-must-replace-liberal-international-order-by-joseph-s-nye-2020-07

Nyman, Mikaela. *Cyber Attacks as Armed Attacks? The Right of Self-Defence When a Cyber Attack Occurs*. Stockholm: Stockholm Üniversitesi Hukuk Fakültesi, Yüksek Lisans Tezi, 2023. https://su.diva-portal.org/smash/record.jsf?pid=diva2%3A1754047&dswid=-9194

O'Connell, Mary Ellen, "Cyber Security without Cyber War". *Journal of Conflict and Security Law* 17 (2012), 187-209. Erişim 12 Ocak 2023. https://www.jstor.org/stable/26296226?seq=1

OECD (Organisation for Economic Co-operation and Development), *Recommendation of the Council on the Protection of Critical Information Infrastructures*. 2008, C(2008)35.

Ohlin, Jens David. "Did Russian Cyber Interference in the 2016 Election Violate International Law?". *Texas Law Review* 95 (2024). Erişim 7 Şubat 2024. https://scholarship.law.cornell.edu/facpub/1498/

Okimoto, Keiichiro. *The Distinction and Relationship between Jus Ad Bellum and Jus in Bello*. Oxford: Hart Publishing, 2011.

Oppenheim, Lassa. *International Law: A Treatise*. 1. Cilt. Londra: Longmans, Green and Co., 2. Basım, 1912.

Osborn, Phillip. "Cyber Border Security – Defining and Defending a National Cyber Border". *Homeland Security Affairs* 13/5 (6 Şubat 2024), 3-15.

Paganini, Pierluigi. "Non-State Actors in Cyberspace: An Attempt to a Taxonomic Classification, Role, Impact and Relations with a State's Socioeconomic Structure". *Center for Cyber Security and International Relations Studies (CCSIRS)* (Haziran 2022), 5-15.

Parajuli, Asmita. "Digital Manipulation on Social Media". *Social Media and Online Journalism*, Şubat 2022, 6-12. Erişim 14 Nisan 2023. https://www.researchgate.net/publication/376375056_DIGITAL_MANIPULATION_ON_SOCIAL_MEDIA

Pazarcı, Hüseyin. *Uluslararası Hukuk*. Ankara: Turhan Kitabevi, 18. Baskı.

Percy, Sarah. *Mercenaries: The History of a Norm in International Relations*. New York: Oxford University Press, 2007.

Peters, Anne. "Surveillance without Borders? The Unlawfulness of the NSA-Panopticon". *EJIL: Talk!*. Erişim 6 Kasım 2023. www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/.

Pillay, Navi. *Report of the Office of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age*. Birleşmiş Milletler, 2014.

Plakokefalos, Ilias. "Causation in the Law of State Responsibility and the Problem of Overdetermination: In Search of Clarity". The European Journal of International Law 26/2 (2015), 471–492. https://doi.org/10.1093/ejil/chv023

Pirker, Benedikt. "Territorial Sovereignty and Integrity and the Challenges of Cyberspace." In *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski, 190–191. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2013.

Pisillo-Mazzeschi, Riccardo. "The Due Diligence Rule and the Nature of International Responsibility of States". *German Yearbook of International Law* 35 (1992), 9-51.

Prucher, Jeff (ed.). *The Oxford Dictionary of Science Fiction*. Oxford: Oxford University Press, 2006.

Quadri, R. A. Lukman Adewale – Rasaq, Monsuru Olaitan. "Cyber Theatre: A Fifth Domain of International Politics: Africa and the Rest of the World in the Cyberspace". *AHBV Akdeniz Havzası ve Afrika Medeniyetleri Dergisi* 2/2 (Aralık 2020), 98–111. Erişim 18 Aralık 2024. https://dergipark.org.tr/en/download/article-file/1308002

Qureshi, Waseem Ahmad. "Information Warfare, International Law, And The Changing Battlefield". *Fordham International Law Journal* 43/4 (2020), 901-938.
Radziwill, Yaroslav. *Cyber-Attacks and the Exploitable Imperfections of International Law*. Boston: Brill–Martinus Nijhoff Publishers, 2015.
Radziwill, Yaroslav. *Cyber-Attacks and the Exploitable Imperfection of International Law*. Leiden: Brill & Martinus Nijhoff Publishers, 2015.
Radziwill, Yaroslav. *Cyber-Attacks and the Exploitable Imperfection of International Law*. Leiden: Brill & Martinus Nijhoff Publishers, 2015.
Ran, Congjing – Yan, Liu. "Dynamic Logic, Mode Selection, and Reconstruction Path of Platform Governance in the Perspective of Data Sovereignty". *Journal of Library Science in China*, 16 Şubat 2023, 1–23.
Ranchordas, Sofia – De Gregorio, Giovanni – Goanta, Catalina. "Big Tech War Activism." *VerfBlog*. Erişim 15 Şubat 2023. https://verfassungsblog.de/big-tech-war-activism/
Rato, M. – Petit, N. "Abuse of Dominance in Technology-Enabled Markets: Established Standards Reconsidered?" *European Competition Journal* 9/1 (2013), 1-65.
Reinalda, Bob (ed.). *The Ashgate Research Companion to Non-State Actors*. London: Ashgate Publishing, 1. Baskı, 2011.
RIAA, Reports of International Arbitral Awards. K. Arbitral Award (16 Nisan 1938 ve 11 Mart 1941).
RIAA, Reports of International Arbitral Awards. *Sambiaggo Davası* (Italy v. Venezuela) (1903), Cilt 10.
RIAA, Reports of International Arbitral Awards. Underhill Davası (United Kingdom v. Venezuela), Cilt 9, 155, 159 (1903).
Rid, Thomas. "All Signs Point to Russia Being behind the DNC Hack". *Motherboard*. Erişim 25 Temmuz 2016. https://motherboard.vice.com/read/all-signs-point-to-russia-being-behind-the-dnc-hack.
Rid, Thomas. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35/1 (Ekim 2011), 3-32. Erişim 12 Aralık 2023. https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939
Rid, Thomas. *Cyber War Will Not Take Place*. Oxford: Oxford University Press, 2013.
Riley, Michael – Robertson, Jordan. "Russian Hacks on U.S. Voting System Wider than Previously Known". *Bloomberg*, Erişim 13 Haziran 2017. https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.
Rinwigati, Patricia. "The Legal Position of Multinational Corporations in International Law". *Jurnal Hukum & Pembangunan* 49/2 (Haziran 2019), 377-396.
Roscini, Marco. "World Wide Warfare – Jus ad bellum and the Use of Cyber Force". *Max Planck Yearbook of United Nations Law Online* 14/1 (2010), 85–130.
Roscini, Marco. *Cyber Operations and the Use of Force in International Law*. London: Oxford University Press, 2014.
Rosenne, Shabtai (ed.). *League of Nations Conference for the Codification of International Law*. 2 Cilt. Dobbs Ferry, NY: Oceana Publications, 1975.
Rosenne, Shabtai. *League of Nations Conference for the Codification of International Law*, Cilt 2. Dobbs Ferry, NY: Oceana Publications, 1975.
Roth, Andrew. "Putin Says Trump Is 'Absolute Leader' in U.S. Presidential Race." *The Washington Post*, Erişim 17 Aralık 2015. https://www.washingtonpost.com/world/putin-no-major-gaps-with-washington-over-efforts-to-end-syria-conflict/2015/12/17/a178255e-a431-11e5-8318-bd8caed8c588_story.html.

Roth, Andrew. "Russia Denies DNC Hack and Says Maybe Someone 'Forgot the Password'". *The Washington Post*, Erişim 15 Haziran 2016. https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/russias-unusual-response-to-charges-it-hacked-research-on-trump/.

Ruggie, John Gerard. *Just Business: Multinational Corporations and Human Rights*. Norton Global Ethics Series, 1. Baskı.

Ruys, Tom. "The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter Article 2(4)?". *American Journal of International Law* 108 (2014), 159-163.

Ruys, Tom. *"Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*." Cambridge: Cambridge University Press, 2010.

Sanger, David E. and Eric Schmitt. "Spy Agency Consensus Grows That Russia Hacked D.N.C." *The New York Times*, Erişim 26 Temmuz 2024. https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html.

Sanger, David E. and Nick Corasaniti. "D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump." *The New York Times*, Erişim 14 Haziran 2016. https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

Sanger, David E. and Nicole Perlroth. "U.S. Said to Find North Korea Ordered Cyber Attack on Sony." *The New York Times*, Erişim 17 Aralık 2014. https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

Schmidt, Andreas. "The Estonian Cyberattacks". *Delft University of Technology* (Ocak 2013), 3-28. Erişim 12 Mayıs 2023. https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

Schmitt, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Schmitt, Michael N. "Cyber Operations and the Jus Ad Bellum Revisited". *Villanova Law Review* 56/3 (2011), 569-606.

Schmitt, Michael N. "The Use of Cyber Force and International Law." In *The Oxford Handbook of the Use of Force in International Law*, edited by Marc Weller, 1116. Oxford: Oxford University Press, 2015.

Schneier, Bruce. "By November, Russian Hackers Could Target Voting Machines." *The Washington Post*, Erişim 27 Temmuz 2023. https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/.

Shany, Yuval. "Big Tech Companies' Obligations under International Human Rights Law". Cambridge University Press 58/3 (2025), 3-27.

Shaban, Hamza. "Google for the First Time Outspent Every Other Company to Influence Washington in 2017". *Washington Post*. Erişim 14 Şubat 2024. https://www.washingtonpost.com/news/the-switch/wp/2018/01/23/google-outspent-every-other-company-on-federal-lobbying-in-2017/

Shachtman, Noah. "Hackers, Troops Rejoice: Pentagon Lifts Thumb-Drive Ban (Updated)". *WIRED*. Erişim 18 Şubat 2014. https://www.wired.com/2010/02/hackers-troops-rejoice-pentagon-lifts-thumb-drive-ban/.

Shachtman, Noah. "Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)". *WIRED*. Erişim 25 Ağustos

2024. https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/.
Shachtman, Noah. "Under Worm Assault, Military Bans Disks, USB Drives". *WIRED*. Erişim 19 Kasım 2008. https://www.wired.com/2008/11/army-bans-usb-d/.
Shackelford, Scott J. *Managing Cyber Attacks in International Law, Business, and Relations*. Cambridge University Press, 2014.
Sharp Sr., Walter G. *Cyberspace and the Use of Force*. Falls Church: Aegis Research Corporation, 1999.
Sharp, Robin. 2007. "An Introduction to Malware". DTU Library, Danimarka Teknik Üniversitesi, Kopenhag.
Shaw, Malcolm. *International Law*. Cambridge: Cambridge University Press, 4. Baskı, 1997.
Sigholm, Johan. "Non-State Actors in Cyberspace Operations". *Journal of Military Studies* 4/1 (Aralık 2013), 9–25.
Silver, Daniel B. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter". *International Law Studies* 76 (2002), 73–85.
Simma, Bruno – Khan, Daniel-Erasmus – Nolte, Georg – Paulus, Andreas (eds.). *The Charter of the United Nations: A Commentary*. 1 Cilt. Oxford: Oxford University Press, 3. Baskı, 2012.
Sloan, James. "Prosecutor v. Dragan Nikolic: Decision on Defence Motion on Illegal Capture". *Leiden Journal of International Law* 16 (2003), 541-548.
Smith, John. "Cyber Influence in Eastern Europe." In *The Russian Federation in Global Knowledge Warfare Influence Operations in Europe and Its Neighbourhood*, ed. Holger Mölder, Vladimir Sazonov, Archil Chochia ve Tanel Kerikmäe, 45-68. Almanya: Springer, 2021.
Sobande, Francesca – Kanai, Akane – Zeng, Natasha. "The hypervisibility and discourses of 'wokeness' in digital culture". *Media, Culture and Society* 44/8 (2022), 1576-1587.
Sobotta, Christoph – Kokott, Juliane. "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR". *European Data Protection Law Review* 3 (2013).
Sopilko, Iryna – Svintsytskyi, Andrii – Krasovska, Yevheniia – Padalka, Andrii – Lyseiuk, Andrii. "Information Wars as a Threat to the Information Security of Ukraine". *Conflict Resolution Quarterly* 39/3 (Kasım 2021), 77–92.
Spector, Phil. "In Defense of Sovereignty, in the Wake of Tallinn 2.0.". *AJIL Unbound* 111 (2017), 219–223.
Stouffer, Clare. "What is a Script Kiddie? Definition + Examples." *Norton*. Erişim 22 Haziran 2023. https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie
Sun Tzu. *The Art of War*. çev. Samuel B. Griffith. Oxford: Oxford University Press, 1963.
Swedish Armed Forces (SAF). "Confirmed Submarine in the Stockholm Archipelago." Swedish Armed Forces, 14 Kasım 2014. Erişim 29 Nisan 2025. www.forsvarsmakten.se/en/news/2014/11/confirmed-submarine-in-the-stockholm-archipelago/.
Şafak, Erdi. "Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırılar". *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 28/1 (Şubat 2020), 138-158.
Takano, Akiko. "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications". *Laws* 7/4 (2018), 2–18.
Talmon, Stefan. "The Responsibility of Outside Powers for Acts of Secessionist Entities". *International and Comparative Law Quarterly* 58/3 (2009), 503–529.
Tang, Dan – Kuang, Xiao-Hong. "A Generic Model for Trojan Horse Attacks Prevention and Handling". *Atlantis Press* (Ekim 2015), 189-196.

Teke, Aynur – Lale, Aybala. "Sosyal Medyada Etik, Bilgi Manipülasyonu ve Siber Güvenlik". *Akademik İncelemeler Dergisi* 16/2 (Ekim 2021), 49–65.
The White House, The White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: The White House, Mayıs 2009.
Thill, Scott. "March 17, 1948: William Gibson, Father of Cyberspace". *WIRED*. Erişim 8 Haziran 2023. https://www.wired.com/2009/03/march-17-1948-william-gibson-father-of-cyberspace-2/
Timur, Fitri Bintang. "Cyber Mercenaries: The Failures of Current Responses and the Imperative of International Collaboration". *Observer Research Foundation*, (Aralık 2023). Erişim 12 Aralık 2024. https://www.orfonline.org/public/uploads/posts/pdf/20231211112312.pdf
Townsend, Gregory. "State Responsibility for Acts of De Facto Agents". *Arizona Journal of International and Comparative Law* 14 (1997), 635-879.
Treves, Tullio. "International Courts and Tribunals: Alternatives to Treaty Making". *Developments of International Law in Treaty Making*. ed. Rüdiger Wolfrum – Volker Röben, 600. Berlin: Springer, 2005.
Tsagourias, Nicholas. "Cyber Attacks, Self-Defence and the Problem of Attribution". *Journal of Conflict & Security Law* 17/2 (2012), 238-239.
Türkay, Şeyda. "Siber Savaş Hukuku ve Uygulanma Sorunsalı". *İstanbul Hukuk Mecmuası* LXXI/1 (Ağustos 2013), 1177-1227.
U.S. Department of Defense (DoD), *The Definition of "Cyberspace"*. Washington, DC: U.S. Department of Defense, 12 Mayıs 2008. Erişim 13 Temmuz 2025. https://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm.
UAD, Uluslararası Adalet Divanı. K. [1980] ICJ Rep 3 (24 Mayıs 1980).

UAD, Uluslararası Adalet Divanı. K. 1949 ICJ 174 (11 Nisan 1949).
UAD, Uluslararası Adalet Divanı. K. 30 (1 Kasım 1979).
UAD, Uluslararası Adalet Divanı. K. Bosna-Hersek-Sırbistan ve Karadağ Davası (Soykırım Suçunun Önlenmesi ve Cezalandırılması Sözleşmesi), 26 Şubat 2007, para. 391, 397. Erişim 13 Temmuz 2025. http://www.icj-cij.org/docket/files/91/13685.pdf.
UAD, Uluslararası Adalet Divanı. K. Case Concerning the Gabčíkovo–Nagymaros Project (Macaristan v. Slovakya), [1997] ICJ 7 (25 Eylül).
UAD, Uluslararası Adalet Divanı. K. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, I.C.J. Reports 1986.
UAD, Uluslararası Adalet Divanı. K. Nicaragua v. United States of America (Military and Paramilitary Activities in and against Nicaragua), Judgment of 27 June 1986, para. 114. Erişim 19 Kasım 2024. http://www.icj-cij.org/docket/index.php?p1=3&p2=3&k=66&case=70&code=nus&p3=4.
UDAD, Uluslararası Daimi Adalet Divanı. K. Jurisdiction of the Courts of Danzig (Advisory Opinion), Series B, No. 15 (1928).
UDAD, Uluslararası Daimi Adalet Divanı. K. Phosphates in Morocco Davası, Ön İtirazlar, PCIJ (Ser. A/B) No. 74 (14 Haziran 1938).
UDAD, Uluslararası Daimi Adalet Divanı. K. The Case of the S.S. Lotus (France v. Turkey), Judgment of 7 Eylül 1927, PCIJ Series A No. 10.
Uluslararası Hukuk Komisyonu (ILC), *Commentary to the Articles on State Responsibility*, 2 Yearbook of the International Law Commission (Part II) (2001).
UN GA, United Nations General Assembly. *Official Records of the General Assembly, Fifty-Sixth Session, Supplement No. 10, II/II*. New York: United Nations, 2001.

UNGA, United Nations General Assembly. 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', UN Doc A/70/174 (22 July 2015), para. 13.
UNGA, United Nations General Assembly. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, Karar No: A/RES/58/199, 30 Ocak 2004.
UNGA, United Nations General Assembly. Definition of Aggression, Resolution 3314 (XXIX), 14 December 1974, A/RES/3314.
UNGA, United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: United Nations, 2010. UN Doc A/65/201, 30 July 2010.
UNGA, United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: United Nations, 2015. UN Doc A/70/174, 22 July 2015.
UNGA, United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: United Nations, 2023. UN Doc A/68/98, 24 June 2023.

UNIC, Birleşmiş Milletler Enformasyon Merkezi. *Saldırı'nın (Tecavüzün) Tanımı: Birleşmiş Milletler Genel Kurulu'nun 3314 (XXIX) sayılı ve 1974 Tarihli Kararı*. Ankara: Birleşmiş Milletler Enformasyon Merkezi, 1. Basım, 2002. https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf
United Nations, General Assembly (UN GA), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (New York: United Nations, 2010).
United Nations, General Assembly (UN GA), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (New York: United Nations, 2023).
United Nations, General Assembly (UN GA), *Official Records of the General Assembly, Fifty-Sixth Session, Supplement.10/2* (Brüksel: United Nations, 2001).
Untersinger, Martin. "MacronLeaks: L'enquête Pointe Vers un Piratage 'Simple et Générique'". *Le Monde*, Erişim 2 Haziran 2024. https://www.lemonde.fr/pixels/article/2017/06/02/macronleaks-l-enquete-pointe-vers-un-piratage-simple-et-generique_5137945_4408996.html.
UTA, Uluslararası Tahkim Mahkemesi. K. Spanish Zone of Morocco Case v. Spain, K. 2 (1923).
Uzun, Elif. *Devletin Milletlerarası Hukuka Aykırı Eyleminden Sorumluluğu.* Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, 2007.
Valeri, Lorenzo. "The Information Warrior". *Journal of Financial Crime* 6/1 (1998), 52-53.
van Benthem, Tsvetelina – Dias, Talita – Hollis, Duncan B. "Information Operations under International Law". *Vanderbilt Law Review* 55/5 (Kasım 2022), 1217-1251.
van der Meer, Sico. "How States Could Respond to Non-State Cyber-Attackers". *Clingendael Institute* (Haziran 2024) 15. Erişim 13 Temmuz 2025. https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf
Vattel, Emmerich de. *The Law of Nations or, the Principles of Natural Law: Applied to the Conduct and to the Affairs of Nations and Sovereigns*, cilt 2, çev. CG Fenwick. New York, NY: Legal Classics Library, 1916, 72.
Veerasamy, Namosha. "A High-level Conceptual Framework of Cyber-terrorism". *Journal of Information Warfare* 8/1 (2009), 45-55.

Waagstein, Patricia Rinwigati. Corporate Human Rights Responsibility: Continuous Search for a Regulatory Framework. Uppsala: Uppsala University, Disciplinary Domain of Humanities and Social Sciences, Faculty of Law, Department of Law, Yüksek Lisans Tezi, 2009.

Wagner, Ben – Bronowicka, Joanna – Berger, Thomas. Surveillance and Censorship: The Impact of Technologies on Human Rights. European Parliament, 2015. Erişim 13 Haziran 2025.

Wagner, Markus. "Non-State Actors". *Max Planck Encyclopedia of Public International Law*. Erişim 3 Mart 2024. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1445

Warofka, Alex. "An Independent Assessment of the Human Rights Impact of Facebook in Myanmar". *Meta.* Erişim 14 Şubat 2024. https://about.fb.com/news/2018/11/myanmar-hria/

Watts, Sean. "Low-Intensity Cyber Operations and the Principle of Non-intervention". *Baltic Yearbook of International Law* 14 (2015), 137-144.

Waxman, Matthew C. "Regulating Resort to Force: Form and Substance of the UN Charter Regime". *European Journal of International Law* 24/1 (2013), 151-189.

Waxman, Matthew C. "Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions". *International Law Studies* 89 (2013), 109-122.

Waxman, Michael C. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)". *Yale Journal of International Law* 36 (2011), 422-459.

Weimann, Gabriel. *Cyberterrorism: How Real Is the Threat? United States Institute of Peace* (2004), 1-12, Erişim 14 Haziran 2024. https://www.usip.org/sites/default/files/sr119.pdf

Weller, Marc (ed.). *The Oxford Handbook of the Use of Force in International Law*. Oxford: Oxford University Press, 2015.

Whitley, Angus. "Facebook Ends Australia News Blackout After Law Compromise". *Bloomberg*. Erişim 16 Şubat 2024. https://financialpost.com/technology/facebook-ends-australia-news-blackout-after-compromise-on-world-first-legislation

Whittaker, Jason. *The Cyberspace Handbook*. Londra–New York: Routledge, 2004.

Wijayarathne, Senesh N. "Trojan Horse Malware – Case Study". *Sri Lanka Institute of Information Technology (SLIIT)*, (Temmuz 2022), 1-10. Erişim 13 Mart 2025. https://www.researchgate.net/publication/362657622_Trojan_Horse_Malware_-_Case_Study

Wijninga, Peter – Oosterveld, Willem Theo – Galdiga, Jan Hendrik – Marten, Philipp. "State and Non-State Actors: Beyond the Dichotomy". *Hague Centre for Strategic Studies*. (Ocak 2014), 139-162. Erişim 1Mart 2024. https://www.jstor.org/stable/resrep12608.8?seq=1

Wilhelmsen, Vivi Cathrine Ringnes. *Soft War in Cyberspace: How Syrian Non-State Actors Use Hacking to Influence the Conflict's Battle of Narratives*. University of Oslo, Yüksek Lisans Tezi, 2014.

Woltag, Johann-Christoph. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law*. *Intersentia* (2014), 90–93.

Wood, Michael. "Peace, Breach of." *Max Planck Encyclopedia of Public International Law (MPEPIL)*. Oxford: Oxford University Press, 2009. Erişim 13 Temmuz 2025. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e372.

SWood, Michael. The Principle of Non-intervention in Contemporary International Law: Non-interference in a State's Internal Affairs Used to be a Rule of International Law: Is It Still? Chatham House, 2007.
Wood, Steven. *Patriotic Hackers*. Manchester: Faculty of Business and Law Manchester Metropolitan University, Yüksek Lisans Tezi, 2017.
Yan, Li. "The Role and Impact of Nonstate Actors from the Perspective of the Russia—Ukraine Crisis." *China Institutes of Contemporary International Relations* 32/4 (Temmuz-Ağustos 2022), 89-107. Erişim 13 Mayıs 2024. https://www.jstor.org/stable/26326442?seq=1
Yeager v. Islamic Republic of Iran (Yeager), K. 326-10583-2 (1987), *Iran–US Cl. Trib. Rep.* 17 (1987), 92.
Zekoll, Joachim. "Jurisdiction in Cyberspace." In *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization*, edited by Günther Handl, Peer Zumbansen and Joachim Zekoll, 341. Boston: Martinus Nijhoff Publishers, 2012.
Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.
Ziolkowski, Katharina. "General Principles of International Law as Applicable in Cyberspace". *Peacetime Regime for State Activities in Cyberspace*, ed. Katharina Ziolkowski (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2013).
Ziolkowski, Krzysztof. "Computer Network Operations and the Law of Armed Conflict". *Military Law and Law of War Review* 49/1-2 (2010), 47-90. Erişim 1 Ocak 2025. https://www.elgaronline.com/view/journals/mllwr/49/1-2/article-p47.xml
Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books, Ocak 2019.

İntnernet Kaynakları

DHS, U.S. Department of Homeland Security. "Statement by Secretary Johnson on Cyber Attack on Sony Pictures Entertainment." Erişim 6 Temmuz 2025. https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.
DoD, U.S. Department of Defense. "Joint Terminology for Cyberspace Operations." Erişim 13 Temmuz 2025. https://info.publicintelligence.net/DoD-JointCyberTerms.pdf.
DoD, U.S. Department of Defense. *The National Military Strategy for Cyber Operations.* Erişim 7 Haziran 2023. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.
FBI, Federal Bureau of Investigation. "Hillary R. Clinton." *FBI Records: The Vault.* Erişim 13 Temmuz 2025. https://vault.fbi.gov/hillary-r.-clinton
HRW, Human Rights Watch. "Video Unavailable – Social Media Platforms Remove Evidence of War Crimes." Erişim 13 Şubat 2024. https://www.hrw.org/news/2024/02/12/video-unavailable-social-media-platforms-remove-evidence-war-crimes.
ICJ, International Court of Justice. *Case Concerning Application of Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 26 February 2007.* Erişim: https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf.
ICRC, International Committee of the Red Cross. *Cenevre Sözleşmeleri ve Şerhleri*, 12 Ağustos 1949. Erişim 6 Temmuz 2025. https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions-1949additional-protocols-and-their-commentaries.
IDI, Institut de Droit International. *Multinational Enterprises.* Oslo: Institut de Droit International, 1977. Erişim 13 Temmuz 2025. https://www.idi-iil.org/app/uploads/2017/06/1977_oslo_02_en.pdf.

ILM, International Legal Materials. “Claim against the Union of Soviet Socialist Republics for Damage Caused by Soviet Cosmos 954.” 18 (1979): 18.
Law.com Dictionary. “Actor.” Erişim 3 Mart 2024. https://dictionary.thelaw.com/actor/
OED, Oxford English Dictionary. Erişim 26 Kasım 2024. https://www.oed.com/search/dictionary/?scope=Entries&q=control.
Pastebin. “EMLEAKS.” Erişim 6 Temmuz 2025. https://pastebin.com/bUJKFpH1 (sayfa kaldırılmıştır, arşiv: http://archive.fo/eQtrm).
RFE/RL, Radio Free Europe/Radio Liberty. “Behind The Estonia Cyberattacks.” Erişim 6 Temmuz 2025. https://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.
RIA, RIA Novosti. “Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks.” Erişim 6 Temmuz 2025. https://en.ria.ru/world/20070906/76959190.html.
Sangfor Technologies. “What Are Script Kiddies in Cybersecurity?” Erişim 8 Nisan 2024. https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie
Spiegel Online. “BND Scandal: How German Spies Eavesdropped on an Afghan Ministry.” Erişim 6 Temmuz 2025. https://www.spiegel.de/international/germany/bnd-scandal-how-german-spies-eavesdropped-on-an-afghan-ministry-a-550212.html.
The Economist. “Cyberwar: War in the Fifth Domain.” Erişim 12 Temmuz 2025. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain.
TransLegal. *World Law Dictionary.* “Actor.” Erişim 3 Mart 2024. https://dictionary.translegal.com/en/actor/noun.
U.S. Department of State. Clinton, Hillary Rodham. “Internet Rights and Wrongs: Choices and Challenges in a Networked World, Remarks.” 2011.
U.S. Department of State. Clinton, Hillary Rodham. “Remarks on Internet Freedom.” Erişim 14 Haziran 2025.
UAB, Republic of Türkiye Ministry of Transport and Infrastructure. *National Cyber Security Strategy and Action Plan (2020–2023).* Erişim 22 Ocak 2023. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.
UN ILC, United Nations International Law Commission. *Uluslararası Hukuk Komisyonu’nun Elli Üçüncü Oturumunda Yürüttüğü Çalışmalara İlişkin Rapor (23 Nisan–1 Haziran ve 2 Temmuz–10 Ağustos 2001).* New York: Birleşmiş Milletler, 2001. Erişim 6 Temmuz 2025. https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf.
UN, United Nations. *Charter of the United Nations.* San Francisco: 1945. Erişim 6 Temmuz 2025. https://treaties.un.org/doc/publication/ctc/uncharter.pdf.