T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU BİLİM DALI

SİLAHLI ÇATIŞMA SIRASINDA SİBER SALDIRILAR YÖNÜNDEN "HEDEF" KAVRAMININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

BETÜL NUR ÖZLÜ

BURSA – 2025

T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU BİLİM DALI

SİLAHLI ÇATIŞMA SIRASINDA SİBER SALDIRILAR YÖNÜNDEN "HEDEF" KAVRAMININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Betül Nur ÖZLÜ

DANIŞMAN: Dr. Öğr. Üyesi Gülsüm KAYA

BURSA-2025

ÖZET

Yazar adı soyadı	**Betül Nur Özlü**
Üniversite	**Bursa Uludağ Üniversitesi**
Enstitü	**Sosyal Bilimler Enstitüsü**
Anabilim dalı	**Kamu Hukuku**
Bilim dalı	**Kamu Hukuku**
Tezin niteliği	*yüksek lisans*
Mezuniyet tarihi	**…/…/2025**
Tez danışmanı	**Dr. Öğretim Üyesi Gülsüm KAYA**

Silahlı Çatışma Sırasında Siber Saldırılar Yönünden "Hedef" Kavramının Değerlendirilmesi

Bu çalışmada, siber saldırıların insancıl hukuk kapsamında tanımlanan hedef kavramı ile ilişkisi ve bu ilişkinin hukuki boyutu ele alınmıştır. İnsancıl hukukun temel kaynakları olan 1949 tarihli Cenevre Sözleşmeleri ve Ek Protokoller'de düzenlenen silahlı çatışmaların tanımının, araç ve yöntemlerinin siber saldırılara uygulanabilirliği incelenmiştir. Söz konusu sözleşmeler ve protokoller çerçevesinde sivil nesne-askeri nesne ayrımlarının nasıl yapıldığı, hangi hedeflerin meşru kabul edildiği hangilerinin ise insancıl hukuk ihlali teşkil ettiği, siber saldırılar bağlamında değerlendirilmiştir.

Çalışmada öncelikle insancıl hukukta nesne ve hedef kavramlarının gelişimi ile bu kavramların hukuki işlevi ele alınmıştır. Ardından siber operasyon çeşitleri incelenmiş, bu operasyonlardan hangilerinin siber saldırı olarak kabul edildiği ve siber saldırıların insancıl hukuk kapsamına nasıl girdiği ortaya konulmuştur. Son olarak sivillerin ve sivil nesnelerin siber saldırılar karşısındaki korunma düzeyi, bu duruma mevcut standartların uygulanabilirliği ve doktrindeki yorum farklılıkları değerlendirilmiştir. Çalışma, siber saldırıların mevcut uluslararası insancıl hukuk kuralları kapsamında değerlendirilmesi gerektiğini, ancak teknolojik gelişmelerin ortaya çıkardığı hukuki boşluklar nedeniyle yeni hukuki düzenlemelere ihtiyaç duyulduğunu göstermektedir.

Anahtar kelimeler: *uluslararası insancıl hukuk, silahlı çatışmalar, siber saldırılar, hedef*

ABSTRACT

Name & surname	**Betül Nur Özlü**
University	**Bursa Uludağ University**
Institute	**Institute of Social Sciences**
Field	**Public Law**
Subfield	**Public Law**
Degree awarded	*Master*
Date of degree awarded	**…/…/2025**
Supervisor	**Assistant Professor Gülsüm KAYA**

The Concept of Target in Terms of Cyber Attacks During Armed Conflict

This study examines the relationship between cyberattacks and the concept of target, as defined under humanitarian law, and the legal dimension of this relationship. The applicability of the definition, means, and methods of armed conflict stipulated in the 1949 Geneva Conventions and their Additional Protocols, the fundamental sources of humanitarian law, to cyberattacks is examined. The distinctions between civilian and military objects are made within the framework of these conventions and protocols, and which targets are considered legitimate and which constitute violations of humanitarian law are evaluated in the context of cyberattacks.

This study first examines the development of the concepts of object and target in humanitarian law and their legal function. It then examines the types of cyber operations, identifying which of these operations are considered cyberattacks and how cyberattacks fall within the scope of humanitarian law. Finally, it evaluates the level of protection afforded to civilians and civilian objects against cyberattacks, the applicability of existing standards to this situation, and the differences in interpretation within the doctrine. The study shows that cyberattacks should be evaluated within the scope of existing international humanitarian law rules, but new legal regulations are needed due to legal gaps created by technological developments.

Keywords: *international humanitarian law, armed attacks, cyber attacks, target*

ÖNSÖZ

Bu çalışmayı hazırlama sürecinde bana en büyük desteği veren, yardımı, sevgisi, sabrı ve motivasyonuyla her zaman yanımda olan sevgili eşim Mücahit Güleç'e en içten teşekkürlerimi sunuyorum. Her koşulda yanımda olan, beni destekleyen, akademik başarılarımla gurur duyan ve bu yolu benim için kolaylaştıran sevgili annem Mürvet Özlü ve sevgili babam Muhammet Özlü'ye, bana güç ve teşvik veren ablalarım ve kardeşime ve dostlarıma da oldukça minnettarım. Akademik sürecimin her aşamasında bilgisi ile yol gösteren, yapıcı eleştirileri ile bana rehberlik edip bu serüvenimde bana yardımcı olan değerli danışman hocam Dr. Öğr. Üyesi Gülsüm Kaya'ya katkıları için gönülden teşekkür ederim.

İÇİNDEKİLER

TEZ ONAY SAYFASI iii

YÜKSEK LİSANS/DOKTORA İNTİHAL YAZILIM RAPORU iv

YEMİN METNİ v

ÖZET vi

ABSTRACT vii

ÖNSÖZ viii

İÇİNDEKİLER ix

GİRİŞ 1

I- ULUSLARARASI İNSANCIL HUKUK BAĞLAMINDA HEDEF VE NESNE KAVRAMLARI 3

1. İNSANCIL HUKUKTA HEDEF VE HEDEFİ BELİRLEME 3
2. HUKUKİ ÇERÇEVE 7
2.1. 1949 TARİHLİ CENEVRE SÖZLEŞMELERİ VE EK PROTOKOLLER 7
2.2. ULUSLARARASI MAHKEME KARARLARI 11
2.3. DİĞER İLGİLİ ULUSLARARASI BELGELER VE METİNLER: 14
3. SİVİLLER VE SİVİL NESNELER 15
3.1. SİVİLLERİN HEDEF ALINMASI 16
3.2. SİVİL NESNELERİN HEDEF ALINMASI 17
4. ASKERİ KİŞİLER VE ASKERİ NESNELER 18
4.1. ASKERİ KİŞİLER (COMBATANTS) 18
4.2. ASKERİ NESNELER 20
5. SİVİL HEDEF VE ASKERİ HEDEFLERİN AYRIMI 23
6. ASKERİ GEREKLİLİK 25
7. TALİ HASAR 27
8. ÇİFT KULLANIM NESNELERİ (DUAL-USE OBJECTS) 28

II. BÖLÜM 32

ULUSLARARASI İNSANCIL HUKUKTA SİBER SALDIRI KAVRAMI 32

1. SİBERUZAY 33
2. SİBER OPERASYONLAR 34
2.1. TANIMI VE ÖZELLİKLERİ 34
2.2. SİBER OPERASYON TÜRLERİ 35
3. İNSANCIL HUKUK KAPSAMINDA SİBER SALDIRILAR 40
3.1. SİBER SALDIRILARIN TANIMI 40
3.2. SİBER SALDIRILARIN ULUSLARARASI İNSANCIL HUKUK KAPSAMINA GİRMESİ 41
3.3. İNSANCIL HUKUKTA SALDIRI KAVRAMI İLE İLİŞKİSİ 43
3.4. SİBER SALDIRILARIN SİLAHLI ÇATIŞMA OLARAK KABUL EDİLMESİ 45

4. ULUSLARARASI HUKUKTA SİBER SALDIRILARLA İLGİLİ MEVCUT DÜZENLEMELER VE BOŞLUKLAR 48
4.1. TALLİNN KILAVUZU (NATO) 49
4.2. BİRLEŞMİŞ MİLLETLER ÇALIŞMALARI 52

III BÖLÜM 55

SİBER SALDIRILARDA SİVİL HEDEF 55

1. SİVİL HEDEF VE SİBER SALDIRILARA UYGULANABİLİRLİĞİ 55
2. SİBERUZAYDA ASKERİ KİŞİ VE NESNELER 56
2.1. ASKERİ KİŞİLER 56
2.2. ASKERİ NESNELER 56
3. SİVİLLER VE SİVİL NESNELER 59
3.1. SİBERUZAYDA SİVİL KİŞİLER 59
3.2. SİVİL HACKERLAR VE HUKUKİ STATÜLERİ 64
4. KRİTİK ALTYAPILAR 69
4.1. ELEKTRİK ÜRETİM VE DAĞITIM AĞLARI 71
4.2. SU VE KANALİZASYON ALTYAPISI 72
4.3. NÜKLEER ENERJİ TESİSLERİ ALTYAPILARI 73
4.4. ULAŞIM VE LOJİSTİK ALTYAPISI 73
4.5. İLETİŞİM ALTYAPISI 74
5. VERİ TABANLARI 75
5.1. SAĞLIK SİSTEMLERİ 75
5.2. KAMU HİZMETLERİNE AİT BİLGİ SİSTEMLERİ 75
5.3. FİNANS VE BANKACILIK SİSTEMLERİ 76
6. SİVİL NESNE STATÜSÜ: DİJİTAL EKONOMİK VE KÜLTÜREL VARLIKLAR 77
7. ÇİFT KULLANIM İLKESİ VE SİBERUZAYDA SİVİL NESNELER 78
8. SİBERUZAYDA BELİRSİZLİK DURUMU 80
9. HUKUKİ DEĞERLENDİRME 84

SONUÇ 88

KAYNAKÇA 90

Giriş

"Silahlı Çatışmalar Hukuku"[1] olarak da adlandırılan "Uluslararası İnsancıl Hukuk", genel olarak silahlı bir çatışma esnasında o çatışmaya taraf olan devletlerin ve bireylerin davranışlarını düzenlemektedir[2]. İnsancıl hukukun temel amaçlarından biri, silahlı çatışma esnasındaki davranışları düzenlerken aynı zamanda savaşa katılmayan sivillerin korunmasıdır. Temelinde sivillerin korunması amacını taşıyan bu hukuk dalı aynı zamanda silahlı çatışmaların araç ve yöntemlerini belirleyerek bu tarz çatışmalarda ortaya çıkacak zararı olabildiğince azaltmayı amaçlamaktadır. Silahlı çatışmalar ve bu çatışmalarda uyulması gereken kurallar, uluslararası hukukun kapsamına ise 1864 yılında kabul edilen "Savaş Alanında Yaralıların Durumunun İyileştirilmesi Sözleşmesi" ile dahil edilmiştir[3]. Bu sözleşmeye takiben, 1889 ve 1907 tarihli Lahey Düzenlemeleri, 1949 tarihli Cenevre Sözleşmeleri ve Ek Protokoller gibi insancıl hukukun temelini oluşturan sözleşmeler yürürlüğe girmiştir. Uluslararası hukukun diğer alt dallarında olduğu gibi insancıl hukuk da devletlerin kendi aralarında yaptığı anlaşmalara dayanmaktadır ancak kökleri uluslararası teamül hukukuna dayanmaktadır[4]. Kökleri bu kadar sağlam olan insancıl hukuk, gelişmiş bilgi ve iletişim sistemlerinden oluşan siberuzaya taşınmıştır. İnsancıl hukuk ile siberuzayda gerçekleşen siber operasyonların nasıl bir ilişki içerisinde olacağı, hangi durumlarda insancıl hukukun siber saldırılara uygulanacağı, bu bağlamda siberuzayda sivillerin ve sivil nesnelerin nasıl varlık gösterdiğinin belirlenmesi önem arz etmektedir. Bu çalışmanın ilk bölümünde insancıl hukuk genel hatları ile ele alınacak olup ikinci bölümde insancıl hukuk ile siberuzayın

[1] "Silahlı Çatışmalar Hukuku" ve "Uluslararası İnsancıl Hukuk" kavramları çoğu zaman eş anlamlı bir şekilde kullanılsa da aralarında ince bir nüans bulunmaktadır. Genellikle Kızılhaç (ICRC), Birleşmiş Milletler ve diğer uluslararası kuruluşlarla akademik camiada "İnsancıl hukuk" kavramı kullanılır. İnsancıl hukuk kavramının kullanılmasının temel dayanağı ise savaşa katılım göstermeyen sivillerin ve savaş tutsaklarının korunmasının düzenlendiği 1949 tarihli Cenevre Sözleşmeleridir. "Silahlı Çatışmalar Hukuku" ise genellikle askeri çevreler tarafından kullanılır ve temel dayanağı genel olarak silahlı çatışmaların yürütülmesini, çatışma esnasında savaşanların haklarını ve sorumluluklarını düzenleyen 1899 ve 1907 tarihli Lahey Sözleşmeleridir. Bu terim daha çok NATO gibi askeri kuruluşlar ve ABD gibi ülkeler tarafından kullanılmaktadır. Ancak "Uluslararası İnsancıl Hukuk" ve "Silahlı Çatışmalar Hukuku" kavram olarak farklılıklar içerse de ikisi de aynı uluslararası hukuk kurallarını kapsamaktadır *bkz.* Antoine A. Bouvier, *International Humanitarian Law and the Law of Armed Conflict*, ed. Harvey J. Langholtz (Williamsburg, VA: Peace Operations Training Institute, 2020), 12.

[2] Laurie R. Blank and Gregory P. Noone, *International Law and Armed Conflict*, (New York: Wolters Kluwer Law& Business, 2013), 3.

[3] Hüseyin Pazarcı, *Uluslararası Hukuk Dersleri IV. Kitap*, (Ankara: Doruk Kitabevi, 2020), 379.

[4] Gary D. Solis, The Law of Armed Conflict: International Humanitarian Law in War, (New York: Cambridge University Press, 2010), 119.

nasıl birleştiği, geleneksel hukuk kurallarının yeni bir alan olan siber savaşa nasıl uygulanacağı değerlendirilecektir. Son bölümde ise özellikle sivil kişiler ve nesneler bağlamında insancıl hukuk kapsamına giren siber saldırılar söz konusu olduğunda hangi şekillerde varlık gösterebilecekleri ve dikkat edilmesi gereken hususlar ele alınacaktır.

I- ULUSLARARASI İNSANCIL HUKUK BAĞLAMINDA HEDEF VE NESNE KAVRAMLARI

1. İnsancıl Hukukta Hedef ve Hedefi Belirleme

İnsancıl hukuk kuralları, silahlı çatışma esnasında meydana gelecek zarar ve kayıpların etkilerini azaltmak amacıyla çatışan tarafların uyması gereken kuralları düzenler ve bu kurallara uyulması ile silahlı çatışmaya katılmamış olan sivilleri ve onlara ait nesneleri korumayı amaçlar[5]. Silahlı çatışma esnasında çatışan taraflar, kendi kontrolleri dışındaki kişi ve nesnelere karşı güç kullanıp bu kişi ve nesneleri saldırıların hedefi olarak belirlemektedir[6]. Çatışan kişilerin saldırılarını yönlendirdiği yere ise hedef denmektedir; ancak insancıl hukuk kuralları gereği her kişi ve nesne saldırının hedefi haline getirilememektedir. Uluslararası hukuk, her kişinin ve her nesnenin saldırının hedefi haline gelmemesini koruma altına almıştır.

Birçok kuralın teamül hukuk kuralı sayıldığı insancıl hukukta en temel ilkelerden biri "Ayırt Etme İlkesi"dir (Principle of Distinction)[7]. Bir uluslararası teamül hukuku kuralı olan ve 1949 Tarihli Cenevre Sözleşmeleri Ek Protokol I (bundan sonra Ek Protokol I), madde 48'de tedvin edilen bu ilke uyarınca, silahlı çatışmanın taraflarının her zaman savaşan ve savaşmayanlar arasında ayrım yapma zorunluluğu bulunmaktadır. Ayırt Etme ilkesi sadece kişilerle sınırlı olmayıp nesneler üzerinde de geçerliliğini sağlamaktadır. Çatışma esnasında hedef alınacak kimselerin ve nesnelerin niteliğinin ne olduğunun belirlenmesi büyük bir önem arz etmektedir. Çünkü asıl amaç; silahlı çatışma süresince siviller ve sivil nesneler korunurken savaşan askerlerin veya silahlı grup üyelerinin birbirlerini çatışma dışı bırakması ve buna göre hareket etmeleridir[8]. Hedef belirlemede en önemli hususlardan biri de sivilleri ve onlara ait nesneleri (ya da amaç gereği sivillerin kullanımına hizmet eden nesneler) hedef belirlemeyi önleyen tedbirler almaktır. Ek

[5] Ayşe Nur Tütüncü, *İnsancıl Hukuka Giriş*, (İstanbul: Beta Basım Yayım, 2019): 1-2.
[6] Yoram Dinstein, *Targeting under International Humanitarian Law* (Geneva: International Committee of the Red Cross, 2020), 1, https://www.icrc.org/en/document/targeting-under-international-humanitarian-law.
[7] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (AP I) art. 48.
[8] Blank ve Noone, *International Law and Armed Conflict,* 498-499.

Protokol 1 madde 57[9] uyarınca devamlı bir şekilde sivil halkı korumak ve onları saldırı hedefi haline getirmemek için gerekli önlemlerin alınacağı düzenlenmiştir. Madde uyarınca çatışan taraflar, saldırı öncesinde sivillerin kaybını, yaralanmasını veya onlara ait nesnelerin zarar görmesini önlemek üzere mümkün olan tüm önlemleri almak zorundadır.

Saldırı anında nesnenin askeri bir nesne olmadığı ya da uluslararası insancıl hukuk kuralları tarafından koruma altında olan bir nesne olduğu anlaşılırsa bu durumda saldırıyı yaparken gerekli önlemlerin alınması ya da saldırının sona erdirilmesi gerekmektedir. Maddede geçen *"mümkün olan tüm önlemler"* ifadesi, düşman askerleri ve nesnelerine ait bilgi akışı komutan ve askerler arasında doğrudan gerçekleştiği için çatışma anında hedef belirlemek için alınacak önlemlerin karar verme sürecini daha kolay hale getirmektedir; ancak çatışma halleri oldukça çeşitli olduğu için her durumda böyle bir bilgi akışı sağlanamayabilir[10]. Nitekim hedef belirlemede gerekli önlemlere başvurmamak, gerçek çatışmalarda da sivillerin ya da koruma statüsüne sahip olanların kaybına neden olabilir. Örnek olarak hedefin yanlış tanımlanmış olması dolayısıyla Etiyopya'da bulunan Kızılhaç'a ait tesisler İtalya tarafından bombalanmış ve Kızılhaç personelleri zarar görmüştür[11]. Aynı zamanda güncel olarak Gazze'de bulunan Kızılhaç binasının yakınına İsrail tarafından atılan bomba nedeniyle hem ofis zarar görmüş hem de Kızılhaç'a mensup 22 personel hayatını kaybetmiştir[12]. Bu iki olayda da hedef alınması meşru olmayan ve uluslararası insancıl hukuk kuralları ile teamül hukuk kurallarına aykırılık taşıyan kişi ve nesneler saldırıya uğramıştır.

Savaş esnasında çatışan tarafların hedeflerini doğru belirlemeleri için kesinlik gerekmektedir[13]. Bu durumda kesinlik, saldırıda bulunacağı kişi ve nesneye yönelik

---

[9] Additional Protocol I, art 57.
[10] Fredrik Petersson, Legitimate Targets of Attack, (Yüksek Lisans Tezi: University of Lund, 2003), 36-37.
[11] Haberin tamamı için bknz. https://blogs.icrc.org/cross-files/the-cross-in-the-crosshairs-a-photographic-record-of-the-bombing-of-red-cross-field-hospitals-during-the-second-italo-ethiopian-war/ (Erişim Tarihi: 24 Mayıs 2024).
[12] Haberin tamamı için bknz. https://www.bbc.com/news/articles/cmjj6ej3ne1o (Erişim Tarihi: 4 Ağustos 2024).
[13] Ek Protokol I madde 85, madde 57'de düzenlenen önlemlerin alınmadığı durumları insancıl hukukun ağır ihlali olarak kabul etmiştir. İnsancıl hukukun ağır ihlalleri ise Roma Statüsü madde 8 uyarınca savaş suçu oluşturmaktadır ve uluslararası ceza yargılaması gündeme gelmektedir. Bu yüzden Ek Protokol I'in yapım aşamasında ceza hukukun gerektirdiği gibi kesinlik seviyesinin oldukça yüksek tutulması birçok

gözetleme, tespit etme, ayırt etme, doğru yöntemi bulma ve saldırı sonucunda istenilen gerekli sonuca ulaşmanın kesinliğidir[14]. Bu kesinliğe ulaşmak için alınan tüm önlemlerle yapılacak saldırı sonunda olası sivil kaybı, yaralanması ya da sivillere ait nesnelerin zarar görmesi ihtimalleri en aza indirilmektedir.

Hedef belirlemede diğer bir önemli husus ise "Ölçülülük" ilkesidir. Ek Protokol I madde 51[15] ve madde 57[16]'de düzenlenen bu ilke ile amaç, savaş anında askeri operasyonlarla yapılan saldırıların sebep olacağı zararı askeri gereklilik ve avantajla orantılı bir şekilde sınırlamaktır[17]. Silahlı çatışma anında çatışan taraflar arasında gerçekleştirilen saldırılar sınırlara tabiidir. Ölçülülük ilkesi, saldırının yapılmasında amaçlanan askeri avantaj ve gereklilikle saldırının neticesi arasında doğru ve dengeli bir ölçü olması gerektiğini öne sürmektedir. Böylelikle çatışma taraflarının kendi hareketlerini askeri gereklilik ve avantajı aşacak ölçüde bir zarar veya kaybın oluşmaması için sınırlandırması gerekmektedir[18].

Saldırı ile elde edilmek istenen avantaj arasında doğru oran kurulduğunda ise sivillerin ve sivil nesnelerin saldırı hedefi haline gelmeleri önlenmekte, en kötü ihtimalle yapılan saldırı sonucu oluşan tesadufi kayıplar (incidental loss)[19] olabildiğince azaltılmaktadır. Örneğin Amerikan Ordusuna ait 1956 tarihli Kara Savaşı Hukuku (Law of Land Warfare) adlı kılavuzunda ölçülülük ilkesi, *" Saldırılar sonucu can kaybı ve mal hasarı, elde edilmesi beklenen somut ve doğrudan askeri avantajla kıyaslandığında aşırı olmamalıdır*." şeklinde açıklanmıştır[20]. Bu durumda yapılan saldırının askeri gereklilik

katılımcı tarafından savunulmuştur. *Bknz.* Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Commentary of 1987, ¶ 2187.

[14] Michael N. Schmitt, "Precision attack and international humanitarian law," *International Review of the Red Cross 87*, no. 859 (Eylül 2005): 446.

[15] *"Elde edilmesi beklenen somut ve doğrudan askeri avantaja kıyasla aşırı olarak kabul edilecek miktarda sivil halkta insan hayatının kaybına, yaralanmalara ve sivil nitelikteki mallara zarar verilmesine ya da bu kayıp ve zararların hepsinin birlikte oluşmasına arızi şekilde sebep olması beklenebilecek saldırılar"*

[16] *"Bir saldırı, hedefin askeri bir hedef olmadığının ya da özel korumaya tabi olduğunun ya da yapılacak saldırı ile ondan elde edilmesi beklenen somut ve doğrudan askeri avantaja kıyasla aşırı olarak kabul edilecek miktarda sivil halkta insan hayatının kaybına, yaralanmalara ve sivil nitelikteki mallara zarar verilmesine ya da bu kayıp ve zararların hepsinin birlikte oluşmasına arızi şekilde sebep olacağının açıklık kazanması durumunda durdurulacak ya da askıya alınacaktır."*

[17] "Proportionality", erişim 5 Ağustos 2024, https://casebook.icrc.org/a_to_z/glossary/proportionality .

[18] Blank ve Noone, *International Law and Armed Conflict*, 51.

[19] Additional Protocol I, Art.55 (5)(b)

[20] Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, 274.

ve avantajla orantılı olması durumunda ortaya çıkan sınırı aşmayacak bir sayıdaki sivil kaybı insancıl hukuk kurallarına aykırılık teşkil etmemektedir. Ek olarak, askeriyeye ait bir cephanelik üreten fabrikanın bombalanması durumunda fabrika içerisinde çalışan sivil işçilerden kayıp olursa aşırıya kaçılmadığında bu durumda insancıl hukuk kuralları ihlal edilmemiş olmaktadır[21].

Sonuç olarak insancıl hukuk ve uluslararası teamül hukuku kuralları gereğince, silahlı çatışma anında askeri gruplara ait olmayan, çatışmalara doğrudan katılım göstermeyen kişiler sivil olarak kabul edilmektedir. Bu kişilere ait yerleşim yerleri, kişisel eşyalar ve kritik altyapı gibi unsurlar da ise sivil nesne statüsündedir[22]. Genel kural olarak, silahlı çatışma anında sivillerin, onlara ait nesnelerin ve hukuken koruma statüsünde olanların bir saldırı hedefi haline getirilmesi yasaktır.

Çatışan taraflar her zaman siviller ve savaşanlar arasında ayırım yapmak zorundadır. Üstelik yapılacak her bir saldırı öncesinde ve sırasında bu ayrım yasağını ihlal etmemek için çatışan tarafların mümkün olan tüm önlemleri alma zorunlulukları vardır. Ancak bazı durumlarda sivillerin kayıpları önlenemez hale gelebilmektedir; çünkü hukuk, saldırı sonucunda oluşan tesadüfi sivil kayıplarını belli bir noktada tolere etmektedir[23].

Örneğin Amerikan Ordusuna ait 1956 tarihli Kara Savaşı Hukuku (Law of Land Warfare) adlı kılavuzunda ölçülülük ilkesi, *" Saldırılar sonucu can kaybı ve mal hasarı, elde edilmesi beklenen somut ve doğrudan askeri avantajla kıyaslandığında aşırı olmamalıdır.*" şeklinde açıklanmıştır. Ölçülülük ilkesi ise sivillerin bu tesadüfi kaybının ya da sivil nesnelerin gördüğü zararın oldukça sınırlı bir seviyede tutulmasını amaçlar. Bu durum literatürde "tali hasar (collateral damage)" şeklinde adlandırılmaktadır; ancak "tali hasar" durumu, "Askeri Gereklilik" başlığı altında ileride daha detaylı ele alınacaktır.

[21] Anthony Aust, Handbook of International Law, (New York: Cambridge University Press, 2010): 242.
[22] Diakonia International Humanitarian Law Centre, "Principle of Distinction: Protection of People and Objects," *Diakonia*, accessed August 8, 2024, https://www.diakonia.se/ihl/resources/international-humanitarian-law/principle-of-distinction-protection-of-people-and-objects/.
[23] Blank ve Noone, *International Law and Armed Conflict*, 51-52.

2. Hukuki Çerçeve

2.1. 1949 Tarihli Cenevre Sözleşmeleri ve Ek Protokoller

Herhangi bir çatışan gruba ait olmayan ve çatışmalara doğrudan katılım sağlamayan sivillerin korunması, saldırı hedefi haline getirilmemesi ve onlara ait nesnelerin korunması insancıl hukukun en temel amacıdır[24]. Sivillerin korunmasının yanında onların askeri personel ve askeri nesnelerden ayırt edilmesi ise ayırt etme ilkesi gereği hem uluslararası insancıl hukukun hem de teamül hukukunun en temel ilkelerinden biridir. İnsancıl hukukta silahlı çatışmalar, uluslararası nitelikte olan ve uluslararası nitelikte olmayan silahlı çatışmalar şeklinde ikiye ayrılmaktadır. Ayrılan bu iki çatışma türü ise 1949 Tarihli Cenevre Sözleşmeleri ve Ek Protokollerde düzenlenmiştir. Uluslararası nitelikte olan silahlı çatışmalar 1949 Tarihli Cenevre Sözleşmelerinin hepsinde ve Ek Protokol I'de düzenlenmişken; uluslararası nitelikte olmayan silahlı çatışmalar 1949 Tarihli Cenevre Sözleşmlerinin ortak 3. maddesi ve Ek Protokol II'de düzenlenmiştir[25].

2.1.1. Uluslararası Nitelikte Olan Silahlı Çatışmalar

1949 tarihli Cenevre Sözleşmeleri ortak 2. madde uyarınca uluslararası nitelikte olan silahlı çatışmalar, sözleşmeye taraf olan devletlerden ikisi ya da daha fazlasının ilan ettiği bir savaş veya silahlı çatışmaların tüm durumları olarak tanımlanmıştır[26]. Uluslararası nitelikteki silahlı çatışmalar devletler arasında silahlı çatışmalar ve uluslararasılaşmış silahlı çatışmalar olmak üzere ikiye ayrılmaktadır. Devletler arasındaki silahlı çatışmalar ise, ortak madde 2'de düzenlenen taraf devletler tarafından ilan edilen savaşlar ve henüz savaşa varmamış, sınırlı nitelikteki silahlı çatışmalar olmak üzere ikiye ayrılmaktadır. Devletlerin başka bir devlete karşı savaş ilan etmesi ile o devletle savaşa varmayan silahlı bir çatışmanın içerisinde olmasının temel farkı, çatışan devletin kendi eylemlerini savaş

[24] International Committee of the Red Cross (ICRC), "What Is International Humanitarian Law?," *International Committee of the Red Cross*, accessed August 9, 2024, https://www.icrc.org/en/document/what-international-humanitarian-law#:~:text=International%20humanitarian%20law%20(IHL)%20is,means%20and%20methods%20of%20warfare.

[25] Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction*, (Geneva: ICRC, 2022): 21, Erişim Tarihi: 6 Ekim 2023, https://www.jep.gov.co/Sala-de-Prensa/Documents/4231_002-IHL_WEB_13.pdf .

[26] Maddenin tamamı için bknz. https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3 (Erişim Tarihi: 9 Ağustos 2023).

amacı ile yapmış olup olmamasına dayanmaktadır[27]. Böyle bir ayrım yapılmasının temel sebebi ise savaşa varmayan silahlı çatışmaların daha çok askeri müdahale şeklinde gerçekleşmesidir[28]. Ek olarak bir çatışmaya taraf devletlerden ikisi veya daha fazlası silahlı çatışma içerisindeyken aynı bölge içerisinde o bölgeye ait silahlı gruplar arasında da silahlı çatışmalar aynı anda gerçekleşebilmektedir[29].

Uluslararası nitelikte olan silahlı çatışmalar açısından sivillerin ve onlara ait nesnelerin saldırıya uğramaması veya saldırının hedefleri haline getirilmemeleri ile ilgili düzenlemeler 1949 Tarihli Harp Zamanında Sivillerin Korunmasına İlişkin IV. Cenevre Sözleşmesi (bundan sonra IV. Cenevre Sözleşmesi) ve Ek Protokol I'de yapılmıştır. IV. Cenevre Sözleşmesinin 27. maddesinde, temelinde insaniyet ilkesinin yattığı, sivillerin her zaman insanca muameleye tabi tutulacağı ve her türlü şiddet eyleminden uzak tutulacağı düzenlenmiştir. Aynı zamanda siviller bu türden bir korumaya sahip olurken herhangi bir ayrımcılığa maruz kalmayacakları da aynı madde içerisinde düzenlenmiştir[30]. Madde 31 ve 32'de ise hukuki olarak korunan sivillerden bilgi almak veya onlara tedbir uygulamak için fiziki olarak acı verecek veya onları yok edecek her türlü eylem yasaklanmıştır[31]. Sivillere ait nesneler açısından ise 53. maddede kesin bir askeri gereklilik hali dışında, sivillere ait kişisel mülklere saldırılarda bulunup bu kişisel mülkler üzerinde bir tahribata yol açılması yasaklanmıştır.

Ek Protokol I'de, sivillerin ve onlara ait nesnelerin saldırı hedefi haline gelmemesi için 48. maddede savaşan ve savaşmayanlar arasında ayrım yapma ilkesi düzenlenmiştir. Bu ilke uyarınca, çatışmanın tarafları mümkün olduğu ölçüde çatışma sırasında çatışan ve çatışmayan siviller arasında ayrım yapmak zorunda olup sivilleri saldırı hedefi haline getirmemekle yükümlüdürler[32]. Madde 51/1'de sivillerin çatışma esnasında genel koruma kurallarından yararlanacağı düzenlenmişken Madde 51/2'de saldırıların hedefi haline

---

[27] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 156-158.
[28] Askeri müdahale genel olarak bir devletin, kuvvet kullanma yolu ile diğer devlete kendi iradesini Kabul ettirmesi olarak açıklanmaktadır. *Bkz.* Pazarcı, Uluslararası Hukuk Dersleri IV, 159.
[29] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 2nd ed. (Cambridge: Cambridge University Press, 2010), 40-41.
[30] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 266-267.
[31] Maddelerin tam metinleri için bknz. Erişim Tarihi: 9 Ağustos 2024, https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf .
[32] Luigi Daniele, "Incidentality of the civilian harm in international humanitarian law and its Contra Legem antonyms in recent discourses on the laws of war", *Journal of Conflict & Security Law 29*, (2024): 27.

gelmeleri yasaklanmıştır. Madde 51/4'te ise sivillere ve sivillere ait olan nesnelere karşı ayrım gözetilmeyen saldırılar yasaklanmıştır. Madde 51/4 uyarınca, çatışan taraf askerlerinin saldırı esnasında askeri kişi ve nesneleri hedef haline getirmesi gerekmektedir. Askeri kişilerin ve sivillerin bir arada bulunduğu alanlarda silahın nereye isabet edeceğinin belirlenmesi ve bu belirlemeye göre hedef alınması zorunludur[33]. Madde 52'de ise sivillere ait nesnelerin genel koruması düzenlenmiş olup sivillere ait nesnelerin saldırı hedefi haline getirilmeleri yasaklanmıştır.

2.2.2. Uluslararası Nitelikte Olmayan Silahlı Çatışmalar

Uluslararası nitelikte olmayan silahlı çatışmalar, 1949 tarihli Cenevre Sözleşmelerinin ortak 3. maddesinde ve Ek Protokol II'de düzenlenmiştir. Ortak 3. Madde ile uluslararası nitelikte olmayan silahlı çatışma aşamasına ulaşan hallere, insancıl amaçlı bir takım kuralların uygulanması öngörülmüştür[34]. Maddeye göre silahlı çatışmaya doğrudan iştirak etmeyenler ve diğer koruma statüsüne sahip kişiler her surette insancıl muameleye tabi tutulacak, kişilerin vücut bütünlüğüne zarar verecek her türlü eylem yasaklanacak, rehin alma gibi hürriyeti tahdit eden durumlara müsaade edilmeyecek ve bu kişiler onurları korunup adil yargılanma hakkından yararlanacaktır[35]. Ortak madde 3, genel olarak belirli bir devletin toprakları içinde gerçekleşen, örgütlü silahlı kuvvetler veya gruplar arasında yoğun ve açık silahlı çatışmaları kapsayacak şekilde düzenlenmiştir[36].

Hangi türden silahlı çatışmaların uluslararası nitelikte olmayan silahlı çatışma olarak kabul edildiği ise Cenevre Sözleşmeleri ortak madde 3'e destek olacak şekilde, Ek Protokol II 1. maddede tanımlanmıştır. Söz konusu madde uyarınca uluslararası nitelikte olmayan silahlı çatışmanın olması için, sözleşmeye taraf olan devletlerden birinin topraklarında gerçekleşmiş olması ve gerçekleşen bu çatışmada askeri gruplar arasında bir komuta zincirinin bulunması, çatışmaların askeri operasyon şeklinde yürütülmesi, muhalif silahlı kuvvetlerin veya diğer örgütlü silahlı grupların operasyonlarını yürütürken

[33] Michael N. Schmitt, "Precision attack and international humanitarian law," 454-455.
[34] Pazarcı, *Uluslararası Hukuk Dersleri IV,* 163-164.
[35] Tütüncü, *İnsancıl Hukuka Giriş*, 63-64.
[36] Blank ve Noone, *International Law and Armed Conflict*, 106.

çatışmanın olduğu bölgede kontrol sağlaması gerekmektedir[37]. Nitekim Ek Protokol II'nin uygulanması için kendi sınırları içerisinde silahlı çatışma çıkan devletin sözleşmeye taraf olması gerekmektedir, aksi takdirde ise Ek Protokol II'nin hükümleri uygulanamamaktadır[38].

Eski Yugoslavya Uluslararası Ceza Mahkemesi'nin (EYUCM) *Tadic*[39] kararında, uluslararası nitelikte olan silahlı çatışmalar için geçerli olan uluslararası teamül hukuku kurallarının uluslararası nitelikte olmayan silahlı çatışmalar için de geçerli olduğu kabul edilmiştir[40]. Ek olarak, organize olmuş bir silahlı grubun varlığı gerektiği için toplum içerisindeki iç karışıklıklar ve haydutluk eylemleri uluslarası nitelikte olmayan silahlı çatışmaların kapsamı dışındadır[41].

Eski Yugoslavya Uluslararası Ceza Mahkemesi'nin aynı kararında mahkeme, var olan bir silahlı çatışmanın uluslararası nitelikte olmayan bir silahlı çatışma olarak kabul edilmesi için bir test uygulamıştır; yapılan test uyarınca, silahlı çatışmanın yoğunluğu ve çatışma taraflarının kendi aralarında organize olması, söz konusu çatışmanın uluslararası nitelikte olmayan bir silahlı çatışma olarak kabul edilip insancıl hukuk kurallarının uygulanabilir hale gelmesi için temel kriter teşkil etmektedir[42].

Çatışmanın yoğunluğunun belirlenmesi ise, çatışmaların sayısı ve süresi; kullanılan silahların ve diğer askeri teçhizatın türü; ateşlenen mühimmatların sayısı ve kalibresi; çatışmaya katılan kişi sayısı ve güç türü; can kaybı sayısı; maddi yıkımın boyutu; ve çatışma bölgelerinden kaçan sivillerin sayısı değerlendirilerek yapılmaktadır[43]. Böylelikle gerekli çatışma yoğunluğu ve tarafların askeri organizasyona sahip olduğu silahlı çatışmalar, uluslararası nitelikte olmayan silahlı çatışmalar olarak kabul edilmektedir.

---

[37] *Ek Protokol II'nin tam metni için bknz.* Erişim Tarihi: 10 Ağustos 2024 https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.35_AP-II-EN.pdf.
[38] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 169.
[39] *Kararın tam metni için bknz.* Erişim Tarihi: 10 Ağustos 2024, https://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf.
[40] Aust, *Handbook of International Law*, 237-238.
[41] Artem Sergeev, "Applying Additional Protocol II of the Geneva Conventions to the United Nations Forces," *Journal of International Humanitarian Legal Studies 8* (2017): 236.
[42] Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, 152-153.
[43] Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction*, 70-71.

Uluslararası nitelikte olmayan silahlı çatışmalarda da öncelik, sivillerin ve onlara ait nesnelerin herhangi bir saldırıya uğraması veya saldırının hedefi haline gelmesini önlemek olup bu durumların gerçekleşmemesi için çatışmanın taraflarına mümkün olan her türlü tedbiri aldırmaktır. Ek Protokol II'nin 4. maddesinde[44] özellikle sivillerin yaşam hakları korunup onlara karşı yapılacak doğrudan saldırılar yasaklanmıştır. Madde 13[45]'te ise sivillerin askeri operasyonlara karşı genel bir korumaya sahip olduğu düzenlenmiş ve sivillerin çatışma sırasında saldırıların hedefi haline getirilmeleri kesin bir şekilde yasaklanmıştır. Madde 14[46]'te ise sivillere ait olup sivillerin kullandığı tarım alanları, içme su tesisleri ve depoları gibi nesnelere yapılacak saldırılar da yasaklanmıştır.

2.2. Uluslararası Mahkeme Kararları

2.2.1. Uluslararası Adalet Divanı

Uluslararası Adalet Divanı (UAD), 1945 yılında Birleşmiş Milletler Şartı tarafından kurulmuş ve 1946 yılında faaliyete geçmiş uluslararası bir mahkemedir[47]. Birleşmiş Milletler Şartı madde 7 ve madde 92 uyarınca UAD, Birleşmiş Milletler'in ana yargı organıdır[48]. Divan'da uluslararası hukuktan doğan uyuşmazlıklar değerlendirilmekte ve yalnızca devletler dava tarafı olabilmektedir[49]. UAD'ın verdiği kararlar taraf devletler için bağlayıcıdır ve kesindir[50]. UAD'ın, tarafları bağlayıcı olan kesin kararlarının yanında

---

[44] *Madde 4/1: "Özgürlükleri sınırlandırılmış olsun olmasın, muhasamata doğrudan katılmayan ya da katılmaya son veren tüm kişilerin kişiliklerine, şereflerine, kanaatlerine ve dini ibadetlerine saygı gösterilmesini isteme hakları vardır. Her türlü durumda, herhangi bir aleyhte ayrım gözetilmeksizin her yerde insanca muamele göreceklerdir. Kimsenin hayatta kalmamasına yönelik emir verilmesi yasaktır." Madde 4/2: …1. fıkrada belirtilen kişilere karşı yapılan aşağıdaki davranışlar her zaman ve her yerde kesinlikle yasaktır: a) Kişilerin canına, sağlığına, fiziksel ya da manevi varlığına karşı şiddet; başta cinayet ve işkence gibi acımasız muameleler, sakatlama ya da herhangi bir bedensel ceza türü olmak üzere…*

[45] *Madde 13: "1. Sivil halk ve sivil kişiler, askeri operasyonlardan kaynaklanan tehlikelere karşı genel korumadan yararlanır. Bu korumayı etkin kılabilmek için her koşulda aşağıdaki kurallar dikkate alınacaktır.*

2. Ne sivil halk ne de sivil kişiler saldırı hedefi olmayacaktır. Birincil amacı sivil halk arasında dehşet yaymak olan şiddet hareketleri ya da tehdidi kesinlikle yasaktır."

[46] *Madde 14: "...gıda maddeleri, gıda maddelerinin yetiştirildiği tarım alanları, ekinler, hayvanlar, içme suyu tesisleri ve depoları ile sulama tesisleri gibi sivil halkın hayatta kalması için vazgeçilmez olan mallara saldırmak, bunları yok etmek, yerinden kaldırmak ve kullanılamaz hale getirmek yasaktır."*

[47] International Court of Justice, Erişim Tarihi: 12 Ağustos 2024, https://www.icj-cij.org/court .

[48] Robert Kolb, International Court of Justice, (Oxford: Hart Publishing, 2013): 61.

[49] Hakkı Hakan Erkiner, "Birleşmiş Milletler Uluslararası Adalet Divanı Kararlarının Birleşmiş Milletler Güvenlik Konseyi Aracılığıyla Uygulatılması", *MÜHF-HAD 23*, (2017): 89.

[50] Erkiner, "Birleşmiş Milletler Uluslararası Adalet Divanı Kararlarının Birleşmiş Milletler Güvenlik Konseyi Aracılığıyla Uygulatılması", 90.

görüş olarak sunduğu tavsiye kararları (advisory opinion) bulunmaktadır. UAD Statüsü 65.maddesinde Divan'ın tavsiye görüşü verme yetkisinden bahsedilmiştir. Söz konusu madde uyarınca, *"Divan, Birleşmiş Milletler Antlaşması gereğince ya da bu Antlaşma hükümlerine uygun olarak görüş istemeye yetkili kılınmış her organ ya da kuruluşun isteği üzerine her türlü hukuksal sorun konusunda görüş verebilir*[51]*."* Divan'ın verdiği tavsiye kararların bağlayıcılığı bulunmamaktadır[52]. Bu yüzden mahkemeden tavsiye görüşü talep eden organ, kurum veya kuruluş, bu görüşlere nasıl bir tepki vereceğine uygun gördüğü şekilde karar vermekte özgürdür. Tavsiye görüşleri ayrıca uluslararası hukukun açıklığa kavuşturulmasına ve geliştirilmesine ve dolayısıyla devletler arasındaki barışçıl ilişkilerin güçlendirilmesine katkıda bulunur[53]. Sivillerin ve sivil nesnelerin korunması ile onların saldırı hedefi haline gelmemesi hususunda UAD'ın önemli tavsiye görüşleri bulunmaktadır.

1996 yılında UAD tarafından, *"Nükleer Silahların Tehdit veya Kullanımının Hukuka Uygunluğu" (Legality of the Threat or Use of Nuclear Weapons)* adında bir tavsiye kararı verilmiştir. Nükleer silahların kullanılmayıp yasaklanmasını isteyen savunucular, nükleer silahların kullanılmasının sivillerin yaşama hakkını tehdit edip Medeni ve Siyasi Haklar Uluslararası Sözleşmesinin yaşam hakkını düzenleyen 6. maddesine aykırı olduğunu iddia etmiştir[54]. Bu hususu ele alan Divan, tavsiye kararının 78. paragrafında insancıl hukukun temel ilkesi olan ayırt etme ilkesinden bahsedip sivillerin ve sivil nesnelerin korunmasının asıl hedef olduğuna değinmiş, ardından siviller ile savaşanları ve bu iki tarafa ait nesneleri birbirinden ayırt etme zorunluluğuna atıf yapmıştır[55]. Kararın 95. paragrafında ise Divan, nükleer silahların kullanımının insancıl hukuk kuralları ile çelişeceğinin garantisini vermemiştir. Böylelikle nükleer silahların kullanımı bütünüyle yasaklanmamıştır. Ancak nükleer bir silahın kullanımının hukuki olduğu durumlarda da sivil hedeflerin ve askeri hedeflerin arasında mutlaka bir ayrım yapılması gerektiği, Divan

[51] Statünün tam metni için bknz. Erişim Tarihi: 12 Ağustos 2024, https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020093041bm_02.pdf .
[52] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI, art 96; Statute of the International Court of Justice (adopted 26 June 1945), art 65.
[53] Advisory Jurisdiction, Erişim Tarihi: 14 Ağustos 2024, https://www.icj-cij.org/advisory-jurisdiction .
[54] International Court of Justice, "Legality of the Threat or Use of Nuclear Weapons," Advisory Opinion, July 8, 1996, para. 24.
[55] Kararın tam metni için bknz. Erişim Tarihi: 14 Ağustos 2024, https://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/Advisory%20Opinion,%201996%20I.C.J.%20226.pdf .

tarafından kesin bir şekilde belirtilmiştir[56]. Silahların bu yasağı delecek şekilde kullanılması da insancıl hukuk ihlalinden dolayı yasaklanmıştır[57].

2.2.2. Eski Yugoslavya Uluslararası Ceza Mahkemesi

Siviller ve sivil nesne hedeflerinin asker ve askeri nesne hedeflerinden ayrımı ve korunmasına yönelik bir diğer önemli karar, Eski Yugoslavya Uluslararası Ceza Mahkemesi tarafından verilen *Galic* kararıdır. Karara konu olan olay; 6 Nisan 1992'de Sırp militanların Saraybosna'daki binlerce barış göstericisine ateş açıp en az beş kişiyi öldürmesi, 30 kişiyi yaralaması ve yaklaşık 400.000 kişinin kuşatma altında mahsur kalması sonucu yiyecek, ilaç, su ve elektriğe ulaşamamalarıdır.[58]. Mahkeme, Sırp militanları tarafından Saraybosna'daki sivil halkın öldürülmesi ve sivil halka ait nesnelerin saldırı hedefi haline getirilmesini Ek Protokol I madde 50 ve 52'ye dayanarak insancıl hukuk kurallarına aykırı bulmuştur[59].

Mahkeme uyarınca, sivillere saldırma yasağı, savaşan tarafları her zaman sivil halk ile savaşçılar ve sivil nesneler ile askeri hedefler arasında ayrım yapmaya ve buna göre operasyonlarını yalnızca askeri hedeflere yöneltmeye mecbur eden temel bir uluslararası insancıl hukuk ilkesi olan ayrım ilkesinden kaynaklanmaktadır[60]. Aynı zamanda Mahkeme kararında, Uluslararası Adalet Divanı'nın Nükleer Silahların Yasallığı Konusundaki Danışma Görüşüne değinerek, ayrım ilkesini sivil halkın korunması ilkesiyle birlikte "İnsancıl hukukun yapısını oluşturan metinlerde yer alan temel ilkeler" olarak tanımlamış ve "Devletler asla sivilleri saldırı hedefi yapmamalıdır." demiştir[61]. Yargılama Dairesi, Ek Protokol I Madde 51(2)'nin ilk kısmında belirtilen yasaklanmış davranışın, sivil nüfusa ve düşmanlıklara katılmayan bireysel sivillere karşı bir saldırı (Ek Protokol I'in Madde 49'unda tanımlandığı şekilde) yöneltmek olduğunu ileri sürmüştür[62].

[56] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, [1996] ICJ Rep 226, para 95.
[57] Blank ve Noone, *International Law and Armed Conflict,* 48.
[58] Blank ve Noone, *International Law and Armed Conflict,* 310.
[59] Prosecutor v Stanislav Galic, Case No IT-98-29-T, Judgment (ICTY, 5 December 2003) para 35.
[60] Galic (n 55) para 45.
[61] Blank ve Noone, *International Law and Armed Conflict,* 312.
[62] Galic (n 55) para 53.

2.3. Diğer İlgili Uluslararası Belgeler ve Metinler:

2.3.1. Lahey Düzenlemeleri

"Lahey Düzenlemeleri" terimi, Lahey'de kabul edilen ve savaşları düzenleyen kurallar içeren antlaşmaları ve bildirgeleri tanımlamaktadır. Bu sözleşmelerden kaynaklanan kurallar; savaş araçlarının ve yöntemlerinin kullanımını, düşmanlıkların yürütülmesini ve işgali düzenlemektedir[63]. Bu düzenlemelerden 1907 tarihli IV sayılı Kara Savaşı Kurallarına İlişkin olan Lahey Sözleşmesi (bundan sonra IV sayılı Lahey Sözleşmesi), sivillerin ve sivil nesnelerin korunup saldırı hedefi haline getirilmemeleri husunda önem arz etmektedir.

IV sayılı Lahey Sözleşmesinin 25. maddesinde sivillere ait olan herhangi bir yerleşim yerinin, kasabanın, köyün ve binanın saldırı hedefi haline getirilmesi yasaklanmıştır[64]. 1949 Tarihli Cenevre Sözleşmelerinin Lahey Düzenlemelerinin uluslararası hukuk bakımından daha yeni tarihli ve kapsamlı olması yüzünden yerine geçtiği kabul edilmektedir; ancak halen 1907 tarihli Lahey Düzenlemeleri (III sayılı Çatışmaların Başlamasına İlişkin Sözleşme ve XIV sayılı Balonlardan Patlayıcı Madde Atılmasının Yasaklanması Sözleşmesi hariç) büyük ölçüde uygulanmaktadır[65]. Cenevre Sözleşmeleri daha çok silahlı çatışma durumunda savaş mağdurlarının korunmasını düzenlerken Lahey düzenlemeleri savaşın nasıl yürütüleceği, hangi araç ve yöntemlerin kullanılacağı gibi hususları düzenlemektedir[66].

2.3.2. Uluslararası Ceza Mahkemesi Statüsü

2002 yılında faaliyete başlayan Uluslararası Ceza Mahkemesi, uluslararası olarak savaş suçlarının engellenmesi, işlenmesi durumunda ise bu suçları işleyenlerin yargılanması amaçlanan 1998 tarihli Roma Statüsü ile kurulmuştur[67]. Statünün 8. Madde (2) (b) (i) de

---

[63] Hague Conventions, Erişim Tarihi 14 Ağustos 2024, https://casebook.icrc.org/a_to_z/glossary/hague-conventions .

[64] International Peace Conference. *Regulations concerning the Laws and Customs of War on Land (Hague IV)*, Article 25. 1907. https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907/regulations-art-25 .

[65] Pazarcı, Uluslararası Hukuk Dersleri IV, 148-149.

[66] International Committee of the Red Cross, "Hague Conventions," *How does law protect in war?* (International Committee of the Red Cross, 2025), https://casebook.icrc.org/a_to_z/glossary/hague-conventions.

[67] Davut Ateş, "Sovereignty, Anarchy and the Rome Statute," *Review of International Law and Politics* 6, no. 24 (2010): 1

sivillere karşı herhangi bir saldırıda bulunmak ve onları saldırının hedefi haline getirmek insancıl hukuk kuralı ihlali olarak sayılmış ve savaş suçu[68] olarak kabul edilmiştir. Bu maddeye müteakiben 8. Madde (2) (b) (ii) de ise sivillere ait olan nesnelere saldırmak ve sivil nesneler saldırının hedefi haline getirmek de savaş suçu olarak kabul edilmiştir[69].

3. Siviller ve Sivil Nesneler

Siviller, 1949 tarihli Cenevre Sözleşmeleri ve Ek Protokollerinde "savaşan" olarak tanımlanan sınıflandırmalara dahil olmayıp herhangi bir silahlı grubun üyesi sayılmayan ve silahlı çatışmalara doğrudan katılmayan kişilerdir[70]. Ek Protokol 1 madde 52'de sivil nesneler, negatif bir anlamda askeri nesne olmayan nesneler olarak tanımlanmıştır[71]. İnsancıl hukuk ve genel olarak uluslararası hukuk tarafından korunan sivillerin hedef alınmaması, bir silahlı çatışmanın tüm katılımcıları tarafından uyulması gereken bir kuraldır. Bu bağlamda, silahlı çatışma anında hangi nesnelerin hedef haline getirileceği ve hangilerinin koruncağı büyük bir önem arz etmektedir. Hangi nesnelere karşı saldırıda bulunacağının belirlenmesi ise olabilecek herhangi bir sivilin kaybını engellemeye yöneliktir[72]. Siviller ile onlara ait nesneler ve savaşanlarla onlara ait nesnelerin birbirlerinden ayırılması kuralı, 1949 tarihli Cenevre Sözleşmeleri Ek Protokol 1'in 48. maddesinde düzenlenmiştir[73]. Bu madde uyarınca, savaşan tarafların daima sivilleri ve savaşanları birbirinden ayırması, aynı zamanda bu iki gruba ait nesneleri de bu ayrıma dahil etmesi gerekmektedir. Bu ilkenin amacı sivillerin güvenliğini ve korunmasını

[68] Bir suçun savaş suçu olarak kabul edilmesi için iki elemente ihtiyaç duyulduğu kabul edilmektedir; söz konusu suçun savaş anında yapılan saldırı ile insancıl hukuk kurallarını ihlal etmesi ve bu ihlalin ciddi bir derecede bulunması (Ek Protokol I, madde 85'teki ağır ihlalleri, grave breaches, gerçekleştirmesi). *Bkz.* Oona A. Hathaway; Paul K. Strauch; Beatrice A. Walton; Zoe A. Y. Weinberg, "What Is a War Crime," *Yale Journal of International Law 44, no. 1* (Winter 2019): 81-91.

[69] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 90, art 8(2)(b)(i)–(ii).

[70] "Attacks on Civilians and Other Unlawful Killings, and Attacks on Civilian Objects" , erişim 30 Mayıs 2024, https://www.globalprotectioncluster.org/sites/default/files/2023-02/protection_risk_02_0.pdf.

[71] Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction*, 91-92.

[72] Marco Sassoli and Lindsey Cameron, "The Protection of Civilian Objects: Current State of Law and Issues de lege feranda" *The Hague: Eleven International* (2006): 35.

[73] *48.madde*: Sivil halkın ve sivil nitelikte malların saygı görmesini ve korunmasını sağlamak için, çatışmanın tarafları daima, sivil halk ile muharipleri, sivil mallar ile askeri hedefleri birbirinden ayırt etmeli ve buna uygun olarak operasyonlarını sadece askeri hedeflere yöneltmelidirler.

sağlamaya yöneliktir[74]. Ek Protokol 1, madde 51 uyarınca da sivil nüfusu oluşturan kişilerin saldırı hedefi olması yasaklanmıştır[75]. Bu yönden protokol uyarınca, her ne kadar aynı koruma şartlarına sahip olsalar da sivil hedef bakımından sivil ve sivillere ait nesneler arasında bir ayrıma gidilmiştir.

3.1. Sivillerin Hedef Alınması

Birleşmiş Milletler İnsan Hakları Evrensel Bildirgesi 3. madde uyarınca, *"Herkesin yaşama hakkı ile kişi özgürlüğü ve güvenliğine hakkı vardır."*. Genel insan hakları kurallarından farklı olarak uluslararası insancıl hukukta ise yaşama hakkı sınırlandırılmıştır. İnsancıl hukuk kurallarınca, silahlı çatışmalar sırasında yaşama hakkından siviller yararlanmaktadır. Başka bir deyişle, çatışma boyunca savaşan tarafların askeri kişileri ve askeri hedefleri vurmasına izin verilirken; sivillerin yaşam haklarının ellerinden alınması ve onlara ait nesnelere zarar verilmesi yasaklanmıştır. Çünkü insancıl hukuk kapsamında, *jus in bello*[76]'nun mevcut olduğu anlarda çatışanların birbirlerini öldürmesi hukuka uygun bir durum olarak kabul edilmektedir[77]. Ek Protokol I 52.madde gereğince sivillerin ve savaş dışı kalmış kişilerin hedef haline getirilmesi insancıl hukuk kurallarının ihlali olarak kabul edilmiştir[78]. Sivillerin korunmasına yönelik olan hükümler, hem uluslararası nitelikte olan hem de uluslararası nitelikte olmayan silahlı çatışmalarda geçerli olup Cenevre Sözleşmelerine taraf olan ya da olmayan devletleri ve silahlı grupları da bağlamaktadır[79].

Ek Protokol I madde 48 uyarınca, çatışmaya taraf olan katılımcıların her zaman sivil ve askeri nüfusun ve sivillere ait olanlarla askeri gruplara ait olan nesnelerin ayrımını

---

[74] Eno Prasetiawan ve diğerleri, "Distinction Principle in International Humanitarian Law Related to Civilian Objects and Military Objects" *Proceedings of the 2nd International Conference Postgraduate School (ICPS 2018):* 649.

[75] *51.madde:* Sivil halk ve bireysel olarak siviller saldırının hedefi olmayacaktır. Esas amacı sivil halk arasında terör yaymak olan şiddet hareketleri ya da tehditleri yasaktır.

[76] *Jus in bello: Silahlı çatışmaya giren tarafların çatışma esnasındaki hareketlerini düzenleyen ve çatışma taraflarının uymakla yükümlü olduğunu kuralları ifade eder.*

[77] Saadat Rustemova Demirci, "İnsancıl Hukukta Hedef Alarak Öldürme" *Uluslararası İnsancıl Hukuk: Kavramlar, İlkeler ve Yeni Gelişmeler* içinde, ed. Fatma Taşdemir ve Gökhan Albayrak (Ankara: Adalet, 2018): 161.

[78] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 231.

[79] Camilla Waszink, *Protection of Civilians under International Humanitarian Law: Trends and Challenges* (NOREF Report, August 2011), 3.

yapmak zorundadır. Başka bir deyişle, çatışma sırasında sivillerle onlara ait nesnelerin korunması ve yapılacak saldırıların, çatışma taraflarına ve onlara ait nesnelere karşı yapılması gerekmektedir. Bu bakımdan ayrım sadece kişiler üzerinden değil, onlara ait nesneler üzerinden de yapılmıştır. Bu kural uyarınca, ayrım ilkesini gözetmek için çatışma tarafları, kendilerini sivil nüfustan ayıran üniforma, amblem kullanmalı ve saldırı gerçekleştirirken sivil halkın yerleşim yerlerini (askeri bir sebeple kullanılmıyorlarsa) hedef almamaları gerekmektedir[80]. Ek Protokol II madde 13 uyarınca da uluslararası nitelikte olmayan silahlı çatışmalar sırasında çatışmaya doğrudan bir katılım göstermemiş olan sivilleri, saldırının hedefi haline getirmek yasaklanmıştır[81].

3.2. Sivil Nesnelerin Hedef Alınması

Ek Protokol 1, madde 52 uyarınca sivil nesneler (civilian objects), askeri olmayan nesneler olarak tanımlanmıştır[82]. Bu tanıma göre sivil nesnelerin belirlenmesi için askeri nesnelerin neler olduğunun tanımlanması gerekmektedir. Askeri nesneler, sahip oldukları doğa, amaç, konum ve kullanım bakımından askeri faaliyetlere hizmet eden nesneler olup gösterdiği faaliyetlerle askeri avantajın elde edilmesine sebep olan nesnelerdir[83]. Bu durumda sivil nesnelerin hedef gösterilmesinden farklı olarak, askeri nesnelerin çatışma esnasında hedef olarak alınması hukuka uygun kabul edilmektedir. Ek Protokol I'in 49, 51 ve 52. maddeleri uyarınca da sivil ve sivillere ait nesnelerin korunmasının yanında bu kişiler ve nesneleri hedef haline getirerek bir şiddet eylemi veya bu eylemin yapılacağına dair bir tehditte bulunmak da yasaklanmıştır[84]. Böylelikle sivillere ait olan ve askeri amaçla çatışan bir tarafın avantaj sağlamasına hizmet etmeyen nesneler sivil nesne olarak kabul edilmekte ve bu nesnelerin çatışmada hedef haline getirilmesi yasaklanmaktadır. Uluslararası nitelikte olmayan silahlı saldırılar için ise Ek Protokol II, madde 14 uyarınca

[80] Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, 251-252.
[81] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), adopted 8 June 1977, 1125 U.N.T.S. 609, Article 13.
[82] https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52?activeTab=undefined (Erişim Tarihi: 29 Temmuz 2024).
[83] "The Practical Guide to Humanitarian Law", Medecins Sans Frontieres, Erişim Tarihi: 29 Temmuz 2024. https://guide-humanitarian-law.org/content/article/3/protected-objects-and-property/#:~:text=Rule%209%20of%20the%20customary,in%20international%20and%20non%2Dinternational
[84] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 43.

da çatışma tarafları, sivillerin sağlık bakımına dair kullanılan ve sivil nesne olarak kabul edilen tıbbi ekipmanlarla malzemelere sahip olamaz[85].[86]

4. Askeri Kişiler ve Askeri Nesneler

4.1. Askeri Kişiler (Combatants)

Askeri kişiler (bir diğer adıyla savaşanlar, combatants), silahlı çatışmalara katılmaya hakkı olup savaşan statüsünden yararlananlardır[87]. Bu kişiler kendi aralarında askeri bir grubun (silahlı kuvvetler) üyesi olan ve çatışmaya bireysel olarak doğrudan katılanlar olmak üzere ikiye ayrılmaktadır.[88] Çatışma esnasında savaşanların hangi türlerden oluştuğuna dair tanımlama, Ek Protokol I madde 43'te yapılmıştır. Maddeye uyarınca, *"çatışmanın bir Tarafının Silahlı Kuvvetleri, bu Taraf, karşı Tarafça tanınmayan bir hükümet ya da otorite tarafından temsil ediliyor olsa bile, astlarının davranışlarından bu Tarafa karşı sorumlu bir komutanlığın emri altında bulunan bütün organize silahlı kuvvetlerden, gruplardan ve birimlerden oluşur.*[89]. Bu kapsama giren savaşan kişiler, yasal savaşanlar olarak kabul edilirken bu tanımın dışında kalanlar yasadışı savaşanlar (unlawful combat) olarak kabul edilmektedir[90].

Savaşanın hukuki tanımı ise Ek Protokol I'de sadece uluslararası nitelikte olan silahlı çatışmalar için yapılmış olup uluslararası nitelikte olmayan silahlı çatışmalar için Ek Protokol II ve 1949 Tarihli Cenevre Sözleşmeleri ortak madde 3'te böyle hukuki bir tanım bulunmamaktadır[91]. Ancak uluslararası nitelikte olmayan silahlı çatışmalarda, bazı durumlarda savaşa doğrudan katılım gösteren bireylerin savaşan statüsünde olduğu kabul

[85] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), adopted 8 June 1977, 1125 UNTS 609, art 14.
[86] Ancak çatışma taraflarına ait yaralı veya hasta olan askerlerin tedavisi için sivillere ait tıbbi malzemelerin kullanılması gereklilik gösteriyorsa ve askerlerin bu malzemelerle tedavi edilmesi süresince sivillerin tedavilerinde herhangi bir aksama olmuyorsa, çatışma tarafı olan askerler sivillere ait tıbbi malzemeleri kullanabilmektedir.
[87] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 220-221.
[88] Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, 187.
[89] AP I, Article 43.
[90] Mary Ellen O'Connell, "Combatants and the Combat Zone," University of Richmond Law Review 43, no. 3 (March 2009): 851.
[91] Blank ve Noone, *International Law and Armed Conflict*, 213.

edilmektedir. Nitekim Birleşmiş Milletlerin 1970 tarihli bir kararında, savaşan statüsünün her türden silahlı çatışmalarda olduğu ifade edilmiştir[92].

Savaşan bir kişinin savaşan statüsüne sahip olması için savaşan devletin askeri gücüne üye olma zorunluluğu yoktur. Ek Protokol I madde 43 ve III Cenevre Sözleşmesi madde 4 uyarınca savaşan devletlerin silahlı kuvvetlerinin yanında, uluslararası nitelikte olan bir silahlı çatışmaya katılan savaşın tarafı olan ordulara bağlı hareket eden milisler ve gönüllü birlikleri de savaşan statüsünden yararlanmaktadır[93]. Bu kişilerin savaşan olarak sayılması için bazı şartların varlığı aranmaktadır. İlk olarak 1907 tarihli Lahey Sözleşmesi madde 1'de ve 1949 Tarihli Cenevre Sözleşmelerinin sırası ile 13/2, 13/2, 4/2 maddelerinde bu durum düzenlenmiştir[94]. Söz konusu maddeler uyarınca bu grupların başlarında gruptan sorumlu olan bir komutanın bulunması, siviller ve diğer birliklerden kendilerini ayırt edecek bir işaret ya da amblem taşıyor olmaları, ellerindeki silahları açık bir şekilde tutuyor olmaları ve uluslararası insancıl hukukun getirdiği sorumlulukları yerine getirmeleri gerekmektedir.

Savaşan olarak sayılan bir diğer grup ise uluslararası nitelikte olan silahlı çatışma esnasında kitlesel bir şekilde ayaklanan kişilerdir[95]. *Levée en masse*[96] olarak adlandırılan bu grupların savaşan olarak kabul edilmesi için kendiliğinden toplu ve açık bir şekilde silahlanmış olmaları ve topraklarının işgal tehdidi ile karşılaşması gerekmektedir. Ancak silahlı çatışma esnasında askeri birliklerin bir parçası olan sağlık ve din personelleri savaşçı statüsünde kabul edilmemektedir[97].

[92] UN General Assembly, Resolution 2676 (XXV), "Respect for Human Rights in Armed Conflicts," 9 December 1970, preamble and § 5.
[93] Pazarcı, *Uluslararası Hukuk Dersleri IV,* 221.
[94] Pazarcı, Uluslararası Hukuk Dersleri IV, 222.
[95] Pazarcı, Uluslararası Hukuk Dersleri IV, 223.
[96] 1907 Tarihli Lahey Kara Savaşı Yönetmeliği madde 2, III. Cenevre Sözleşmesi madde 4 (A).
[97] International Committee of the Red Cross, "Rule 3. Definition of Combatants," Customary IHL Database, accessed 15 Ağustos, 2024, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule3.

4.2. Askeri Nesneler

Askeri nesneler; doğaları, konumları, amaçları veya kullanımları itibariyle askeri eyleme etkili bir katkıda bulunan ve kısmen veya tamamen imha edilmeleri, ele geçirilmeleri veya etkisiz hale getirilmeleri, o anki koşullar altında kesin bir askeri avantaj sağlayan nesnelerle sınırlıdır[98]. Ek Protokol I, madde 52'nin 2. fıkrası tarafından da bu durum korunmaktadır. Maddedeki tanım uluslararası teamül hukukunun yansıması olarak kabul edilmektedir bu yüzden Ek Protokol I'e taraf olmayanlar için de maddede geçenler bağlayıcılık göstermektedir[99]. Bu maddede iki önemli husus bulunmaktadır: Söz konusu nesnenin askeri eyleme etkili bir katkıda bulunması ve nesnelerin imhasının kesin bir askeri avantaj sağlamasıdır[100]. Söz konusu maddede tanımlanan askeri nesnelere, askeri amaçlara hizmet eden silahlar, kullanılan teçhizatlar, depolar, karargahlar, silahlı kuvvetler tarafından işgal edilen binalar ve silahlı kuvvetler mensuplarının haberleşmesini sağlayan merkezler örnek olarak verilebilir[101].

Özetle, silahlı kuvvetler tarafından kullanılan ve doğrudan askeri avantaj sağlamaya yarayan nesneler, askeri nesneler olarak kabul edilip bu nesnelerin hedef haline getirilmesi uluslararası insancıl hukuk ve uluslararası teamül hukuk kuralları gereğince hukuka uygun kabul edilmektedir. Askeri nesneler; maddi bir varlığa sahip ve elle tutulur nesnelerden ibaret olmayıp insanlar ve hayvanlar da çatışma esnasında hedef alınabilecek askeri nesneler olabilmektedir[102].

Nitekim Ek Protokol I madde 52'de sivil nesneler tanımlanırken negatif anlamda bir tanımlama yapılmış ve "askeri olmayan nesneler" şeklinde belirtilmiştir. Aynı zamanda söz konusu maddede askeri nesneler ise; doğaları, konumları ve amaçları üzerinden tanımlanmıştır. Böyle bir durumda askeri nesnelerin doğalarının, konumlarının ve

---

[98] Uluslararası Kızılhaç Komitesi (ICRC), *Customary International Humanitarian Law: Rule 8*, erişim tarihi 15 Ağustos 2024, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule8.
[99] Heather A. Harrison Dinniss, "The Nature of Objects: Targeting Networks and The Challenge of Defining Cyber Military Objectives", Israel Law Review 48, (2015): 40.
[100] Blank ve Noone, *International Law and Armed Conflict*, 396-397.
[101] Heather Harrison Dennis, *Cyber Warfare and the Laws of War*, (Cambridge: Cambridge University Press, 2012): 206-207.
[102] Yoram Dinstein, "Legitimate Military Objectives Under the Current Jus in Bello", *International Law Studies 78*, (2002): 141-142.

amaçlarının ne olduğunun sivil nesnelerin kapsamının belirlenmesi ve aralarında ayrımın yapılması açısından da önem arz etmektedir.

4.2.1. Doğası Gereği Askeri Nesneler

Doğası gereği askeri olan nesneler, içsel karakter olarak askeri faaliyet amacını temsil etmektedir[103]. Başka bir deyişle, söz konusu nesnenin aslen askeri bir karaktere sahip olması gerekmektedir[104]. Bu ölçüte göre bir nesnenin doğası gereği askeri bir nesne olması için askeri eylemin gerçekleştirilmesine etkili bir katkı sağlaması gerekmektedir. Böylelikle doğası gereği askeri bir nesne olarak kabul edilen kişi veya nesnelere, *jus in bello*'nun varlığında her zaman saldırmak mümkündür ancak bu durumun da istisnaları bulunmaktadır[105]. Askeri nesneler hem taşınabilir hem de taşınamaz nitelikte olabilmektedir. Doğası gereği taşınabilir askeri nesneler; askeri uçaklar, zırhlar, savaş gemileri ve askeri uydular olarak (tahdidi olmayacak şekilde) sayılabilir[106].

4.2.2. Konumu Gereği Askeri Nesneler

Bir nesnenin konumu gereği askeri nesne olup saldırının hedefi olarak belirlenmesinde önemli olan, coğrafi konumudur[107]. Coğrafi konum, bir nesneye stratejik önem katmaktadır. Çünkü coğrafi konum gereği belirli bir alanın askeri alan olarak belirlenmiş olması, saldırıların meşru hedefi olması için önem taşımaktadır[108]. Bu yüzden sivillere ait yerler ile askeriyeye ait yerlerin arasında ayrım yapmak çok önemlidir. Nitekim askeri nesne olarak kabul edilen ve herhangi bir saldırının meşru hedefi olan bir cephaneliğin içinde sivillere ait bir marketin olması durumunda bu marketin de askeri nesne olarak

[103] Yoram Dinstein, "Legitimate Military Objectives Under the Current Jus in Bello", 146.
[104] Gloria Gaggioli Gasteyger ve George Dvaladze, "Military Objectives," in *Companion to International Humanitarian Law* (Leiden: Brill, 2018), 1, https://doi.org/10.1163/9789004342019_009.
[105] Örneğin müzede sergilenen askeri araçlar, saldırının hukuki olduğu bir askeri nesne kategorisine girmezler çünkü askeri eylemin gerçekleşmesi için herhangi bir katkı sağlamıyordur, doğası gereği saldırmak için değil sergilenmek için vardır. Bknz. Yoram Dinstein and Arne Willy Dahl, *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary* (Cham: Springer Open, 2020), 72.
[106] Dinstein and Dahl, *Oslo Manual*, 73.
[107] Gaggioli Gasteyger and Dvaladze, "Military Objectives," 2.
[108] Yoram Dinstein, "Legitimate Military Objectives Under the Current Jus in Bello", 150.

sayılması gerekmektedir; çünkü konum gereği askeri bölge içerisindedir ve çatışmanın karşı tarafı tarafından yapılan bir saldırıda askeri gereklilik ve avantaj bulunmaktadır.

Sivil kaybının oluşma ihtimalini önlemeye yönelik örnek olarak 1949 tarihli 1. Cenevre Sözleşmesi madde 19'da tıbbi kuruluşların mümkün olduğunca askeri hedeflere yönelik saldırılardan uzak duracak konumlarda ikamet etmesinin gerekliliği düzenlenmiştir[109]. Ancak günümüz şartlarında geleneksel savaş yöntemlerinin dışında belirli bir bölge içerisinde belirli bir sınıra sahip olmayan askeri nesneler de mevcuttur[110]. Savaşlar kara, deniz ve hava sınırlarını aşıp siberuzaya taşınmıştır. Bu noktada askeri nesnenin coğrafi bir bölge içerisinde olmasının getirdiği keskin sınırlar ortadan kalkmaya başlamıştır.

4.2.3. Amaç ya da Kullanım Gereği Askeri Nesneler

Askeri bir amaca hizmet eden ve bu saik ile kullanılan nesneler, askeri nesnelerdir. Çoğu zaman, bir askeri hedefin "amacı" ya doğası yönünden doğal olarak ya da kullanımı yönünden fiili olarak belirlenir[111]. Böylelikle, sivil olan bir nesne, askeri amaçlarla kullanıldığında askeri bir hedefe dönüşür[112]. Ancak sivil bir nesnenin askeri bir amaçla kullanılması durumunda bu amacın ve niyetin kesin olması gerekmektedir. Potansiyel olması durumunda askeri nesneye saldırı sonucunda sivillerin kaybına yol açma ihtimali vardır[113]. Bu ihtimalin tamamen göz ardı edilip her koşulda saldırıda bulunmak ise insancıl hukuk kurallarını ihlal etmek anlamına gelmektedir.

Askeri bir amaca hizmet eden; veri hatları, fiber optik kablolar, telefon hatları ve telgraf hatları da askeri nesne olarak kabul edilip saldırı hedefi haline gelebilmektedir[114]; ancak siviller de bu veri hatlarını veya kablolarını kullanabilmektedir. Bu durumda ortak kullanım nesnelerinin varlığı söz konusudur; çünkü nesne hem siviller hem de askerler/savaşanlar tarafından kullanılmaktadır. Böyle bir durumda öne çıkan ve dikkat

[109] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, August 12, 1949, art. 19, 75 U.N.T.S. 31.
[110] Horrace B. Robertson, Jr, "The Principle of the Military Objective in the Law of Armed Conflict", International Law Studies 72, (1998): 207.
[111] Yoram Dinstein, "Legitimate Military Objectives Under the Current Jus in Bello", 148.
[112] Heather Harrison Dennis, *Cyber Warfare and the Laws of War*, 48.
[113] Bu yüzden Ek Protokol I, madde 57/3'te eş değerde bir askeri avantajın elde edileceği birkaç hedef varsa sivillerin ve sivil nesnelerin en az zarar göreceği hedefin seçilmesi gerektiği düzenlenmiştir.
[114] Dinstein and Dahl, *Oslo Manual*, 76.

edilmesi gereken husus, askeri gereklilik ve avantajdır. Çift kullanım nesneleri ise ileriki bölümlerde ele alınacaktır.

5. Sivil Hedef ve Askeri Hedeflerin Ayrımı

İnsancıl hukuk kuralları uyarınca, yalnızca askeri kişiler ve onlara ait nesnelerin saldırı hedefi haline getirilmesi meşru kabul edilmektedir[115]. Böylelikle, askeri hedef kriterlerini karşılamayan sivil hedeflere yönelik saldırılar yasaklanmıştır[116]. Ancak silahlı çatışmaya doğrudan katılım gösteren siviller bu korumanın dışında kalmaktadır[117]. Bu nedenle, silahlı çatışma esnasında siviller ve onlara ait nesneler ile askeri kişiler ve onlara ait nesneler arasında meşru hedefe ulaşmak adına kesin bir ayrımın yapılması gerekmektedir. Nitekim, askeri kişi ve nesneleri saldırının hedefi haline getirmek ne kadar meşru olsa da bu durumun da istisnası bulunmaktadır.

Askeri bir hedef, hedef olduğunda, saldırı yine de sivilleri veya sivil nesneleri etkileyen aşırı yan hasar bekleniyorsa yasadışı hale gelebilmektedir[118]. Ek Protokol I, madde 48'de düzenlendiği gibi söz konusu iki taraf arasında her şartta ayrım yapılması ve çatışma taraflarının bu ilkeye uyması beklenmektedir. Nitekim 1977 tarihli Ek Protokol I'i onaylayan ve bu onaylama ile protokol hükümlerine bağlı olan ülke sayısı az olsa da ayrım yapma ilkesi bir uluslararası teamül hukuku kuralı olduğundan dolayı Protokol, tarafı olmayan herkese karşı bağlayıcı özelliğini göstermektedir.

Önceki bölümde incelendiği gibi askeri nesneler, düşmanın "savaşma" kapasitesiyle yeterli bir bağlantının olduğu nesnelerdir[119]. Ancak bir nesne her ne kadar sivillere ait olsa da askeri bir amaçla kullanıldığında askeri nesneye dönüşür ve saldırının meşru hedefi haline gelir. Örneğin normal şartlarda okullar ve yerleşim yerleri sivillere ait olduğundan saldırının hedefi haline getirilemezler ancak bu yerler çatışmanın tarafı olan silahlı kuvvetlerce kullanıldığında artık askeri hedef haline gelir ve hukuken meşru bir

[115] *Bknz*. Ek Protokol I madde 48, madde 52 (2), 1907 tarihli Lahey Düzenlemeleri madde 25, madde 27.
[116] Blank ve Noone, *International Law and Armed Conflict*, 410.
[117] "Direct Participation in Hostilities," *ICRC Casebook on International Humanitarian Law*, accessed August 16, 2024, https://casebook.icrc.org/a_to_z/glossary/direct-participation-hostilities.
[118] Marco Sassoli, *Legitimate Targets of Attacks Under International Humanitarian Law* (International Humanitarian Law Initiative, 2003), 1.
[119] Gaggioli Gasteyger and Dvaladze, "Military Objectives,", 3.

hedefi oluşturur[120]. Ancak bir nesnenin askeri bir nesne olduğundan ya da bir kişinin silahlı kuvvet üyesi olduğundan şüphe duyuluyorsa bu durumda o nesne ya da o kişi, askeri bir hedef olarak değerlendirilemez hale gelir[121]. Böylelikle silahlı bir çatışma sırasında çatışma taraflarının saldırı öncesinde ve esnasında sivil hedef ve askeri hedef arasındaki ayrımı, taraflarda hedefin özelliğine dair herhangi bir şüphe bırakmayacak şekilde yapması gerekmektedir ve bu durum için ise tüm gerekli önlem ve tedbirleri almak zorundalardır[122].

Sivil ve askeri hedeflerin arasında ayrım yapılması ilkesi ve bu ilkeye uyulmaması durumunda hangi hukuki sonuçların ortaya çıkabileceği hakkında Uluslararası Adalet Divanı'nın *Demokratik Kongo Cumhuriyeti v. Uganda* kararı oldukça önem taşımaktadır[123]. Söz konusu yargılama, Demokratik Kongo Cumhuriyeti'nin Uganda'nın kendisine karşı silahlı saldırı eylemlerinde bulunduğunu iddia ederek Mahkemeye bir başvuruda bulunmasıyla 1999 yılında başladı. Her iki tarafın da Divanın zorunlu yargı yetkisini kabul ettiği davada, Demokratik Kongo Cumhuriyeti ile Uganda arasındaki yirmi üç yıllık bir hukuki anlaşmazlık, 2022 yılında bu kararla sonlandırıldı[124].

Divan, Uganda'nın Demokratik Kongo Cumhuriyeti (bundan sonra DRC) topraklarında yaptığı insan hakları hukuku ve uluslararası insancıl hukuk kuralları ihlallerini inceledi. Yapılan inceleme sonucunda hem 1999 yılında hem de 2022 yılında verilen kararda Divan, Uganda'nın ilgili zamanda Ituri'de işgalci bir güç olduğu sonucuna varmış ve Uganda'nın uluslararası insancıl hukukun getirdiği yükümlülükleri ihlal eden askeri eylemlerde bulunduğunu aynı zamanda da insan haklarını ihlal ettiğini tespit etti[125]. Söz konusu ihlalin nedeni ise Divan'ca, Uganda Cumhuriyeti'nin silahlı kuvvetlerinin Kongo sivil halkına yönelik öldürme, işkence ve diğer insanlık dışı muamele eylemlerinde bulunması gibi birçok savaş suçu teşkil eden fiillerin yanında, sivil ve askeri hedefler

[120] Blank ve Noone, *International Law and Armed Conflict*, 410.
[121] Tütüncü, *İnsancıl Hukuka Giriş*, 88., bknz. Ek Protokol I, madde 52/3.
[122] Ek Protokol I madde 51, madde 57, madde 58.
[123] Daha detaylı bilgi için bknz. Erişim Tarihi: 18 Ağustos 2024, https://www.icj-cij.org/case/116 .
[124] Jaemin Lee "Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)." *American Journal of International Law* 117, no. 1 (2023): 113. https://doi.org/10.1017/ajil.2022.84.
[125] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I.C.J. Reports 2005, p. 67.

arasında ayrım yapmaması ve diğer savaşçılarla çatışmada sivil halkı korumaması gibi eylemler olarak açıklanmıştır[126]. Divan, yargılama sonucunda Uganda'nın DRC'nin iddialarının çoğu uyarınca verdiği zararlardan[127] sorumlu olduğuna karar verdi. Yargılama sonucunda ise Divan, dava tarafı Uganda aleyhine kişilere verilen zarar için 225.000.000 ABD doları, mala verilen zarar için 40.000.000 ABD doları ve doğal kaynaklara verilen zarar için 60.000.000 ABD doları tazminata hükmetmiştir[128].

6. Askeri Gereklilik

Bu ilke uyarınca uluslararası insancıl hukuk, meşru bir askeri amacı gerçekleştirmek için gerçekten gerekli olan ve uluslararası insancıl hukuk tarafından başka türlü yasaklanmayan önlemlere izin verir[129]. Çünkü bir silahlı çatışmanın içerisinde çatışan tarafların amacı karşısındaki silahlı kuvvetin askeri gücünü zayıflatmak olmalıdır. Bu ilkenin amacı, savaşan tarafların kendi amaçlarına ulaşmak için gerekli eylemleri gerçekleştirirken aynı zamanda uluslararası insancıl hukuk kurallarına da riayet etmesini sağlamaktır[130]. 1863 yılında Abraham Lincoln 'ün isteği ile hazırlatılan ve Amerika Birleşik Devletleri'nde var olan iç savaş döneminde silahlı çatışma esnasında uyulması gereken kuralları düzenleyen *Lieber Code* 14. maddede ise askeri gereklilik ilkesi; savaşın amaçlarını güvence altına almak için vazgeçilmez olan ve modern savaş hukuku ve teamüllerine göre yasal kabul edilen tedbirleri ifade eder[131].

Askeri gereklilik ilkesi, 1949 tarihli Cenevre Sözleşmeleri ve Ek Protokol I'de ayrı bir madde olarak düzenlenmiş olmayıp 1907 tarihli Lahey Düzenlemeleri IV'ün 23. maddesinde yer almıştır. Söz konusu madde uyarınca da *savaşın gereklilikleri tarafından*

---

[126] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Reparations, Judgment, I.C.J. Reports 2022, p. 16.
[127] Divan, Uganda'yı DRC'nin iddia ettiği çevresel zarardan delil yetersizliği nedeniyle sorumlu tutmamıştır. DRC bu hasarın boyutuna dair hiçbir kanıt ve değerlendirilmesi için bir metodoloji de sunmamıştır.
[128] International Court of Justice, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Case No. 116, Judgment of 19 December 2005, accessed August 18, 2024, https://www.icj-cij.org/case/116.
[129] "Military Necessity," *ICRC Casebook on International Humanitarian Law*, accessed August 19, 2024, https://casebook.icrc.org/a_to_z/glossary/military-necessity.
[130] Adem Özer, Uluslararası İnsancıl Hukukta Askeri Gereklilik İlkesi ve İnsani Mülahazalar Arasındaki Denge, *Türk Savaş Çalışmaları Dergisi 4*, (2023): 191.
[131] Francis Lieber, *Instructions for the Government of Armies of the United States in the Field* (Washington, D.C.: Government Printing Office, 1863), §14.

zorunlu kılınmadıkça düşman mülkünü yok etmek veya ele geçirmek yasaklanmıştır[132]. Aynı tanımlama Uluslararası Ceza Mahkemesi'nin Statüsünün 8. Maddesinde de yapılmış ve savaşın yol açtığı bir gerekliliğin olmadığı durumlarda söz konusu eylemlerin yapılması savaş suçu olarak kabul edilmiştir.

Askeri gereklilik ilkesi, insancıl hukuk kurallarının temel ilkelerinden olan gereksiz acıların önlenmesi (unnecessary suffering) ve ölçülülük (proportionality) ilkesi ile kopmayacak bir bağlantıya sahiptir[133]. Çünkü bir silahlı çatışma durumunda çatışan taraflar, askeri gerekliliği yerine getirmek için saldırıda bulunur ancak yapılan bu saldırıların insancıl hukuk kurallarını ihlal etmemesi gerekmektedir. Bu nedenle, askerî gereklilikten dolayı bir saldırı gerçekleştirilse bile, bu saldırının uluslararası insancıl hukuk kurallarına aykırı olmaması gerekir. Saldırı, her zaman ölçülü olmalı ve gereklilik bulunmasına rağmen sivillere gereksiz acılar yaşatmamalıdır. Nitekim askeri gereklilik için kuralın dışına çıkmak; ancak insancıl hukuk kurallarının istisnai[134] olarak buna izin vermesi ile mümkün hale gelmektedir[135].

1949 Tarihli Cenevre Sözleşmelerinde ve Ek Protokol I'de, askeri gereklilik ilkesini tanımlayan ve sınırlarını çerçeveleyen bir madde olmasa da Ek Protokol I, 51.madde'de askeri gerekliliğe dair zımni bir düzenlemenin yapıldığı öngörülmektedir[136]. Söz konusu madde uyarınca, *"elde edilmesi beklenen somut ve doğrudan askeri avantaja kıyasla aşırı olarak kabul edilecek miktarda sivil halkta insan hayatının kaybına, yaralanmalara ve sivil nitelikteki mallara zarar verilmesine ya da bu kayıp ve zararların hepsinin birlikte oluşmasına arızi şekilde sebep olmasının beklenebileceği saldırılar*" uluslararası insancıl hukuk kuralları ihlali sayılıp yasaklanmıştır. Maddeden de anlaşılacağı üzere, yapılan saldırı ile gerçekleşmesi beklenen somut avantajın aşırıya kaçma durumunda ortada

---

[132] *Convention (IV) Respecting the Laws and Customs of War on Land*, Annex to the Convention: Regulations Respecting the Laws and Customs of War on Land, October 18, 1907, art. 14.
[133] Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, 259.
[134] Örneğin normal şartlarda hastaneler, silahlı çatışma esnasında koruma statüsüne sahiptir ve herhangi bir saldırıya uğramaktan muaftır. Ancak çatışma esnasında bu hastane çatışmanın tarafı olan silahlı kuvvetler tarafından ele geçirilir ve kullanılırsa bu durumda çatışmanın diğer tarafının söz konusu hastaneye saldırması askeri gereklilik ilkesi öne sürülerek hukuka uygun hale gelecektir.
[135] International Committee of the Red Cross, *The Principles of Humanity and Necessity*, PDF, p. 2, accessed August 20, 2024, https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf.
[136] Gökhan Güneysu, Askeri Gereklilik İlkesi ve Uluslararası İnsancıl Hukuk, *Ankara Barosu Dergisi 4*, (2012): 102.

saldırının askeri gerekliliği ile neticesi arasında orantısızlık oluşmaktadır. Bu orantısızlık ise insancıl hukuk ihlali olup savaş suçu olarak kabul edilir.

7. Tali Hasar

Askeri gereklilik ilkesi ile bağlantılı bir başka önemli husus, çatışma sırasında yapılan saldırılar sonucu oluşan tali hasarlardır. Tali hasar (collateral damage) kavramı, savaş sırasında hedef alınmasına izin verilmeyen kişilere, hayvanlara veya nesnelere verilen zararı ifade edip bu zararın, savaş sırasında hedef alınmasına izin verilen kişilere, hayvanlara veya nesnelere yönelik saldırıların bir yan etkisi olarak ortaya çıkması durumudur[137]. İnsancıl hukukun ve uluslararası teamül hukukunun başlıca ilkelerinden biri olan ayrım ilkesi uyarınca savaşanlar ve savaşmayanlar arasında ve onlara ait nesneler arasında her zaman ayrım yapmak zorunluluğu bulunmaktadır.

Askeri kişi ve nesneleri saldırı hedefine getirip zarar vermek hukuka uygun olandır; ancak bazı durumlarda meşru hedefe yapılan saldırı sivilleri de etkileyebilmektedir. Her ne kadar savaş sırasında siviller veya sivil nesneler öldürülebilir, yaralanabilir veya yok edilebilir olsa da bu tür kayıplar yalnızca meşru bir askeri hedefe yönelik bir saldırının yan etkisi olarak ortaya çıktığında tolere edilebilir[138]. Dikkat edilmesi gereken husus ise ortaya çıkan tali hasarın askeri gereklilik ilkesi ile doğru orantıda olup aşırılığa kaçmamasıdır.

Askeri gereklilik ve tali hasarla bağlantılı olarak Eski Yugoslavya Uluslararası Ceza Mahkemesi'nin *Kupreškić* kararı oldukça önem taşımaktadır. Özet olarak; Nisan 1993'te Bosnalı Hırvat güçleri, Müslüman sakinleri kendilerine karşı suçlar işleyerek uzaklaştırmayı amaçlayarak köye saldırdı ve saldırıda yüzlerce Müslüman sakin öldü, çok sayıda kişi yaralandı ve Müslüman evleri ve camileri yıkıldı[139]. Bu durumun üzerine Zoran Kupreškić, Mirjan Kupreškić, Vlatko Kupreškić, Drago Josipović, Dragan Papić

[137] David Lefkowitz, "Collateral Damage." In War: Essays in Political Philosophy, edited by Larry May, 145-64. (New York: Cambridge University Press, 2008): 145.
[138] Valerie Epps, "Civilian Casualties in Modern Warfare: The Death of the Collateral Damage Rule," Georgia Journal of International and Comparative Law 41, no. 2 (2013): 330.
[139] "Prosecutor v. Kupreškić et al. (IT-95-16-T)." *International Crimes Database*. Accessed August 20, 2024. https://www.internationalcrimesdatabase.org/Case/77/Kupre%C5%A1ki%C4%87-et-al/.

ve Vladimir Šantić, Bosnalı Müslüman nüfusa karşı işlenen suçlardaki rolleri nedeniyle Eski Yugoslavya Uluslararası Ceza Mahkemesi'nin önüne çıkarıldı. Yapılan yargılama sonucu "tali hasar" bağlamında Mahkeme, sivil halka verilen herhangi bir tesadüfi ve (kasıtlı olmayan) zararın askeri saldırıyla elde edilen doğrudan askeri avantajla orantısız olmaması gerektiğine değindi[140]. Mahkeme, askeri hedeflere yapılan saldırılar sonucunda sivillerin ikincil olarak zarar görmesinin hukuki açıdan şüpheli olabileceğini belirtti; ancak, Ek Protokol I madde 57 ve 58'de düzenlenen tedbirler alındığında, sivillerin zarar görmesinin, aşırılığa kaçılmadıkça hukuka aykırı olarak değerlendirilemeyeceği Mahkeme tarafından belirtildi[141]. Kararın sonunda ise yargılanan failler, "insanlığa karşı suç" tan hapis cezası aldılar.

Kupreškić kararında da değinildiği üzere önemli olan husus, uluslararası insancıl hukuk kurallarına riayet edilmesidir. Temelinde askeri gereklilik ilkesinin yattığı ve çatışmanın karşı tarafının gücünü zayıflatmanın amaçlandığı saldırılarda saldırının hedefi her ne kadar hukuken meşru olsa da bu saldırıda hedef olmamalarına rağmen siviller de zarar görebilmektedir. Buradaki hukuka uygunluk turnusolü ise neticesinde sivillerin zarar gördüğü söz konusu saldırının Ek Protokol I madde 57 ve 58'de düzenlenen gerekli tedbir veya önlemlerin alınıp alınmadığıdır. Saldırıda bulunan kişilerin yapması gereken ilk şey sivilleri ve savaşanları ayırt etmek ve siviller ile onlara ait olan nesneleri saldırı hedefi haline getirmemektir. Askeri gerekliliğin tedbirden önde tutulduğu durumlarda orantısızlık ve askeri gereklilikte aşırıya kaçma meydana geldiği için uluslararası insancıl hukuk ihlali gerçekleşmektedir. Gerçekleşen bu ihlal ise savaş suçu oluşturmaktadır.

8. Çift Kullanım Nesneleri (Dual-use Objects)

Çift kullanım nesneleri hem askeri hem de sivil işlevleri olan ve saldırıya uğraması halinde sivil nüfusa hukuka aykırı şekilde zarar verme ihtimali olan nesnelerdir[142]. Ek Protokol I'de ise yalnızca sivil ve askeri nesneler hukuken düzenlenmiş ve sivil nesneler

[140] International Criminal Tribunal for the Former Yugoslavia (ICTY), *Prosecutor v. Kupreškić et al.*, Case No. IT-95-16-T, Judgment, January 14, 2000, para. 524, https://www.internationalcrimesdatabase.org/Case/77/Kupre%C5%A1ki%C4%87-et-al/.
[141] International Criminal Tribunal for the Former Yugoslavia (ICTY), *Prosecutor v. Kupreškić et al.*, Case No. IT-95-16-T, Judgment, January 14, 2000, para. 526, https://www.internationalcrimesdatabase.org/Case/77/Kupre%C5%A1ki%C4%87-et-al/.
[142] Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, 534.

için negatif bir tanımlama yapılarak *"askeri nesne olmayan nesneler"* şeklinde bir tanımlama getirilmiştir [143]. Ancak Ek Protokol I madde 52 (2)[144]'den anlaşılan, bir nesnenin doğası, konumu amaçları ya da kullanımları gereği askeri eyleme katkıda bulunması ve bu katkının askeri bir avantaj sağlama hedefi sağlaması, o nesnenin askeri bir nesne olarak kabul edilmesi için yeterli kabul edilmiştir; böylelikle söz konusu maddede değinilen özelliklere sahip olan bir nesnenin ek olarak sivillerin hayatına bir katkıda bulunup bulunmamasına değinilmemiştir[145].

Genel olarak Çift kullanım nesneleri, askeri bir hedef olarak nitelendirilen, ancak aynı zamanda siviller tarafından da kullanılabilen nesnelere atıfta bulunmak için kullanılır[146]. Örnek olarak, çatışma anında iletişim ve ulaşım ağları hem askeri kişiler hem de siviller tarafından kullanılabilmektedir[147]. Önemli olan husus, çatışma anında hem savaşanlar hem de siviller tarafından kullanılan bu Çift kullanım nesnelerinin saldırı hedefi haline getirilmesinin nasıl bir maddi ve hukuki bir sonuç yaratacağıdır.

Savaş yöntemlerinin teknoloji ile iç içe olduğu dönemde devletlerin silahlı kuvvetlerinden, organize olmuş silahlı gruplara kadar elektrik kullanımı; silahlı kişiler arasında emir-komuta zincirinin sağlanması, savaş uçaklarının kullanılması ve bunun için kara ile iletişimde bulunulması gibi durumlarda hiç olmadığı kadar fazla hale gelmiştir. Bu yüzden çift kullanım nesnesi olarak sayılan elektrik sistemine yapılan bir saldırı sonucu, düşman ciddi şekilde engellenebilir ve belki de lidersiz bir şekilde saldırılara karşı savunmasız hale gelebilir[148]. Ancak elektrik tesislerine yapılan bir saldırının sivillerin kaybına ya da sivil nesnelerin zarar görmesine yol açma ihtimali vardır. Ya da demiryolu yönlendirme bilgisayarlarına, hava trafik kontrol sistemlerine veya telefon

[143] Sivil nesneler ve askeri nesneler, Ek Protokol I madde 52.
[144] *"Saldırılar sadece askeri hedeflerle sınırlı olacaktır. Mallar söz konusu olduğunda, askeri hedefler, doğaları, konumları, amaçları ya da kullanımları gereği askeri eylemlere etkin bir katkıda bulunan ve tamamen ya da kısmen yok edilmesi, ele geçirilmesi ya da etkisiz hale getirilmesi durumunda, mevcut koşullar altında, kesin bir askeri avantaj sağlayan objelerle sınırlıdır."*
[145] Henry Shue; David Wippman, "Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions," *Cornell International Law Journal 35*, no. 3 (Winter 2002): 563.
[146] Maurice Cotter, "Military Necessity, Proportionality and Dual-Use Objects at the ICTY: A Close Reading of the Prlic et al. Proceedings on the Destruction of the Old Bridge of Mostar," Journal of Conflict and Security Law 23, no. 2 (2018): 297.
[147] International Committee of the Red Cross, "Rule 8. Definition of Military Objectives," *Customary IHL Database*, accessed August 21, 2024, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule8.
[148] Solis, *The Law of Armed Conflict: International Humanitarian Law in War,* 535.

santrallerine yönelik bilgi savaşı saldırılarının varlığının sivil toplum üzerindeki etkisi devasa ve ağır olabilmektedir[149]. Bu yüzden Çift kullanım nesnelerinde temel ölçüt, orantılılığın sağlanmasıdır.

Orantılılık ise önceki bölümde değinildiği gibi askeri gereklilik ile bağlantılıdır. Çatışan taraf, askeri gereklilik olarak bir saldırıda bulunduğunda bu saldırının neticesi ve amacı arasında orantı ve denge olmak zorundadır. Bir uluslararası teamül hukuku olan orantılılık ilkesi, Çift kullanım nesnelerine yapılan saldırılarda da hayati öneme sahiptir.

Çift kullanım nesnelerin saldırı hedefi haline getirilmesinin hukukiliği ile ilgili doktrinde ise ortak bir görüş bulunmamaktadır. Nitekim NATO üyesi olan Amerika Birleşik Devletleri'nin bu konuya yaklaşımı tüm çift kullanım nesnelerinin askeri nesneler olarak kabul edilmesidir; ancak bazı Avrupa merkezli yorumcular ABD'nin bu görüşüne katılmayıp çift kullanım nesnelerine yapılan saldırıların hukuken meşru olmadığını savunmaktadır[150].

Çift kullanım nesneleri, saldırı hedefi haline getirildiğinde bu saldırı sonucunda sivillerin veya sivil nesnelerin zarar görmesi neticesi meydana gelebilmektedir. Böyle bir durumda hukuka uygunluktan bahsedilmesi için söz konusu saldırının, siviller bağlamında kasten yapılmaması ve sivil kaybının veya sivil nesnenin zararının bir tali hasar olarak ortaya çıkması gerekmektedir.

Tali hasar ve tesadüfi yaralanmalar genellikle üç faktörün etkileşimi sonucu ortaya çıkmaktadır: Neyin vurulduğunun belirsizliği, uygulanan kuvvet miktarının tam olarak ölçülememesi ve hedefin vurulabileceğine dair bir kesinliğin olmaması[151]. Bu faktörlerin varlığı sonucunda meydana gelen tesadüfi sivil kaybının büyüklüğü ise, saldırının hukuken izin verilebilir olup olmadığına ilişkin genel yargıya etki eder[152]. Saldırı sonucu

[149] Michael N. Schmitt, "The Principle of Distinction in 21th Century", 2 Yale Hum. Rts. & Dev. L.J. (1999): 168.
[150] Solis, *The Law of Armed Conflict: International Humanitarian Law in War,* 536.
[151] Michael N. Schmitt, "The Principle of Distinction in 21th Century", 167.
[152] Henry Shue, "Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Function", 564.

orantı sağlanamamış ve aşırılığa kaçılmışsa bu durumda insancıl hukuk ihlali ortaya çıkmış sayılmaktadır.

II. BÖLÜM

ULUSLARARASI İNSANCIL HUKUKTA SİBER SALDIRI KAVRAMI

1990'lı yıllardan beri içerisine interneti de alan bilgi teknolojilerinin ortaya çıkması, yayılması ve geliştirilmesi, teknolojiyi günlük hayata oldukça yakından dahil etmiştir[153]. Teknolojik gelişmeler sadece günlük hayatı etkilemekle kalmamış; siyaset, ekonomi ve güvenlik gibi alanları da etkisi altına almaya başlamıştır. Silahlı çatışmalar anlamında ise meydana gelen teknolojik gelişmeler savaşın kapsamını değiştirmiş ve yeni tanımlar getirmiştir. Teknolojinin ulusal sosyo-ekonomik sistemlerden, finans sektörüne, sivillere ve askerlere ait temel altyapıların kurulum ve işleyişine kadar her alana yayılması, tüm bu sistemleri ve sistemlerin muhataplarını birbirine bağlı kılmıştır[154].

Geleneksel savaş yöntemlerinde; devletler arasında uluslararası alanda yapılan silahlı çatışmalar; hava, kara ve deniz olarak üçe ayrılmıştır. Ancak söz konusu teknolojik gelişmeler ışığında saldırının yapılmasının kolaylığının ve hızının daha fazla etkili olduğu siberuzay ortaya çıkmıştır[155]. Siberuzayda meydana gelen siber operasyonların kullanımının savaş yöntemi olarak yaygınlaşması ve gelecekte de kullanılması oldukça muhtemel hale gelmiştir[156]. Bu yüzden siberuzayın, siber operasyonların ve siber saldırıların içeriklerinin ne olduğu ile teori ve pratiğe nasıl yansıdığının detaylı bir şekilde ele alınması oldukça önem arz etmektedir.

---

[153] Semin Töner Şen, *Siber Uzay ve Uluslararası Hukuk*, (İstanbul: Onikilevha Yayınları, 2021), 1.
[154] Hemen Philip Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, And Cyber Warfare in the 21st Century" Baltic Journal of Law and Politics 10, (2017): 3.
[155] Kenan Dülger, Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar, (İstanbul: Onikilevha Yayınları, 2023): 7.
[156]Laurent Gisel, Tilman Rodenha¨user ve Knut Do¨rmann, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts" International Review of the Red Cross 102, (2020): 288.

1. Siberuzay

Siberuzay, doktrinde genel olarak kabul edilen bir tanımlamaya sahip değildir; ancak en genel anlamı ile ağ sistemleri anlamına gelmektedir[157]. Birçok türden yazılıma ve donanıma sahip olan bu ağ sistemleri ile diğer bilgi sistemleri arasında bilgiler tanımlanıp kaydedilmekte ve aktarılmaktadır[158]. Bilginin iletimini oldukça kolaylaştıran siberuzay aracılığıyla; hava, kara ve deniz gibi bilinen klasik sınırların dışına çıkılmış ve sanal bir alan meydana gelmiştir. Siberuzay bir alan oluştur ki bu alana birçok yerden ve birçok farklı kişiler tarafından kolaylıkla ulaşılabilir hale gelmiştir[159]. Aynı zamanda da sınırları olmayan bir alan olmuştur[160].

Siberuzay temel olarak; internet, URL (uniform resource loader) ara yüzünden erişilen World Wibe Web (www) ve içinde bilgisayar sistemlerini bulunduran siber takımadası olarak tanımlanmaktadır[161]. Bu üç araç ile sanal alanda birçok türde faaliyet yapılmaktadır. Dünya genelinde de devletler, özel kurum ve kuruluşlar ile bireyler gelişmiş üretkenlik gösteren siberuzayı oldukça fazla kullanmakta olup kamu hizmetlerinin birçoğu e-devlet şeklinde dijitale taşınmış, şirketler faaliyetlerini çevrimiçi sistemlerden yürütmeye başlamıştır[162]. Siberuzayın bu yaygın kullanımı aynı zamanda devletlerin savaş stratejilerine de etki etmekte olup, savaşlarda kullanılmak üzere üretilen askeri araçlarda dijitalleşmeye ve otomatik sistemlere geçilmeye başlanmıştır[163].

Dijitalleşmenin yanında siberuzay, güvenlik açıklıklarına da sebep olmaktadır. Söz konusu ağ sistemlerine virüs denilen kodlar yüklenip ağa kayıtlı olan bilgilerin izinsiz bir şekilde aktarılması, yok edilmesi ya da değiştirilmesi söz konusu olmaktadır. Bir ağ sistemine saldırırken birçok farklı kötü amaçlı kod türü kullanılabilmektedir[164]. Kod

---

[157] Şen, *Siber Uzay ve Uluslararası Hukuk*, 3.
[158] Dülger, *Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar*, 8.
[159] Merve Leman Bulut Mişe, *Uluslararası Hukukta Müdahale Ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar*, (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2024), 6.
[160] Merve Erdem ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 68, (2019): 128.
[161] Şen, *Siber Uzay ve Uluslararası Hukuk,* 5.
[162] U. M. Mbanaso ve E.S. Dandaura, "The Cyberspace: Redefining a New World", IOSR Journal of Computer Engineering 17, (2015):17.
[163] Jeffrey Biller, Cyber Operations and the Second Geneva Convention, *International Review of the Red Cross 100*, (2018): 166.
[164] Dülger, Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar, 32.

düzeyinde, rootkitleri[165] yüklemek için siteler arası komut dosyası oluşturma (XSS) veya arabellek taşmaları gibi saldırı vektörlerini veya sisteme arka kapı görevi gören ve saldırıyı yaymak için kullanılan, *Truva atı* adı verilen solucanlar veya virüsler bulunmaktadır[166]. Ağ sistemlerine yapılan bu saldırılar ise siber operasyon olarak adlandırılmaktadır[167].

2. Siber Operasyonlar

2.1. Tanımı ve Özellikleri

Siber operasyonlar terimi genel olarak, siberuzayda veya siberuzayın kullanımıyla hedeflere ulaşma amacıyla siber yeteneklerin kullanılması anlamına gelmektedir[168]. Aynı zamanda bilgisayar ağlarının savunulması, ağdaki bilgilere karşı yapılacak saldırıların engellenmesi; karşı tarafa ait bilgi ağlarının kendilerini savunma ve saldırma yeteneğinin ortadan kaldırılması gibi düşmana ait bilgilerin yürütülmesini sabote eden faaliyetler de siber operasyon olarak kabul edilmektedir[169].

Siber operasyonlar, bireylerin kullandığı bilgi ağları arasında gerçekleştirildiği gibi devletlerin bilgi ağ sistemlerine yönelik de gerçekleştirilmektedir. Hem bireyler arasında hem de devletlere yönelik yapılan bu operasyonlar, birçok alanda dijitalleşen temel hizmetler için korunma zafiyeti ortaya çıkarmış olup bu zafiyet konusunda devletleri aksiyon almak üzere harekete geçirmiştir[170]. Örneğin 1988 yılında Amerika Birleşik Devletleri Savunma Bakanlığının bilgi sistemine yönelik yapılan bir siber operasyon sonucunda orduya ait F-35'lerin üretim bilgileri çalınmış ve hava araçlarının konumları bulunmuştur[171]. Devletlerin güvenlik sistemlerine yönelik yapılan siber operasyonlar

---

[165] "Rootkit", *siber suçluların tespit edilmeden makine verilerine erişmesini ve sızmasını sağlayan bir tür kötü amaçlı yazılım programıdır. Daha fazla bilgi için bknz.* https://www.fortinet.com/resources/cyberglossary/rootkit (Erişim Tarihi: 13 Ekim 2024).
[166] Steve Winterfeld ve Jason Andress, The Basics of Cyber Warfare: Understanding the Goals of Cyber Warfare Theory and Practice, (Waltham, Syngress: 2013): 6.
[167] Dülger, Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar, 59.
[168] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 24.
[169] Blank ve Noone, *International Law and Armed Conflict*, 132.
[170] International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Geneva: ICRC, November 2019), 3.
[171] Noah Simmons, "A Brave New World: Applying International Law of War to Cyber-Attacks," *Journal of Law & Cyber Warfare 4*, (Winter 2014): 43.

zamanla artış göstermiş ve operasyonlar etki alanı olarak daha da derinleşmiştir. Devletlerin dijital sistemlerine zarar veren, para kaybına sebebiyet veren, güvenlik zafiyeti yaşatan siber operasyonlar ise birçok ülkede siber suç olarak düzenlenmiş olup bu suça dair kendi hukuki düzenlemelerini yapmışlardır[172] [173].

2.2. Siber Operasyon Türleri

Siber operasyonlar, saldırı olarak yapıldığı ağ sisteminde güvenlik zafiyetine yol açmaktadır. Sistemde ortaya çıkan bu zafiyetler sonucu saldırıya uğramanın engellenmesi için ise siber güvenlik kavramı ortaya çıkmıştır. Böylelikle, bilişim sistemlerine karşı yapılan siber operasyonların engellenmesi ve bu alanda güvenliğin sağlanması için gizlilik, bütünlük ve erişebilirlik gibi hususların güvence altına alınıp yapılan operasyonları tespit edecek mekanizmaların geliştirilmesi söz konusu olmuştur[174]. Siber güvenliğin sağlanması için devletler; kendi iç hukuklarında koruyucu kanunlar yürürlüğe koymuş, uluslararası hukukta ise ortak hukuki düzenlemeler yapılmıştır[175].

Siber güvenlik mekanizması geliştiren siber operasyonların ise hangi türlerde olup bilişim sistemlerine ne tür etki ve kayıplarda bulunabileceği önem taşımaktadır. Genellikle devletlere ait hizmetlerin internet uygulamaları, çevrimiçi birçok amaca hizmet eden sayfalar ve sosyal medya gibi alanlar, siber operasyonların muhataplarını oldukça geniş bir alana yaymıştır.

---

[172] Merve Erdem ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü,", 130.

[173] Örneğin Türk hukukunda; 5651 Sayılı, "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Hakkında Kanun*", Alman hukukunda; "*Alman Ceza Kanunu (Strafgesetzbuch)*", Amerika Birleşik Devletleri hukukunda; "*Computer Fraud and Abuse Act (CFAA)*".

[174] Şen, *Siber Uzay ve Uluslararası Hukuk*, 122.

[175] NATO tarafından yapılan Tallinn Manuals (Tallinn Kılavuzu), Birleşmiş Milletlerin Siber Uzman Grupları kurması gibi.

2.2.1. Hizmet Dışı Bırakma Yöntemi (Denial of Service)

Bu yöntemde, saldırıya uğrayan ağ, ağı aşırı yükleyen ve tüm erişime kapatan değersiz mesajlarla boğulur ve böylelikle saldırıya uğrayan sistem, hizmet edemez hale gelir[176]. DDoS (Distrubuted Denial of Service) versiyonunda ise siber operasyonu gerçekleştirecek olan saldırgan, bu saldırı öncesinde bir makine ya da bilgisayar topluluğu oluşturur ve bu sistemlere program yükler; yüklenen bu programla ise aynı anda tüm makine ve bilgisayarlar birden aynı hedefe giriş talebi göndererek saldırı gerçekleştirir[177]. Bu iki benzer türde de amaç aynıdır. Yapılan operasyon sonucu saldırıya uğrayan sistemin işlemesi ve hizmet etmesi engellenmiş olur. Bu yönteme, bir web sitesini şantaj yapmak, komuta ve kontrol sistemlerini bozmak, tıklama dolandırıcılığı veya karmaşık problemleri derlemek için başvurulmaktadır[178].

2.2.2. Virüs ve Solucan Kullanma Yöntemi (Usage of Viruses and Worms)

Bu yöntemde, siber operasyonu gerçekleştirmek için virüs ve solucanlar kullanılır. Bu virüs ile solucanlar; kendilerini sürekli kopyalar ve genellikle e-posta yoluyla gönderilip sıklıkla alıcının kişisel bilgisayarındaki veri dosyalarını ve programları bozar[179]. Virüsler, internet üzerinden ağ sistemine bulaşıp çoğalabildiği gibi çevrimdışı olarak hard disk, USB gibi araçlarla da bu çoğalmayı devam ettirebilmektedirler[180]. Ancak solucanlar ve virüslerin kullanımı hususunda temel fark bulunmaktadır. Bilişim sisteminin içine sokulan solucanlar (Worms) ağın kullanıcısının herhangi bir yardımına veya etkileşimine gerek duymadan yayılmakta iken virüsler genelde saldırıya uğrayan ağın kullanıcısının bir dosyayı açması, bir linke tıklaması gibi etkileşimler sonucu sisteme yayılmaktadır[181].

1989 yılında NASA'nın bilişim sistemleri, sisteme solucan yüklenmesi ile önemli bir siber saldırıya uğramıştır. "WANK (Worms Against Nuclear Killers)" adı verilen bu

[176] Robert W. Hahn and Anne Layne-Farrar, "The Law and Economics of Software Security," *AEI-Brookings Joint Center Working Paper* No. 06-08 (April 2006), 4, (Erişim Tarihi: 20 Ekim 2024), https://ssrn.com/abstract=897725.
[177] Şen, Siber Uzay ve Uluslararası Hukuk, 125.
[178] Winterfeld ve Jason Andress, *The Basics of Cyber Warfare*, 7.
[179] Hahn and Layne-Farrar, The Law and Economics of Software Security, 5.
[180] Merve Leman Bulut Mişe, *Uluslararası Hukukta Müdahale Ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar*, 14.
[181] Winterfeld ve Jason Andress, *The Basics of Cyber Warfare*, 6.

saldırı, kimlikleri bilinmeyen bir grup tarafından NASA'nın nükleer faaliyetlerde bulunmasını engellemek amacı ile gerçekleştirilmiştir[182].

Bilgisayara yüklenen virüs hususunda ise tarihte bilinen ilk örnek 1986 yılında ortaya çıkan "Brain" adlı virüstür. IBM BC[183] tabanlı olan bu virüs, disket kullanımının yaygın olması sebebi ile yayılmıştır; ancak girdiği sistemlerde zarara yol açmamıştır[184].

2.2.3. Truva Atı (Trojan Horse)

Truva Atı, solucan ve virüslerle bağlantılı olan kötü amaçlı yazılımlardır. Bu yazılım, iyi huylu bir uygulama olarak görünse de sisteme girdikten sonra içindeki kötü amaçlı olan yazılım kodlarını kullanmaktadır[185]. Adını Yunan mitolojisinden alan Truva atı, bir sisteme girdikten sonra sistemdeki verileri silip yok etmekte ve bunun dışında da sistemi tümüyle çalışamaz hale getirmektedir[186]. Bu kötü amaçlı yazılımı diğerlerinden ayıran ve daha zararlı kılan husus ise, bu yazılımın yüklü olduğu sistemin yararlı bir yazılım olarak görünmesidir. Görünürde kötü amaçlı yazılımın belli olmaması hususu yüzünden Truva Atı'nın sistemden silinip atılması da zorlaşmaktadır. Genelde bir e-mailin ekinde ya da bedava olarak indirilebilen dosyaların içinde gizlenmektedir[187]. Siber operasyon yapılırken Truva Atı yöntemine başvurulmasının temel sebebi ise saldırıya uğrayan ağ sisteminin siber saldırıyı gerçekleştiren kişi tarafından müdahale ve kontrol edilmesidir[188].

Truva Atı kullanarak yapılan siber operasyonların en önemli olanlarından biri 2010 yılında, İran'a ait *Natanz* adlı nükleer tesise karşı yapılan "Stuxnet" adlı saldırıdır. Bu

---

[182] Purdue University, "The Mystery of the WANK Worm," *CyberTAP Blog*, erişim tarihi 22 Ekim 2024, https://cyber.tap.purdue.edu/blog/articles/the-mystery-of-the-wank-worm/.
[183] Büyük bilgisayar sistemleri anlamına gelmektedir.
[184] Dülger, *Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar*, 55.
[185] Hahn and Layne-Farrar, The Law and Economics of Software Security, 5.
[186] Dülger, *Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar*, 58.
[187] "Trojan Horse Virus," *Fortinet*, erişim tarihi 22 Ekim 2024, https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus.
[188] Merve Leman Bulut Mişe, *Uluslararası Hukukta Müdahale Ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar,* 15.

saldırı ile söz konusu nükleer tesisin ağ sistemindeki santrifüj kontrol sistemleri manipüle edilmiş ve İran'ın uranyum zenginleştirme çalışmaları engellenmeye çalışılmıştır[189].

2.2.4. Rootkit

Rootkit, işletim sisteminin kontrolünü ele geçiren ve sistemde olup bitenler hakkında yanlış bilgi veren bir programdır ve kullanımı durumunda bilgisayar korsanının klasörlerini gizleyip (örneğin, bilgisayar korsanı araçları, yasadışı filmler, çalınan kredi kartı numaraları) veya sistemin durumunu yanlış gösterebilmektedir[190]. Rootkit yolu ile siber operasyon gerçekleştirecek kişi sisteme gizli bir şekilde giriş yapmakta ve kontrolü sağlamak için sistemin bir parçası gibi hareket etmektedir[191]. Rootkiti kullanan kişi, saldırı düzenlediği sistemde yönetici konumuna gelebildiği için bu yöntem en tehlikeli ve zararlı siber operasyon türlerinden biri olarak kabul edilmektedir.

Rootkit yöntemi ile kayıtlara geçen önemli siber operasyonlardan biri Amerika Birleşik Devletleri ve NASA'nın bilişim sistemlerine yönelik yapılan "*Moonlight Maze*" operasyonudur. Yapılan siber operasyonda, Amerika Birleşik Devletleri'ne ait askeri uygulamalara sahip teknolojilerle ilgili binlerce hassas ancak sınıflandırılmamış belgenin Rusya'da olan hackerlar tarafından çalındığını iddia edilmiştir[192]. Üstelik söz konusu saldırının yaklaşık 2 yıldır yapıldığı tespit edilmiştir. Yapılan bu saldırı üzerine ise Amerikan Ordusu, siber güvenliğin güçlendirilmesi için 200 milyon Dolar kadar güvenlik donanımına harcama yapmıştır.

2.2.5. Sosyal Mühendislik (Social Engineering)

Sosyal mühendislikte, saldırıyı gerçekleştiren kişi, birini kandırarak güvenli olan bilgileri ifşa etmesini sağlar ve böylece yetkili gibi görünen ancak olmayan ağ veya veri tabanı erişimini etkinleştirir; sosyal mühendisliğin büyüyen bir biçimi olan "phish" sahte bir e-

---

[189] "Stuxnet Nedir?" *Elfanet*, erişim tarihi 22 Ekim 2024, https://elfanet.com.tr/tr/main/article/stuxnet-nedir/105.
[190] Winterfeld ve Jason Andress, *The Basics of Cyber Warfare*, 6.
[191] Dülger, *Uluslararası Hukukta Siber Savaşa İlişkin Esaslar*, 64.
[192] "Moonlight Maze," *ScienceDirect*, [erişim tarihi: 22 Ekim 2024], https://www.sciencedirect.com/topics/computer-science/moonlight-maze.

posta olarak solucan veya Truva atının aksine kendi başına herhangi bir hasara yol açmaz, bunun yerine gizli verileri suçlulara iletmeye yardımcı olur ve onlar da bunu hırsızlık ve dolandırıcılık için kullanır[193].

Sosyal mühendislik, insanları aldatma üzerine kurulmuştur ve hem bilgisayar hem de insan olmak üzere iki kolu bulunmaktadır. İlk olarak kandırılmak istenen kişiye telefon, e-mail gibi yollarla ulaşılmakta ve sonrasında o kişinin aldatma teknikleri ile bilgisayar kullanması teşvik edilmektedir[194].

2.2.6. Arka Kapı (Backdoor)

Arka kapı yönteminde ise yapılan siber operasyonla, saldırıya uğrayan sistemin güvenlik politikaları aşılıp sisteme izinsiz giriş yapılmakta ve bu yolla sadece sisteme izinsiz giriş yapılmayıp sistem, bir sonraki saldırılara da açık hale getirilmektedir[195]. Bir arka kapı saldırısı gerçekleştirmek, sistem zayıflıklarından faydalanmayı veya saldırgan için bir giriş noktası oluşturan kötü amaçlı yazılım yüklemeyi içermekte olup diğer arka kapı saldırıların artışına, hassas verilerin sızdırılmasına ve operasyonlarda kesintilere neden olmaktadır[196]. Bu yöntemle programcının (veya onun yakınlarının) daha sonra oluşturulacak resmi parola korumaları ve diğer güvenlik önlemlerini geçmeden programa erişmesine olanak tanınmaktadır[197]. Yapılan birçok siber operasyon, diğer yöntemlerle birlikte arka kapı yöntemi içermektedir bundan dolayı bu yöntemin kullanılması oldukça yaygındır. Oldukça yaygın olan bu siber operasyonun başkaları tarafından tespit edilip müdahale edilmesi ise oldukça zordur[198].

---

[193] Hahn and Layne-Farrar, The Law and Economics of Software Security, 6.
[194] Dülger, *Uluslararası Hukukta Siber Savaşa İlişkin Esaslar,* 74-75.
[195] Dülger, *Uluslararası Hukukta Siber Savaşa İlişkin Esaslar,* 69.
[196] CrowdStrike, "Backdoor Attack," *CrowdStrike*, last modified 2024, Erişim Tarihi 22 Ekim, 2024, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/backdoor-attack/?srsltid=AfmBOor04RH9fd6FmtMHfVhnh1wpKjJTto9EefqxDYeW-iY1KFzZGdus.
[197] Hahn and Layne-Farrar, The Law and Economics of Software Security, 7.
[198] Merve Leman Bulut Mişe, *Uluslararası Hukukta Müdahale Ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar,* 17.

3. İnsancıl Hukuk Kapsamında Siber Saldırılar

3.1. Siber Saldırıların Tanımı

Siber saldırılar, bilgi sistemi kaynaklarında var olan verileri değiştirmeye, tahrip ve yok etmeye çalışan kötü niyetle yapılan işlemlerdir[199]. Başka bir deyişle siber saldırılar, kişilere zarar, ölüm veya nesnelere hasar veya yıkım getirmesi makul olarak beklenen, saldırı ya da savunma amaçlı yapılan siber operasyonlardır[200]. Önceki bölümde ele alınan siber operasyonların da temel kullanım amacı aynıdır. Bu yüzden siber operasyonlarla siber saldırıları birbirinden ayırmanın temel ölçütü, insancıl hukuk kurallarına hangi türden siber operasyonların dahil olup olmadığının belirlenmesidir. Teknolojinin gelişmesi ile siberuzayda yapılan faaliyetler dünya genelinde hızlı bir yayılımla artış göstermiş ve bu kullanım alanı özellikle de devletlerin silahlı kuvvetleri teknolojilerine dahil olmuştur. Silahlı çatışmalar sırasında bu tür teknolojilerin devletler tarafından kullanılması yaygınlaşmıştır. Birçok devlet ordusunun silahları ya bir ağ sistemine ve yazılıma bağlı hale gelmiştir ya da doğrudan siberuzaya özel geliştirilmiştir[201]. Silahlı çatışmalar esnasında yapılan siber operasyonlar sonucunda özellikle siviller ve sivillere ait altyapılar zarar görmüştür[202]. Siber operasyonların sivil halk için hayati önem taşıyan hizmetlerin sağlanması için gerekli altyapının işleyişini engellemek ya da bozmak amacıyla kullanılması, bu türden siber operasyonları insancıl hukuk kapsamına sokmuştur[203].

Hangi türden siber operasyonların siber saldırı olarak kabul edilip insancıl hukuk kapsamına sokulacağı hangi siber operasyonların bu kapsam dışında kalacağının belirlenmesi oldukça önem taşımaktadır. Siber saldırılar ve insancıl hukuka dair şu ana kadar bağlayıcı olan herhangi bir uluslararası sözleşme yapılmamıştır. Aynı zamanda

---

[199] National Institute of Standards and Technology, "Cyber Attack," *NIST Glossary*, accessed December 10, 2024, https://csrc.nist.gov/glossary/term/cyber_attack.
[200] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 91, Rule 30.
[201] Şeyda Türkay, "Siber Savaş Hukuku ve Uygulanma Sorunsalı," *Journal of Istanbul University Law Faculty* 71, (2013): 1179.
[202] International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations During Armed Conflicts," *International Review of the Red Cross* 102, no. 913 (2020): 483, https://doi.org/10.1017/S1816383120000478.
[203] Eitan Diamond, "Applying International Humanitarian Law to Cyber Warfare", Law and National Security: Selected Issues 67 (Pnina Sharvit Baruch and Anat Kurz Eds., INSS Memorandum No. 138), (2014): 67.

1949 tarihli Cenevre Sözleşmelerinde de siber operasyon ve siber saldırı ayrımı ile insancıl hukukun bu konuyu nasıl düzenleyeceğine dair herhangi bir hüküm bulunmamaktadır. Ancak bu konuya dair NATO (North Atlantic Treaty Organization) 'nun öncülüğünde hazırlanan Tallinn Kılavuzu, detaylı düzenlemelere sahiptir. İnsancıl hukuk ve siber saldırıların ilişkisi Cenevre Sözleşmeleri ve Tallinn Kılavuzu birlikte değerlendirilerek ele alınacaktır.

3.2. Siber Saldırıların Uluslararası İnsancıl Hukuk Kapsamına Girmesi

İnsancıl hukuk, silahlı çatışma esnasında çatışmaya taraf olan devlet ve bireylerin davranışlarını düzenlemektedir. Bu sayede, silahlı çatışma esnasında hangi silahların kullanılacağı, bu silahların nasıl bir etkiye sahip olacağı, çatışan kişilerin çatışma yöntemlerinin neler olacağı belirlenmektedir. Silahlı çatışmalarda savaşanların kullandığı yöntemler zarar verici, yaralayıcı ve öldürücü niteliktedir. Önemli olan husus, çatışma esnasında yapılan siber saldırıların, insancıl hukukun konusu oluşturan geleneksel savaş yöntemlerinin verdiği etkiye sahip olup olamayacağının belirlenmesidir[204]. Aynı zamanda çatışma esnasında yapılan siber saldırıların dışında başlı başına siber savaşın insancıl hukukta var olan silahlı çatışma kapsamına girip girmeyeceğinin belirlenmesi de önem arz etmektedir.

Sivillerin günlük hayatta hizmet olarak sıklıkla yararlandığı enerji santralleri, barajlar, su arıtma tesisleri, doğal gaz hatları, bankalar ve hastanelerin çevrimiçi sistemleri gibi altyapılar; siber saldırılara uğrayabilmektedir[205]. Nitekim Estonya, 2007 yılında büyük çaplı bir siber saldırının mağduru olmuştur. Vatandaşlarına verdiği hizmet yönünden oldukça dijitalleşen Estonya'nın, bankacılık, finans gibi hizmet veren sistemleri saldırıya uğramış ve bu sistemler bir süre boyunca faaliyet gösterememiştir[206]. 22 gün boyu süren ve Hizmet Dışı Bırakma (DoS) türünde olan bu siber saldırının gerçekleştirilme nedeni ise siyasi olarak kabul edilmektedir ve faili Rusya Federasyonu olarak görülmektedir[207].

---

[204] Dülger, *Uluslararası Hukukta Siber Savaşa Dair Temel Esaslar*, 161.
[205] Eitan Diamond, "Applying International Humanitarian Law to Cyber Warfare", 67.
[206] Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal 6*, (2015): 477.
[207] Daha detaylı bilgi için *bknz.* Aapo Cederberg and Rain Ottis, *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2008),

Aynı şekilde 2008 yılında Gürcistan devletine ait websiteleri ve haber sitelerine karşı siber saldırılar düzenlenmiştir. Tıpkı Estonya'ya yapılan saldırıda olduğu gibi bu saldırı da DoS yöntemiyle yapılmıştır[208]. Aynı şekilde 2010 yılında İran'a ait nükleer santrallere karşı Amerika Birleşik Devletleri tarafından siber saldırıda bulunulmuş ve bu saldırıdan yüzbinlerce bilgisayar etkilenip bazıları çalışamaz hale gelmiştir[209]. Söz konusu vakalar, bu tür saldırıların yapılması durumunda yaralı ya da ölü olmasa bile bu saldırıların ne kadar savaşçı bir doğaya sahip olduğunu ve ne kadar geniş kitleleri etkileyebileceğini göstermektedir[210].

Siber saldırıların geniş çaplı etkileri göz önüne alındığında yaralama ve öldürme durumlarının meydana gelmesi muhtemel görünmektedir. Yapıldığında bu tür etkilere sahip olan saldırılar ise insancıl hukukun kapsamına girmektedir. Nitekim Gürcistan'a yapılan siber saldırı esnasında herhangi bir sivil kaybı ya da zarar görmesi gerçekleşmemiştir. Yapılan saldırılarda nesnelere fiziksel zarar veya kişilerin yaralanması gibi durumlar oluşmamıştır[211]. Ancak saldırının geniş kesimleri etkilemesi yapılacak diğer siber saldırıların sivillerin kaybına yol açabilecek kadar etkili olabileceği ortaya çıkmıştır. Gürcistan'daki durumun diğerlerinden farklı olmasının sebebi, siber saldırı esnasında Rusya ile halihazırda devam eden bir savaşın olmasıdır. Gürcistan ve Rusya arasında geleneksel yöntemlerle yapılan bir savaş mevcut bulunmakta olup savaş, ek olarak siberuzaya da taşınmıştır[212].

Bir siber saldırının insancıl hukuk kapsamında bir saldırı (attack) olarak kabul edilmesi için hangi şartları taşıması gerektiği oldukça önem arz etmektedir. Siber operasyonlar ve siber saldırıları birbirinden ayıran ölçütü de bu şartlar oluşturmaktadır.

---

https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[208] Paulo Shakarian, "The Criticality of Captains' Education: Now and in the Future," *Military Review* (November-December 2011): 63.

[209] Detaylı bilgi için bknz. https://casebook.icrc.org/case-study/iran-victim-cyber-warfare (Erişim Tarihi: 12 Aralık 2024).

[210] Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks", 478.

[211] Michael N. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues", International Law Studies 87, (2011): 95.

[212] Michael N. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues", 89.

Siber saldırıların nasıl insancıl hukuk kapsamına girdiğinin belirlenmesi için öncelikle insancıl hukukta genel olarak "saldırı" (attack) kavramının nasıl düzenlendiği ele alınmalıdır. Bu husus ise genel olarak savaşın yürütülmesine ilişkin esaslar içeren ve birçok hükmü uluslararası teamül hukuk kuralı olarak kabul edilen 1977 tarihli Cenevre Sözleşmeleri Ek Protokol I'de düzenlenmiştir[213].

3.3. İnsancıl Hukukta Saldırı Kavramı ile İlişkisi

Ek Protokol I madde 49 uyarınca, *"saldırılar, hücum ya da savunma nitelikli olan ve düşmana karşı yöneltilen şiddet eylemleri anlamına gelmektedir"*. Bu hükümden anlaşılacağı üzere silahlı çatışmanın kapsamında giren saldırılar, şiddet eylemi niteliğinde olmalıdır. Şiddet eyleminden kastın ne olduğunun belirlenmesi önem taşımaktadır. Protokolün gerekçeli açıklamasında (commentary) söz konusu maddede düzenlenen saldırı tanımı, bir savaş eylemi (combat action) olarak nitelendirilmiştir[214]. Maddede saldırı çeşitlerinin ne olacağı ve hangi yöntemlerle bu saldırıların gerçekleştirileceği belirtilmemiştir.

Savaşın genel etkilerine karşı genel koruma kurallarını içeren bölümde düzenlenen maddenin 3. fıkrası uyarınca bu hükümler sivillerin etkileneceği kara, hava ve deniz savaşlarını kapsamaktadır. Anlaşılacağı üzere saldırının tanımında da maddenin kapsamında da siberuzay ve saldırılara ilişkin herhangi bir atıf bulunmamaktadır. İnsancıl hukuka ilişkin diğer uluslararası metinlere bakıldığında da güncel olarak siber saldırıları düzenleyen hükümler bulunmamaktadır; Estonya, İran ve Gürcistan'ın uğradığı siber saldırılar önemli örnek oluştursa da hala insancıl hukuk ve siber saldırıların *jus ad bellum* ve *jus in bello*'ya yönelik düzenlendiği bir uluslararası sözleşme bulunmamaktadır[215]. Ancak siber saldırılara dair bir düzenlemenin bulunmaması siber saldırıların insancıl

---

[213] Eitan Diamond, "Applying International Humanitarian Law to Cyber Warfare", 75.

[214] ICRC Database, **Treaties, States Parties and Commentaries**, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977., Commentary of 01.01.1987 , Article 49 - Definition of attacks and scope of application, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49/commentary/1987?activeTab= (Last accessed on 20.12.2024).

[215] Hemen Philip Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, And Cyber Warfare In The 21st Century", *Baltic Journal of Law & Politics* 10:1 (2017): 16.

hukukun kapsamına girmeyeceği anlamına gelmemektedir. Bu durumun en önemli kanıtlarından biri Ek Protokol I, madde 36'da düzenlenmiştir.

Söz konusu maddede silahlı çatışma anında yeni silahların kullanımı ele alınmış ve kullanılacak yeni silahlar için herhangi bir sınırlama getirilmemiştir. Önemli olan husus, sözleşme tarafı olan Devletin yeni bir silah kullanması durumda bu yeni silahın uluslararası hukuk ve insancıl hukuk kuralları bağlamında hukukiliğini ya da aykırılığını bildirme yükümlülüğünü yerine getirmesidir. Yeni silahın hukuki olup olmadığının ölçütü ise bir önceki madde olan 35. maddede düzenlenen gereksiz yaralama ve acı çektirme özelliklerine sahip olup olmamasıdır[216]. Kısacası madde 36 ile devletlerin, uluslararası hukuk tarafından yasaklanıp yasaklanmadığını belirlemek amacıyla tüm yeni silahların, araçların ve savaş yöntemlerinin yasal incelemesini yapması yükümlülüğü getirilmiştir[217]. Böylelikle, yeni silahların kullanımında herhangi bir fiziki sınırlama getirilmemiş ancak silahların kullanımının hukuki bir değerlendirmeden geçirilmesi yükümlülüğü getirilmiştir.

Ek olarak Uluslararası Adalet Divanı, 1966 yılında Nükleer Silahların Tehdit veya Kullanımının Yasallığı'na dair verdiği tavsiye görüşünde Birleşmiş Milletler Antlaşması madde 51'e atıf yaparak savaş esnasında silah çeşidinde herhangi bir sınırlama yapılıp yasaklama getirilmediğine ancak olası yasağın kullanılan silahların gereklilik ve orantılılık koşullarına göre değerlendirildiğine değinmiştir[218]. Özetle, siber saldırılara ilişkin insancıl hukuk bağlamında uluslararası sözleşme bulunmasa da yukarıda açıklanan nedenlerden ötürü siber saldırılar, Cenevre Sözleşmeleri kapsamına girebilmektedir.

Ek Protokol I, madde 49'da düzenlenen saldırı tanımı, açıklanan nedenlerden ötürü sadece kinetik kuvvetle yapılan faaliyetlerle sınırlı olarak kabul edilmemektedir. Nükleer silahlar başta olmak üzere diğer kimyasal ve biyolojik silahlarla yapılan saldırılar da

---

[216] International Committee of the Red Cross (ICRC), "Article 36: New Weapons," *Commentary of 1987 on the Additional Protocol I of 1977 to the Geneva Conventions of 1949*, accessed December 20, 2025, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36/commentary/1987?activeTab=.

[217] Vincent Boulanin, "Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon System", *SIPRI Insights on Peace and Security 1*, (2015): 2.

[218] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* [1996] ICJ Rep 226, 4.

insancıl hukuk kapsamında saldırı olarak kabul edilmektedir ve bu saldırılar kinetik kuvvetle yapılmamaktadır[219]. Bu sayede gerekli şartları taşıyan siber saldırıların da insancıl hukuk kapsamına giren saldırı tanımına dahil olabileceği kabul edilmektedir[220]. Bu bağlamda şiddet niteliği taşımayan siber saldırıların insancıl hukuk kapsamına girmeyeceği ve siber operasyon olarak kabul edilecekleri açık hale gelmektedir[221].

3.4. Siber Saldırıların Silahlı Çatışma Olarak Kabul Edilmesi

Ek Protokol I'in 49. maddesi uyarınca düzenlenen saldırı tanımı, şiddet eylemi ile açıklanmıştır. Bu durum uyarınca yapılması sonucunda şiddet eyleminin ortaya çıktığı siber operasyonlar siber saldırı olarak kabul edilmekte ve insancıl hukuk kuralları uygulanabilir hale gelmektedir. Siber saldırının yapıldığı sistemin siviller için ne kadar hayati olduğunun belirlenmesi önem taşımaktadır. Nitekim siviller için hayati önem yaşayan ve günlük hayatta kullanımının zorunlu ve sık olduğu sistemlere karşı yapılan saldırılar, sivillerin yaşamlarını sürdürmesi açısından tehlike oluşturabilmektedir. Bu durumda yapılan siber saldırıların fiziksel zarara yol açması tıpkı bir kinetik saldırının yol açtığı zararla eşit olmaktadır[222].

Kinetik olan silahları kullanırken uyulması zorunlu olan insancıl hukuk kuralları siber saldırılarda da geçerlidir. Böylelikle, siber saldırı esnasında ayrım gözetmeyen ve sınırı aşan tüm fiiller insancıl hukuk ihlali oluşturmaktadır[223]. Siberuzayda saldırının tanımı, etkisi ve kullanım şekli kontrol edilebilse de hukuka uygunluk durumunun göz ardı edildiği durumlarda, internetle erişilebilen her şey dünya çapında herhangi bir yerden hedef alınabileceği için saldırının da etkisi ve hukuki ihlali de ağır olmaktadır.

---

[219] International Group of Experts, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N Schmitt ed, CUP 2017) 92.
[220] Eitan Diamond, "Applying International Humanitarian Law to Cyber Warfare", 75.
[221] James E. Mcghee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy," *Journal of Law & Cyber Warfare* 2, (2013): 70.
[222] International Committee of the Red Cross, *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting 21–22 January 2020 – Geneva* (Geneva: ICRC, 2021): 19.
[223] International Committee of the Red Cross (ICRC), *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Position Paper, November 2019), 2.

Sivillerin ve sivil nesnelerin olumsuz anlamda etkilenmesinin istendiği ancak sonucunda böyle bir etkinin gerçekleşmediği siber saldırıların da insancıl hukuk kapsamına girip girmeyeceğinin değerlendirilmesi gerekmektedir. Her ne kadar istenilen sonuç gerçekleşmese de tıpkı silah atışı sonucunda hedefin ıskalanmasının, yapılan atışın saldırı olma niteliğini değiştirmeyeceği gibi zarar doğurmayan siber saldırının da saldırı olarak kabul edilme niteliği değişmemektedir[224]. Özetle, siber saldırının amacı sivillere ve sivil nesnelere zarar vermek olup yapılan saldırı sonucunda böyle bir zararın gerçekleşmemesi söz konusu saldırıyı insancıl hukuk kapsamı dışına çıkarmamaktadır; çünkü böyle bir durumda esas olan saldırıyı yapmaktaki amaç ve kasıttır. Saldırıyı yapma amacı ile sonucun farklı olması kastı ortadan kaldırmamaktadır.

Yapılan siber saldırı sonucu zarar veya yaralanmaların hatta ölümlerin gerçekleşmesi mümkündür. Nitekim en güncel olarak 17 Eylül 2024 tarihinde İsrail tarafından Lübnan'da bulunan Hizbullah üyelerinin çağrı cihazları patlatılmıştır. Patlama sonucunda 12 kişi hayatını kaybetmiş ve 3000 civarı kişi yaralanmıştır[225]. Yaşanan bu saldırı Hizbullah tarafından "bir siber saldırı" olarak nitelendirilmiş ve saldırının sorumlusu olarak İsrail devleti tutulmuştur[226]. Hizbullah, yaşanan çağrı cihazı patlamalarının, çağrı cihazlarının içindeki lityum iyon pillerde bulunan kötü amaçlı yazılımların neden olduğu "termal kaçak" nedeniyle meydana geldiğini ileri sürmüş olup söz konusu saldırıyı siber saldırı olarak nitelemiştir[227]. Söz konusu saldırı sonucunda ise yalnızca Hizbullah üyeleri zarar görmekle kalmamıştır. Ölen 12 kişiden birinin 8 yaşında bir kız çocuğu olması ve 3000 civarı yaralanan kişiler arasında Hizbullah ile bağlantısı bulunmayan sivillerin olması bu saldırının ayrım yapma ve orantılı olma niteliğini zedelemekte olması uluslararası hukuk bakımından ihlal gerçekleşmesine olanak tanımıştır.

---

[224] Michael N. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues", 94.

[225] Euronews Türkçe, "Lübnan'da Yeni Patlama: Hizbullah Militanlarının Kullandığı Cihazlar İnfilak Etti," *Euronews*, 18 Eylül 2024, https://tr.euronews.com/2024/09/18/lubnanda-yeni-patlama-hizbullah-militanlarinin-kullandigi-cihazlar-infilak-etti.

[226] İsrail devleti bu konuda herhangi bir açıklama yapmayıp sorumluluk almamıştır. Hizbullah'ın görüşünden farklı olarak yapılan saldırının İsrail'in önceden Hizbullah üyelerinin telefonlarına patlayıcı madde yerleştirdiği de iddia edilmektedir ancak henüz kanıtlanmış bir durum bulunmamaktadır. Detaylı bir bilgi için *bknz*. DW Türkçe, "Lübnan'da Çağrı Cihazları Nasıl Patladı?," *Deutsche Welle*, 19 Eylül 2024, https://www.dw.com/tr/l%C3%BCbnanda-%C3%A7a%C4%9Fr%C4%B1-cihazlar%C4%B1-nas%C4%B1l-patlad%C4%B1/a-70250569.

[227] Lawfare, "Reflections on the Lebanon Pager Attack," *Lawfare*, 22 Eylül 2024, https://www.lawfaremedia.org/article/reflections-on-the-lebanon-pager-attack.

Siber saldırıların fiziki zararlara yol açtığı durumlardan tarihteki ilk örnek ise Amerika Birleşik Devletleri tarafından 2009 yılında, İran'a ait Natanz nükleer yakıt zenginleştirme tesisine yapılan "Stuxnet" saldırısıdır. Önceki bölümde de değinilen bu saldırının uluslararası insancıl hukuk ve siber saldırılar bağlamı açısından en büyük önemi, fiziki zarara sonuç veren ilk siber saldırı olmasıdır. Saldırı sonrası yapılan araştırmalar sonucu saldırının yapıldığı bilişim sisteminin "Simatic WinCC Step7" adlı program olduğu belirlenmiştir[228]. Programı oluşturan şirket olan Siemens'in yaptığı açıklama uyarınca saldırı, kötü amaçlı yazılımın güvenlik açıklarını istismar eden bir USB bellek ya da bir cihaz yolu ile programa sızması şeklinde yapıldığıdır[229]. Bu saldırının temel olarak yapılma amacının ise saldırıya uğrayan nükleer tesisin işleyişini durdurmak ve süreci sekteye uğratmak olarak açıklanmaktadır[230]. Söz konusu siber saldırıya dair tartışılan önemli noktalardan biri, bu saldırının bir siber saldırı olarak başlı başına insancıl hukuk kapsamında bir silahlı çatışma oluşturup oluşturmayacağıdır. Bu husus ele alınırken genel olarak Ek Protokol I, madde 49'da geçen saldırı tanımına başvurulmaktadır. Söz konusu madde gereği saldırı, şiddet içeren bir eylemdir ve yapılması sonucu ortaya insanlar açısından kayıp ya da yaralama, nesneler açısından ise zarar görme ve yok olma durumları meydana gelmektedir[231].

Silahlı çatışma, bir grubun yaralanmasına, öldürülmesine, hasar görmesine veya yok edilmesine yönelik önlemler alındığında ortaya çıkmakta olup bu terim, aynı zamanda bu tür sonuçları hedefleyen veya öngörülebilir sonuçlar doğuran eylemleri de kapsamaktadır[232].

Bir siber saldırının jus ad bellum kapsamında silahlı çatışma olarak kabul edilmesi için ise söz konusu eylemin şiddet içeren eylemlerden ziyade şiddet içeren sonuçlar anlamında

---

[228] Şener Çelik, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 1,* (2013): 145.

[229] John Charles Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield" *John Marshall Journal of Information Technology & Privacy Law 1,* (2011): 9.

[230] Şener Çelik, "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi", 148.

[231] John Charles Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", 9.

[232] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", *International Review of the Red Cross* 84, (2002): 374.

ele alınması gerekmektedir[233]. Stuxnet saldırısı bağlamında da birçok devlet, Stuxnet saldırısının bir güç kullanımı (use of force) kapsamında bir silahlı çatışma olarak kabul etmektedir. Bunun nedeni olarak ise siber saldırıda kullanılan solucanın (worm) doğrudan ve ölçülebilir fiziksel hasara neden olması, meşruiyet varsayımından yoksunluğu ve devlet desteği içermesi hususları gösterilmektedir[234] [235]. Ancak jus ad bellum'a dair verilen bu bilginin dışında, bu araştırmaya konu olan siber saldırılar genel olarak jus in bello kapsamında ele alınmaktadır.

4. Uluslararası Hukukta Siber Saldırılarla İlgili Mevcut Düzenlemeler Ve Boşluklar

Siberuzay ve bu alanda gerçekleşebilecek hukuk ihlalleri ile hak kayıpları, geleneksel hukuk kuralları ve düzenlemeleri karşısında oldukça yeni kalmakta olup hukuksal düzenlemelere daha çok ihtiyaç duyulan alanlardır. Siberuzay ve bu alanda gerçekleşen siber operasyonların hukukiliğine yönelik düzenleyici işlem getiren anlaşmaların yapılması önemli bir husustur. Özellikle de insancıl hukuk kurallarının uygulanabilir hale geldiği durumlarda siber saldırıların ayrıntılı ve kapsayıcı bir şekilde düzenlendiği uluslararası bir anlaşmanın varlığı silahlı çatışmalar bakımından günümüz ve gelecekte gerçekleşecek saldırıları hukuki bir zeminde ele almayı kolaylaştıracaktır. Uluslararası insancıl hukuk kuralları arasında doğrudan siber saldırıların hukuki durumunu, kullanımını, sınırlarını ve sorumluluğunu düzenleyen herhangi bir anlaşma ya da protokol halen bulunmamaktadır[236].

Siberuzay ve hukuk kurallarının bir arada olması durumunda iki durumun ortaya çıktığı iddia edilmektedir; mevcut hukuki düzenlemelerin ve kurallarının siberuzaya

[233] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", 377.
[234] Philip A. Foltz, "Cyber Deterrence: A Practice-Based Framework for Deterrence by Denial," *Joint Force Quarterly* 67 (2012): 45, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.
[235] Stuxnet saldırısının jus ad bellum kapsamında bir silahlı çatışma olarak kabul edilmesi için yalnızca eylemin sonuçlarının şiddet içermesi hususuna bakılmamış, bu durumda bir saldırının silahlı çatışma olarak kabul edilmesi için aşılması gereken eşikler (thresholds) incelenmiştir. Bu eşikler ise saldırının hangi yoğunlukta, nasıl bir organizasyonla ve saldırının yaralanmaya, ölüme, hasara veya yıkıma neden olup olmayacağının tespiti ile aşılmaktadır. Bkz. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, *International Review of the Red Cross* 84, no. 846 (2002): 381.

[236] Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", 368.

uygulanabilir hale getirilmesi ve siberuzay için yeni hukuki düzenlemelerin yapılması[237]. Siberuzaydan önce kullanılan hukuki kuralların siber uzay faaliyetlerine uyarlanması, uyarlanamayan kuralların ise siberuzay için baştan düzenlenmesi gerekmektedir. Özellikle siberuzay için baştan düzenlenen kuralların ne amaçla düzenlendiğinin iyi anlaşılması gerekmektedir. Örnek olarak, insancıl hukuk kurallarında sivillerin mülkiyet hakkı korunmaktadır.

Sivillerin dijital malvarlıklarını koruma altına alan hukuk kurallarının yapılması için temelde mülkiyet hakkının öneminin gözden geçirilip bu hakkın ve getirilerinin dijital ortamda geçerli olup olmayacağının belirlenmesi gerekmektedir[238]. Yapılacak bu tespit ve değerlendirmeler sonucunda söz konusu hakların siber ortamda da mevcudiyet gösterip göstermediği, gösterdiği durumda ise bu hakkın nasıl korunacağı söz konusu olmaktadır. Böylelikle, insancıl hukuk ve siber saldırılar bağlamında tarafları bağlayıcı, uluslararası hukukta geçerlilik ve yaygınlık kazanmış olan devletler arası herhangi bir sözleşme ya da anlaşma halen mevcut değildir. Ancak siber saldırlara ilişkin NATO'nun ve Birleşmiş Milletlerin, çalışmaları bulunmaktadır. Bu çalışmalar uluslararası hukuk kapsamında bir bağlayıcılık göstermese de siber saldırılar ve insancıl hukukun sentezlenmesi için büyük önem arz etmektedir.

4.1. Tallinn Kılavuzu (NATO)

NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi (NATO CDD COE) nin davetiyle katılan uluslararası hukuk uzmanları tarafından insancıl hukukun geçerli olduğu zamanlarda siber saldırıların hukuki durumuna yönelik düzenlemeler içeren kılavuz, 2009 yılında, Estonya'nın Tallinn kentinde hazırlanmıştır[239]. NATO CDD COE'nin bir araya getirdiği uluslararası hukuk uzmanları tarafından siber saldırılar ile insancıl hukuk (hem jus ad bellum hem de jus in bello), devletlerin sorumluluğu, diğer hukuk dalları ile ilişkisi ayrıntılı bir şekilde ele alınmıştır[240]. Uluslararası anlaşma statüsünde olmadığı için

[237] Heather Harrison Dennis, *Cyberwarfare and the Laws of War*, 8.
[238] Heather Harrison Dennis, *Cyberwarfare and the Laws of War*, 9.
[239] Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 16.
[240] Merve Erdem and Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü,", 136.

kılavuzun herhangi bir hukuki bağlayıcılığı bulunmamaktadır. Ancak siber saldırılara ilişkin önemli düzenlemeler içermektedir. Kılavuz, siber saldırılara insancıl hukuk kurallarının uygulanıp uygulanmadığını, uygulandığı durumlarda ise bu durumun uluslararası insancıl hukuk kuralları ile işbirliği içerisinde nasıl gerçekleşeceğini detaylı bir şekilde ele alıp Estonya'nın, Gürcistan'nın ve Ukrayna gibi ülkelerin farklı zamanlarda uğramış olduğu siber saldırılara atıf yapmaktadır[241].

NATO'nun siber saldırıları içeren böyle bir kılavuzu hazırlamasının temel sebeplerinden biri söz konusu ülkelere yapılan siber saldırlar ve yapılan bu saldırıların devlet egemenliğine, kamu düzenine ve güvenliğine büyük ölçüde zarar verme potansiyeli taşımasıdır. Nitekim NATO'nun diplomatik zirvelerinde değinildiği gibi siber saldırılar, hiç olmadığı kadar yaygınlaşmış, sıklaşmış, daha organize hale gelmiş ve özellikle de Avrasya devletlerinde fiziki, ekonomik ve sosyal açıdan bir güvenlik açığı meydana getirmişlerdir[242]. Böylelikle siber saldırıları hukuki bir çerçeve entegre etmek daha önce yaşanmış ve yaşanması muhtemel saldırıları hukuki sonuçlara tabi kılacak olup insancıl hukukun haklar üzerindeki koruma kalkanı, siber saldırılar söz konusu olduğunda da devam etmiş olacaktır. Bu yüzden NATO'nun Tallinn Kılavuzu'nu hazırlamasının sebeplerinden biri de ülkeler arasında siber saldırı farkındalığını arttırıp bu türden saldırılara ülkelerin müdahale etmesini kolaylaştırmak ve siber saldırılarla uluslararası hukuku entegre etmektir[243].

Tallinn Kılavuzu'ın 2017 tarihli en güncel verisyonu, "Genel Uluslararası Hukuk ve Siberuzay", "Uluslararası Hukuk ve Siberuzayın Uzmanlaştırılmış Rejimleri", "Uluslararası Barış, Güvenlik ve Siber Aktiviteler" son olarak da "Siber Savaş Hukuku" olmak üzere dört bölümden oluşmaktadır. Kılavuz, siber operasyonları ele alıp bunların bir saldırı oluşturup oluşturmadığını inceleyip bu türden saldırıların silahlı çatışma olarak kabul edilip edilmeyeceğine değinip jus in bello yönünden inceleme yaptığı gibi jus ad bellum yönünden de inceleme yapmaktadır ve bu saldırıların olası hukuki sonuçlarını da ele almaktadır[244]. Toplamda 154 tane kuraldan oluşan kılavuzda siber saldırılar ve savaş

[241] Roberta Arnold, "Book Reviews", *International Criminal Law Review 20*, (March 2020), s. 157.
[242] NATO, *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Lisbon: NATO Public Diplomacy Division, 2010), 3.
[243] NATO, *Active Engagement, Modern Defence*, 5.
[244] Roberta Arnold, "Book Reviews", 157.

hukukuna dair birçok düzenleme, siber saldırılar esnasında savaşanlar ve siviller ayrımı ve bu kişilere ait nesneler, saldırıların tanımı ve kapsamları, korunması gereken hukuki değerler ile ilgili birçok konu ele alınmıştır. Kılavuz ile ilgili bir diğer önemli husus ise siber – siber (cyber to cyber) saldırılara yönelik olmasıdır. Bir diğer deyişle savaşan tarafların birbirlerinin bilişim sistemlerine sızarak kritik altyapılarına zarar vermesi kılavuzun konusu iken bir devletin savaş uçağı ile diğer devletin siber savunma ve saldırı merkezini bombalaması kapsam dışındadır[245].

Siber saldırılar, beraberinde belirsizliği de getirmektedir. Saldırının nasıl ve kim tarafından yapıldığı, etki alanının ne olduğu, saldırıdan kimin sorumlu tutulacağına dair konularda birçok belirsizlik (uncertainity) mevcuttur. Bu bağlamda kılavuz iki şekilde okunabilmektedir: ilk olarak kılavuzdaki "siber" kavramı, askeri müdahalelerin düşünebileceği ya da düşünmesi gereken şekilde olması gerektiğidir ki bu şekilde belirsizlikler azalmaktadır, ikinci olarak da bu belirsizlikler hukuki akıl yürütme ve kuralların uygulanması yoluyla giderilmektedir.[246] Belirsizliklerin oluşmasının en büyük nedeni ise siber saldırıların hedef aldığı kritik altyapılarında sivil-askeri ayrımının kesin olmaması sonucunda iki tarafın da saldırıdan etkilenmesidir[247] [248]. Kılavuzun amacı da siber saldırıları detaylı bir şekilde ele alıp uluslararası hukukla entegre edip bu belirsizlikleri minimuma indirmektir.

Özetle Tallinn Kılavuzu, siber saldırılarla insancıl hukukun genel ilkeleri ve bunların insan hakları hukuku, uzay hukuku ve telekomünikasyon hukuku gibi uzmanlaşmış uluslararası hukuk rejimleriyle etkileşimini ortaya koymaktadır[249]. Ancak devletlerin söz konusu kılavuzu sınırlı oranda desteklediği ve insancıl hukuk kurallarının siber saldırılara

[245] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 18.
[246] Oliver Kessler and Wouter Werner, "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare," *Leiden Journal of International Law* 26, (2013): 797.
[247] Oliver Kessler and Wouter Werner, "Expertise, Uncertainty, and International Law", 798-799.
[248] Özellikle son zamanlarda elektrik santrallerine yapılan siber saldırılar yalnızca devlet organlarının işleyişine zarar vermemekte aynı zamanda aynı santralin elektriğinden yararlanan sivil halk da elektrik kesintilerinden ötürü zarara uğramaktadır.
[249] Dan Efrony, Yuval Shany, "A Rule Book on the Shelf: Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law 112*, (October 2018): 584.

da uygulanması konusunda kılavuzda geçen kuralların bağlayıcı olup olmamasına yönelik bir istekte bulundukları hala kesinlik içermemektedir[250].

4.2. Birleşmiş Milletler Çalışmaları

Birleşmiş Milletler, insancıl hukuk ve siber saldırılara dair hukuki bir düzenleme yapmayıp bu konuları kendi çalışma gruplarında ve bu grupların hazırladıkları yıllık raporlarda ele almaktadır. Nitekim Birleşmiş Milletler, uluslararası hukukun yasama organı olmamakla birlikte uluslararası hukuk kurallarının tartışmalarının merkezi konumu olarak kabul edilmektedir. Bu yüzden siber saldırılar ve uluslararası insancıl hukuka dair çeşitli çalışma gruplarında raporlar hazırlanmıştır; ancak önemli husus şudur ki bu raporların herhangi bir bağlayıcılığı bulunmamaktadır.

4.2.1. Devlet Uzmanları Grubu (Governmental Group of Experts, GGE)

Birleşmiş Milletler Genel Kurulu'nun 73/266 sayılı kararı uyarınca Genel Sekreterden uluslararası güvenliği tesis ve temin etmek amacıyla siber alan söz konusu olduğunda devletlerin davranışlarının geliştirilmesi amacıyla bu grup kurulmuştur[251]. Grup, yirmi beş üyeden oluşmakta olup bir başkana sahiptir.

Grubun 30 Temmuz 2013 tarihli, A/68/98 sayılı raporunda uluslararası hukuk kurallarının ve Birleşmiş Milletler şartının bilgi ve iletişim teknolojilerine uygulanabileceği, bu sayede siber alanda yapılan operasyonların da uluslararası hukuka tabi olduğu açıklanmıştır[252]. Söz konusu raporda siber saldırılar ve insancıl hukuk kurallarından doğrudan birlikte bahsedilmese de uluslararası hukuk kurallarının siber operasyonlara uygulanabileceği kabul edilip insancıl hukuk için açık bir kapı bırakılmıştır.

---

[250] Dan Efrony, "A Rule Book on the Shelf: Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", 585.

[251] United Nations Office for Disarmament Affairs, "Group of Governmental Experts," United Nations, accessed May 15, 2025, https://disarmament.unoda.org/group-of-governmental-experts/.

[252] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (June 24, 2013), para. 19.

Aynı kurulun 22 Haziran 2015 tarihli ve A/70/174 sayılı raporunda ise devletlerin bilgi iletişim teknolojileri kullanırken uluslararası hukuk kurallarına uyma zorunluluğundan bahsetmiş ve bu teknolojilerin kullanımının devletlerin siyasi ve fiziki güvenliğine tehdit oluşturmayacak şekilde olmasına değinilmiştir[253]. Raporun devamında ise bilgi iletişim teknolojilerinin kullanılması durumunda insancıl hukuk kurallarının temel ilkelerini oluşturan insaniyet ilkesi, gereklilik ilkesi, orantılılık ilkesi ve ayrımcılık yasağı ilkesine uyma zorunluluğuna değinilmiştir[254].

4.2.2. Açık Uçlu Çalışma Grubu (Open-ended Working Group, OEWG)

Birleşmiş Milletler Genel Kurulunun 73/27 sayılı kararıyla kurulan bu grup, Birleşmiş Milletlerin tüm üyelerine açık olarak tasarlanmıştır[255]. Adından da anlaşılacağı üzere birçok konu başlığı altında bu çalışma grubu toplanabilmektedir. 18 Mart 2021 tarihli ve A/75/816 sayılı raporda da devletler tarafından kullanılan bilgi iletişim teknolojilerinin uluslarararası hukuk kurallarıyla uyumlu olması, devletlerin uluslararası hukukun kendilerine yüklediği sorumluluğa uygun olarak hareket etmesi gerektiği düzenlenmiştir[256]. Bu raporda da doğrudan insancıl hukuk kuralları ve siber saldırılardan bahsedilmemiştir; ancak insancıl hukukun uluslararası hukukun bir parçası olması sebebiyle söz konusu rapor önem arz etmektedir. Nitekim aynı vurgu OEWG'nin 8 Ağustos 2022 tarihli ve A/77/275 sayılı raporunda da yapılmıştır. Söz konusu raporda da uluslararası hukukun ve Birleşmiş Milletler Şartı'nın bilgi iletişim teknolojilerinin kullanımına uygulanmasına değinilmiş olup yapılacak olan tartışmaların bu hususu içermesine yönelik katılımcı devletler görüş sunmuştur[257]. Bilgi iletişim teknolojilerinin kullanımının uluslararası hukuk kurallarına riayet etmemesi durumunda raporlarda genel

---

[253] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (July 22, 2015), para. 26.
[254] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (July 22, 2015), para. 28.
[255] United Nations Office for Disarmament Affairs, *Open-ended Working Group* (https://disarmament.unoda.org/open-ended-working-group/ accessed 15 May 2025)
[256] United Nations General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816 (March 10, 2021), para. 7.
[257] United Nations General Assembly, *Annual Progress Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/77/275 (July 27, 2023), para. 15(a).

olarak kabul edilen görüş, Birleşmiş Milletler Şartı'nın 33. Maddesi uyarınca uyuşmazlığın barışçıl bir yolla çözülmesi gerektiğidir[258].

Sonuç olarak Birleşmiş Milletler, NATO gibi uluslararası kuruluşlar tarafından siber saldırılar ve insancıl hukuk adına çalışmalar gerçekleştirilmiştir ve halen bu çalışmalar sürdürülmektedir. Birleşmiş Milletler Genel Kurulu tarafından kurulan GGE ve OEWG gruplarının yayımladıkları raporlar genel olarak bilgi iletişim teknolojileri ve uluslararası hukuka ilişkin genel bilgiler içeren raporlardır. Siber saldırıların olması durumunda insancıl hukuk kurallarının nasıl uygulanacağı ya da uygulanması gerektiğine dair herhangi bir detaylı açıklama yapmamaktadır. Ancak insancıl hukuk kuralları adına uluslararası hukuk kurallarının genel olarak uygulanması söz konusudur. NATO işbirliğinde hazırlanan Tallinn Kılavuzu ise tam olarak siber operasyonlar- siber saldırılar söz konusu olduğunda insancıl hukuk kurallarının nasıl uygulanabilir hale geleceği, nasıl uygulanacağı, saldırı tanımları ve kapsamının ne olduğu, sivil-askeri kişiler ve hedeflerin nasıl belirleneceği gibi hususlar detaylı bir şekilde düzenlenmiştir. Tallinn Kılavuzu siber saldırılar ve insancıl hukuk bağlamında büyük bir öneme sahip olsa da hukuki bir bağlayıcılığa sahip değildir. Ancak çalışmanın bir sonraki bölümünde siber saldırılar ve sivil hedef konularına odaklanırken Tallinn Kılavuzu kurallarına içeriği ve uluslararası hukuka dayandığı için değinilecektir.

[258] Maria Tolppa, "First UN OEWG Concludes with a Consensus Report – What Does It Mean for Future Cybersecurity Discussions under the Auspices of the First Committee?", NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), March 30, 2021, https://ccdcoe.org/library/publications/first-un-oewg-concludes-with-a-consensus-report-what-does-it-mean-for-future-cybersecurity-discussions-under-the-auspices-of-the-first-committee/.

III BÖLÜM

SİBER SALDIRILARDA SİVİL HEDEF

1. Sivil Hedef ve Siber Saldırılara Uygulanabilirliği

Ek Protokol I, madde 51 uyarınca silahlı çatışma esnasında çatışmaya doğrudan katılmayan sivillerin saldırının hedefi haline getirilmesi yasaklanmıştır. Aynı şekilde sivillerin yaşadığı yerler, sivillerin kullanıp yararlandığı nesnelere karşı tehdit edici ya da doğrudan saldırıda bulunulan tüm eylemler uluslararası hukuka aykırı sayılmaktadır. Burada dikkat edilmesi gereken husus ise koruma statüsüne sahip olan sivillerin gerçekleşmekte olan silahlı çatışmalara doğrudan bireysel ya da bir grubun üyesi olacak şekilde katılım göstermemiş olmasıdır. Ek Protokol I, madde 52 uyarınca da sivil nesnelerin saldırı hedefi haline getirilmeleri yasaklanmış olup getirilmeleri durumunda uluslararası hukukun ihlalinin gerçekleştiği ve hukuki sorumluluğun doğacağı düzenlenmiştir. "Askeri nesne olmayan nesneler" şeklinde negatif bir şekilde tanımlanan sivil nesnelerin saldırı hedefi haline getirilmesi ise uluslararası hukukun en temel kurallarından biri olan ayrım yasağının ihlalini oluşturmaktadır.

Çalışmanın birinci bölümünde sivil ve askeri nesnelerin tanımı, kapsamı ve korunması gibi hususlar ele alınmıştır; ancak yapılan inceleme 1949 tarihli Cenevre Sözleşmeleri, Lahey Düzenlemeleri ve bunlara yönelik uluslararası mahkeme kararları ışığında geleneksel savaş yöntemlerine yönelik ele alınmıştır. Siber saldırı durumunda sivil hedefin ne olacağı, sivillerin ve onlara ait nesnelerin neleri kapsayacağı, saldırıların nasıl gerçekleşeceği ve tüm bu hususların kapsamlarının hukuki bir zeminde nasıl belirleneceği bu bölümde ele alınacaktır. Nitekim önceki bölümde de incelenip açıklandığı üzere siber saldırılara, gerekli eşikleri geçtikleri durumda, insancıl hukuk kuralları uygulanabilir hale gelmektedir. Yapılması sonucunda şiddet eyleminin ortaya çıkması durumundan yola çıkarak siber saldırı yöntemlerinin ve bu yöntemleri gerçekleştiren araçların geleneksel savaş yöntem ve araçları ile aynı sonuca hizmet etmesi açısından yeni bir silah olarak kabul edilip insancıl hukuk kurallarına tabi olacağı kabul görmektedir[259]. Buradan yola

[259] Dülger, Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar, 162.

çıkarak siber saldırılar bağlamında sivil ve askeri nesnelerin ele alınması kapsamı belirlemek açısından önem taşımaktadır.

2. Siberuzayda Askeri Kişi ve Nesneler

2.1. Askeri Kişiler

Askeri kişiler, Ek Protokol I madde 43 uyarınca savaşan tarafların silahlı kuvvetleri, organize olmuş örgütlü silahlı gruplar ve silahlı çatışmaya doğrudan katılım gösteren sivillerdir. Siber saldırı söz konusu olduğunda da saldırının hedefi olarak silahlı kuvvetlerin üyeleri, organize olmuş örgütlü silahlı grupların üyeleri, savaşa aktif katılım gösteren bireyler ve uluslararası nitelikte bir silahlı çatışma olması durumunda *levée en masse*[260] kişileri alınabilmektedir[261]. Ancak bu silahlı kuvvetler ve askeri birlikler ile birlikte çalışan sağlık ve din personellerinin, Kızılhaç ve Kızılay görevlilerinin, savaşırken esir düşmüş askerlerin ya da yaralanmış olan askerlerin siber saldırıların hedefi haline getirilmesi hukuka aykırılık teşkil etmektedir[262]. Sonuç olarak yukarıda verilen Ek Protokol I'in ilgili maddelerinde düzenlenen kişiler, askeri kişiler olarak kabul edilip siber saldırıların meşru hedefi olarak belirlenebilmektedir[263].

2.2. Askeri Nesneler

Askeri nesneler, Ek Protokol I, madde 52 uyarınca, doğası, konumu, amacı ve askeri operasyona etkili bir şekilde katkı yapan (zarar verme, ele geçirme, etkisiz hale getirme gibi durumlar) nesnelerle sınırlıdır. Bu türden nesneler, silahlı çatışma durumunda saldırının meşru hedefleri olarak kabul edilmektedir. Tallinn Kılavuzu, 38. Kural[264]

---

[260] *Levée en masse: Bir ülkenin vatandaşlarının işgale uğraması durumunda düzenli bir birlik oluşturmayıp kendi başlarına silahlanan gruplarıdır.*

[261] Michael N. Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare, 99.

[262] Ek Protokol I, madde 41.

[263] Tallinn Kılavuzu'nun ilgili kuralı (Rule 35) hazırlanırken uluslararası nitelikte olan silahlı çatışmalarda bu kurala dahil olan kişilerin silahlı çatışmaya taraf olan devletin silahlı kuvvetleri üyeleri olduğunu kabul eden hukukçular da olmuştur. Kılavuzun hazırlanma aşamasında hukukçular arasında görüş ayrılığı yaşanan bu konuda silahlı çatışmanın doğrudan tarafı olmayıp siber saldırı yönüyle taraflara destek olan ve herhangi bir sağlık ya da dini konuda hizmet etmeyen gruplar bazı hukukçular tarafından bu kuralın kapsamı dışında bırakılmıştır. *Bkz.* Michael N. Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare, 100.

[264] Rule 38*: "Civilian objects are all objects that are not military objectives. Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action*

gereği de sadece askeri nesneler siber saldırıların hedefi haline gelebilmektedir. Siber saldırının hedef alabileceği askeri nesnelerin ne olduğu ve bu nesnelerin siber saldırı yoluyla nasıl zarara uğrayabileceğinin belirlenmesi büyük bir önem arz etmektedir.

Siberuzay bağlamında siber saldırıların hedefi haline gelebilecek askeri nesnelerin kapsam ve sınırlarının belirlenmesi, ayrım ilkesinin değerinin korunması yönünden oldukça kritiktir. İnsancıl hukukta genel olarak nesnelerin *görünür ve elle tutulabilir (visible and tangible)* özelliklere sahip olması gerekmektedir[265]. Ancak siberuzayda bu özellikler büyük bir ölçüde bulunmamaktadır. Nitekim silahlı kuvvetlere ait bilgisayarlar, bilgisayar ağları, ve diğer elle tutulur yardımcı araçlar askeri nesne olarak kabul edilmekte ve saldırının hedefi haline getirilebilmektedir. Bilgisayar biliminde ağlar arasında yapılan işlemler elle tutulur özellikte değildir ancak gerekli koşulların varlığında elle tutulamayan nesneler de askeri nesne olarak kabul edilmektedir. Bu duruma en çarpıcı örnek "data[266]" lardır. Data, elle tutulabilecek nesneler kategorisine girmemektedir; ancak bu durum onu nesne olmaktan çıkarmamaktadır; çünkü data'lara karşı yapılan yok edici, tahrip edici, değiştirici siber saldırılar, insancıl hukuk kapsamına giren saldırılar olarak sayılabilmektedir[267].

2.2.1. Doğası Gereği Askeri Nesneler ve Siber Saldırılar

Ek Protokol I, madde 52'nin düzenlemelerinden biri de; bir nesnenin askeri nesne olarak kabul edilmesi için doğası gereği askeri eylemler yararına katkıda bulunması gerekmektedir. Bu sayede askeriyeye ait bilgisayarlar, ağ sistemleri ve altyapılar doğaları gereği askeri eylemler yararına kullanıldığı kabul edilmektedir; dolayısıyla bu nesneler doğaları gereği askeri nesnelerdir. Böylelikle askeri operasyonlara yönelik komuta, kontrol, iletişim, bilgisayar, istihbarat, gözetleme ve keşif (C4ISR) yapan nesneler askeri nesneler olarak kabul edilmektedir[268].

---

and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Military objectives may include computers, computer networks, and cyber infrastructure"

[265] Rule 38, para 4.

[266] Türkçe söylenişiyle "veri".

[267] Rule 38, para 5.

[268] Rule 38, para 6.

2.2.2. Konumu Gereği Askeri Nesneler ve Siber Saldırılar

Konumları gereği bazı nesneler, askeri nesneler olarak kabul edilmektedir. Konum, genellikle geleneksel savaşta coğrafi bir alanı temsil etse de siberuzayda böyle fiziki sınırlar içerisinde bulunan coğrafi bir alan mevcut değildir. Siber saldırıyı gerçekleştiren bilgisayarların IP adresleri askeri nesne olarak kabul edilebilmektedir[269]. Silahlı çatışma esnasında yapılan saldırının bilişim ağının konumu, o yeri konumu itibariyle askeri nesne haline gelmekte ve böylelikle saldırının meşru hedefi olmaktadır[270].

2.2.3. Kullanımı Gereği Askeri Nesneler ve Siber Saldırılar

Bir nesnenin kullanımı gereği askeri nesne olup olmamasının belirlenmesi için o nesnenin saldırıyı yaparkenki işlevinin ne olduğuna bakılması gerekmektedir[271]. Bir nesnenin askeri eyleme etkili bir katkıda bulunacak şekilde fiili kullanımı, aynı şekilde nesneyi askeri bir hedef haline getirmekte olup bu sayede söz konusu nesne saldırıya açık durumuna gelmektedir[272]. Bu yüzden sivillere ait olan bir nesne, askeri amaçlar için kullanıldığı an, o nesne artık askeri nesne olarak kabul edilmektedir. Siberuzay söz konusu olduğunda ise savaşan taraflardan biri askeri avantaj ve gereklilik yüzünden sivillere ait bir iletişim ağı (network) üzerinden bir siber saldırıda bulunursa bu durumda o iletişim ağı da askeri nesne olarak kabul edilmektedir [273].

2.2.4. Amacı Gereği Askeri Nesneler ve Siber Saldırılar

Amaç kriteri, nesnenin gelecekte askeri avantaj ve gereklilik amaçları için kullanımına atıfta bulunmaktadır[274]. Örnek olarak, çatışmaya taraf olan birinin askeri bir amaç için belirli bilgisayar yazılımı veya donanımı satın almak üzere olduğuna dair güvenilir bilgi elde edilirse, bu nesneler hemen askeri hedefler haline gelmektedir.

---

[269] Rule 38, para 7.
[270] Harrison Dinniss, Cyber Warfare and the Laws of War, 186.
[271] Harrison Dinniss, Cyber Warfare and the Laws of War, 187.
[272] Harrison Dinniss, 188.
[273] Rule 38, para 7.
[274] Rule 38, para 11.

3. Siviller ve Sivil Nesneler

3.1. Siberuzayda Sivil Kişiler

Siberuzay, herhangi bir fiziki alan ile sınırlara sahip olmayan ve internet, bilgisayar sistemleri, yazılımlar, telekomünikasyon gibi bileşenlerden oluşan bir platformdur[275]. Siberuzayda siviller ise bu bileşenleri bireysel olarak kullanan ancak askeri bir amaca hizmet etmeyip saldırıda bulunmayan kişiler olarak kabul edilmektedir[276].

2025 yılı Şubat ayında yapılan tespite göre günümüzde dünya çapında 5,56 milyar insan internet kullanmaktadır[277]. İnternet kullanan bu kalabalık nüfus ise siberuzayda pek çok farklı şekilde ortaya çıkmaktadır. Bu yüzden internet kullanıcısı olan sivillerin hangi karakterde var olabilecekleri detaylı bir şekilde ele alınmalıdır.

3.1.1. Sıradan internet kullanıcıları

İnternet, insanların çevrimiçi olarak etkinlik gösterdiği yeni mekanlar ortaya çıkarmıştır[278]. Günlük hayatlarını paylaşıp birbirleri ile etkileşim içine giren, film/müzik gibi sanatsal faaliyetlere çevrimiçi şekilde ulaşan, alışveriş, fatura ödemeleri gibi birçok günlük faaliyetlerini internet üzerinden yürüten dünya genelinde milyarlarca sıradan internet kullanıcısı bulunmaktadır. Günümüzde siviller, elektronik araçların kullanımı ile sağlanan sanal topluluklar kurmakta ve birbirileriyle bu şekilde iletişime geçmektedir[279]. Bu türden faaliyetler, saldırı olarak insancıl hukuk kapsamına giren fiiller sınıfına girmemektedir; çünkü bu türden faaliyetler şiddet içerikli düşmanca davranışlar olarak nitelendirilmemektedir[280].

---

[275] Semin Töner Şen, *Siber Uzay ve Uluslararası Hukuk*, 5.
[276] Schmitt, *Tallinn Manuals 2.0*, Rule 29.
[277] We Are Social and Meltwater, "Digital 2025: The Essential Guide to the Global State of Digital," *We Are Social*, February 2025, https://wearesocial.com/uk/blog/2025/02/digital-2025-the-essential-guide-to-the-global-state-of-digital/.
[278] Roger Clarke, "Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations." *Business & Professional Ethics Journal* 18, (1999): 156.
[279] Roger Clarke, "Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations.", 157.
[280] Dülger, Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar, 162.

3.1.2. Öğrenciler ve akademisyenler

Günümüzde çoğu eğitim içeriğinin internet üzerinden çevrimiçi olarak servis edilmekte olması, interneti bir eğitim aracı haline getirmiştir[281]. Özellikle Covid-19'un küresel bir pandemi haline gelmesi yüz yüze eğitimi sekteye uğratmış ve bu durum çevrimiçi eğitimi zorunlu kılmıştır[282]. Böylelikle bir eğitim aracı haline gelen internet, günlük hayatta öğrenciler ve akademisyenler tarafından sıklıkla kullanılmaktadır. Öğrenciler ve akademisyenler bu şekilde sivil kişiler olarak siberuzayda var olmaktadır.

3.1.3. Gazeteciler ve medya çalışanları

Gazeteler, kitle iletişim araçlarından biri olarak, geleneksel habercilik tekniklerinin yanı sıra haberleri çevrimiçi olarak da yayınlamaya başlamıştır[283]. Çevrimiçi şekilde yayımlanan gazeteler, bu gazetelerdeki haberlerin gazeteler tarafından abonelere e-posta olarak gönderilmesi gibi işlemler çeşitli donanım ve yazılımla gerçekleştirilmektedir[284]. Böylelikle gazeteciler ve bu alanda birlikte faaliyet gösteren medya çalışanları, varlıklarını siberuzayda da gösterir hale gelmiştir. Günlük hayattan sosyal, siyasi, ekonomik ve sanatla ilgili çeşitli haberleri yayınlayarak ve bu haberleri abonelerine ileterek herhangi bir askeri amaç gütmeyen gazeteciler ve medya çalışanları siberuzayın sivil kişileri olarak nitelendirilebilmektedir.

3.1.4. Siber güvenlik uzmanları

İnternet üzerinde sosyal medya kullanımı, bilgi aktarımları, yapılan alışveriş ve ödemeler gibi konular sayesinde kullanıcıların hassas bilgileri paylaşılmakta olup bu bilgilerin muhafaza edilip herhangi bir siber saldırıdan korunması için siber güvenliğin sağlanması

---

[281] Salih Usun, *Educational Uses of Internet in the World and Turkey: A Comparative Review*, *Turkish Online Journal of Distance Education (TOJDE)* 4, no. 3 (July 2003), PDF, 1, https://tojde.anadolu.edu.tr/tojde11/articles/usun.htm.

[282] Aleksander Aristovnik et al., "Impact of the COVID-19 Pandemic on Online Learning in Higher Education: A Bibliometric Analysis," *Frontiers in Education* 8 (2023): 1, https://doi.org/10.3389/feduc.2023.1225834.

[283] Hatice Öz, "An Analysis of Interactivity Possibilities in Online Journalism", *folklor/edebiyat 66*, (2011): 57.

[284] Hatice Öz, "An Analysis of Interactivity Possibilities in Online Journalism", 58.

büyük bir önem arz etmektedir[285]. Bu bilgilerin güvenliğini sağlamak ise siber güvenlik uzmanları tarafından yapılmakta olup bu uzmanlar bilginin korumasını, güvenliği tehdit eden ya da edebilecek hareketleri tespit ederek, durdurarak veya bunlara yanıtlar vererek gerçekleştirmektedir[286]. Ancak bu uzmanların siberuzayda sivil kişiler olarak kabul edilmesi için Ek Protokol I, madde 43/2'de belirtilen "silahlı kuvvetlere üye olma" halinin bulunmaması gerekmektedir. Nitekim Protokol hükümlerinden de anlaşılacağı gibi silahlı kuvvetler üyesi olup bu amaçla hareket eden kimseler askeri kişiler olarak kabul edilmekte olup sivil korumasına sahip değillerdir.

3.1.5. Yazılım geliştiriciler ve mühendisler

Hesaplamayı gerçekleştirmek için gerekli olan işlemlerin sırasını tek tek belirleyen bilgisayar programını hazırlama sürecine yazılım denmektedir[287]. Bu süreç, yazılım geliştiriciler ve mühendisleri tarafından yapılmaktadır. Özellikle Covid-19 sonrası dönemden itibaren sivil olan toplumlar içerisinde işleri gereği yazılım yapan birçok kişi bulunmaktadır[288]. Özel şirketlerin ticari amaçlarını yerine getirmek üzerine yapılan yazılımları yapan kişiler de siberuzayda siviller olarak kabul edilmektedir.

3.1.6. Sivil toplum kuruluşları çalışanları

Sivil toplum kuruluşları, insanların dayanışma amacıyla bir araya gelip çeşitli faaliyetlerde bulunan, herhangi bir siyasi ve askeri operasyon amacına hizmet etmeyen, günümüz dünyasında büyük bir öneme sahip olan yapılardır[289]. Bu tür kuruluşlar, devletlerden ayrı olarak faaliyet gösteren gönüllü kişilerden oluşmaktadır[290]. Sivil toplum kuruluşlarının faaliyetlerini çevrimiçi yürütüp siberuzayda varlık gösteren sivil toplum kuruluşları çalışanları çatışmanın tarafı olan örgütlü silahlı gruba hizmet etmedikçe

[285] European Commission, "Mind the Cyber Skills Gap: A Deep Dive," *Digital Skills and Jobs Platform*, last modified February 5, 2024, https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive.
[286] Cisco, "What Is a Cybersecurity Specialist?," *Cisco*, accessed June 15, 2025, https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cybersecurity-specialist.html.
[287] Alan F. Blackwell, "What is Programming", *PIGG 14*, (2002): 204.
[288] Alan F. Blackwell, "What is Programming", 206.
[289] Mustafa Talas, "Sivil Toplum Kuruluşları ve Türkiye Perspektifi", *Türklük Bilimi Araştırmaları 29*, 389.
[290] Mustafa Talas, "Sivil Toplum Kuruluşları ve Türkiye Perspektifi", 390.

uluslararası insancıl hukuk tarafından korunan kişiler olarak kabul edilmektedir[291]. Önemli olan husus, sivil toplum kuruluşları üyelerinin insani faaliyetlerini İnsancıl Hukuk anlaşmaları ve protokollerine uygun olarak yerine getirmesidir[292].

3.1.7. Sağlık çalışanları (dijital sistemler kullanan)

Birinci Cenevre Sözleşmesi (madde 24) ve Ek Protokol I'de (madde 8 ve madde 15) sağlık çalışanlarının (medical personals) tanımı yapılmış olup, genel anlamda çatışma esnasında tıbbi müdahale ile görevlendirilmiş kişiler olarak tanımlanmıştır. Bu kişiler insancıl hukuk kuralları tarafından korumaya tabi tutulmuşlardır. Birinci Cenevre Sözleşmesi madde 15 uyarınca, çatışma esnasında sağlık çalışanlarının korunması ve görevlerini gereğiyle yerine getirebilecek ortamın sağlanması gerekmektedir.

Siberuzayda ise sağlık çalışanları, hastanelerin dijital sistemlerini kullanarak, bu sistemlerle hastalara tedavi sağlayarak ortaya çıkmaktadır. Sağlık sektöründe dijitalleşmenin yaygınlaşması sonucunda gerek hastalar için hayati önem taşıyan makineler gerekse sağlık çalışanları için kişisel dijital asistanlar ve diğer kablosuz cihazlar, sağlık çalışanları tarafından oldukça sık bir şekilde kullanılmaktadır[293]. Siberuzayda sağlık çalışanları dijital sistem kullananlar olarak ortaya çıkmaktadır ve bu kişiler korumaya tabiidir.

3.1.8. *Finans ve bankacılık personeli (askeriyeyle bağlantısı olmayan kurumlarda)*

Gelişen teknoloji sayesinde bankacılık ve finans işlemleri dijital alana da taşınmıştır. Herhangi bir yerde ve zamanda finansal işlem yapmayı mümkün kılan dijital bankacılık

[291] Bruno Demeyere, *IHL and Civil Society Organizations: Thematic Brief* (Cambridge, MA: Harvard Humanitarian Initiative, Advanced Training Program on Humanitarian Action, 2016), 14, https://hhi.harvard.edu/sites/g/files/omnuum6866/files/humanitarianinitiative/files/atha_thematic_brief_ihl_and_civil_society_organizations.pdf.
[292] Bruno Demeyere, *IHL and Civil Society Organizations: Thematic Brief*, 15.
[293] Yeliz Mercan, Kübra Dizlek, Gamze Süsim vd. "Sağlık Amaçlı İnternet Kullanımı ve Mobil Sağlık Uygulamaları Üzerine Bir Araştırma" *Kırklareli Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi 1*, 68.

sayesinde ekonomik faaliyetlerde hızlanma meydana gelmiştir[294]. Dijital bankacılık ve finans işlemleri sayesinde akıllı telefonlar ya da bilgisayarlar aracılığı ile temel para işlemleri kolaylıkla halledilmekte ve bu dijital ortamda hem müşteriler hem de banka ve finans sektörü çalışanları varlık göstermektedir[295].

3.1.9. Kamu kurumlarında çalışan memurlar

Bilgi, iletişim ve teknoloji alanında yaşanan gelişmeler müteakibinde kamu kurumlarında verilen hizmetler de dijital olarak yerine getirilmeye başlanmıştır[296]. "*E-Devlet*"[297] adı verilen bu hizmetler, vatandaşların günlük yaşama, uzaktan yönetim ve politik katılıma yönelik bilgi ile iletişim hizmetleri veren ve çeşitli programlara kayıt olma, referanduma katılma, devlet dairelerinden randevu alma gibi durum ve ihtiyaçlara yönelik çevrimiçi işlem hizmeti sunmaktadır[298]. Kamu kurumlarında çalışan memurlar, siberuzayda bu şekilde varlık göstermektedirler.

3.1.10. Telekomünikasyon şirketlerinde çalışan personel

Telekomünikasyon şirketleri, sesi, yazıyı ya da videoyu müşterilerinin istediği yerlere ulaştıran altyapıyı sağlayan hizmeti vermektedir[299]. Bu hizmeti sağlamakla görevli olan personel, siberuzayda sivil olarak varlık göstermektedir. Uluslararası telekomünikasyonu sağlama, bu hizmet için gerekli altyapıyı kurma ve denetleme görevi ise devletlere verilmiştir[300]. Uluslararası telekomünikasyon hizmetini dijital olarak verme durumunda da devletin görevlendirdiği kurumların çalışanları siberuzayda sivil olarak varlık göstermektedir.

---

[294] Esra Bulut ve Gülay Çizgici Akyüz, "Türkiye'de Dijital Bankacılık ve Ekonomik Büyüme İlişkisi" *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi 42,* (2020):223.
[295] Esra Bulut ve Gülay Çizgici Akyüz, "Türkiye'de Dijital Bankacılık ve Ekonomik Büyüme İlişkisi", 225.
[296] Volkan Göçoğlu, "Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine bir İnceleme", *MANAS Sosyal Araştırmalar Dergisi 9*, (2020): 615.
[297] E- devlet (İngilizce adıyla, Open Government Data), hükümet tarafından üretilen, herkesin istediği bir amaçla özgürce erişebileceği, kullanabileceği, değiştirebileceği ve paylaşabileceği verilerdir. *Bkz*. Open Knowledge Foundation, *What Is Open Government Data?*, January 2016, 1, https://opencouncildata.org/wp-content/uploads/2016/01/what-is-open-government-data.pdf.
[298] Volkan Göçoğlu, "Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine bir İnceleme", 620.
[299] Brian Beers, "What Is the Telecommunications Sector?" *Investopedia*, last modified July 30, 2022, https://www.investopedia.com/ask/answers/070815/what-telecommunications-sector.asp.
[300] Schmitt, *Tallinn Manuals 2.0*, Rule 61.

3.2. Sivil Hackerlar ve Hukuki Statüleri

İnsancıl hukuk, hiçbir kategorideki kişilere savaşa katılmayı yasaklamamıştır; bu duruma siviller de dahildir[301]. Sivil hackerlar, çatışmaya doğrudan katılım gösteren siviller olarak kabul edilmektedir[302]. Sivil hackerlar tarafından yapılan siber saldırılar ile verilerin zarar görmesi veya tahribatı, özellikle hükümet veya askeri veri tabanları gibi önemli verilerin etkilenebileceği durumlarda kritik derecede bir zarara meydan açabilmektedir[303]. Bu duruma örnek olarak Suriye Elektronik Ordusu (Syrian Electronic Army) ve Rusya-Ukrayna Savaşında Ukrayna lehine hareket eden "Worldwide IT Community" verilebilmektedir.

Suriye Elektronik Ordusu, *bir diğer adıyla Esad'ın siber savaşçıları*, DDoS yöntemi kullanarak BBC, TheGuardian ve Associated Press'e yönelik siber saldırıda bulunup toplamda 130 Milyon Dolarlık para kaybına sebep olmuş, aynı zamanda da insan hakları gruplarına ait olan sistemler de bu kişiler tarafından Esad'ın düşüncelerini yayma amacıyla hacklenmiştir[304]. Worldwide IT Community ise Ukrayna adına Rusya'ya ait hayati önem taşıyan finansal, altyapısal hükümet hizmetlerinin yerine getirildiği sistemlerini engelleyen siber saldırılarda bulunup hastanelerin web sitelerini hacklemişlerdir[305]. Bu iki örnekten de anlaşılacağı üzere sivil hackerların, silahlı çatışma esnasında yaptıkları siber saldırılar, devletler genelinde büyük çaplı etkiler yaratabilmektedir. Böyle büyük etkiler yaratabilen sivil hackerların hukuki statülerinin ne olacağının belirlenmesi ise büyük bir önem arz etmektedir.

---

[301] Schmitt, *Tallinn Manuals 2.0*, Rule 86.
[302] Tilman Rodenhäuser, "8 Rules for Civilian Hackers during War – and 4 Obligations for States to Restrain Them," *Humanitarian Law & Policy Blog* (International Committee of the Red Cross), October 4, 2023, https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.
[303] Michał Byczyński, "The Legal Status of Civilian Hackers under International Humanitarian Law", *Acta Universitatis Lodziensis 106*, (2024): 102.
[304] Luke Harding and Charles Arthur, "Hacking the Guardian: How Syria's Electronic Army Took on the West." *The Guardian*, April 30, 2013. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.
[305] Tilman Rodenhäuser, "8 Rules for Civilian Hackers during War – and 4 Obligations for States to Restrain Them".

İnsancıl hukuk, savaşanlar ve siviller arasında ayırt etme ilkesi uyarınca net bir şekilde sınır çizse de çatışma esnasında sivillerin hacker olup siber saldırıda bulunması, hukuken çekilen bu sınırı bulanıklaştırmaktadır[306]. Sivil olan kişilerin düşmanlık anlamına gelen ve insancıl hukuk kapsamında saldırı olarak kabul edilen siber saldırılara katılması mümkündür; ancak saldırıya katılımı dolayısıyla bu kişiler koruma statülerini kaybetmektedirler[307]. Sivil olup saldırıya katılan kimseler yasadışı savaşçı (unlawful combatant) olarak kabul edilmekte olup savaşanların sahip olduğu haklardan mahrum bırakılmaktadırlar[308]. Bu kuraldan anlaşılacağı üzere düşmanlık anlamına gelen siber saldırılara katılım göstermeyen siviller ise, uluslararası hukuk tarafından korunmaya ve saldırı hedefi haline gelme yasağına tabii olmaya devam ederler.

İnternetin siviller arasında oldukça yaygın bir şekilde kullanılması, siberuzayda kimlerin sivil kimlerin ise askeri kişiler olduğu yönünde ayrım yapmayı zorlaştırmaktadır. Çünkü sivil hackerlar, siviller ve askeri kişilerin yanında üçüncü bir grup olarak ortaya çıkmıştır[309]. Yukarıda bahsedildiği üzere bu kişiler silahlı çatışma esnasında siber saldırıda bulunurlarsa sivil koruma statüsünü kaybetmektedirler ancak bu kişilerin ilerleyen zamanlarda teknolojik gelişmelerin yarattığı etki yüzünden savaşçı sayılıp sayılmayacağı tartışmalı olup bu konu hakkında günümüzde hala kesin bir sonuca varılamamıştır[310].

Tallinn Kılavuzunun yapım aşamasında da uluslararası hukuk uzmanları arasında siber saldırılara katılan sivillerin sivil olma statülerini kaybedip kaybetmediklerine yönelik hukuki tartışmalar yaşanmış olup bu tartışmaların sonucunda genel görüş olarak bu sivillerin sivil statülerini kaybetmediği kabul edilmiştir[311]. 1949 Tarihli III. Cenevre Sözleşmesi madde 4'te kimlerin savaşçı statüsüne sahip olacağı düzenlenmiştir; bu kişiler düzenli ordu birlikleri, sivil kuvvetler ve levée en masse (işgale karşı toplu bir şekilde

[306] Michał Byczyński, "The Legal Status of Civilian Hackers under International Humanitarian Law", 98.
[307] Schmitt, *Tallinn Manuals 2.0*, Rule 29.
[308] Angelo Stirone, "Hacking and International Humanitarian Law: The Anonymous Group and the Syrian Electronic Army." *Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict 3*, (2020): 130.
[309] Michał Byczyński, "The Legal Status of Civilian Hackers under International Humanitarian Law, 98.
[310] Pazarcı, *Uluslararası Hukuk Dersleri IV*, 230.
[311] Schmitt, *Tallinn Manuals 2.0*, Rule 29, para 3.

silahlanıp ayaklanan halk) dir[312]. Bu yüzden siber saldırıya katılım gösteren siviller savaşan statüsünü (combatant status) ve bu statünün getirdiği özel korumayı kazanamamaktadır. Öte yandan bu kişiler savaşan olarak sayılmadığı gibi sivil koruma statüsünü de kaybetmektedirler[313]. Bu kişiler, vatansever olarak ülkesini işgalden korumak için silahlı bir şekilde ayaklanan levée en masse olarak sayılmadıkları sürece savaşan statüsünden yararlanamamaktadır[314].

Kızılhaç (ICRC) silahlı çatışmalara siberuzayda aktif bir şekilde doğrudan katılım gösteren sivil hackerların statüsünü ve çatışma yöntemleri üzerine belirsizlikleri önlemek için bir araştırma ve bu araştırmanın sonucunda da 8 kuraldan oluşan bir değerlendirme yapmıştır[315].

3.2.1. Kızılhaç (ICRC)'ın Sivil Hackerlar için Kullandığı 8 maddelik yöntem

Kızılhaç'ın sivil hackerlar için siber saldırıda bulunulduğu sırada uyulması gereken kurallar kılavuzu hazırlamasının temel sebebi, sivil hackerlar siber saldırıda bulunurken bu saldırılardan sivillerin zarar görme ihtimalidir[316]. Bu zararın gerçekleşmesini önlemek için Kızılhaç sivil hackerların uyması gereken 8 adet kural koymuştur.

(1) *Sivil hedeflere siber saldırı yöneltmeme kuralı;* bu kural uyarınca siviller ve sivil nesneler ile askeri kişiler ve askeri nesneler aynı korumaya sahip değillerdir. Sivillere ait altyapının, kamu hizmetlerine ve şirketlere ait sistemler, özel mülk olarak nitelendirilen sistemler ve sivil veriler insancıl hukuk tarafından korunmaktadır. Bu yüzden sivil bir hacker siber saldırıda bulunduğu zaman askeri hedeflerin dijital altyapılarını hedef almak zorundadır. Ek olarak her ne kadar sivil

[312] Geneva Convention (III) relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135, art 4.
[313] Ek Protokol I, madde 51 (3).
[314] Schmitt, *Tallinn Manuals 2.0*, Rule 91, para 3.
[315] Michał Byczyński, "The Legal Status of Civilian Hackers under International Humanitarian Law",101.
[316] Tilman Rodenhäuser, "8 Rules for Civilian Hackers during War – and 4 Obligations for States to Restrain Them," *International Committee of the Red Cross (ICRC)*, March 28, 2023, https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them.

nesne olarak kabul edilse de askeri amaçlarla kullanılan sivil nesneleri de sivil hackerlar, siber saldırı hedefi haline getirebilirler[317].

(2) *Askeri ve sivil hedefler arasında bir ayrım yapmayan zarar veren kötü amaçlı yazılımların kullanılmaması kuralı;* Ek Protokol I, madde 48'de düzenlenen ayrım yapma ilkesi, sivil hackerlar tarafından da gözetilmek zorundadır. Kızılhaç, bu kuralı açıklarken ayrım yapma ilkesine aykırılık teşkil edecek örneği, otomatik olarak yayılıp askeri ve sivil hedefleri birbirinden ayırt etme yetisine sahip olmayan kötü amaçlı yazılımların kullanılması şeklinde vermiştir[318]. Kısacası halihazırda aralarındaki sınırların siberuzayda bulanık olduğu sivil ve askeri hedefleri ayırt edecek bir donanımda olmayan yazılımların sivil hackerlar tarafından kullanılması bu kural ile yasaklanmıştır.

(3) *Askeri bir operasyon yapmadan önce yapılacak saldırının sivil hedeflere zarar vermemesi için gerekli olan bütün önlemlerin alınması kuralı;* bu kuralın temelinde de Ek Protokol I, madde 57'de düzenlenen harekât öncesi önlemler (precautions in attack) bulunmaktadır. Bu madde uyarınca silahlı çatışma öncesi ve esnasında öngörülebilecek durumlar için alınması gereken önlemlerin hepsinin alınması ve sivillerin zarar görmesi veya görülecek zararın en az olması amacıyla hareket etmek gerekmektedir. Kızılhaç, bu önlemlere örnek olarak askerler tarafından kullanılan orduya ait elektrik ya da demiryolu hizmetlerine yönelik yapılacak bir siber saldırı durumunda bu saldırının siviller üzerindeki etkisinin önlenmesini sağlama görevini yerine getirmeyi vermiştir[319]. Elektrik ya da demiryolu sistemine karşı yapılan bir siber saldırıda oluşacak elektrik kesintisi ya da demiryolundaki aksaklıklar yüzünden sivillerin zarar görmesi, yaralanması veya ölmesi gibi durumlar meydana gelirse bu durumda sivil hacker, gerekli önlemleri zamanında almadığı için insancıl hukuk ihlalinde bulunmuş sayılmaktadır.

[317] Bu durumun temeli Ek Protokol I, madde 52 (2)'de atılmıştır.
[318] Rodenhäuser, "8 Rules for Civilian Hackers.", Rule 2.
[319] Rodenhäuser, "8 Rules for Civilian Hackers.", Rule 3.

(4) *Sağlık ve insani tesislere herhangi bir siber saldırıda bulunmama kuralı;* bu kuralın temelinde I. Cenevre Sözleşmesi madde 19, IV. Cenevre Sözleşmesi madde 18, Ek Protokol I madde 12 ve 13 bulunmaktadır. Tüm bu maddeler gereğince silahlı çatışmalar esnasında hastaneler, seyyar sağlık birimleri gibi sağlık hizmeti verenler saldırı hedefi haline getirilememektedir. Aynı zamanda Ek Protokol I madde 70 ve 71 uyarınca da insani yardım kuruluşları ve bu kuruluşların çalışanları saldırı hedefi haline gelmekten muaf tutulmuşlardır. Bu kuralın temel amacı da siber saldırı ile sivil hackerların bu türden faaliyet gösteren yerleri ve kişileri saldırılarının hedefi haline getirmemesidir.

(5) *Nüfusun yaşaması için vazgeçilemez olan ve saldırıya uğraması durumunda oldukça tehlikeli durumların ortaya çıkabileceği hedeflere karşı siber saldırıda bulunmama kuralı;* bu kuralın temelinde de Ek Protokol madde 54 (2) ve madde 56 (1) bulunmaktadır. Söz konusu maddeler uyarınca sivillerin yaşamsal faaliyetlerini sürdürdüğü yerlere (tarım alanları, içme suyu kaynakları gibi) ve saldırıya uğraması durumunda sivil halk için tehlike yaratacak yerlere (nükleer santraller, barajlar gibi) karşı saldırıda bulunmak yasaktır. Bu yasağa, siberuzaydaki sivil hackerlar da tabiidir.

(6) *Sivil halk arasında korkuyu çıkarıp yaymak ve bu korkuyu körüklemek için şiddet içeren eylemde bulunmama kuralı;* bu kuralın temelinde Ek Protokol I madde 51(2) bulunmaktadır. Madde uyarınca silahlı çatışma esnasında birincil amacı siviller arasında korku ve terör yaymak olan şiddet eylemleri yasaktır. Kızılhaç bu yasağa örnek olarak siviller arasında terörü yaymak için iletişim ağlarının hacklenip kullanılması ve grafik içerik hazırlanıp bu içeriğin yayımlanmasını vermiştir[320].

(7) *Uluslararası insancıl hukukun ihlal edilmesini teşvik etmeme kuralı;* bu kural gereğince, siber saldırıda bulunan sivil hackerın yaptığı saldırı ile saldırının tüm

[320] Rodenhäuser, "8 Rules for Civilian Hackers.", Rule 6.

katılımcılarını insancıl hukuk kurallarının ihlal edilmesi yönünde teşvik etmesi, yönlendirmesi veya oluşacak ihlallere göz yumulması yasaklanmıştır. Kızılhaç, kural ihlalinin teşvikine örnek olarak sivillere ait kurumların çalışmalarını bozmak ya da engellemek amacıyla bu kurumlara ait iletişim kanallarında teknik bilgilerin herkesle paylaşılmasını vermiştir[321].

(8) *Silahlı çatışmanın karşı tarafı kurallara riayet etmese bile sivil hackerların kurallara uyma zorunluluğu kuralı;* bu kuralın temelini, insancıl hukuk kurallarının en temelini oluşturan ve *"genel yükümlülük"* başlığı altında düzenlenen Ek Protokol I madde 1 ve 2'dir. Bu maddeler uyarınca taraflar, silahlı çatışma esnasında insancıl hukuk kurallarına riayet etmekle yükümlüdürler. Ek olarak Kızılhaç, saldırıya karşılık intikam ya da misilleme ile hareket etmenin kurallara riayet etmemenin mazereti olmayacağını açıklamıştır[322]. Temel kural, çatışmanın tüm taraflarının kurallara aynı şekilde riayet edip herhangi bir tarafın dezavantajlı durumda kalmamasıdır (karşılılık ilkesi, principle of reciprocity); ancak Kızılhaç'ın bu konudaki duruşu, bu kuraldan da anlaşılacağı üzere insancıl hukuk kurallarına uymanın karşılıklılık ilkesine bağlı olmadığına yöneliktir[323].

4. Kritik Altyapılar

İlk bölümde de anlatıldığı üzere insancıl hukuk kapsamındaki sivil nesneler, askeri hedef olmayan tüm nesneler olarak olumsuz bir şekilde tanımlanmıştır[324]. Burada önemli olan husus, söz konusu nesnenin askeri bir amaç ve gereklilikle kullanılıp silahlı çatışmaya hizmet etmemesidir[325]. Ayrım yapma ilkesi[326] gereğince de sivil nesneler, askeri nesnelerden ayırt edilerek saldırının hedefi haline getirilmemelidir. Aynı kural Tallinn Kılavuzu, Kural 99'da da düzenlenmiştir. Kural uyarınca, siberuzayda yalnızca askeri nesne olarak sayılan altyapılar siber saldırı hedefi haline getirilebilmektedir.

[321] Rodenhäuser, "8 Rules for Civilian Hackers.", Rule 7.
[322] Rodenhäuser, "8 Rules for Civilian Hackers.", Rule 8.
[323] Emily Chertoff; Zachary Manfredi, "Deadly Ambiguity: IHL's Prohibition on Targeting Civilian Objects and the Risks of Decentered Interpretation," *Texas International Law Journal 53*, (2018): 270.
[324] Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction*, 91.
[325] Ek Protokol I, madde 52 (1).
[326] Ek Protokol I, madde 48.

Fiziki yapıdaki sivil nesneler ile siberuzaydaki sivil nesneler birbirlerinden farklılık göstermektedir. Ancak her iki sisteme siber saldırı yoluyla saldırmak hem daha elde edilebilir bir eylemdir hem de geleneksel savaş yöntemlerinde kullanılan silahlarla yapılan saldırılardan çok daha az maliyetlidir[327]. Siberuzaydaki sivil nesneler bu çalışmada altyapılar ve veritabanları şeklinde ikili bir ayrıma gidilerek ele alınacaktır.

Genel olarak kritik altyapılar, devletler için oldukça önemli olan fiziksel ve siber sistemleri ve varlıkları içermektedir ki, bu altyapıların yetersiz olması veya yok edilmesi, devletlerin fiziksel veya ekonomik güvenliği, kamu sağlığı veya emniyeti üzerinde telafi edilmesi güç bir zayıflığın ortaya çıkmasına sebep olmaktadır[328]. Özetle kritik altyapılar, devlet ve toplum için gerekli olan temel hizmetleri sağlamaktadır. Devletler, kendi sınırları içerisinde inşaa edilen ve kurulan her türlü kritik altyapı ve bu altyapı ile bağlantılı olarak yapılan faaliyetler üzerinde egemenlik yetkisine sahiptir[329].

Devletlerin altyapıları üzerinde sahip olduğu bölgesel egemenlik, diğer devletlerin bu altyapılara yönelik yapacağı siber operasyonlara dair sınırlamalar getirmektedir[330]. Bu sınırlamalar, devletlerin kendi altyapıları üzerinde sahip olduğu egemenliğe bağlı olarak yapılan koruma ile sağlanmaktadır[331]. Korumanın olmadığı durumlarda kritik altyapılara karşı düzenlenecek siber saldırılar; devlet, toplum ve ulusal güvenlik açısından hayati önem taşımakta olan işlevlerde zararlı kesintilere yol açabilmekte ve bu kesintiler siviller için büyük tehditler oluşturmaktadır[332]. Bu zararlı kesintiler ise bilgisayarlar aracılığı ile kodlanmış zararlı algoritmalarla gerçekleştirilmektedir (Ddos, Trojan Horse saldırıları gibi)[333].

---

[327] Bilge Karabacak, "Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri," *Siber Güvenlik Çalıştayı*, Bilgi Güvenliği Derneği, Ankara, 29 (2011): 3.
[328] Martti Lehto and Pekka Neittaanmäki. *Cyber Security*. (Cham: Springer Nature, 2022), 4.
[329] Schmitt, *Tallinn Manuals 2.0*, Rule 1.
[330] Schmitt, *Tallinn Manuals 2.0*, Rule 4.
[331] Schmitt, *Tallinn Manuals 2.0*, Rule 2.
[332] Martti Lehto, *Cyber Security*, 6.
[333] Antonio Carlo and Kim Obergfaell, "Cyber Attacks on Critical Infrastructures and Satellite Communications," *International Journal of Critical Infrastructure Protection* 46 (2024): 3, https://doi.org/10.1016/j.ijcip.2024.100701.

4.1. Elektrik Üretim ve Dağıtım Ağları

Elektrik üretim ve dağıtım ağları, devletlerin sosyal düzen ve sağlığı, ekonomisi ve güvenliğinin sağlanması için oldukça büyük bir öneme sahip olan altyapılardır[334]. Bu türden altyapılar; elektrik santralleri, trafo merkezleri ve elektrik şebekelerinden oluşmaktadır[335]. Bu altyapılara karşı yapılan siber saldırılarla yalnızca veriler zarar görmeyip saldırının şiddeti ve uzunluğuna göre insanların günlük aktiviteleri ve trafikte aksama da görülebilmekte olup daha kötü bir senaryoda ise sağlığı elektrikle çalışan sistemlere bağlı olan sivillerin hayatı tehlikeye girebilmektedir[336].

İnsancıl hukuktaki saldırımı kavramı yalnızca şiddet içerikli eylemlerle sınırlı kalmayıp yapılması sonucu şiddet eylemi ortaya çıkan eylemler olarak da değerlendirilmektedir; bu değerlendirmenin sonucunda ise bir elektrik şebekesinin *SCADA*[337] sistemine yönelik gerçekleştirilen bir siber saldırı sonucunda yangın çıktığı durumda elektrik şebekesine karşı yapılan saldırı, insancıl hukuk kapsamında yapılan saldırı olarak kabul edilmektedir[338]. Bu tespitten yola çıkarak, elektrik şebekesine karşı yapılan bir siber saldırı sonucu sivillerin kullandığı altyapı zarar görüyorsa, siviller bu zarar görmeden olumsuz bir yönde etkileniyorsa bu durumda siviller için kritik bir altyapı zarar gördüğü için insancıl hukuk ihlali gerçekleşmiş olmaktadır.

Elektrik üretim ve dağıtım altyapılarına yönelik gerçekleştirilen siber saldırılardan biri, 23 Aralık 2015 tarihinde, Rusya-Ukrayna savaşı sırasında Ukrayna'da bulunan 3 adet elektrik dağıtım şirketine karşı yapılan siber saldırıdır[339]. Bu saldırı, üçüncü bir tarafın *sosyal mühendislik* ve *Trojan Horse* ile elektrik dağıtım şirketi bilgisayarına ait SCADA sistemine yasadışı girişi ile yapılmış olup saldırının sonucunda Ukrayna'da yaklaşık

---

[334] Gerd H. Kjølle, Ingrid Bouwer Utne, and Oddbjørn Gjerde, "Risk Analysis of Critical Infrastructures Emphasizing Electricity Supply and Interdependencies," *Reliability Engineering & System Safety 105* (2012): 81.

[335] Global Security and Sustainability Center (GSSC), "Energy Security and Critical Infrastructure Protection," accessed June 24, 2025, https://www.gssc.lt/en/publication/energy-security-and-critical-infrastructure-protection/.

[336] Martti Lehto, *Cyber Security*, 219.

[337] Supervisory Control and Data Acquisition. Detaylı bilgi için bkz. *Inductive Automation*, "What Is SCADA?," accessed June 24, 2025, https://inductiveautomation.com/resources/article/what-is-scada.

[338] Schmitt, *Tallinn Manuals 2.0*, Rule 92.

[339] ICS-CERT, *Cyber-Attack Against Ukrainian Critical Infrastructure*, February 25, 2016, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.

225.000 kişi bir süreliğine elektriksiz kalmıştır[340]. Bu saldırı, Ek Protokol I madde 52 gereğince, sivillerin kullanımında olan kritik altyapıya karşı yapıldığı için insancıl hukuka aykırıdır.

4.2. Su ve Kanalizasyon Altyapısı

Su ve kanalizasyon altyapıları, iki işlevi bir arada yerine getirerek hem su hizmeti sağlamakta hem de bulunduğu devlet içerisinde sel, kuraklık ve içme suyu bulma sorunları gibi hususları çözüme kavuşturmaktadır[341]. Su ve kanalizasyon altyapı sistemleri genel olarak; su şebekeleri, normal su ve atık su arıtma tesisleri, hidroelektrik santralleri ve barajlardan oluşmaktadır[342]. Özellikle barajlar ve setler, bilgisayar ve birçok farklı bilgisayar ağlarına bağlı olmak zorunda olduğu için siber saldırılar karşısında daha savunmasız kalmaktadır[343].

Barajlar, su pompa tesisleri, kanallar ve setleri ile ülke genelindeki yaşam alanlarına su temini, güç üretimi, gezilebilir su yolları ile de taşkından korunma sağlamakta ve çevresel iyileştirmeler yapmaktadır[344]. Ancak yukarıda açıklanan nedenlerden ötürü bu türden tesislerin siber saldırıya uğraması oldukça olasıdır. Nitekim 2013 yılında ABD'de bulunan "The Bowman Avenue" adlı su barajına İranlı hackerlar tarafında siber saldırıda bulunulmuş olup yapılan siber saldırı ile hackerlar, barajın yönetim ve bilgi sistemine uzaktan bir şekilde erişim ve kontrol sağlamıştır[345]. Baraj kapıları, hackerlar tarafından açılamamış olsa da açılmış olması durumunda barajın yakınında bulunan yerleşim yerlerinde yaşayan sivillerin hayatlarını kaybedeceği, yaralanacağı, evlerinin ve yaşam alanlarının zarar göreceği oldukça öngörülebilir bir durumdur.

---

[340] Defense Use Case, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Electricity Information Sharing and Analysis Center (E-ISAC) 388.1–29 (2016): 3.
[341] United Nations Office for Disaster Risk Reduction (UNDRR), *Water Infrastructure Resilience: Examples from Dams, Wastewater Treatment Plants and Water Supply Systems*, accessed June 24, 2025, https://www.preventionweb.net/publication/water-infrastructure-resilience-examples-dams-wastewater-treatment-plants-and-water.
[342] Simplicable, "40 Examples of Water Infrastructure," Simplicable, 2025, accessed June 25, 2025, https://simplicable.com/world/water-infrastructure.
[343] Michael Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", 385.
[344] Martti Lehto, *Cyber Security*, 17.
[345] Daha fazla detay için *bkz.* Gary Cohen, "Throwback Attack: How the Modest Bowman Avenue Dam Became the Target of Iranian Hackers." *Control Engineering*. August 12, 2021. Accessed June 25, 2025. https://www.controleng.com/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/.

4.3. Nükleer Enerji Tesisleri Altyapıları

Nükleer enerji tesisleri; nükleer santraller, yakıt döngüsü tesisleri, radyoaktif atık yönetimi işlemleri, reaktörlerin devre dışı bırakılması ile birlikte tıbbi, endüstriyel ve akademik alanlarda kullanılan nükleer ve radyoaktif maddeler ile nükleer malzeme taşımacılığını kapsamaktadır[346]. Siber saldırılar sayesinde nükleer enerji tesislerine ait bilgisayar ve diğer bağlı ağlarına müdahale edilerek tesislerin işleyişi bozulabilmekte olup bu bozulma, çevredeki sivil halkın hayatını tehlikeye sokabilmektedir[347]. Örneğin nükleer enerji tesisinin bilgisayar sistemine yapılacak bir siber saldırı ile veri sisteminde yapılacak değişikliklerle nükleer reaktörlerin erimesi, zehirli ve tehlikeli maddelerin sızıntı yapması gibi hem siviller hem de çevre için oldukça tehlikeli durumlar ortaya çıkabilmektedir[348].

Önceki bölümde de bahsedildiği üzere İran'da bulunan Natanz nükleer enerji tesislerine yapılan Stuxnet adı verilen siber saldırı, çarpıcı bir örnek olarak hala varlığını sürdürmektedir. Bu yüzden çalışma sistemi bilgisayarlara bağlı olan nükleer enerji tesislerinin siber saldırıya uğramaması için gerekli olan öngörülebilir tüm önlemlerin alınması gerekmekte olup bu önlemlerin saldırıda bulunan tarafça da alınması gerekmektedir[349].

4.4. Ulaşım ve Lojistik Altyapısı

Ulaşım ve lojistik altyapıları, insanların günlük olarak hareket etmelerini sağlamakta olup malların üretim ve dağıtımının gerçekleşmesini yerine getirir[350]. Bu altyapılar; karayolları, havacılık, demiryolları ve denizcilik faaliyetlerinden oluşmaktadır[351]. Siberuzay aracılığıyla, havaalanı kontrol sistemlerine sızıp kasıtlı olarak müdahale ederek havayolları şirketlerinin uçaklarının çarpışmasına, kaza geçirmesine sebep verilebilmesi

[346] Martti Lehto, *Cyber Security*, 30.
[347] Sean Watts, "Combatant Status and Computer Network Attack," *Virginia Journal of International Law 50*, (2010): 404.
[348] Michael Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello", 374.
[349] Nils Melzer, *ICRC Handbook of IHL*, 54.
[350] United Nations Economic Commission for Europe (UNECE), "Transport Infrastructure Development," *UNECE*, n.d., accessed June 25, 2025, https://unece.org/transport/transport-infrastructure-development.
[351] Martti Lehto, *Cyber Security*, 31.

öngörülmektedir[352]. Küresel ekonominin bir parçası olan deniz taşımalarında gerek yolcu gerekse kargolar taşınmakta olup bu taşımacılık yüksek oranda bilgisayar sistemlerine bağlı olarak gerçekleştirilmektedir[353]. Bilgi ve iletişim teknolojisinin birçok kritik altyapı hizmetlerinde kullanılması, bu sistemlerin siber saldırı yolu ile saldırıya uğrayıp ağlarında bozulma ya da hasar görme riskini arttırmaktadır böylece yukarıda havaalanı üzerinden verilen örnekteki gibi siber saldırılar, ulaşım altyapıları üzerinde yıkıcı etkilere yol açabilmektedir[354]. Bir başka örnek olarak, silahlı çatışmanın taraflarından birinin nüfus merkezlerine gıda taşınmasını engellemek için gıdaların üretilip işlendiği veya depolanıp dağıtıma çıkarıldığı yerleri hedef alarak siber saldırıda bulunabilmekte ve bu saldırı sonucunda sivil nüfus açlıkla mücadele etmek zorunda kalabilmektedir[355]. Ancak her durumda olduğu gibi böyle bir durumda da söz konusu gıda tesislerinde ve bu gıdaların taşınması ve ulaştırılmasında amacın askeriyenin yararı veya hizmeti olmaması gerekmektedir. Böyle bir askeri amacın varlığında, artık söz konusu tesislerin siber saldırıya uğrayıp gıda taşımacılığının aksaması sivillerin hedef alındığı bir saldırı olmaktan çıkmaktadır (ancak sivillerin de zarar gördüğü hallerde gereklilik ve ölçülülük ilkelerine göre bir değerlendirme yapılmalıdır)[356].

4.5. İletişim Altyapısı

İletişim altyapıları; telekomünikasyon şebekeleri, posta hizmetleri ve internetten oluşmaktadır[357]. Özellikle de internet için kurulan telekomünikasyon altyapılarının bilgi ve iletişim sistemlerinin güvenliğinin sağlanması ve siber saldırılardan korunması, devletlerin kendi sorumluluğundadır[358]. İletişim altyapılarına yapılacak siber saldırılar; yukarı veya aşağı bağlantı iletişim sinyallerine müdahale etmek, verileri almak veya değiştirmek, uzaydan uzaya iletişimi bozmak, sistemdeki yazılım veya donanımı kısmen veya tamamen imha etmek veya uydu kontrollerini manipüle etmek gibi amaçlarla

[352] Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," *International Review of the Red Cross 94*, (2012): 559.
[353] Martti Lehto, *Cyber Security*, 31.
[354] Simon McKenzie, "Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute," *Journal of International Criminal Justice 19*, (2021): 1171.
[355] Schmitt, *Tallinn Manuals 2.0*, Rule 107.
[356] Ek Protokol I, madde 52 (2).
[357] Martti Lehto, *Cyber Security*, 15.
[358] Tallinn Manual 2.0, Rule 61.

yapılabilmektedir[359]. Ancak iletişim ağlarına karşı yapılan bir siber saldırı sonucu iletişimde aksaklık meydana gelmesi gibi durumlarda insancıl hukuk kapsamında başlı başına bir saldırı niteliği taşımamaktadır; çünkü bir siber operasyonun insancıl hukuktaki saldırı kapsamına girmesi için şiddet içerikli bir zarar vermenin meydana gelmesi gerekmektedir.[360].

5. Veri tabanları

5.1. Sağlık Sistemleri

Özellikle son yirmi yılda sağlık sektöründe bilgi teknolojilerinin kullanımı oldukça yaygınlaşmış olup hastaların sağlığının iyileştirilmesi, kontrol edilmesi ve izlenmesi için elektronik sağlık kayıtları (EHR) ve biyomedikal veri tabanları geliştirilmiştir[361]. Hastanelerin sağlık sistemleri, denetleyici kontrol ve veri toplama (veya SCADA) sistemlerine (DCS) güvenmekte olduğu için bu sistemler, hemen hemen her saldırganın dışarıdan müdahalesine karşı son derece savunmasız kalmaktadır[362]. Örneğin bir hastanenin veri tabanına kayıtlı bir hastanın bilgileri manipüle edilirse ve bu manipülasyon sonucu yanlış medikal bilgi yüzünden hastanın sağlık durumunun kötüleşmesi ya da hayatının sona ermesi gibi ihtimallerin oluşması mümkün olmaktadır[363]. Bu yüzden sağlık sistemlerindeki kayıtlı verilerin korunması, sivillerin yaşamlarını sağlıklı bir şekilde sürdürmesi açısından oldukça büyük bir öneme sahiptir.

5.2. Kamu Hizmetlerine Ait Bilgi Sistemleri

Gelişmiş bilgi iletişim teknolojileri, kamu kurumlarının vatandaşlara verdiği hizmette de kendini göstermiş, birçok devlet kurumu hizmetlerini dijital ortama da taşımış ve bu durum çevrimiçi aplikasyonlar, nüfus kayıt sistemleri, belediye hizmet portalları, e-devlet uygulamaları ve sosyal medya hesapları gibi şekillerde ortaya çıkmıştır[364]. Bu sistemler, dünyanın dört bir yanında dijitali kullanan toplumların bilgi sistemleri ve veri depolaması

[359] Tallinn Manual 2.0, 270.
[360] Norwegian Centre for Humanitarian Studies, *Oslo Manual on Select Topics of the Law of Armed Conflict*, Rule 8 (Oslo: NCHS, 2020), 7.
[361] Martti Letho, *Cyber Security*, 184.
[362] Cordula Droege, "Get off my cloud", 538.
[363] Schmitt, *Tallinn Manuals 2.0*, Rule 94, para 5.
[364] Volkan Göçoğlu, "Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm", 619.

ile uzun zamandır birbirine bağlı olan vatandaşlar tarafından günlük olarak kullanılmaktadır; ancak vatandaşların dışında siber saldırganlar da bu sistemlerden kolayca yararlanabilmekte ve saldırılarını bu sistemlere yöneltebilmektedir[365]. Bu durumun en çarpıcı örneklerinden biri ise önceki bölümlerde bahsedilen Estonya'nın devlet kurumlarının bilişim sistemlerine karşı yapılan siber saldırıdır. 2007 yılında gerçekleşen bu saldırı; hackerlar tarafından DDoS türünde e-kamu hizmetlerinin sekteye uğratılması için yapılmış ve bu saldırı, NATO'yu harekete geçirip Tallinn Kılavuzu'nun hazırlanması konusunda teşvik etmiştir[366].

5.3. Finans ve Bankacılık Sistemleri

Finans sektörü, dünya ekonomisinin merkezinde olan ve dünya çapında farklı yerlerden birçok insanın, şirketlerin ve devletlerin finanslarını ayarlamalarını, ticaretlerini yönetmelerini, para akışının sağlanması gibi eylemlerin yapıldığı önemli bir sektördür[367]. Finans ve bankacılık sistemlerine yönelik yapılan siber saldırılar ile amaç genel olarak bankalara kayıtlı müşterilerin kayıtlı bilgilerini çalmak, belirli müşterilerin kendi hesaplarındaki paralarla yaptıkları finansal işlemleri takip edip gözlemlemek, finansal işlemler için yapılan operasyonları manipüle edip para çalmaktır[368]. Örneğin bir devletin finans ve uluslararası bankacılık ödeme sistemine (SWIFT) karşı yapılacak bir siber saldırı, küresel çapta bir mali karışıklığa ve kayba neden olabilmektedir[369].

[365] Martti Letho, *Cyber Security*, 154.
[366] Schmitt, *Tallinn Manual 2.0*, xix–xxii.
[367] Martti Letho, *Cyber Security*, 22.
[368] Martti Letho, *Cyber Security*, 23.
[369] Schmitt, *Tallinn Manuals 2.0*, Rule 4, para 26.

6. Sivil Nesne Statüsü: Dijital Ekonomik ve Kültürel Varlıklar

Dijital ekonomik varlıklar (digital economic assets), dijital formda bulunması durumunda sahibi olan kişi ya da kuruma ekonomik zarar verebilecek varlıklar olarak tanımlanmaktadır[370]. Bu varlıklar, internet üzerinde ya da bilgisayarda bulutlarda saklanan ve bu varlıklara sahip olan kişilerin üzerinde mülkiyeti olan verilerdir[371]. Kripto para olan bitcoinler, NFT'ler[372] gibi varlıklar, dijital ekonomik varlık olarak kabul edilmektedir[373]. Dijital kültürel varlıklar ise birçoğu ya önceden var olan kültürel eserlerin online hale getirilmesi ile ya da başlı başına dijital ortamda kültürel eserin meydana getirilmesi ile oluşturulan varlıklardır[374]. En başından beri dijital olarak ortaya çıkmış kültürel ya da ekonomik varlıklar; yaratıldığı anda dijital olarak kodlanmakta olup dijital formatta tamamlanan ve gösterilen sanat eserleri ve ekonomik varlıklar, elektronik formatta saklanan belgeler ve arşivler içermektedir[375].

İnsancıl hukuk kapsamında ekonomik ve kültürel varlıkların sivil nesne olarak kabul edilip edilmemesi, edilmesi durumunda ise hangi durumlarda bu varlıklara karşı yapılan siber operasyonların insancıl hukuk kapsamında saldırı sayılıp sayılmayacağı oldukça yeni ve tartışmaya açık bir konudur. Bu varlıkların insancıl hukukta nasıl ortaya çıkacağı, hukuki statüsünün ne olacağı hakkında kesinleşmiş bir tanım ya da kategori bulunmamaktadır. Ancak kültürel varlıklar söz konusu olduğunda bu varlıklar, insancıl hukuk kapsamında korunmaktadır ve askeri gereklilik bulunmadığı sürece saldırı hedefi haline getirilmeleri yasaklanmıştır[376].

---

[370] Keyun Ruan, *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*, 1st ed. (San Diego: Academic Press, 2019), 6, https://books.google.com.tr/books?id=c6nRDgAAQBAJ.
[371] Toygar Alp, C. E. Rohm Jr, and Jake Zhu. "A new asset type: digital assets." *Journal of International Technology and Information Management 22*, (2013): 113.
[372] Bir diğer adıyla *"non-fungible tokens"*, değiştirilemez tokens anlamına gelen NFT'ler fotoğraf, müzik dosyası, dijital sanat eserleri gibi varlıklardan oluşmaktadır. Bu varlıklar, blokchain sisteminde mülkiyeti tanımlanmış bir şekilde durmakta ve ekonomik değere sahip olmaktadır. Daha fazla bilgi için bkz. Merve Kadriye Yurdabak, "NFT: Dijital Sanatta Yeni Bir Perspektif ve Getirdiği Fırsatlar Üzerine Bir Derleme," *Nişantaşı Üniversitesi Sosyal Bilimler Dergisi* 10, (2022): 143–153.
[373] Muhammed Acar, "Siber Uzay ve Egemenlik: Kripto Paraların Etkisi", (Yüksek Lisans Tezi, Selçuk Üniversitesi, 2022), 73.
[374] Harrison Dinniss, *Cyber Warfare and the Laws of War*, 231.
[375] Harrison Dinniss, 232.
[376] Lahey Düzenlemeleri madde 51, Ek Protokol I madde 51.

Saldırı hedefi haline getirilme yasağı, bu varlıklar dijital ortamda olsa da geçerliliğini sürdürmektedir[377]. Bir başka deyişle, fiziki formda bulunan kültürel varlıklar insancıl hukuk kuralları tarafından nasıl korunuyorsa dijital alanda varlık gösteren kültürel varlıklar da aynı korumaya tabi tutulmaktadır. Böylelikle bu varlıklar, sivil nesne olarak kabul edilmektedir. Ancak doktrinde tartışmalar hala devam etmektedir[378].

7. Çift Kullanım İlkesi ve Siberuzayda Sivil Nesneler

Çalışmanın ilk bölümünde de anlatıldığı üzere, insancıl hukuk kapsamına giren silahlı çatışmalar esnasında savaşan tarafların her zaman savaşanlar ve siviller arasında ayrım yapma zorunluluğu bulunmaktadır[379]. Böylelikle çatışma esnasında sivillerin ve sivil nesnelerin saldırıların hedefi haline getirilmeleri de yasaklanmıştır[380]. Cenevre Sözleşmeleri ve Ek Protokollerde sivil ve askeri nesneler ayrı ayrı düzenlenmiş ve farklı kurallara tabi tutulmuş olsa da bazı durumlarda nesneler hem sivil hem de askeri nitelikte olabilmektedir; örneğin nehir üzerindeki bir köprünün hem bir çiftçinin traktörü ile geçerek kullanılması hem de askeri bir tankın geçerek kullanılması söz konusu olabilmektedir[381].

Siberuzayda çift kullanılan nesneler bir yana, genel olarak sivil nesneler ve askeri nesneler arasında bir ayrımın yapılması ve bu iki türün arasına belirli bir sınırın çekilmesi oldukça zor bir değerlendirme süreci gerektirmektedir[382]. Siberuzay ve yapay zeka (AI) gibi ortamlar doğaları gereği genel olarak çift kullanımlı olarak kabul edilmektedir; çünkü

[377] Harrison Dinniss, *Cyber Warfare and the Laws of War*, 233.
[378] Data'ların sivil ya da askeri nesneler olarak kabul edilip edilmeyeceği, bu verilerin insancıl hukuk kapsamında düzenlenen görülebilir ve elle tutulabilir nesnelerle aynı şekilde değerlendirilebileceğini savunan ve bu savunmaya katılmayan uluslararası hukukçular bulunmaktadır. Bu konuda ayrıntılı bilgi için *bkz*. Tallinn Manuals Rule 100, Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel Law Review* 48, no. 1 (2015): 55–80. Karşıt görüş için bkz. Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law," *Journal of Conflict and Security Law* 28, no. 2 (2023): 349–387.
[379] Ek Protokol I, madde 48.
[380] Ek Protokol I, madde 51.
[381] Adem Özer, "Düşmanlıkların Yürütülmesinde Orantılılık İlkesi: Teorik Ve Pratik Zorluklar." *Yalova Sosyal Bilimler Dergisi 13*, (2023): 276.
[382] Michael Gervais, "Cyber attacks and the laws of war." *Journal of Law & Cyber Warfare 1*, (2012): 74.

askeri siber operasyonlar bilgi ve iletişim sistemlerine, ağ kablolarına ve sunucularına karşı yapılmaktadır ki bu sistemler halihazırda siviller tarafından da kullanılmaktadır[383].

Silahlı çatışmalar esnasında askeri operasyonların yapıldığı tespit edilen bir ağ sistemine karşı çatışma taraflarından biri siber saldırıda bulunursa bu durumda o ağ sistemi, siviller tarafından da kullanılıyor olsa bile sivil nesne olma karakterini kaybetmektedir[384]. Siviller tarafından da kullanılıp aynı zamanda askeri operasyon gerçekleştirme amacına da hizmet eden nesnelere örnek olarak ise; demiryolu ağları, askeri bilgil yayımlayan televizyon ve radyo kanalları, sivil havaalanı olsa da askeri uçakları indirmek, kaldırmak ya da füze fırlatmak için kullanılan havaalanı ağ sistemleri verilebilir[385].

Bir nesnenin hem sivillere hem de askerlere hizmet etmesi durumunda ya da bu nesneler, iki tarafça kullanılıp saldırı hedefi haline getiriliyorsa bu durumda saldırının çatışma sırasındaki düşman tarafı bertaraf etmek amacı ile askeri gerekliliğin bulunması gerekmektedir[386]. Kullanım yolu ile askeri nesne haline gelen nesneler, askeri amaçla kullanımlarının son bulması ile tekrardan sivil nesne olma statüsüne geri dönebilmektedir; aynı durum amaç yolu ile askeri nesne haline gelen nesneler için de geçerlidir, bu nesneler de askeri amacın ortadan kalkması ile tekrardan kendi sivil nesne statülerine kavuşmaktadırlar[387]. Burada önemli olan husus, saldırıda bulunacak askeri kişinin sahip olduğu mevcut bilgilerin, sivil nesnenin askeri kullanıma dönüştürülebileceği sonucuna güvenilir bir şekilde varıp varmamış olmasıdır; böyle bir güvenilirlik mevcutsa o zaman saldırı da meşru olarak kabul edilmektedir[388]. Çünkü hâkim olan görüşe göre, askeri amaca hizmet eden nesneler çift kullanım nesneleri de olsa askeri nesne ve hedefi olarak kabul edilmektedir[389].

Askeri hedefe katkı sağlayan çift kullanım nesnelerine örnek olarak normalde siviller için bilgisayar donanımı, ağ sistemleri hizmeti gibi faaliyet yapan bir fabrikanın ordu için

[383] Oona A. Hathaway, Azmat Khan, and Mara Redlich Revkin. "The Dangerous Rise of Dual-Use Objects in War", *Duke Law School Public Law & Legal Theory Series 56*, (2024): 97.
[384] Schmitt, Tallinn Manual 2.0, Rule 100 para 10.
[385] Schmitt, Tallinn Manual 2.0, Rule 100 para 11.
[386] Gervais, "Cyber attacks and the laws of war.", 80.
[387] Schmitt, *Tallinn Manual 2.0*, Rule 100 para 12.
[388] Schmitt, Tallinn Manual 2.0, Rule 100 para 14.
[389] Eitan Diamond, Applying International Humanitarian Law to Cyber Warfare, 77.

bilgisayar donanımı üretip ordunun ağ sistemine hizmet etmesi ya da direniş güçlerine kodlanmış mesajlar ileten bir web sitesinin donanımı ve yaptığı yayınlarla askeri eyleme etkili bir katkı sağlaması ve bu durumun web sitesini destekleyen siber altyapıyı askeri bir hedef haline getirmesi verilebilir[390]. Bu iki durumda da nesneler, sivil nesne olma statüsünü kaybedip meşru saldırı hedefi haline gelmektedir. Sonuç olarak eğer askeri bir amaca hizmet eden söz konusu nesne saldırı hedefi haline getirildiğinde askeri avantaj elde ediliyorsa ve saldırıyı gerçekleştiren kişi öngörülebilecek bütün önlemleri almışsa bu durumda çift kullanılan nesneye yönelik yapılan siber saldırı, hukuka aykırılık teşkil etmemektedir[391].

8. Siberuzayda Belirsizlik Durumu

Siberuzay, bilgi ve iletişim teknolojilerinin gelişmesi ve yayılması ile birlikte günden güne birçok uluslararası nitelikte olan ve uluslararası nitelikte olmayan silahlı çatışmalar sırasında kullanılmakta; ancak Tallinn Manual gibi rehber kılavuz bulunsa da bu konuya dair bağlayıcılığı bulunan herhangi bir uluslararası anlaşma ya da uluslararası mahkeme kararı bulunmamaktadır[392]. Siberuzay ve uluslararası insancıl hukuka ilişkin hukuki bir düzenlemenin halihazırda yapılmamış olması, siberuzayda kişilerin, nesnelerin ve varlıkların ayrımını yapma ve hukuki statüsünü belirleme gibi noktalarda belirsizlikler ortaya çıkarmaktadır. Bu belirsizliğin diğer önemli nedenleri de siber saldırıların kinetik eylem olmayıp siberuzayda gerçekleştirilen saldırılar olması, sivil-askeri kişiler arasındaki ayrımın ve çıkacak sorunlara karşı çözüm getiren hukuki çerçevenin sınırlarının belirlenmesinin zorluğudur[393].

Özetle siber saldırılar söz konusu olduğunda belirsizliklerin ortaya çıkmasının temel sebepleri; siber saldırıların yeni bir tehdit olarak ortaya çıkması yüzünden deneyim eksikliği ile hukuki düzenleme eksikliği yüzünden benzetme ve yorumlama usulü ile hareket etmek ve askeri ve sivil kişilerle nesneler ayrımının zorluğu sayılabilmektedir[394].

---

[390] Schmitt, Tallinn Manual 2.0, Rule 100 para 15.
[391] Gervais, "Cyber attacks and the laws of war.", 84.
[392] Pasupathieswaran M and Kapilan Bharathi, "Digital Battlefronts: Rethinking Legal Frontiers in Cyberwarfare and AI Conflicts", *International Journal for Multidisciplinary Research 6*, (2024): 1.
[393] Antonia Chayes, "Rethinking warfare: The ambiguity of cyber attacks." *Harv. Nat'l Sec. J. 6* (2015): 474.
[394] Oliver Kessler and Wouter Werner. "Expertise, uncertainty, and international law: a study of the Tallinn Manual on Cyberwarfare." *Leiden Journal of International Law 26*. (2013): 798.

DDoS, sosyal mühendislik, Trojan Horse veya Rootkitler gibi birçok yöntemle yapılabilen ve sonucunda basit bir veri manipülasyonu, ciddi bir sivil kaybı ya da zarar görmesi gibi durumların da gerçekleşme ihtimali olan siber saldırılara karşı, deneyimsizliğin ve bu konuya özel bağlayıcı hukuki metinlerin eksikliği yüzünden hangi savaş kurallarının nasıl uygulanacağı kesinlik içermemektedir[395]. En temel olan sivil kişilerle askeri kişiler arasında ayrım yapma ilkesine riayet etme zorunluluğu varken siberuzayda kimlerin askeri kişiler olarak kabul edileceği kimlerin ise sivil olma statüsünü koruduğunun belirlenmesi hususunda da sorunlar çıkmaktadır.

Askeri kişiler gerek giydikleri üniformalarla gerekse üzerlerinde taşıdıkları ayırt edici sembollerle ve silahlarını açık bir şekilde taşıyarak kendilerini sivillerden ayrı göstermek zorundadır[396]. Ancak siberuzaydaki saldırganların, insancıl hukuk kapsamında savaşan statüsüne girmesi için sayılan şartların varlığının yanında statülerinin açıklık kazanması amacıyla saldırının amacı ve bu amaca giderken uygulanan saldırı yöntemlerinin, seçilen hedefin, ağ sistemlerine yapılan saldırının nasıl bir etki ve zarar ortaya çıkardığı gibi durumların da incelenmesi gerekmektedir[397]. Aynı ayrım yapma zorluğu sivil ve askeri nesneler söz konusu olduğunda da ortaya çıkmaktadır; bu durumun en temel sebebi ise yukarıda bahsedilen konu olan çift kullanımlı (dual-use) nesnelerin varlığıdır. Siberuzayda birçok veri tabanı ve kritik altyapılar askeri güçler ve siviller tarafından ortak olarak kullanılmaktadır[398].

Bir nesnenin hem askeri güçler tarafından kullanılıp askeri operasyonlara etkili bir yardım ve hizmet yapması hem de sivillerin yararına kullanılması durumunda söz konusu nesne askeri nesne olarak kabul edilse de bu durumda siviller de aynı nesneyi kullandığı için saldırının ölçülü ve gerekli olması durumlarının incelenmesi gerekmektedir[399]. Saldırganın, çift kullanımlı olan nesneye karşı siber saldırı düzenlemeden önce sivillerin zarar görmemesi için gerekli önlemleri alması ya da zarar görecekse de bu zararla askeri

[395] Harrison Dinniss, *Cyber Warfare and the Laws of War*, 72.
[396] Ek Protokol I, madde 44. Ayrıca *bkz*. Sean Watts, "The Notion of Combatancy in Cyber Warfare," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (Tallinn: IEEE, June 2012), 236.
[397] Sean Watts, "The Notion of Combatancy in Cyber Warfare", 246.
[398] Schmitt, *Tallinn Manual 2.0*, Rule 100.
[399] Schmitt, *Tallinn Manual 2.0*, Rule 101.

avantaj arasında bir orantının olması gerekmektedir; ancak siberuzayda bu ölçünün doğru sağlanması da ayrı bir zorluk ve belirsizlik ortaya çıkarmaktadır[400].

Siber saldırılarda, çoğu zaman saldırıyı yapan kişinin kimliğinin belirlenmesi ve saldırıyı yapanın sorumlu olarak atfedilmesi söz konusu olduğunda da zorluk çıkmaktadır[401]. Saldırıyı bir kişiye, gruba ya da devlete atfetme sorununun oluşmasının temel nedeni ise internetteki ağların birçok alt katmandan oluşması ve bu katmanlar arasında siber saldırı gerçekleştirecek kişilerin kimliklerini gizleyerek rahatça hareket edebilmesidir[402]. Günümüzde IP adresleri belirlenip takip edilse de kısa süre içinde harekete geçilmezse bu adresler internet ağlarındaki yoğunluk nedeniyle kayıt edilmediği için bulunamaz hale gelmektedir[403]. Örneğin birçok çalışanın kullandığı şirket bilgisayarı ya da kullanıcılara ücretsiz hizmet sağlayan kafelerde bu IP adreslerinin kısa süre içerisinde tespit edilip siber saldırıyı yapan kişinin bulunması oldukça zor bir durumdur[404].

Normal şartlarda, siber saldırının devlete ait organlardan biri tarafından yapıldığı tespit edildiğinde söz konusu devlet, uluslararası hukuk sorumluluğunun ihlalini oluşturan bir siber saldırı eyleminden sorumlu tutulabilmektedir; ancak böyle bir tespitin yapılamadığı durumlarda ortada sorumlu olan devlet de bulunmamaktadır ve böylece yapılan siber saldırı failsiz kalmaktadır[405]. Aynı şekilde normal şartlarda bir siber saldırı devlet tarafından değil de bir grup tarafından yapıldığında da devletin bu saldırıdan sorumlu tutulabilmesi için söz konusu saldırıyı yapan grubun, devlet tarafından saldırının nasıl gerçekleştirileceğine yönelik belirli talimat ve direktifler almış olduğunun tespiti gerekmektedir[406]. IP adresinden siber saldırıyı kimin yaptığını belirlemek bile zorlu bir süreç iken bu saldırıdan bir devletin sorumlu tutulması daha da güç bir durum haline gelmektedir.

---

[400] Schmitt, *Tallinn Manual 2.0*, Rule 101 para 3.
[401] Cassandra Steer, "International Humanitarian Law in the 'Grey Zone' of Space and Cyber," *Centre for International Governance Innovation* (CIGI), 29 Ocak 2023, https://www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/
[402] Duncan B. Hollis, "An e-SOS for Cyberspace." *Harv. Int'l LJ 52*, (2011): 397.
[403] Private Internet Access. "Is a Dedicated IP Traceable?" *Private Internet Access Blog*, April 5, 2024. https://www.privateinternetaccess.com/blog/is-a-dedicated-ip-traceable/.
[404] Duncan B. Hollis, "An e-SOS for Cyberspace.", 399.
[405] Schmitt, *Tallinn Manual 2.0*, Rule 14.
[406] Michael N. Schmitt, "Classification of cyber conflict." *International Law Studies 89*, (2013): 243.

Uluslararası nitelikte olan silahlı çatışmalarda devletin dışındaki aktörler tarafından yapılan siber saldırıların devlete atfedilmesi, kinetik bir saldırının devlete atfedilmesinden daha zor bir durum olup uluslararası nitelikte olmayan silahlı çatışmalarda da sanal örgütlenme büyüdükçe, örgütlerin kullandığı yöntem ve sistemler geliştikçe ve bu tarz örgütlerin yaptığı saldırılar yaygınlaştıkça bu saldırılardan kimin sorumlu tutulacağı, saldırganların bireysel mi organize bir grup olarak mı hareket ettiğinin belirlenmesi şu anki vaziyetten daha da zor bir duruma evrilmektedir[407]. Ancak devlete sorumluluk atfedilemese bile yine de siber saldırılara karşı devletlerin hukuki düzenleme, yaptırım belirleme, koruma mekanizmaları geliştirme sorumlulukları mevcut bulunmaktadır[408].

Siberuzayda birçok belirsizliğin ortaya çıkmasının bir diğer sebebi de otonom silahlardır. Genel olarak otonom silahlar, saldırı hedefi belirlerken ya da saldırıyı gerçekleştirirken olabildiğince az insan müdahalesi içeren silahlardır[409]. Bu silahlar yarı otonom ve tam otonom olmak üzere ikiye ayrılmaktadır. Yarı-otonom olan silahlarda asgari miktarda insan müdahalesi bulunmakla birlikte söz konusu silah, saldırı hedefi belirlerken ya da saldırırken onu komuta eden insanın yönlendirmesi ile hareket etmektedir[410]. Ancak sistemin tam otonom olduğu silahlarda böyle bir insan müdahalesi bulunmamaktadır[411]. Bu tür silahların kullanımının sınırlandırılması ya da tümüyle yasaklanması için hukuk camiasında tartışmalar bulunmaktadır; bu tartışmaların temel sebebi ise insan müdahale ve karar mekanizmasının oldukça az bulunması sonucunda bu silahların siviller ve savaşanlar arasında gözetilmesi gereken ayrım ilkesini ihlal etmesi yönündeki endişelerdir[412]. Bu durumun temel nedeninin ise otonom silah sistemlerinin sahip olduğu yapay zeka ve bu zekanın kendi başına icraatta bulunabilmesi yüzünden hiçbir zaman insanların sahip olduğu ayırt etme gücüne, merhametine, ahlaka ve empatiye sahip

[407] Michael N. Schmitt, "Classification of cyber conflict.", 250.
[408] Merve Leman Bulut Mişe, *"Uluslararası Hukukta Müdahale Ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar"*, 63.
[409] Adem Özer, "Cin Şişeyi Terk Etti: Geleceğin Kalaşnikofları Otonom Silah Sistemleri ve Uluslararası İnsancıl Hukuk," içinde *Uluslararası İnsancıl Hukuk: Kavramlar, İlkeler ve Yeni Gelişmeler*, der. Fatma Taşdemir ve Gökhan Albayrak, 199.
[410] İsmail Ataş, "Otonom Silah Sistemlerinin İnsancıl Hukukun Temel İlkelerine Uygunluğunun Sağlanmasında Anlamlı İnsan Kontrolünün Etkisi," *Hacettepe Hukuk Fakültesi Dergisi* 12, (2022): 772.
[411] İsmail Ataş, "Otonom Silah Sistemlerinin İnsancıl Hukukun Temel İlkelerine Uygunluğunun Sağlanmasında Anlamlı İnsan Kontrolünün Etkisi", 773.
[412] Adem Özer, "Cin Şişeyi Terk Etti: Geleceğin Kalaşnikofları Otonom Silah Sistemleri ve Uluslararası İnsancıl Hukuk,", 203.

olamayacağı şeklinde açıklanmaktadır[413]. Özet olarak otonom silah sistemlerinin kullanılması gerektiğini savunanlar olsa bu savunmanın tam tersini iddia eden hukukçular da bulunmaktadır; bu türden silahların kullanılmamasını savunanların temel dayanakları ise teknolojik bir aletin tüm kontrolü eline alıp saldırı için karar vermesi ve bu durumun ayrım yapma ilkesini ihlal eden durumlar doğurabileceğini, otonom silah tarafından yapılan bir saldırının çok kısa sürede gerçekleştirildiği ve yanlış bir durum olduğunda hızından ötürü müdahale edilememesi, son olarak da genelde insanların özelde ise askerlerin teknolojik sistemlere olan güveni olduğu söylenebilmektedir[414].

Sonuç olarak insancıl hukuk kurallarının uygulanabilir hale geldiği silahlı çatışmalarda savaşanların saldırı yolu olarak siberuzayı seçmesi bu alanın kara, hava ve deniz savaşlarından oldukça farklı ve yeni bir alan olması, bu alandaki silahlı çatışmalara dair yapılmış bağlayıcılığı olan uluslararası metin bulunmaması, siberuzayda sivil kişilerin ve askeri kişilerin ayrımının zor olması ve bu durumun en büyük sebebinin de siberuzayın birçok elementinin hem siviller hem de çatışanlar tarafından çift kullanılması birçok belirsizliğe yol açmaktadır. Bu belirsizlik ise yeni hukuki düzenlemeler ve güncel olayların analizi ile büyük ölçüde giderilebilecek, gelecek sorunlara karşı daha sağlam çözümler bulunacaktır.

9. Hukuki Değerlendirme

Siberuzay; insancıl hukuktaki kara, deniz ve havadan oluşan savaşın fiziksel alanlarına sanal bir boyut katan yeni bir silahlı çatışma alanı olarak ortaya çıkmıştır[415]. Devletler, organize silahlı gruplar ve hackerlık yapan sivillere kadar bu alan, sıkça kullanılmaktadır. Bu durum uluslararası insancıl hukukun geleneksel savaş yöntemlerini ve amaçlarını düzenleyen 1899 ve 1907 tarihli Lahey Sözleşmeleri hükümlerinin, 1949 tarihli Cenevre Sözleşmeleri ve Ek Protokoller hükümlerinin siberuzaya ve bu alanda gerçekleştirilen siber saldırılara karşı nasıl uygulanacağı, askeri-sivil kişi ve nesneler arasında nasıl ayrım

[413] Hakan Candar, *Silahlı Çatışma Hukuku Perspektifinden Otonom Silah Sistemleri*, (Doktora Tezi, Selçuk Üniversitesi, 2022), 220.
[414] Gökhan Güneysu, "Otonom Silah Sistemleri ve İnsancıl Hukuk", *TBB Dergisi 108*, (2013): 268.
[415] Hans Klein, *Cyberspace: Definition and Implications* (Tallinn: NATO CCDCOE, 2021), https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/.

yapılacağı ve buna bağlı olarak siber saldırıda bulunurken nelerin ve kimlerin saldırı hedefi haline getirilebileceği hallerine uyarlanması tartışma konusu olmuştur.

İnsancıl hukuk kapsamında saldırının tanımı, silahlı çatışmadaki düşman tarafa karşı saldırı ya da savunmadaki şiddet içerikli eylemler olarak verilmiştir[416]. Buradaki saldırı tanımının siber saldırılara nasıl uygulanacağı ya da hangi niteliklere sahip olan siber saldırıların insancıl hukuktaki saldırı olarak kabul edileceğinin belirlenmesi büyük bir önem arz etmiştir. Halihazırda uzunca süredir uygulanmakta olan insancıl hukuk kuralları siber saldırılara uygulandığında ortaya çıkan sonuç ise yapılması halinde ölüm veya yaralanmalara ya da nesnelerin zarar görmesine yol açan siber operasyonların insancıl hukuk kapsamındaki saldırı tanımına dahil olduğu kabul edilmiştir[417].

Silahlı çatışmalar esnasında gerçekleştirilen siber saldırıların sivil ve askeri kişiler ile nesneler arasında nasıl bir ayrım yapacağı, saldırı hedefini nasıl belirleyeceği gibi konular da en az saldırı tanımı kadar önem arz etmektedir. Ayırt etme ilkesi, uluslararası teamül hukuku kuralı olarak kabul edilen ve insancıl hukukun temelini oluşturan bir ilke olarak[418] siberuzaydaki siviller ve askerler arasında, fiziksel alanda uygulanandan farklı olarak net olmayan sınırlar üzerinde uygulanmaktadır. Bunun temel sebebi çalışmanın önceki bölümlerinde belirtildiği üzere, internetin ve ona bağlı ağ sistemleri ile elektrik, su, ulaşım gibi kritik altyapıların hem savaşanlar hem de siviller tarafından ortak kullanılmasıdır. Örneğin askeri birlik ve komuta arasındaki iletişimin sağlanması genellikle uydular üzerinden sivil ağlar kullanılarak gerçekleşmekte olup silahlı kuvvetlerin, sivillerin kullanımında olan nesnelere olan bağımlılığı yüksektir[419].

Sivil-askeri kişiler ile nesneler arasında ayrım yapıp bu ayrıma göre saldırıların hedefi belirlenirken siberuzayda sivillerin hangi görünümlerde ortaya çıkabileceğinin belirlenmesi de büyük bir önem arz etmektedir. Ek Protokol I, madde 51'de düzenlendiği üzere sivillerin saldırının hedefi haline getirilmeleri yasaktır. Ancak bu yasağın doğru bir şekilde uygulanabilmesi için sivillerin siberuzayda nasıl faaliyet gösterdiğinin tespit

[416] Ek Protokol I, madde 49.
[417] Schmitt, *Tallinn Manuals 2.0*, Rule 92.
[418] Ek Protokol I, madde 38.
[419] Harrison Dinniss, *Cyber Warfare and the Laws of War*, 26.

edilmesi, bu faaliyetlerin askeri bir amaç ve avantaja hizmet edip etmediğinin belirlenmesi gerekmektedir. Nitekim siberuzayda iki tarafın arasındaki sınırların oldukça bulanık olmasının sonuçlarından biri de siber saldırıda bulunan sivil hackerlardır. Bu hackerların hukuki statüsü de tartışmalı olup uluslararası hukuk uzmanlarının çoğunluğunun vardığı sonuç; bu kişilerin savaşan statüsünü kazanmadığı (levée en masse olarak sayılmadıkları) sürece, sivil statülerini kaybetmediği ancak saldırı hedefi haline getirilebilecekleri kabul edilmiştir [420].

Siberuzayda; sivil hackerlar dışında günlük işlerini halleden, vatandaşlık görevini yerine getiren, çalıştığı işin hizmetini dijital bir şekilde veren, sosyal medya yolu ile başkalarıyla iletişime geçen, sağlık durumunu dijital varlıklar aracılığıyla kontrol altına alan, askeri amaç ve avantajdan yoksun faaliyetler gösteren birçok sivil mevcuttur. Bu siviller, önceki bölümlerde açıklanan nedenler ve verilen örnekler uyarınca koruma statüsüne sahiptirler ve saldırı hedefi haline gelmekten muaftırlar.

Sivillerin hizmetinde olan veritabanları ile kritik altyapılar, sivillerin hayatlarını normal ve sağlıklı bir şekilde idame ettirmeleri için büyük öneme sahip hatta bazı durumlarda hayati olan nesnelerdir. Bu nesnelerin korunup siber saldırı hedefi haline getirilmemeleri gerekirken birçoğu çift kullanımlı olma niteliğine sahip olduğundan pratikte hak ihlalleri görülebilmektedir. Örneğin hastanede bulunan askerlerin kan grupları verilerinin manipüle edilerek değiştirilmesi ve değişen kan grupları sonucunda o hastanede bulunan sivillerin de bilgilerinin değişmiş olması sebebiyle zarar görmesi söz konusu olabilmektedir[421]. Tüm bu belirsizliklere ek olarak dijital verilerin (data) ve dijital ekonomik ve kültürel varlıkların siberuzayda sivil nesne sayılıp sayılmayacağına dair tartışmalar mevcuttur. Dijital verinin (data), tek başına sivil nesne olarak kabul edilmediğini savunan uluslararası hukuk uzmanları bulunsa da bu konuda kesin ve ortak bir yorum bulunmamaktadır[422]. Dijital veri, kültürel varlık kategorisine giriyorsa ya da ekonomik bir değeri var ise bu durumun değiştiği yönünde görüşler de mevcuttur[423].

[420] Schmitt, *Tallinn Manuals 2.0*, Rule 91.
[421] Schmitt, "Computer Network Attacks and Use of Force" in *Tallinn Manual 2.0*, 66.
[422] Schmitt, "Computer Network Attacks and Use of Force" in *Tallinn Manual 2.0*, 69.
[423] Lahey Düzenlemeleri madde 51, Ek Protokol I madde 51.

Son olarak siber saldırılarda saldırıyı yapan kişi, grup ya da devlet organını tespit etmek ve bu tespit uyarınca saldırıyı yapan kişiye sorumluluk atfetmek zorlu bir eylemdir. Nitekim önceki bölümlerde anlatıldığı üzere bilgi ve iletişim teknolojilerinin ağ sistemleri ve veri tabanları içerisinde kimlik gizlemek ve anonim olarak faaliyet göstermek oldukça yaygın bir sorun olarak baş göstermektedir[424]. Anonimlik ve siber saldırılarda sorumluluk atfedilmesi sorunu günümüzde hala güncelliğini korumaktadır.

[424] Sheel Batt, Vertisystem Platform Services. "The Power of Anonymity: Unveiling Ethical Hacking Secrets and Digital Privacy Tools." *Medium*, October 23, 2023. https://medium.com/vertisystem-platform-services/the-power-of-anonymity-unveiling-ethical-hacking-secrets-and-digital-privacy-tools-360f0a0d9394.

Sonuç

Sonuç olarak bu çalışmada, siber saldırılar ile bu saldırıların uluslararası insancıl hukukla ilişkisi, bu ilişkinin nasıl kurulacağı, insancıl hukuk kurallarının siber saldırılara nasıl uygulanacağı ve en önemlisi siviller ile sivil nesnelerin hangi durumlarda varlık gösterip saldırı hedefi olmalarının engelleneceği incelenmiştir. Tezin ilk bölümünde insancıl hukuk; temel kavramlarıyla sözleşmelerle, uluslararası yargı kararları ve örnek olaylarla ele alınmıştır. Siviller ve savaşanlarla sivil nesneler ve askeri nesneler tanımlanmış, ayrım yapılmış, insancıl hukukun temel ilkelerine başvurarak kimlerin ve hangi nesnelerin saldırı hedefi haline getirilebileceği kimlerinse korunabileceği tartışılmıştır. İkinci bölümde ise siberuzayın insancıl hukukta nasıl yeni bir alan olduğu, siber operasyonların nasıl ve hangi yollarla gerçekleştirildiği incelenmiştir. Bölümün devamında ise hangi türden siber operasyonların insancıl hukuktaki saldırı kapsamına girdiği, bu kapsama giren siber saldırıların hukuki durumu ele alınmıştır. Üçüncü bölümde ise siber saldırılar esnasında kimlerin sivil kimlerin askeri kişiler olarak kabul edildiği, bu kişilerin siberuzayda nasıl varlık gösterebileceği gibi hususlar ele alınmıştır. Bölümün devamında da siberuzayda sivil nesnelerin neler olabileceği, bu nesnelerin askeri nitelik taşıyanlardan ne farkının olduğu, siviller ve askeri kişiler tarafından ortak kullanım olduğunda ise bu nesnelerin ve bu nesnelere karşı yapılan siber saldırıların hukuki statülerinin ne olacağı tartışılmıştır.

Yapılan değerlendirmeler sonucunda, insancıl hukuk kapsamındaki siber saldırılarda geleneksel savaşlardan farklı olarak sivil-askeri ayrımının ne kadar zor olduğu, siberuzayın kara, hava ve denize göre hukuki açıdan çok daha fazla gri alana sahip olduğu, bu alanda nesnelerin hukuki statüsü ve saldırı hedefi haline getirilmelerinin değerlendirilmesinde birçok belirsizliğin ortaya çıktığı görülmüştür. Bu belirsizliklerin temel nedenlerinin ise, devletlerin ve örgütlü silahlı grupların bu alanda deneyim eksikliği, bu alanı detaylı bir şekilde düzenleyen ve bağlayıcılığı olan insancıl hukuk kapsamına giren bir uluslararası düzenlemenin bulunmaması yüzünden önceden var olan düzenlemelerin yorumlanıp siber saldırılarla bağdaştırılması, siberuzayın kısa zaman içerisinde pek çok gelişim ile değişim göstermesi ve bu duruma ayak uydurmanın zorluğu tespit edilmştir.

Herhangi bir hak kaybının yaşanmaması ve uluslararası insancıl hukuk hükümlerinin ağır bir şekilde ihlal edilmemesi için siber saldırıları düzenleyen bağlayıcı nitelikte uluslararası düzenlemelerin yapılması gerekmektedir. Nitekim bu tarz düzenlemelerin yokluğu, mevcut hükümleri yorumlama ve güncelle bağdaştırma yoluna götürmektedir. Siberuzaydaki mevcut belirsizliklerin giderilmesi için yapılması gereken NATO ve Birleşmiş Milletlerin çalışmaları dışında hukuki bağlayıcılığı olan hukuki metinler hazırlamaktır.

Sonuç olarak, siber saldırıların siviller ve sivil nesneler üzerinde yaratabileceği olumsuz sonuçları önlemek ve insancıl hukukun temel ilkelerini bu yeni savaş ortamına uygun hale getirmek, hem hukuki hem de etik bir görevdir. Uluslararası hukukun gelişimi ve devlet uygulamalarının bu doğrultuda şekillendirilmesi bu bağlamda çok önemlidir. Bu şekillendirme sağlandıktan sonra siber saldırılardan sivillerin korunması, sivillerin askerlerden ayırt edilmesi ve saldırı hedefi haline getirilmemeleri daha kolaylaşacaktır.

KAYNAKÇA

Acar, Muhammed. *Siber Uzay ve Egemenlik: Kripto Paraların Etkisi*, Yüksek Lisans Tezi, Selçuk Üniversitesi, 2022.

Alp, Toygar . C. E. Rohm Jr, and Jake Zhu. "A new asset type: digital assets." *Journal of International Technology and Information Management 22*, (2013): 113-120.

Aristovnik, Aleksander, Konstantinos Karampelas, Lan Umek, and Dejan Ravšelj. "Impact of the COVID-19 Pandemic on Online Learning in Higher Education: A Bibliometric Analysis." *Frontiers in Education* 8 (2023): 1–20. https://doi.org/10.3389/feduc.2023.1225834.

Arnold, Roberta. "Book Reviews", *International Criminal Law Review 20*, (March 2020): 155-159.

Ataş, İsmail. "Otonom Silah Sistemlerinin İnsancıl Hukukun Temel İlkelerine Uygunluğunun Sağlanmasında Anlamlı İnsan Kontrolünün Etkisi." *Hacettepe Hukuk Fakültesi Dergisi* 12, (2022): 767–809.

Ates, Davut. "Sovereignty, Anarchy and the Rome Statute," Review of International Law and Politics 6, no. 24 (2010): 1-34.

"Attacks on Civilians and Other Unlawful Killings, and Attacks on Civilian Objects" , erişim 30 Mayıs 2024, https://www.globalprotectioncluster.org/sites/default/files/2023-02/protection_risk_02_0.pdf.

Aust, Anthony. *Handbook of International Law*, New York: Cambridge University Press, 2010.

Biller, Jeffrey. Cyber Operations and the Second Geneva Convention. *International Review of the Red Cross 100*, (2018): 165-183.

Blackwell, Alan F. “What is Programming”, *PIGG 14*, (2002): 204-218.

Blank, Laurie R. and Gregory P. Noone. *International Law and Armed Conflict*. New York: Wolters Kluwer Law& Business, 2013.

Boulanin, Vincent. “Implementing Article 36 Weapon Reviews in the Light of Increasing Autonomy in Weapon System”, *SIPRI Insights on Peace and Security 1*, (2015): 1-28.

Bouvier, Antoine A. *International Humanitarian Law and the Law of Armed Conflict*. Edited by Harvey J. Langholtz. Williamsburg, VA: Peace Operations Training Institute, 2020.

Bulut, Esra. ve Gülay Çizgici Akyüz, “Türkiye’de Dijital Bankacılık ve Ekonomik Büyüme İlişkisi” *Marmara Üniversitesi İktisadi ve İdari Bilimler Dergisi 42*, (2020):223-246.

Byczyński, Michał. “The Legal Status of Civilian Hackers under International Humanitarian Law”, *Acta Universitatis Lodziensis 106*, (2024): 97-109.

Candar, Hakan. *Silahlı Çatışma Hukuku Perspektifinden Otonom Silah Sistemleri*, Doktora Tezi, Selçuk Üniversitesi, 2022.

Carlo, Antonio. and Kim Obergfaell. "Cyber Attacks on Critical Infrastructures and Satellite Communications." *International Journal of Critical Infrastructure Protection* 46 (2024): 100701. https://doi.org/10.1016/j.ijcip.2024.100701.

Cederberg, Aapo. and Rain Ottis. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence, 2008. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Çelik, Şener. "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 1*, (2013): 137-175.

Chayes, Antonia. "Rethinking warfare: The ambiguity of cyber attacks." *Harv. Nat'l Sec. J. 6* (2015): 474-519.

Chertoff, Emily. Zachary Manfredi, "Deadly Ambiguity: IHL's Prohibition on Targeting Civilian Objects and the Risks of Decentered Interpretation," *Texas International Law Journal 53*, (2018): 239-284.

Clarke, Roger. "Ethics and the Internet: The Cyberspace Behaviour of People, Communities and Organisations." *Business & Professional Ethics Journal* 18, no. 3/4 (1999): 153–67.

Cotter, Maurice. "Military Necessity, Proportionality and Dual-Use Objects at the ICTY: A Close Reading of the Prlic et al. Proceedings on the Destruction of the Old Bridge of Mostar," Journal of Conflict and Security Law 23, no. 2 (2018): 283-305.

Daniele, Luigi. Incidentally of the civilian harm in international humanitarian law and its Contra Legem antonyms in recent discourses on the laws of war, *Journal of Conflict & Security Law 29*, (2024): 21-54.

Defense Use Case. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center (E-ISAC) 388 (2016): 1–29.

Demeyere, Bruno. *IHL and Civil Society Organizations: Thematic Brief* (Cambridge, MA: Harvard Humanitarian Initiative, Advanced Training Program on Humanitarian Action, 2016), 14, https://hhi.harvard.edu/sites/g/files/omnuum6866/files/humanitarianinitiative/files/atha_thematic_brief_ihl_and_civil_society_organizations.pdf.

Demirci, Saadat Rustemova. "İnsancıl Hukukta Hedef Alarak Öldürme" *Uluslararası İnsancıl Hukuk: Kavramlar, İlkeler ve Yeni Gelişmeler* içinde, ed. Fatma Taşdemir ve Gökhan Albayrak (Ankara: Adalet, 2018): 161-176.

Dennis, Heather Harrison. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012.

Diakonia International Humanitarian Law Centre. "Principle of Distinction: Protection of People and Objects." *Diakonia*. Accessed September 2, 2024. https://www.diakonia.se/ihl/resources/international-humanitarian-law/principle-of-distinction-protection-of-people-and-objects/.

Diamond, Eitan. "Applying International Humanitarian Law to Cyber Warfare", *Law and National Security: Selected Issues 67 (Pnina Sharvit Baruch and Anat Kurz Eds., INSS Memorandum No. 138)*, (2014): 67-84.

Dinniss, Heather A. Harrison. "The Nature of Objects: Targeting Networks and The Challenge of Defining Cyber Military Objectives", Israel Law Review 48, (2015): 439-54.

Dinstein, Yoram. "Legitimate Military Objectives Under the Current Jus in Bello", *International Law Studies 78*, (2002): 139-172.

Dinstein, Yoram. *Targeting under International Humanitarian Law*. Geneva: International Committee of the Red Cross, 2020. https://www.icrc.org/en/document/targeting-under-international-humanitarian-law.

Dinstein, Yoram. *The Conduct of Hostilities under the Law of International Armed Conflict*. 2nd ed. Cambridge: Cambridge University Press, 2010.

Dinstein, Yoram, and Arne Willy Dahl. *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*. Cham: Springer Open, 2020.

Dülger, Kenan. *Uluslararası Hukukta Siber Savaşa İlişkin Temel Esaslar*, İstanbul: Onikilevha Yayınları, 2023.

Droege, Cordula. "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," International Review of the Red Cross 94, (2012): 533-578.

Efrony, Dan. Yuval Shany, "A Rule Book on the Shelf: Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law 112*, (October 2018): 583-657.

Erkiner, Hakkı Hakan. "Birleşmiş Milletler Uluslararası Adalet Divanı Kararlarının Birleşmiş Milletler Güvenlik Konseyi Aracılığıyla Uygulatılması", *MÜHF-HAD 23*, (2017): 87-102.

Erdem, Merve. ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 68, (2019): 127–212.

Epps, Valerie. "Civilian Casualties in Modern Warfare: The Death of the Collateral Damage Rule," *Georgia Journal of International and Comparative Law 41*, (2013): 307-356.

Faga, Hemen Philip. "The Implications of Transnational Cyber Threats In International Humanitarian Law: Analysing The Distinction Between Cybercrime, Cyber Attack, And Cyber Warfare In The 21st Century" *Baltic Journal of Law and Politics 10*, (2017): 2-34.

Foltz, Philip A. "Cyber Deterrence: A Practice-Based Framework for Deterrence by Denial." *Joint Force Quarterly* 67 (2012): 40–48. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.

Geneva Convention (III) relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135.

Gervais, Michael. "Cyber attacks and the laws of war." *Journal of Law & Cyber Warfare 1*, (2012): 8-98.

Gisel, Laurent. Tilman Rodenha¨user ve Knut Do¨rmann, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts" *International Review of the Red Cross 102*, (2020): 287-334.

Göçoğlu, Volkan. "Kamu Hizmetlerinin Sunumunda Dijital Dönüşüm: Nesnelerin İnterneti Üzerine bir İnceleme", MANAS Sosyal Araştırmalar Dergisi 9, (2020): 615-628.

Güneysu, Gökhan. Askeri Gereklilik İlkesi ve Uluslararası İnsancıl Hukuk, *Ankara Barosu Dergisi 4*, (2012): 93-108.

Güneysu, Gökhan. "Otonom Silah Sistemleri ve İnsancıl Hukuk", *TBB Dergisi 108*, (2013): 259-272.

Hahn, Robert W., and Anne Layne-Farrar. "The Law and Economics of Software Security." *AEI-Brookings Joint Center Working Paper* No. 06-08, April 2006. (Erişim Tarihi: 20 Ekim 2024). https://ssrn.com/abstract=897725.

Hathaway, Oona A. Azmat Khan, and Mara Redlich Revkin. "The Dangerous Rise of Dual-Use Objects in War", *Duke Law School Public Law & Legal Theory Series 56*, (2024): 1-97.

Hathaway, Oona A.; Paul K. Strauch; Beatrice A. Walton; Zoe A. Y. Weinberg, "What Is a War Crime," Yale Journal of International Law 44, no. 1 (Winter 2019): 53-114

Hollis, Duncan B. "An e-SOS for Cyberspace." *Harv. Int'l LJ 52* (2011): 373-432.

Horrace B. Robertson, Jr, "The Principle of the Military Objective in the Law of Armed Conflict", International Law Studies 72, (1998): 197-223.

International Committee of the Red Cross (ICRC), Commentary on the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Commentary of 1987.

International Committee of the Red Cross (ICRC), "What Is International Humanitarian Law?," International Committee of the Red Cross, accessed August 9, 2024, https://www.icrc.org/en/document/what-international-humanitarian-law#:~:text=International%20humanitarian%20law%20(IHL)%20is,means%20and%20methods%20of%20warfare.

International Committee of the Red Cross. "Rule 3. Definition of Combatants." Customary IHL Database. Accessed August 15, 2024. https://ihl-databases.icrc.org/en/customary-ihl/v1/rule3.

International Committee of the Red Cross. The Principles of Humanity and Necessity. PDF. Accessed August 20, 2024. https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf.

International Committee of the Red Cross, "Rule 8. Definition of Military Objectives," Customary IHL Database, accessed August 21, 2024, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule8.

International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion* [1996] ICJ Rep 226.

ICRC Database, Treaties, States Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977., Commentary of 01.01.1987 , Article 49 - Definition of attacks and scope of application, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49/commentary/1987?activeTab= (Last accessed on 20.12.2024).

International Committee of the Red Cross. *International Humanitarian Law and Cyber Operations during Armed Conflicts.* Geneva: ICRC, November 2019.

International Committee of the Red Cross. "International Humanitarian Law and Cyber Operations During Armed Conflicts." *International Review of the Red Cross* 102, no. 913 (2020): 481–492. https://doi.org/10.1017/S1816383120000478.

International Committee of the Red Cross. *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts: ICRC Expert Meeting 21–22 January 2020 – Geneva*. Geneva: ICRC, 2021.

International Group of Experts, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N Schmitt ed, CUP 2017).

Bilge Karabacak, "Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri," *Siber Güvenlik Çalıştayı*, Bilgi Güvenliği Derneği, Ankara, 29 (2011): 1–11.

Kessler, Oliver. and Wouter Werner. "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare." *Leiden Journal of International Law* 26, (2013): 793–810.

Kjølle, Gerd H., Ingrid Bouwer Utne, and Oddbjørn Gjerde. "Risk Analysis of Critical Infrastructures Emphasizing Electricity Supply and Interdependencies." *Reliability Engineering & System Safety* 105 (2012): 80–89.

Kolb, Robert. *International Court of Justice*, Oxford: Hart Publishing, 2013.

Lee, Jaemin. "Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)." *American Journal of International Law* 117, no. 1 (2023): 113–21. https://doi.org/10.1017/ajil.2022.84.

Lefkowitz, David. ""Collateral Damage." In War: Essays in Political Philosophy", edited by Larry May, 145-64. New York: Cambridge University Press, 2008.

Lehto, Martti. and Pekka Neittaanmäki. *Cyber Security*. Cham: Springer Nature, 2022.

Lieber, Francis. *Instructions for the Government of Armies of the United States in the Field*. Washington, D.C.: Government Printing Office, 1863.

Mbanaso, U. M. ve E.S. Dandaura, "The Cyberspace: Redefining a New World", IOSR Journal of Computer Engineering 17, (2015):17-24.

Mcghee, James E. "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy," *Journal of Law & Cyber Warfare* 2, (2013): 64-103.

McKenzie, Simon. "Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute," *Journal of International Criminal Justice 19*, (2021): 1165-1192.

Melzer, Nils. *International Humanitarian Law: A Comprehensive Introduction*, Geneva: ICRC, 2022, Erişim Tarihi: 6 Ekim 2023, https://www.jep.gov.co/Sala-de-Prensa/Documents/4231_002-IHL_WEB_13.pdf.

Mercan, Yeliz. Kübra Dizlek, Gamze Süsim vd. "Sağlık Amaçlı İnternet Kullanımı ve Mobil Sağlık Uygulamaları Üzerine Bir Araştırma" *Kırklareli Üniversitesi Sosyal Bilimler Meslek Yüksekokulu Dergisi 1*, 66-76.

Mişe, Merve Leman Bulut. *Uluslararası Hukukta Müdahale Ve Kuvvet Kullanımının Yasaklanması İlkeleri Bağlamında Siber Saldırılar*, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, 2024.

NATO. *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisbon: NATO Public Diplomacy Division, 2010.

Norwegian Centre for Humanitarian Studies. *Oslo Manual on Select Topics of the Law of Armed Conflict*. Oslo: NCHS, 2020.

O'Connell, Mary Ellen. "Combatants and the Combat Zone," University of Richmond Law Review 43, no. 3 (March 2009): 845-864.

Öz, Hatice. "An Analysis of Interactivity Possibilities in Online Journalism", *folklor/edebiyat 66*, (2011): 57-64.

Özer, Adem. "Düşmanlıkların Yürütülmesinde Orantılılık İlkesi: Teorik Ve Pratik Zorluklar." *Yalova Sosyal Bilimler Dergisi 13*, (2023): 271-284.

Özer, Adem. "Uluslararası İnsancıl Hukukta Askeri Gereklilik İlkesi ve İnsani Mülahazalar Arasındaki Denge", *Türk Savaş Çalışmaları Dergisi 4*, (2023): 189-211.

Pasupathieswaran M and Kapilan Bharathi, "Digital Battlefronts: Rethinking Legal Frontiers in Cyberwarfare and AI Conflicts", *International Journal for Multidisciplinary Research 6*, (2024): 1-9.

Pazarcı, Hüseyin. *Uluslararası Hukuk Dersleri IV. Kitap.* Ankara: Doruk Kitabevi, 2020.

Petersson, Fredrik. "Legitimate Targets of Attack", Yüksek Lisans Tezi: University of Lund, 2003.

Prasetiawan, Eno. Eka Widi Astuti, Helmi Amnijar and Febryan Topo Ruru Artha "Distinction Principle in International Humanitarian Law Related to Civilian Objects and Military Objects" *Proceedings of the 2nd International Conference Postgraduate School (ICPS 2018):* 649-652.

Prosecutor v. Kupreškić et al. (IT-95-16-T)." *International Crimes Database*". Accessed August 20, 2024. https://www.internationalcrimesdatabase.org/Case/77/Kupre%C5%A1ki%C4%87-et-al/.

Richardson, John Charles. "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield" *John Marshall Journal of Information Technology & Privacy Law 1*, (2011): 1-37.

Rodenhäuser, Tilman. "8 Rules for Civilian Hackers during War – and 4 Obligations for States to Restrain Them." *International Committee of the Red Cross (ICRC)*. March 28, 2023. https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them

Sassoli, Marco. *Legitimate Targets of Attacks Under International Humanitarian Law*. International Humanitarian Law Initiative, 2003.

Ruan, Keyun. *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*. 1st ed. San Diego: Academic Press, 2019. https://books.google.com.tr/books?id=c6nRDgAAQBAJ.

Sassoli, Marco and Lindsey Cameron, "The Protection of Civilian Objects: Current State of Law and Issues de lege feranda" *The Hague: Eleven International* (2006): 35-74.

Schmitt, Michael N. "Classification of cyber conflict." *International Law Studies 89*, (2013): 232-251.

Schmitt, Michael N. "Precision attack and international humanitarian law," International Review of the Red Cross 87, no. 859 (September 2005): 445-466.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017.

Schmitt, Michael N. "The Principle of Distinction in 21th Century", *Yale Hum. Rts. & Dev. L.J. 2*, (1999): 143-182.

Schmitt, Michael N. "Wired Warfare: Computer Network Attack and Jus in Bello." *International Review of the Red Cross* 84, (2002): 365–400.

Sergeev, Artem. "Applying Additional Protocol II of the Geneva Conventions to the United Nations Forces," *Journal of International Humanitarian Legal Studies 8* (2017): 234-254.

Shakarian, Paulo. "The Criticality of Captains' Education: Now and in the Future." *Military Review* (November-December 2011): 63–68.

Shue, Henry and David Wippman, "Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions," *Cornell International Law Journal 35*, no. 3 (Winter 2002): 559-580.

Simmons, Noah. "A Brave New World: Applying International Law of War to Cyber-Attacks," *Journal of Law & Cyber Warfare 4*, (Winter 2014): 42-108.

Stirone, Angelo. "Hacking and International Humanitarian Law: The Anonymous Group and the Syrian Electronic Army." *Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict* 3, no. 1/2 (2020): 123–40. https://www.jstor.org/stable/48636454.

Solis, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War*. New York: Cambridge University Press, 2010.

Şen, Semin Töner. *Siber Uzay ve Uluslararası Hukuk*. İstanbul: Onikilevha Yayınları, 2021.

Talas, Mustafa. "Sivil Toplum Kuruluşları ve Türkiye Perspektifi", *Türklük Bilimi Araştırmaları 29*, 387-401.

Tolppa, Maria. "First UN OEWG Concludes with a Consensus Report – What Does It Mean for Future Cybersecurity Discussions under the Auspices of the First Committee?" NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), March 30, 2021. https://ccdcoe.org/library/publications/first-un-oewg-concludes-with-a-consensus-

report-what-does-it-mean-for-future-cybersecurity-discussions-under-the-auspices-of-the-first-committee/.

Türkay, Şeyda. "Siber Savaş Hukuku ve Uygulanma Sorunsalı," *Journal of Istanbul University Law Faculty* 71, no. 1 (2013): 1177–1227.

Tütüncü, Ayşe Nur. *İnsancıl Hukuka Giriş*. İstanbul: Beta Yayım Basım, 2019.

United Nations General Assembly. *Annual Progress Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/77/275. July 27, 2023.

United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/68/98. June 24, 2013.

United Nations General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/70/174. July 22, 2015.

Usun, Salih. *Educational Uses of Internet in the World and Turkey: A Comparative Review*. *Turkish Online Journal of Distance Education (TOJDE)* 4, no. 3 (July 2003). https://tojde.anadolu.edu.tr/tojde11/articles/usun.htm.

Waszink, Camilla. *Protection of Civilians under International Humanitarian Law: Trends and Challenges*. NOREF Report, August 2011.

Watts, Sean. "Combatant Status and Computer Network Attack," *Virginia Journal of International Law 50*, (2010): 391-448.

Watts, Sean. "The Notion of Combatancy in Cyber Warfare," in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (Tallinn: IEEE, June 2012), 235-248.

Winterfeld, Steve ve Jason Andress, *The Basics of Cyber Warfare: Understanding the Goals of Cyber Warfare Theory and Practice*, Waltham. Syngress, 2013.

Yurdabak, Merve Kadriye "NFT: Dijital Sanatta Yeni Bir Perspektif ve Getirdiği Fırsatlar Üzerine Bir Derleme," *Nişantaşı Üniversitesi Sosyal Bilimler Dergisi* 10, (2022): 143–153.

E- Kaynaklar:

https://blogs.icrc.org/cross-files/the-cross-in-the-crosshairs-a-photographic-record-of-the-bombing-of-red-cross-field-hospitals-during-the-second-italo-ethiopian-war/ (Erişim Tarihi: 24 Mayıs 2024).

https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52?activeTab=undefined (Erişim Tarihi: 29 Temmuz 2024).

https://www.bbc.com/news/articles/cmjj6ej3ne1o (Erişim Tarihi: 4 Ağustos 2024).

https://casebook.icrc.org/a_to_z/glossary/proportionality . (6 Ağustos 2024)

https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf . (9 Ağustos 2024)

https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-3 (9 Ağustos 2024)

https://www.icj-cij.org/advisory-jurisdiction (Erişim Tarihi: 12 Ağustos 2024)

https://www.fortinet.com/resources/cyberglossary/rootkit (Erişim Tarihi: 13 Ekim 2024)

National Institute of Standards and Technology. "Cyber Attack." *NIST Glossary*. https://csrc.nist.gov/glossary/term/cyber_attack. (Erişim Tarihi: 10 Aralık, 2024)

https://casebook.icrc.org/case-study/iran-victim-cyber-warfare (Erişim Tarihi: 12 Aralık 2024).

United Nations Office for Disarmament Affairs, “Group of Governmental Experts,” United Nations, accessed May 15, 2025, https://disarmament.unoda.org/group-of-governmental-experts/.

United Nations Office for Disarmament Affairs, *Open-ended Working Group* (https://disarmament.unoda.org/open-ended-working-group/ accessed 15 May 2025)

Purdue University. "The Mystery of the WANK Worm," *CyberTAP Blog*, erişim tarihi 22 Ekim 2024, https://cyber.tap.purdue.edu/blog/articles/the-mystery-of-the-wank-worm/.

"Trojan Horse Virus". *Fortinet*, erişim tarihi 22 Ekim 2024, https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus.

"Stuxnet Nedir?". *Elfanet*, erişim tarihi 22 Ekim 2024, https://elfanet.com.tr/tr/main/article/stuxnet-nedir/105.

"Moonlight Maze". *ScienceDirect*, [erişim tarihi: 22 Ekim 2024], https://www.sciencedirect.com/topics/computer-science/moonlight-maze.

CrowdStrike. "Backdoor Attack," *CrowdStrike*, last modified 2024, Erişim Tarihi: 22 Ekim, 2024, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/backdoor-attack/?srsltid=AfmBOor04RH9fd6FmtMHfVhnh1wpKjJTto9EefqxDYeW-iY1KFzZGdus.

International Committee of the Red Cross, "Hague Conventions," *How does law protect in war?* (International Committee of the Red Cross, 2025), https://casebook.icrc.org/a_to_z/glossary/hague-conventions.

Cisco, "What Is a Cybersecurity Specialist?," *Cisco*, accessed June 15, 2025, https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cybersecurity-specialist.html.

Global Security and Sustainability Center (GSSC), "Energy Security and Critical Infrastructure Protection," accessed June 24, 2025, https://www.gssc.lt/en/publication/energy-security-and-critical-infrastructure-protection/.

Inductive Automation, "What Is SCADA?," accessed June 24, 2025, https://inductiveautomation.com/resources/article/what-is-scada.

United Nations Office for Disaster Risk Reduction (UNDRR), *Water Infrastructure Resilience: Examples from Dams, Wastewater Treatment Plants and Water Supply Systems*, accessed June 24, 2025, https://www.preventionweb.net/publication/water-infrastructure-resilience-examples-dams-wastewater-treatment-plants-and-water.

Cohen, Gary. 2021. "Throwback Attack: How the Modest Bowman Avenue Dam Became the Target of Iranian Hackers." *Control Engineering*. August 12, 2021. Accessed June 25, 2025. https://www.controleng.com/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/.

United Nations Economic Commission for Europe (UNECE). *"Transport Infrastructure Development."* n.d. Accessed June 25, 2025. https://unece.org/transport/transport-infrastructure-development.

Cassandra Steer, "International Humanitarian Law in the 'Grey Zone' of Space and Cyber," *Centre for International Governance Innovation* (CIGI), 29 Ocak 2023, https://www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/.

Private Internet Access. “Is a Dedicated IP Traceable?” *Private Internet Access Blog*, April 5, 2024. https://www.privateinternetaccess.com/blog/is-a-dedicated-ip-traceable/.

Klein, Hans. *Cyberspace: Definition and Implications*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021. https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/.

Sheel Batt, Vertisystem Platform Services. “The Power of Anonymity: Unveiling Ethical Hacking Secrets and Digital Privacy Tools.” *Medium*, October 23, 2023. https://medium.com/vertisystem-platform-services/the-power-of-anonymity-unveiling-ethical-hacking-secrets-and-digital-privacy-tools-360f0a0d9394.

We Are Social and Meltwater, “Digital 2025: The Essential Guide to the Global State of Digital,” *We Are Social*, February 2025, https://wearesocial.com/uk/blog/2025/02/digital-2025-the-essential-guide-to-the-global-state-of-digital/.

European Commission, “Mind the Cyber Skills Gap: A Deep Dive,” *Digital Skills and Jobs Platform*, last modified February 5, 2024, https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive.

“The Practical Guide to Humanitarian Law”, Medecins Sans Frontieres, Erişim Tarihi: 29 Temmuz 2024. https://guide-humanitarian-law.org/content/article/3/protected-objects-and property/#:~:text=Rule%209%20of%20the%20customary,in%20international%20and%20non%2Dinternational.

Brian Beers, “What Is the Telecommunications Sector?” *Investopedia*, last modified July 30, 2022, https://www.investopedia.com/ask/answers/070815/what-telecommunications-sector.asp.

Luke Harding and Charles Arthur, "Hacking the Guardian: How Syria’s Electronic Army Took on the West." *The Guardian*, April 30, 2013.

https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.

ICS-CERT, *Cyber-Attack Against Ukrainian Critical Infrastructure*, February 25, 2016, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.