Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı

ULUSLARARASI HUKUKTA SİBER SAVAŞ

Hayati PALLI

Doktora Tezi

Ankara, 2023

ULUSLARARASI HUKUKTA SİBER SAVAŞ

Hayati PALLI

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı

Doktora Tezi

Ankara, 2023

KABUL VE ONAY

Hayati Pallı tarafından hazırlanan "Uluslararası Hukukta Siber Savaş" başlıklı bu çalışma, 09.01.2023 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Doktora Tezi olarak kabul edilmiştir.

Prof. Dr. Enver Bozkurt (Başkan)

Prof. Dr. Gökhan Güneysu (Danışman)

Doç. Dr. Erdem İlker Mutlu (Üye)

Doç. Dr. Ali İbrahim Akkutay (Üye)

Dr. Öğretim Üyesi Bahadır Bumin Özarslan (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof.Dr. Uğur ÖMÜRGÖNÜLŞEN

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- o Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- o Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ….. ay ertelenmiştir. (2)
- o Tezimle ilgili gizlilik kararı verilmiştir. (3)

……/……/……

Hayati Pallı

"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

(1) *Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

(2) *Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

(3) *Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*

Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

***** Tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Prof. Dr. Gökhan Güneysu** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

[*İmza*]
Hayati PALLI

TEŞEKKÜR

Bu çalışma, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Doktora programında Prof. Dr. Gökhan GÜNEYSU danışmanlığında hazırlanmış ve Prof. Dr. Enver BOZKURT başkanlığında Prof. Dr. Gökhan GÜNEYSU, Doç. Dr. Erdem İlker MUTLU, Doç. Dr. Ali İbrahim AKKUTAY ve Dr. Öğr. Üyesi Bahadır Bumin ÖZARSLAN'dan oluşan jüri tarafından oybirliğiyle başarılı bulunmuştur. Bu çalışmanın hazırlanması sürecinde kıymetli bilgi ve birikimlerini paylaşan ve desteğini esirgemeyen saygıdeğer danışman hocam Prof. Dr. Gökhan Güneysu'ya, doktora tezi savunma jürimde yer almayı kabul ederek kıymetli zamanlarını ayıran ve değerli fikir ve önerilerinden yararlandığım Prof. Dr. Enver BOZKURT'a, Doç. Dr. Erdem İlker MUTLU'ya, Doç. Dr. Ali İbrahim AKKUTAY'a ve Dr. Öğr. Üyesi Bahadır Bumin ÖZARSLAN'a teşekkürlerimi sunarım.

Ayrıca görevli olduğum istinaf mahkemesindeki iş yoğunluğuma rağmen bu çalışmaya zaman ayırabilmemde büyük desteği olan İstinaf Daire Başkanı ve Sayın Hâkim Aytekin Yakar'a, yoğun mesaiden arta kalan zamanımın büyük bölümünü de bu çalışmaya ayırmak zorunda kalmam nedeniyle fedakârlıkta bulunan biricik kızlarım Duru ve Doğa'ya sonsuz teşekkürlerimi sunarım.

ÖZET

PALLI, Hayati. *Uluslararası Hukukta Siber Savaş*, Doktora Tezi, Ankara, 2023.

Teknolojinin gelişimi ile pek çok alanda olduğu gibi savaş hukukunda da önemli değişimler kendini göstermiştir. Gündelik sosyal yaşamın vazgeçilmezleri olan uydu ve iletişim sistemleri, hastane, trafik ışıkları, doğalgaz, su, elektrik vb. altyapı sistemleri ile tren ve uçak seferleri gibi hizmet alanının ve insansız hava araçları gibi uzaktan kontrol edilen araç sistemlerinin siber ortama dâhil edilmesi, siber savaş durumunda bu sistemlerin bilgisayar başından sabote edilebilmesi tehlikesini de beraberinde getirmiştir. Bu süreç özellikle de kuvvet kullanımına başvurmanın ve silahlı çatışmalar hukukunun yeniden yorumlanmasını gerektirmiştir. Çağın bir gereği olarak ulus devletlerin temel faaliyetlerini siber ortamda gerçekleştirmesi, kaçınılmaz olarak bu sistemlerin kuvvet kullanımı kapsamında kötüye kullanılmasına sebep olmuş ve yeni bir alan olarak uluslararası siber savaş hukukunu ortaya çıkarmıştır. Bu nedenle geleneksel kuvvet kullanımı, meşru savunma, devletin sorumluluğu ve silahlı çatışmalar hukuku konuları uluslararası siber savaş hukuku çerçevesinde yeniden değerlendirilmelidir. Bu tez kapsamında, uluslararası hukukun siber uzayda uygulama alanı bulan ilgili konularının yanında özellikle *jus ad bellum* ve *jus in bello* kavramlarının uluslararası siber savaş hukuku kapsamında yeniden yorumlanması amaçlamaktadır.

Anahtar Sözcükler: Siber Savaş, Siber Saldırı, *Jus ad Bellum*, Kuvvet Kullanma, Silahlı Saldırı, *Jus in Bello*.

ABSTRACT

PALLI, Hayati. *Cyberwarfare in International Law*, Ph.D. Dissertation, Ankara, 2023.

With the development of technology, important changes have shown itself in the law of war, as in many areas. Satellite and communication systems, which are indispensable for daily social life, hospital, traffic lights, natural gas, water, electricity, etc. The inclusion of infrastructure systems and service areas such as trains and flights, and remotely controlled vehicle systems such as unmanned aerial vehicles into the cyber space has brought along the danger that these systems can be sabotaged from the computer in case of cyber warfare. This process in particular required a reinterpretation the use of force and the law of armed conflicts. As a requirement of the age, the realization of the main fields of activity of nation states in the cyber environment has inevitably caused the abuse of these systems within the scope of the use of force and has revealed the international cyber warfare law as a new field. For this reason, traditional use of force concepts, self-defense, responsibility of the state and the law of armed conflict should be re-evaluated within the framework of international cyber warfare law. In context of this thesis; it is aimed to reinterpret the concepts of *jus ad bellum* and *jus in bello* within the scope of international cyber warfare law, as well as related issues of international law that can be applied in cyberspace.

Key Words: Cyber Warfare, Cyber Attack, *Jus ad Bellum*, Use of Force, Armed Attack, *Jus in Bello*.

İÇİNDEKİLER

KISALTMALAR

ABD : Amerika Birleşik Devletleri

ACI : Airports Council International / Uluslararası Havaalanları Konseyi

ARPANET : Advanced Research Projects Agency Network

BM : Birleşmiş Milletler

BMDHS : Birleşmiş Milletler Deniz Hukuku Sözleşmesi

CMK : Ceza Muhakemeleri Kanunu

DEÜ : Dokuz Eylül Üniversitesi

ENISA : European Network and Information Security Agency / Avrupa Ağ ve Bilgi Güvenliği Ajansı

EYUCM : Eski Yugoslavya Uluslararası Ceza Mahkemesi

IANA : The Internet Assigned Number Authority / İnternet Numara Tahsis Otoritesi

IATA : International Air Transport Association / Uluslararası Hava Taşımacılığı Servisi

ICANN : The Internet Corporation for Assigned Names and Numbers / İnternet Tahsisli Sayılar ve İsimler Kurumu

ICAO : International Civil Aviation Organization / Uluslararası Sivil Havacılık Örgütü

ICRC : International Committee of the Red Cross / Uluslararası Kızıl Hac Komitesi

IETF : The Internet Engineering Task Force / İnternet Mühendisliği Görev Gücü

IMF : International Monetary Fund / Uluslararası Para Fonu

ISAF : International Security Assistance Force / Uluslararası Güvenlik Destek Gücü

MC **:** Milletler Cemiyeti

NATO **:** North Atlantic Treaty Organization / Kuzey Atlantik Antlaşması Örgütü

NSF **:** the National Science Foundation / Ulusal Bilim Merkezi

s. **:** Sayfa

SCADA **:** Supervisory Control And Data Acquisition / Veri Tabanlı Kontrol ve Gözetleme Sistemi

SSCB **:** Sovyet Sosyalist Cumhuriyetler Birliği

ŞİÖ **:** Şangay İşbirliği Örgütü

TCK **:** Türk Ceza Kanunu

UAD **:** Uluslararası Adalet Divanı

UDAD **:** Uluslararası Daimi Adalet Divanı

UCM **:** Uluslararası Ceza Mahkemesi

UHK **:** Uluslararası Hukuk Komisyonu

UTB **:** Uluslararası Telekomünikasyon Birliği

VAHS **:** Viyana Antlaşmalar Hukuku Sözleşmesi

v. **:** Versus

GİRİŞ

Uluslararası hukuk, temel olarak devletlerarası ilişkileri incelemektedir. Uluslararası hukukun ilk olarak Roma hukukunda, Roma vatandaşları ile vatandaş olmayanlar arasındaki ilişkilerin düzenlenmesi amacına hizmet ettiği kabul edilmekte iken[1] 1648 Westfalya Barışı'yla gerçek anlamda ulus devletlerin ortaya çıkmasıyla ulus devletler arasındaki ilişkinin düzenlenmesi, modern anlamda uluslararası hukuku ortaya çıkarmıştır[2]. Önceleri temel süjesi devlet olan uluslararası hukuk, uluslararası örgütlerin ortaya çıkmasıyla değişime uğramış, devletler dışında uluslararası hukuk kişisi olma niteliğine sahip uluslararası örgütleri ve hatta bireyleri de tanım kapsamına dâhil etmiştir. Bu değişime uygun bir şekilde yapılan bir tanıma göre uluslararası hukuk, uluslararası düzeyde hak sahibi ve yükümlülük altına girebilme yeteneği olan uluslararası hukuk kişileri arasındaki ilişkileri düzenleyen hukuk olarak tanımlanmaktadır[3].

Yaşanan süreç sonunda uluslararası suçlar nedeniyle bireyler ya da Filistin Kurtuluş Örgütü gibi devlet niteliği taşımayan insan toplulukları uluslararası hukukun süjesi halini almıştır[4]. Ayrıca devlet dışı örgütlerin ya da uluslararası nitelikli ticari ortaklıklar ile devletlerarasında ortaya çıkan ulus üstü uyuşmazlıklar nedeniyle uluslararası hukukun kapsamı genişlemeye devam etmektedir. Belki de bu sürecin son halkası olarak ifade edilebilecek internet teknolojisinin gerek birey ve gerekse devlet ilişkilerinde yarattığı değişim ile ulus devletlerinin temel faaliyet alanlarının sanal ortama yönelmesi

---

[1] Uluslararası Hukukun gelişmesinde Roma kavimler hukukunun yeri hakkında bkz.: Karakoç, İrem. (2004). *Türk Hukuk Tarihi'nde Uluslararası Andlaşmaların Uluslararası Hukukun Gelişim Sürecindeki Yeri*. DEÜ Hukuk Fakültesi Dergisi, Cilt:6, Sayı:2, s. 209.; Güneş Ceylan, Seldağ. (2004). *Roma Hukukunun Günümüz Hukuk Düzenlerine Etkisi*. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt:8, Sayı:2, s. 14.

[2] Devetak, Richard / Burke, Anthony / George, Jim. (2012). *An Introduction to International Relations*. Cambridge: Cambridge University Press, s. 232.

[3] Aksar, Yusuf. (2021). *Teoride ve Uygulamada Uluslararası Hukuk I.* Ankara: Seçkin, s. 28.

[4] Aksar, 2021, (1. Kitap) s. 29.

sonucunda devletlerarasındaki ilişkilerin de bu değişime uygun şekilde düzenlenmesi gerekmiştir.

İlk bakışta, bu değişimin etkisinin sınırlı olacağı düşünülebilirse de beklenenin aksine uluslararası hukukun neredeyse her alanında internet teknolojisinin uygulama olanağı bulduğu görülmektedir. Bu noktada ifade etmek gerekir ki klasik uluslararası hukukta savaş alanının kara, hava, deniz ve uzaydan ibaret olduğu kabul edilirken, süreç içerisinde siber uzay beşinci alan olarak kabul edilir hale gelmiştir[5]. Bu doğrultuda *Nükleer Silahlar Danışma Görüşü*'nde [6] Uluslararası Adalet Divanı'nın (UAD) uluslararası silahlı çatışmalar hukukunun, kullanılan silaha bakılmaksızın, tüm savaş formlarına uygulanacağını ortaya koyması karşısında, siber savaşın etkilerinin silahlı çatışmalar hukukunu da kapsadığı sonucuna varılmaktadır.

Yine, bir devletin temel unsurlarından olan "egemenlik", 1928 *Palmas Adası Davası*'nda[7] tanımlanmış ve bunun devletlerarası bağımsızlık anlamına geldiği kabul edilmiştir[8].

---

[5] The Economist dergisinde 01.07.2010 günü yayınlanan makalede siber savaş nedeniyle internet, beşinci savaş alanı olarak ifade edilmiştir. Bkz.:, Cyberwar: war in the fifth domain, *The Economist.* (01 Temmuz 2010). Erişim: 15.11.2022 https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain; Clarke, Richard A. / Knake, Robert K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threath*. New York: Penguin Press, s. 6.; Craig, Anthony / Valeriano, Brandon. (2016). *Conceptualising Cyber Arms Races*, 8th International Conference on Computational Intelligence, s. 141.; Even, Shmuel. / Siman- Tov, David. (2012). *Cyber Warfare: Concepts and Strategic Trends*. Tel Aviv: Institute for National Security Studies, s. 10.; Ayrıca bkz.: Sağıroğlu, Şeref / Alkan, Mustafa. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları, s. 196.

[6] UAD, "*Legality of the Threat or Use of Nuclear Weapons*", 08 Temmuz 1996, Erişim: 12.06.2022 https://www.un.org/law/icjsum/9623.htm

[7] Hakemlik Kararı, "*Island of Palmas Case*", 04 Nisan 1928, Erişim: 15.07.2022 https://legal.un.org/riaa/cases/vol_II/829-871.pdf

[8] Pazarcı, Hüseyin. (2021). *Uluslararası Hukuk.* Ankara: Turhan Kitabevi, s. 153.; Anılan kararda Hakem Max Huber, devletlerarası ilişkilerde egemenliğin tanımında "bağımsızlık" ölçütünü vurgulamıştır. Bkz.: Sur, Melda. (2022). *Uluslararası Hukukun Esasları.* İstanbul: Beta, s. 121.

Korfu Boğazı Davası'nda[9] ise UAD, bağımsız devletlerarasında ülkesel egemenliğin, uluslararası ilişkilerin temel bir unsuru olduğunu belirtmiştir[10]. Zira mutlak suretle egemenlik hakkının tanındığı ülke sınırları içerisinde kişi ve nesneler ile ilgili olarak devletlere yasa çıkarma ve uygulama yetkisi bahşeden ülkesel egemenlik ilkesi, aynı zamanda diğer devletlerin bu alana karışmasını da yasaklar[11]. Ayrıca *Nikaragua Davası*'nda[12] belirtilen devletlerin egemen eşitliği prensibi ve *Korfu Boğazı Davası*'nda ortaya konulan, devletin bilerek ülkesini diğer devletlere zarar verecek şekilde kullandırmaması yükümlülüğü siber tesisler yönünden de değerlendirilmelidir. Buna göre, devletin kara, deniz ve hava ülkesindeki siber altyapı varlıklarını kontrol etme hakkı da egemenliğin bir parçası olarak kabul edilmelidir.

Ulus devletleri hedef alan siber saldırıların ilk örnekleri olarak kabul edilen 2007 yılında Estonya'ya, 2008 yılında Gürcistan'a, 2010 yılında İran'a ve 2012 yılında Suudi Arabistan'a yönelik gerçekleşen saldırılar, bu devletlerin hukuk düzenine de bir saldırı oluşturmaktadır. Bu saldırıların aynı zamanda uluslararası hukuka aykırı bir eylem oluşturup oluşturmadığının, silahlı saldırı kavramına dâhil edilmesinin gerekip gerekmeyeceğinin, Birleşmiş Milletler (BM) Şartı kapsamında devletin siyasi ve ülkesel bütünlüğüne veya dünya barışına bir saldırı oluşturup oluşturmayacağının genel prensipler dairesinde değerlendirilmesi ve tespiti bir zorunluluktur.

Klasik uluslararası hukukta uygulama alanı bulmakta iken siber alanda da kendini gösteren, uluslararası boyut taşıyan suçların yargılanmasına ilişkin ülkesel yetki dışında kabul edilen saldırganın milliyeti, mağdurun milliyeti, koruma prensibi ve evrensellik

---

[9] UAD, "*Corfu Channel Case*", 09 Nisan 1949, Erişim: 15.07.2022 https://www.icj-cij.org/public/files/case-related/1/001-19491215-JUD-01-00-EN.pdf

[10] Heinegg, Wolff Heintschel von. (2012). *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, s. 8.

[11] Heinegg, 2012, s. 8.

[12] UAD, "*Case Concerning Military and Paramilitary Activities in and Against Nicaragua*", 27 Haziran 1986, Erişim: 12.06.2022 https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

ilkesinin nasıl uygulanacağı konuları da çözümlenmesi gereken sorunlardır. Bu konuda uluslararası siber suçlar ya da siber terörizm ile bu çalışmanın konusunu oluşturan siber savaşı birbirinden ayıran sınırların belirlenmesi gereklidir. Ayrıca uzaydan, uluslararası hava sahasından veya açık deniz gibi alanlardan gerçekleştirilen siber saldırılara ilişkin bayrak devletinin yetkisi konusu da yeniden yorumlanmalıdır. Bu kapsamda, devlet gemilerinin bağışıklığı, ticari uyduların veya devlet uydularının bağışıklığı konuları ile statülerinin ne olduğu ortaya konulmalıdır. Gelinen noktada tartışılması gereken bir diğer konu ise, uluslararası silahlı çatışmalarda tarafsız devletlerin siber altyapı tesislerinin Viyana Diplomatik İlişkiler Sözleşmesi kapsamındaki durumu ve devletin sorumluluğudur.

BM Şartı'nın 2/4. maddesi uyarınca devletler, uluslararası ilişkilerinde gerek bir devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı, gerek Birleşmiş Milletler'in amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınmalıdırlar. Bir siber operasyonun bu yasak kapsamında değerlendirilmesi halinde BM Şartı'na aykırılık oluşturacağı söylenebilir. Bu nedenle, hangi siber operasyonların hukuka aykırılık oluşturacağının belirlenmesi ve siber operasyonlar açısından yasağın sınırlarının çizilmesi gerekir. Ayrıca, bir devletin ülkesi üzerinde bulunan siber altyapı tesisleri kullanılarak gerçekleştirilen saldırıların, ülke devletinin tarafsızlık statüsü kapsamında değerlendirilmesi ve diğer ilkeler nazara alınarak hukuki durumun tespiti yapılmalıdır. Özetle, siber savaş kapsamına dâhil olan saldırılar *jus ad bellum* ve *jus in bello* kavramlarına göre değerlendirilecektir.

Bilindiği üzere uluslararası sorumluluğun söz konusu olabilmesi için uluslararası hukuka aykırı bir devlet eyleminin varlığı ve bu eylemin devlete atfedilebilirliği koşullarının birlikte gerçekleşmesi gereklidir[13]. Öğretide, bu koşullara eylemin zarar ile sonuçlanması gerekliliği de ilave edilmektedir[14]. Siber savaşta uluslararası sorumluluk için zarar gerekip gerekmediği konusu bu çalışmada incelenmiştir. Aynı kapsamda siber saldırıların

[13] Uzun, Elif. (2007). *Milletlerarası Hukuka Aykırı Eylemlerinden Dolayı Devletin Sorumluluğu*. İstanbul: Beta, s. 30.

[14] Pazarcı, 2021, s. 447.

bir bilişim korsanı tarafından gerçekleştirilmesi halinde atfedilebilirlik sorununun üzerinde durulmalıdır. Zira siber saldırıyı gerçekleştiren kişi ya da örgütün, devlet ile bağı konusunda *Nikaragua*[15] ve *Tadić*[16] Davaları ışığında ne tür bir testin uygulanacağı, siber saldırılara karşı alınacak önlemler konusunda muhatap devletin *Naulilaa Davası*'nda[17] ifade edilen ihlal oluşturan eylemin ağırlığıyla orantılı olma testi ve *Gabcikovo-Nagymoros Davası*'nda[18] ifade edilen ikinci test yöntemi olan, meydana gelen zararla orantılılık ilkesinin nasıl uygulanacağı sorunları üzerinde durulmalıdır.

Siber eylemlerin çoğunlukla bir devlet organı tarafından değil, bir grup bilişim korsanı tarafından gerçekleştirilmesi nedeniyle 'atfedilebilirlik' unsuru uluslararası hukukçuları zorlayan bir konudur. Bir devletin uluslararası haksız bir fiilden sorumlu tutulabilmesi ve saldırıya uğrayan devletin meşru müdafaa hakkını kullanabilmesi, ancak saldırının o devlete atfedilebilir olması ile mümkündür. Bu çalışmada, uluslararası hukukta 'meşru müdafaa' ve 'atfedilebilirlik' konularına ilişkin normların siber saldırılara nasıl uygulanabileceği incelenecek, siber savaşta sorun oluşturan atfedilebilirliğe ilişkin olarak teknik ve hukuki değerlendirme yapılacaktır. Bunun yanında, kritik altyapı unsurlarının neler olduğu belirlenerek, Stuxnet ve Aramco gibi operasyonların meşru müdafaa hakkını doğuracak düzeyde olup olmadığını anlamak için öncelikle eylemlerin 'siber saldırı' eşiğini aşıp aşmadığı tespit edilecektir.

---

[15] UAD, "*Case Concerning Military and Paramilitary Activities in and Against Nicaragua*", 27 Haziran 1986, Erişim: 12.06.2022 https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[16] EYUCM, "*Tadi´c Case*", 07 Mayıs 1997, Erişim: 16.07.2022 https://www.icty.org/en/press/tadic-case-verdict

[17] Hakemlik Kararı, "Naulilaa Arbitration", 31 Temmuz 1928, Erişim: 15.07.2022 https://www.scribd.com/document/506919046/Naulilaa-Arbitration-Portugal-vs-Germany-Google-translated

[18] UAD, "*Case Concerning the Gabcikovo-Nagymaros Project*", 25 Eylül 1997, Erişim: 16.07.2022 https://www.icj-cij.org/public/files/case-related/92/092-19970925-JUD-01-00-EN.pdf

Uygulanan uluslararası hukukun genel durumuna bakıldığında siber savaş konusunda genel bir uluslararası antlaşma bulunmamaktadır. Yine, konuya özgü bir yapılageliş hukukunun da oluştuğu kesin olarak söylenemez. Bu noktada, klasik savaş hukukuna ilişkin oluşan yapılageliş hukuku kurallarının uygun düştüğü ölçüde siber savaşa uyarlanması söz konusu olabilecektir. Bunun yanında, uzay ve kıta sahanlığı konularında olduğu üzere siber savaşta ani (*instant*) yapılageliş kurallarının doğmasının mümkün olup olmadığı da irdelenmelidir. Üzerinde tartışılan bir diğer husus olarak siber savaş konusunda uluslararası bir antlaşmanın gerekli olup olmadığının tespiti ve gerekmemesi halinde mevcut uluslararası hukuk normlarının siber uzaya ne şekilde uygulanabileceğinin ve bu süreçte başvurulabilecek yorum metotlarının belirlenmesi de amaçlanmaktadır.

Uluslararası hukukta henüz siber savaşı düzenleyen çok taraflı bir antlaşma bulunmamakla birlikte, 2000'li yılların başından itibaren BM Genel Kurulu'nca siber güvenlikle ilgili pek çok kararın yayınlandığı ve devletlerin kendi siber güvenlik strateji belgelerini oluşturdukları görülmüştür. Ayrıca bazı bölgesel örgütlerce siber güvenliğe dair işbirliği protokolleri hazırlanmıştır. Eylül 2019 tarihi itibariyle BM üyesi 27 devletin uluslararası siber savaş hukukuna ilişkin olarak imzaladıkları ortak bir bildiri vasıtasıyla ulus devletlerin siber uzaydaki faaliyetlerinin uluslararası hukuk kurallarına uygun olması gerekliliğine işaret edilmiş ise de bu çabalar bildiriden öteye gitmemiştir[19]. Bunun sebepleri ve bu alanda yapılması gerekenler de bu tezin konusunu oluşturmaktadır.

Genel olarak, siber savaşın hâlihazırda uluslararası ve uluslararası olmayan silahlı çatışmaları kapsadığı, ancak geleneksel elektronik saldırıları ve siber kontrol merkezlerine fiziki saldırıları kapsamadığı kabul edilmektedir. Bu açıdan çalışmada uluslararası hukukta siber saldırı ve siber savaş kavramlarının sınırlarının çizilmesi, uygulamada yaşanan siber çatışmaların analiz edilmesi amaçlanmaktadır. Bu kapsamda, çalışmada siber savaş hukukuna uygulanacak uluslararası hukuk kurallarının somut

[19] Bkz.: Collier, Kevin. (23 Eylül 2019). 27 Countries Sign Cybersecurity Pledge with Digs at China Russia, *CNN*. Erişim: 09.09.2021 https://edition.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html

örnekleriyle bir çerçevesi çizilecek, siber savaş *jus ad bellum* ve *jus in bello* paradigmasında uygulamada yaşanan örnekleriyle değerlendirilecektir. Siber saldırıların, meşru müdafaa hakkına olanak sağlayan bir silahlı saldırı olarak değerlendirilip değerlendirilmeyeceği, meşru müdafaa koşullarının hangi durumlarda oluşacağı, siber savaşta uluslararası silahlı çatışmalar hukukunun uygulama yeri bulup bulmadığı tespit edilecektir. Siber savaşın uluslararası hukukta düzenlenmemiş olması karşısında *Martens kaydı* kapsamında nasıl yorumlanacağı, 'kuvvet kullanımı' ve 'meşru müdafaa' kavramlarının siber savaş kavramına nasıl uyarlanacağı soruları uluslararası siber savaş hukukunu ilgilendiren konuların başında gelmektedir. Bu nedenle çalışmada bu soruların analizi yapılarak çözüm önerileri aranacaktır.

Geleneksel savaştan farklı olarak siber saldırı halinde meşru müdafaa yoluna devletlerin ne şekilde başvurabilecekleri konusu farklı bir özellik taşımaktadır. Saniyeler içinde olup biten ya da kritik tesisleri günlerce devre dışı bırakabilen bir siber saldırıya karşı devletlerin geleneksel yöntemlerle karşı koyması beklenemez. Bu durumda siber saldırılara karşı alınacak karşı önlemler ya da olaya özgü gerekli meşru müdafaa şeklinin de uluslararası hukuk çerçevesinde belirli kıstaslara bağlanması gereklidir. Ayrıca siber uzayda devlete veya özel sektöre ait hizmet alanlarının birbirine girmiş olması nedeniyle özel sektör eliyle yürütülen bankacılık, finans, iletişim gibi kritik faaliyetlere yönelen siber saldırılara karşı uygulanacak aktif savunma tedbirleri ya da meşru müdafaa yoluna başvuracak birimlerin ve yöntemlerin tespiti ayrı bir meseledir.

Uluslararası hukukun asli kaynaklarının sırasıyla uluslararası sözleşmeler, yapılageliş hukuku ve hukukun genel ilkeleri olması ve ulusal hukuk sistemlerinden farklı olarak merkezi bir yasama organının bulunmaması dikkate alındığında uluslararası hukukun teknolojik gelişime ayak uyduramadığı söylenebilir. Uluslararası sözleşmelerin dışında kalan ve yapılageliş kurallarının henüz oluşmadığı tüm bu sorunlu alanları ele alacak bu çalışmanın uluslararası hukukta siber savaş konusunda öncül ve özgün olması amaçlanmaktadır. Bu yönüyle bu çalışmanın konusunu oluşturan ve gelişmekte olan uluslararası siber savaş hukuku konusunda daha önce yapılan bilimsel çalışmalara ilaveten eski normların yorumlanmasına dair yeni yaklaşımlar geliştiren bir çalışma hazırlanması hedeflenmektedir. Bu alanda ulusal mevzuatlarda yapılmış birtakım

düzenlemeler bulunmakta ise de siber savaşların arttığı bir dönemde uluslararası alanda mevcut düzenlemelerin yeterli olmadığı açık olduğundan uluslararası hukukta siber savaş hukuku konusunda yeni çalışmaların gerekliliği kendini göstermektedir. Bu sebeple konunun önemini kendiliğinden ortaya çıkmaktadır.

Teknolojik gelişmelerin savaş üzerindeki etkileri çalışmanın konusunu oluşturmamakta ise de teknolojik gelişmenin bir sonucu olan siber uzayın kullanılarak devletlerin ya da devlet dışı unsurların gerçekleştirdiği eylemlerin uluslararası hukuk alanında nitelendirilmesi çalışmanın konusunu oluşturduğundan, bu hususta ortaya çıkan sorunlara cevap olacak uluslararası hukuk kaynaklarının araştırılması amaçlanmaktadır. Bu doğrultuda 4 bölümden oluşacak çalışmanın ilk bölümünde temel kavramlar, bu alanda yapılan örgütsel çalışmalar ve uluslararası hukukun diğer alanlarında siber saldırı konusu ortaya konulacaktır. İkinci bölümünde, siber uzayda devletin yetki ve sorumlulukları başlığı altında uluslararası hukukun temel süjesi olan devletin bu yeni alandaki konumu ortaya konulacak, üçüncü bölümde kuvvet kullanma yasağı bağlamında bu yasağa dâhil olan siber operasyonlar ve meşru müdafaa konusu tartışılacaktır. Son bölümde ise, siber savaşta silahlı çatışmalar hukuku incelenecektir. Tezin hazırlanmasında arşiv araştırması, metin çözümlemesi, örnek olay incelemesi, karar tahlili gibi yöntemler uygulanacaktır.

Kaynak araştırması yöntemiyle elde edilen veriler yalnızca tümden gelim yöntemiyle değerlendirilip ortaya konulmayacak, daha önce tartışılmamış alanlarda ortaya çıkan sorunlara ilişkin olarak yeni görüşlerin ortaya konulabilmesi amacıyla gerekli olan durumlarda tümevarım yöntemi tercih edilecektir. Gerek teknik gerekse hukuki verilerin yeni bir bakış açısıyla değerlendirilmesi ve uluslararası hukuk kurallarının yorumunda yeni bir yaklaşımın ele alınması gerekli görüldüğünden, çağın gerektirdiği şekilde teknik gelişmeye ve ulus devletlerin geçirdiği evrime uygun bir bakış açısının gerekliliği gerekçeleriyle ortaya konulacaktır.

Uluslararası siber savaş hukukunun gelişmesine faydalı olabilecek yeni akademik çalışmaların önemi ortada iken, bu çalışmanın bir diğer amacı da uluslararası hukukun

neredeyse tüm alt başlıklarında uygulama alanı bulan yeni bir alanın sınırlarının tespiti ve içeriğinin değerlendirilmesidir.

1. BÖLÜM: TEMEL KAVRAMLAR, ULUSLARARASI ALANDA YAPILAN ÇALIŞMALAR VE ULUSLARARASI HUKUKUN SİBER SAVAŞA İLİŞKİN ÖZEL ALANLARI

1.1.SİBER UZAY

Ağa bağlı bilgi teknolojisi için yaygın şekilde kullanılan siber uzay terimini [20] kavrayabilmek için öncelikle internetin tarihsel gelişiminin incelenmesi, daha sonra siber uzayın tanımlanması ve kapsamının tespiti gereklidir. Pensilvanya Üniversitesinden J. Presper Eckert ve John W. Mauchly'nin, Şubat 1946'da tanıttıkları tarihin ilk tam elektronik genel amaçlı bilgisayarı olan ENIAC (*Elektronic Numerical Integrator and Computer*) [21] , Amerikan ordusunun topçu atışı hesabında kullanılmak amacıyla geliştirilmiştir[22]. 1960 yıllarda ortaya çıkan mikroişlemci sayesinde dört üniversitedeki bilgisayarın birbirine bağlanması sağlanmış ve 1969 yılında *Advanced Research Projects Agency Network* (ARPANET)[23] ile internet[24] ilk kez yaşamımıza girmiştir. Bu ağın

---

[20] Lin, Herbert. (2012). *Cyber Conflict and International Humaniterian Law*, International Review of the Red Cross, Cilt:94, s. 516.; Siber uzay terimi ilk kez 1980'li yılların başında William Gibson'un "Neuromancer" adlı ödüllü romanında "cyber space" kavramı olarak yer almıştır. Bkz.: Dülger, Murat Volkan. (2004). *Bilişim Suçları*, Ankara: Seçkin Yayıncılık, s.50.; Çalışmamızda "cyber space"in Türkçe karşılığı olan "siber uzay" terimi tercih edilmiştir. Öğretide bu terim yerine siber alan ya da siber ortam terimlerinin de kullanıldığı görülmektedir.

[21] Aust, Stefan / Ammann, Thomas. (2018). *Dijital Diktatörlük Kitlesel Gözetim Verilerin Kötüye Kullanımı Siber Savaş* (Çev. Erdinç Yücel, Hasan Yılmaz), Ankara: Hece Yayınları, s. 215.

[22] Key Events in the Development of the First General Purpose Electronic Digital Computer, the ENIAC. Erişim: 02.11.2022, https://www.historyofinformation.com/detail.php?id=636

[23] Betz, David J. / Stevens, Tim. (2011). *Cyberspace and the State.* London New York Routledge, s. 15.; ARPANET internetin öncüsü kabul edilir. Bkz.: Goldsmith, Jack. (2013). *How Cyber Changes the Laws of War*, The European Journal of International Law, Cilt:24, Sayı:1, s. 129.

[24] "İnternet" terimi ilk kez Vinton Cerf ve Bob Khan tarafından TCP (Transmission Control Protocol) hakkındaki bir yazıda kullanılmıştır. Bkz.: Goldsmith, 2013, s. 129.; Sosyal bilimcilerin bir kısmı internetin dünya üzerinde demokrasiyi bir kurum olarak geliştireceğini ve sosyal refahı arttıracağını ileri sürerken diğer bazı felsefeciler ise interneti demokrasi ve özgürlükler için bir tehdit, hatta

özellikle Pentagon ile ilgili projelerle uğraşan Amerikan üniversiteleri ve araştırma merkezlerindeki büyük bilgisayarlara servis sağlaması amaçlanmıştır[25].

İnternetin gelişimi konusunda en yaygın kabul gören bilgi olan Amerikan askeri otoritelerinin nükleer bir savaş durumunda iletişim olanağı sağlamak amacıyla geliştirildiği hususunun[26] gerçeği yansıtmadığı, nükleer bir savaşta telekomünikasyon dâhil çoğu altyapının tahrip olması nedeniyle nükleer füze fırlatma kontrol tesislerini garantiye alma sorunuyla karşılaşan Paul Baran adlı Polonyalı mühendisin, RAND Corporation'da çalıştığı sırada soruna sağlam bir iletişim çözümü üretmesinden ibaret olduğu ileri sürülmüştür[27]. Baran'ın tasarladığı yeni sistemde, her bir ağın yüzlerce yerel merkez üzerinden tek bir merkeze bağımlı olmaksızın birbirleri ile bağlantı kurması ve yerel merkezlerin bir bölümünün zarar görmesi durumunda dahi tüm iletişim sisteminin devre dışı kalması engellenerek bağlantının süreklilik arz etmesi hedeflenmişti[28].

Sonraları Joseph Carl Robnett Licklider'ın *Libraries of the Future* (1965) adlı yayını internet ve World Wide Web fikrine sebep olmuş, ''ARPANET'' tasarımı üzerine çalışan Lawrence Roberts'ın RAND raporlarını incelemesi ve Baran ile irtibata geçerek konu hakkında bilgi almasıyla üniversiteler arası bağlantı sağlanmıştır[29]. 1975 yılında ARPANET devletin bir kurumu olan *Defence Communication Agency*'nin (DCA) yönetimine geçmiştir[30]. Bu ağ daha sonra güvenlik sebeplerinden dolayı kamuya ayrı,

---

insanlığın felaketine sebep olabilecek bir faktör olarak görmekteydiler. Bkz.: Tarcan, Ahmet. (2005). *İnternet ve Toplum*, Ankara: Anı Yayıncılık, s.3.

[25] Aust ve Ammann, 2018, s. 16.

[26] Genel kanı bu yönde olup bu görüş için bkz.: Güreşçi, Ramazan. (2019). *Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi.* Savunma Bilimleri Dergisi, Cilt:18, Sayı:1, s. 79.

[27] Bygrave, Lee A. / Bing, Jon. (2011). *Internet Governance. Oxford New York:* Oxford University Press, s. 9-10.

[28] Güreşçi, 2019, s. 79.

[29] Bygrave ve Bing, 2011, s. 21-23.

[30] Aust ve Ammann, 2018, s. 16.

askeriyeye de Milnet adında ayrı bir hattan hizmet vermeye başlamış; Milnet daha sonra, günümüzde diğer faaliyetlerinin yanı sıra elektronik savaşların ve droneların (insansız hava aracı) yönetiminde kullanılan Pentagon'a ait "*Defence Data Network*" adı altında faaliyet göstermeye devam etmiştir[31].

1985 yılına gelindiğinde, Amerika'ya yayılmış 5 süper bilgisayar merkezi, ulusal bir ağ kurmak için bir çözüm önermiş ve Ulusal Bilim Merkezi'nin (*the National Science Foundation*/NSF) rızasıyla NSFNET olarak bilinen bu siteler arasındaki omurga ağ kurulmuştur[32]. İnternetin omurgası olarak NSFNET, ARPANET'ten 25 kat daha büyük bir hızla internet bağlantısı sağlamıştır[33]. Süreç içerisinde ağ bağlantılarının genişlemesi yeni bir problemi ortaya çıkarmış, 2000'in üzerindeki ağa bağlı bilgisayara bir ad verilmesi gerektiğinden alan adı (DNS) geliştirilmiş, 80'li yılların başında İnternet Numara Tahsis Otoritesi (*The Internet Assigned Number Authority* - IANA) gayri resmi olarak kurulmuş ve Jon Postel tarafından ölüm tarihi olan Ekim 1998 tarihine değin yönetilmiştir[34].

Sonraları 1998 yılı Haziran ayında Amerikan Ticaret Bakanlığı'ndan bir ajans ve Ulusal Telekomünikasyon ve Bilişim İdaresi, alan adı yönetiminin kar amacı gütmeyen bir şirket şemsiyesi altında birleştirilmesi teklifinde bulunması üzerine Eylül 1998 tarihinde ICANN (*the Internet Corporation for Assigned Names and Numbers*) kurulmuş, Aralık 1998'de ise Güney Kalifornia Üniversitesi ile ICANN arasında yapılan antlaşma ile IANA'nın faaliyeti ICANN'a devredilmiştir[35].

Bu tarihsel süreç içerisinde dar anlamda internetin yönetiminin ulusal düzeyde ve teknik açıdan gerçekleştirildiği anlaşılmaktadır. İnternetin işleyiş düzeni bu bağlamda

[31] Aust ve Ammann, 2018, s. 16.

[32] Bygrave ve Bing, 2011, s. 32.

[33] Bygrave ve Bing, 2011, s. 36.

[34] Bygrave ve Bing, 2011, s. 35.

[35] Bygrave ve Bing, 2011, s. 36.

düşünüldüğünde IETF (*the Internet Engineering Task Force*/İnternet Mühendisliği Görev Gücü) ve ICANN gibi özel kurumların, internetin teknik altyapısını ve mimarisini yönettiği söylenebilir [36] . İnternetin yönetimi konusunda uluslararası antlaşma bulunmaması nedeniyle uygulanabilecek ikinci kaynak olarak uluslararası yapılageliş hukukunun, hükûmet dışı bir Amerikan örgütü olan ICANN'ın uluslararası hukukun süjesini oluşturmaması, bu örgütün uygulamalarının siber uzayda yapılageliş hukuku olarak uygulama yeri bulmaması sonucunu doğurmaktadır[37]. Bu durum aynı zamanda diğer devletlerin ulusal egemenlik yetkisinin siber uzayda Amerika Birleşik Devletleri'ne (ABD) nazaran daha dezavantajlı şekilde kullanılmasına sebep olmaktadır.

Belirtilen örgütlere göre dar anlamda internetin yönetimi, internet altyapısının düzenlenmesi, zamanla değişim ve gelişim süreci ve işleyişini ifade eder. Bir diğer ifade ile internetin dar anlamda yönetimi, işlemler, sistemler ve TCP/IP, alan adı ve IP numaralarını düzenleyen kurumlara ilişkindir [38] . İnternetin teknik ve kurumsal yönetiminin yanında sivil yaşamda çok geniş ölçekte yaşamın bir parçasını oluşturması sonrasında ağa bağlanan tüm kullanıcıların internetin işleyişini etkilemesinden dolayı daha geniş ölçekte internetin yönetimi kavramı ortaya çıkmıştır. Geniş anlamda internetin yönetimi, bilgisayar, tablet, akıllı telefonlar veya diğer akıllı cihazlar vasıtasıyla ağa bir şekilde bağlı tüm bireylerin e-posta, facebook, twitter, instagram gibi uygulamalarda sesli, yazılı veya multimedya ve banka işlemleri gibi kayıtları üretmek suretiyle kolektif şekilde işletilen bir sistem olarak ifade edilebilir. Kolektif yönetimin doğası gereği internetin geniş anlamda yönetiminin aslında kaos kuramının sanal ortama uyarlanması olarak kabulü mümkündür[39]. Buradan hareketle kaos kuramının uluslararası siber savaşa

---

[36] Bygrave ve Bing, 2011, s. 48.

[37] Streltsov, Anotoly A. (2017). *Application of Internaional Humanitarian Law to Armed Conflicts in Cyberspace*, s. 4. Erişim: 17.10.2020 https://digital.report/wp-content/uploads/2016/04/169747-Streltsov-ENG.pdf

[38] Bygrave ve Bing, 2011, s. 50.

[39] Newton'un doğrusal ve ardışık fizik kuramından farklı olarak evrenin işleyişinde olduğu üzere karmaşık ve doğrusal olmayan sistemlerin düzensiz ve öngörülemeyen yapısı gereği küçük etkilerin yarattığı büyük sonuçların da kendi içinde bir matematiksel düzen barındırdığı şeklinde özetlenebilecek kaos teorisinin siber uzaya uygulanabilirliği konusunda bkz.; Garrie, Daniel / Simonova, Masha. (2020). *A*

uygulanabilirliği konusu ele alındığında, konvansiyonel savaştan farklı olarak, bir klavye hareketinin siber uzayda ve dolayısıyla fiziki ortamda yarattığı devasa sonuçlar yeni bir bakış açısını zorunlu kılmaktadır. İleride açıklanacağı üzere bu yeni bakış açısı, geleneksel uluslararası normların siber savaşa uygun şekilde yorumlanması şeklinde ortaya çıkmaktadır.

İnternet'in yönetimi konusunda belirsizlik bulunduğundan, bu konuda 5 model önerilmektedir[40]. Bunlardan ilki, hükûmet kontrolünün ötesinde, bireysel serbestlik alanında internetin kendi kendine yönetimidir. İkincisi, ulus ötesi ve uluslararası örgütler modelidir. Üçüncüsü, internetin nasıl işleyeceğini belirleyecek iletişim protokolleri veya diğer yazılımlar tarafından verilen düzenleyici kararlar fikrine dayanan kod ve internet mimarisi modelidir. Dördüncüsü, ulusal hükûmetlerin temel düzenleyici kararlarına dayanan model[41] ve son olarak internetin doğası hakkındaki temel kararları veren piyasa güçlerini öngören piyasa düzenlemesi ve ekonomi modelidir. Bu önerilerden internetin doğasına en uygun olanı belirlemek asıl amaç olursa temelde devletlerin müdahale edemeyeceği düzeyde bir serbestlik ve kaos halinin korunarak daha üst düzeyde hukuksal yönden uluslararası örgütlerin yönetiminde gerçekleştirilmesi kanaatimizce uygun olacaktır.

Öğretide bir kısaltma terimi olarak siber uzay, yaygın olarak internet ve World Wide Web'e atıf yapılan bilgi sistemleri ve telekomünikasyon altyapıları, bilgisayar ortak ağlarının kesişmesiyle ortaya çıkan bir ortam olarak tanımlanmıştır[42]. ABD Savunma

---

Keystroke Causes a Tornade: Applying Chaos Theory to International Cyber Warfare Law, Broklyn Journal of Int'l Law, Cilt:45:2, s. 497.

[40] Bygrave ve Bing, 2011, s. 56-57.

[41] Son 20 yıl içinde dünyanın değişik bölgelerindeki devletler uluslararası hukuk kurallarını siber uzayın idaresine uygulamayı düşündüklerini açıkça bildirmişlerdir. Bkz.: Mačák, Kubo. (2018). *Silent War: Applicability of the Jus in Bello to Military Spaca Operations*, International Law Studies, Cilt:94, s. 13.

[42] Sharp, Walter Gary, Sr. (1999). *Cyberspace and the Use of Force.* Virginia: Aegis Research Corporation, s. 15.

Bakanlığı ise siber uzayı, "internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemci ve denetleyicileri de içeren, bilgi teknolojisi altyapılarının bağımsız ağlarından oluşan küresel etki alanı" olarak tanımlamıştır[43]. Bu bağlamda siber uzay, özel ağların yanında para akışı, borsa işlemleri ve kredi kartı işlemleri ile ilgili veri aktarımı gibi faaliyetlerin gerçekleştirildiği işlemsel ağları da kapsamaktadır[44]. Buna paralel olarak, siber uzayın genel olarak internet ile eşdeğer görülerek bilgisayar teknolojisiyle ortaya çıktığı düşünülmekte ise de mecazi bir kavram olarak siber uzayın makine vasıtasıyla gerçekleştirilen iletişim şekli olduğundan bahisle telefon, televizyon ve bilgisayarın karışımı olduğu, hatta Yunan şehir devletlerinde kamusal tartışma mekanı olan agoraya dayandırıldığı görülmektedir[45]. Bu haliyle siber uzayın, sadece bilgisayarları birbirlerine bağlayan dijital bir ağdan ibaret olmadığını söylemek; bu kavramın insanların da süjesi olduğu ve insanları birbirine bağlayan bir ortam olduğunu ileri sürmek mümkündür[46].

Siber uzayın güvenli olmayan ancak farklı imkanlar sunabilen yapısı, lezzetli yiyeceklerle olduğu kadar insanları yemek isteyen korkunç şeylerle dolu ilk çağ yağmur ormanlarına ve bu yeni ortam ile yeni tanışan ve çoğunluğu oluşturan insanlar, cennet bahçesinden kovulan Adem ve Havva'ya benzetilmektedir[47]. Siber uzay, gündelik insan yaşamında sağladığı alışveriş, eğitim, iletişim, para transferi ve bunun gibi pek çok konuda saymakla bitmeyecek kolaylıklar yanında, ulusal sınırlar içerisinde ya da sınıraşan şekilde suç işleme kolaylığı veya failin kimliğini gizlemesine uygun bir ortam sağlaması gibi olumsuz etkileri bir arada sunmaktadır. Bu yeni alanın sağladığı özgürlükler kadar, barındırdığı tehlikeler, sadece insanları değil devletlerin çıkarlarını da hedef almaktadır.

---

[43] Türkay, Şeyda. (2013). *Siber Savaş Hukuku ve Uygulama Sorunsalı.* İÜHFM, Cilt:71, Sayı:1, s. 1178.

[44] Schreier, Fred. (2015). *On Cyberwarfare*, DCAF Horizon 2015 Working Paper, Sayı:7, s. 10. Erişim: 29.01.2022, https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

[45] Betz ve Stevens, 2011, s. 13.; Tarcan, 2005, s. 69.

[46] Benzer bir tespit için bkz: Sağıroğlu ve Alkan, 2018, s. 193.

[47] Betz ve Stevens, 2011, s. 129.

Siber uzay tamamen insan yapımı olan yegâne alandır[48]. Siber uzayın önemli bir özelliği, farklı devletlerin ülkelerinde konumlu nesneler ve kişiler arasında bilgi etkileşimini mümkün kılan küresel doğasıdır[49]. Siber uzayın dikkat çeken bir diğer özelliği, Wikileaks olayında[50] olduğu üzere, bu ortamda bir verinin çalınması daha kolay iken, gizlenmesi daha zordur[51]. Bahsedilen bu özellikleri yanında, siber uzayın diğer bir karakteristik özelliği ise sürekli kopyalama özelliği ve siber uzaya erişimin göreceli olarak ucuz olmasıdır[52].

Ayrıca siber uzayda güç dengesinin saldırganların lehine olduğu görülmektedir[53]. Bir diğer ifade ile siber uzayda savunmadan ziyade saldırı daha ağır basar[54]. Bu bağlamda ulus devletlerin siber uzay üzerinden hizmet verir hale gelmesi; teknolojinin, savaş ve saldırı sistemlerinde giderek ağırlığının artması gibi sebeplerle ağa bağlı devletler siber saldırılara açık hale gelmiştir. Ayrıca devletlerin bu kırılganlığı artarken devlet gücüne denk olmayan birey ve grupların da asimetrik şekilde saldırı silahı olarak interneti kullanması ve böylelikle siber uzayda devletler karşısında önemli bir aktör halini almaları söz konusu olmuştur.

---

[48] Melzer, Nils. (2011). *Cyberwarfare and International Law*, s. 5. Erişim: 15.05.2020, https://www.files.ethz.ch/isn/134218/pdf-1-92-9045-011-L-en.pdf;

Ulusal sınırları aşan yetkide Jus in Bello konusunda benzer görüş için bkz.; Mačák, s. 34-36.

[49] Streltsov, 2017. s. 4.

[50] Wikileaks, Avusturalyalı bir bilgisayar programcısı ve aktivist olan Julian Assange tarafından 2006 yılında, gizli bilgileri ifşa etmeye yönelik olarak kurulan bir örgüttür. Daha ayrıntılı bilgi için bkz.: Wikileaks media organization and Web site. Erişim: 02.11.2022. https://www.britannica.com/technology/website

[51] Betz ve Stevens, 2011, s. 136.

[52] Schreier, 2015, s. 12. Siber uzayın özellikleri için bkz.: Çifci, Hasan. (2013). *Her Yönüyle Siber Savaş*. Ankara: Tübitak, s.8-9.

[53] Geers, Kenneth, (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory, Information Security Journal: A Global Perspective, Cilt:18, Sayı:1, s.3.

[54] Schreier, 2015, s. 12.

Siber uzay konusunda çeşitli ülkelerin ulusal siber güvenlik strateji programlarında farklı tanımlamaların bulunduğu görülmektedir. Siber uzay terimine ilişkin hâlihazırda evrensel bir kural ya da tanım bulunmamakta olup Şangay İşbirliği Örgütü ve Rusya Federasyonu'nun tarafı olduğu bazı antlaşmalarda "*information space*" terimi bilginin yaratılması, şekillendirilmesi, dönüştürülmesi, aktarılması, kullanılması ve depolanmasıyla ve bireysel ve kamu bilincini, bilgi altyapısını ve mülkiyetini ilgilendiren alanlarda uzmanlık olarak kullanılmaktadır[55].

2009 tarihli Amerikan Strateji Belgesi'nde[56] siber uzay, küresel seviyede birbirine bağlı dijital bilgi ve iletişim altyapısı olarak tanımlanırken, aynı tarihli İngiliz Strateji Belgesi'nde[57] ağa bağlı her türlü dijital aktiviteyi kapsadığı belirtilmiştir. 2010 tarihli Kanada Siber Güvenlik Belgesi'nde[58] ise, birbirine bağlı bilgi teknolojisi ağları ve bu ağlarda bulunan bilgi tarafından yaratılan elektronik dünya olarak ifade edilmiştir[59]. Siber güvenlik alanında çalışma yapan Rus ve Amerikan uzmanlara göre bilişim alanının bir

---

[55] Streltsov, Anotoly A. (2017). *Application of Internaional Humanitarian Law to Armed Conflicts in Cyberspace*, s. 2. Erişim: 17.10.2020 https://digital.report/wp-content/uploads/2016/04/169747-Streltsov-ENG.pdf; "Information space" terimi Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması'nın Ek 1'de tanımlanmıştır. Bunun için bkz.: Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması, s.9. Erişim: 17.12.2021)

Agreement_on_Cooperation_in_Ensuring_International_Information_Security_between_the_Member_States_of_the_SCO.pdf

[56] United States, Office of White House Press. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, s. 1. Erişim: 11.08.2022

https://nsarchive.gwu.edu/document/21424-document-28

[57] United Kingdom, Cabinet Office. (2009). *Cyberspace Security Strategy of the United Kingdom: safety, security and resilience in cyber space*, s. 7. Erişim: 11.08.2022

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

[58] Government of Canada. (2010). *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*, s. 2. Erişim: 11.08.2022

https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

[59] Ayrıntılı bilgi için bkz.; Betz ve Stevens, 2011, s. 36.

parçası olan siber uzay; bilginin yaratıldığı, aktarıldığı, alındığı, depolandığı, işlendiği ve iptal edildiği elektronik ortamı içermektedir[60].

Siber uzayın tanımında donanımı dâhil etmeyen ve dâhil eden olmak üzere iki tür model bulunmaktadır. Biraz önce verilen tanımlara uygun olan ilk modelde, yalnızca bilgisayar ağlarının bileşenleri olan donanımlar arasındaki mecazi alan kastedilmektedir. İkincisinde ise, siber uzayın sosyal alanına giriş için gereken altyapı da tanıma dâhil edilmektedir[61]. İkinci modeli benimseyen Tallinn El Kitabı'nda siber uzay fiziki varlık taşıyan donanımlar ile bunlar arasındaki bağlantının ötesini kapsamaktadır. Zira Tallinn El Kitabı'nda siber uzayın fiziki, mantıki ve sosyal katmanlarına[62] egemenlik prensibi hâkimdir. Fiziki katmanın fiziki ağ bileşenlerini (donanım ve kablo, yönlendirici, sunucu ve bilgisayar gibi) ihtiva ettiği, mantıki katmanın ağ aygıtları arasında var olan bağlantılardan (fiziki katman boyunca veri değişimini sağlayan uygulama, veri ve protokoller) oluştuğu görülmektedir[63]. Sosyal katmanın ise siber aktiviteler ile meşgul olan kişi ve gruplardan oluştuğu ifade edilmiştir[64].

Siber uzayın sosyal katmanını oluşturan akıllı telefon ve internet kullanıcılarının günümüzde dijital veri izleri bırakmakla yetinmeyip üstelik bir de bunun için severek işbirliği yapmalarını şüpheci George Orwell'in bile öngöremediği ifade edilmektedir[65].

---

[60] Streltsov, 2017. s. 3.

[61] Betz ve Stevens, 2011, s. 36-37.

[62] Siber uzayı oluşturan katmaların fiziki (physical), bilgiye ilişkin (informational) ve bilişsel (cognitive) olmak üzere başka şekilde nitelendirilmesine dair bkz.; Schreier, 2015, s. 11. Benzer bir tasnife göre ise siber uzay fiziki, sözdizimsel (syntactic) ve anlamsal (semantic) olarak incelenmelidir. Bkz.: Singh, Brahmanand Pratap. (April 2022). *Cyber War,* International Journal of Innovative Research in Science, Engineering and Technology Cilt:11, Sayı:4, s. 3290. Erişim: 27.06.2022 https://www.researchgate.net/publication/360005307_CYBER_WAR

[63] Belirtilenler dışında bazı kaynaklarda siber sistemlerin kontrolünün dördüncü bir bileşen olarak belirtildiği görülmektedir. Bkz.; Korhan, 2017, s. 82.

[64] Schmitt, Michael N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge New York: Cambridge University Press, s. 12.

[65] Aust ve Ammann, 2018, s. 15.

İnternet kullanıcılarının bu tutumunun rızaya dayandığı savunulabilir ise de rızanın bu derece kutsanması ve bireylerin temel hak ve hürriyetlerinin bir parçası olarak kabul edilen internete erişim hakkının rıza şartına bağlanması da tartışmaya açık bir konudur.

Bireylerin kişisel bilgi ve dijital izlerinin bu sisteme kayıtlı olmasının ve bu kayıtların devlet veya örgütlerce kötüye kullanılabilmesinin yarattığı korkunun, çağın yarattığı şartlar altında azaldığı ve gerek bireyler ve gerekse de devletlerin bir çeşit zorunlu teslimiyet halinde oldukları kabul edilmelidir. Zira sadece bireyler değil devletlerin de siber uzaya bağımlılığı gün geçtikçe artmakta, gelişmiş toplumlarda buna paralel bir değişim kendini göstermektedir. Hatta bireylerin internete erişim hakkı pek çok ülke tarafından temel bir hak olarak kabul edilmektedir[66]. Bu noktada ifade edilmelidir ki siber uzayın kapsam alanının genişlemesi uluslararası ilişkilerdeki dengeleri de değiştirmektedir. Bu sayede realist görüşün uluslararası ilişkilerde temel aktör olarak kabul ettiği devlet yerine, liberal görüşe göre birey dâhil olmak üzere devlet dışı aktörlerin siyasal ve toplumsal süreçlerin işleyişindeki öneminin[67] artması hızlanmaktadır.

Yukarıda ifade edilen şartlar altında, gelişmiş devletlerin siber uzaydaki etkinliklerini arttırma yarışına girdikleri, siber uzayın alt yapısını oluşturan omurga sistemlerini kendi kontrolü altında tutma konusunda istekli oldukları görülmektedir. Siber altyapı sistemlerini üreten ülkelerin istihbarat amacıyla bıraktıkları arka kapılar vasıtasıyla casusluk faaliyetleri yapabildiklerine dair veriler dikkate alındığında ABD ve Çin Halk Cumhuriyeti arasındaki siber ve ticari gerilimin nedeni daha iyi anlaşılabilir[68]. Asimetrik

---

[66] Kesan, Lay P. / Hayes, Carol M. (Spring 2012). *Mitigative Counterstriking: Self-Defence and Deterence in Cyberspace*, Harvard Journal of Law & Technology, Cilt:25, Sayı:2. s. 431.

[67] Korhan, Sevda. (2017). *Siber Uzayda Aktör - Güç İlişkisi*, Siber Politikalar Dergisi, Cilt: 2, Sayı:3, s. 75. Erişim: 10.07.2022 https://www.academia.edu/40571066/S%C4%B0BER_UZAYDA_AKT%C3%96R_G%C3%9C%C3%87_%C4%B0L%C4%B0%C5%9EK%C4%B0S%C4%B0

[68] Günümüzde siber güvenlik ticari işletmelerde ana unsurlardan kabul edilmekte ve bu nedenle ticaret savaşları ile siber güvenlik arasında yakın ilişkiler bulunmaktadır. Bkz.; Mikhail, George. *How the USA and China Trade War Caused Cybersecurity Boom*. Erişim: 11.08.2022 https://datasearchconsulting.com/how-the-us-and-china-trade-war-caused-cybersecurity-boom/ ;

bir savaş imkânı sunan siber uzaya ve siber uzayda saldırı ve savunma gücü sağlayan süper bilgisayarlara ve dolayısıyla teknolojik üstünlüğe tek başına sahip olma arzusunda bulunan merkez batı ülkelerinin bu avantajı doğunun yükselen güçlerine bırakmama hedefini her şeyin üstünde tuttuğu görülmektedir.

Bu bağlamda antik çağlardan beri süren doğu-batı mücadelesinin siber çağda da devam ettiği söylenebilir. Özellikle de batı medeniyetini temsil eden Aka'ların Truva Savaşı'nda doğuyu temsil eden Truvalılara karşı kullandığı truva atının güncel türü olan kötücül yazılımların siber savaşların vazgeçilmez yöntemi olması karşısında, süreç içerisinde değişen bir durumun olmadığı söylenebilir.

İnternetin işleyiş şekline bağlı olarak, mevcut DNS sisteminin, ICANN'ın bulunduğu ABD'ye silahlı çatışmalara taraf olan devletlerin ulusal elektronik araçlarının dijital adres alanları üzerinde önemli derecede manipülasyon imkanı sağlamaktadır[69]. Bu açıdan internetin yönetimi konusu devletlerin egemen eşitliği prensibi açısından sorunlu bir alan oluşturur.

İnternetin yönetiminden başka, tartışmalı diğer bir alan olan siber uzayın hukuksal yapısına ilişkin olarak, Antarktika, derin denizler ve dış uzay gibi küresel kamusal mal olarak değerlendirilip değerlendirilmeyeceği konusunda öğretide farklı yaklaşımlar bulunmaktadır. İnsanlığın ortak mirası olarak da adlandırılan bu alanlar devlet egemenliğine ya da özel mülkiyete ait olmadığı gibi bu alanların kullanımı barışçıl amaçlı

Corbin, Kenneth. (16 Mayıs 2019). When Cybersecurity and Trade Wars Collide, *Forbes.* Erişim: 11.08.2022

https://www.forbes.com/sites/kennethcorbin/2019/05/16/when-cybersecurity-and-trade-wars-collide/?sh=4e0090716774

[69] Streltsov, 2017, s. 6. Gelişmiş devletlerin siber uzaydaki etkinliğinin artmakta olduğu ya da "küresel köylerin" ve devlet dışı aktörlerin ulus devletleri tamamen ortadan kaldıracağına dair görüşler için ayrıca bkz.; Korhan, 2017, s. 92.

olmalıdır[70]. Siber uzayın bu kapsamda değerlendirilmesi halinde barışçıl amaçlar dışında kullanılmasının da yasaklanması gündeme gelebilecektir[71].

Bazılarına göre, deniz, hava ve uzayın yanında siber uzay, dördüncü küresel kamusal malı oluşturmaktadır[72]. Bu konuda öncelikle küresel mal kavramının kapsamının belirlenmesi gerekir. Küresel kamusal malın ne olduğunu anlamak için "kamusal malların trajedisi"[73] kavramına değinmek uygun olacaktır. Bu kavram, küresel kamusal malların kendisini yenileyememesine sebep olacak derecede tüketilmesi ve piyasa tarafından üretilememesi nedeniyle en nihayetinde varlıkların yok olmasına sebep olunmasını ifade etmektedir.

Ekonomi-politik açıdan bakıldığında genişletilmiş tanıma göre kamusal mal, kullanımında kimsenin dışlanamadığı ve fiilen ortak tüketimin söz konusu olduğu mallardır[74]. Siber uzayın ise, mevcut yapısı itibariyle özel mülkiyet haklarına tabi fiziki kaynaklara dayanması ve meşru kullanıcı gerekliliği unsurlarını karşılamamasından

---

[70] Bozkurt, Enver / Erdal, Selcen / Poyraz, Yasin. (2017). *Devletler Hukuku.* Ankara: Yetkin, s. 154.

[71] Siber silahlanma ve silahsızlanma konusunda bkz.; Gomez, Miguel Alberto N. (Spring 2016). *Arming Cyberspace: The Militarization of a Virtual Domain,* Global Security and Intelience Studies, Cilt:1, Sayı:2, Makale:5, s. 42-65.; Kasapoğlu, Can. (2017). *Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında,* EDAM Siber Politikalar Kâğıtları Serisi, Sayı:2. Erişim: 21.04.2020

https://edam.org.tr/wp-content/uploads/2017/10/sibersavas_tr_rbs_logo.pdf

[72] Schreier, 2015, s. 13.; ABD Savunma Bakanlığınca 2005 yılında yayınlanan "The Strategy for Homeland Degfence and Civil Support" adlı belgede ciber uzayın küresel kamusal mal olduğu belirtilmiştir. Bkz.; Yousef LI.M., Ahmed. (2018). *Cyber operations between Jus Ad Bellum and below the Threshold of the use of force,* ResearchGate, s. 31. Erişim: 30.08.2022 https://www.researchgate.net/publication/331639155_Cyber_operations_below_the_threshold_of_the_use_of_force_Principle_of_state_sovereignty

[73] Küresel malların trajedisi kavramını ilk kez ortaya atan Hardin'in makalesi için bkz.: Hardin, Garrett. (1968). *Trajedy of the Commons,* Science, New Series, Cilt:162, s. 1244.

[74] Göker, Zeliha. (Temmuz-Aralık 2008). *Kamusal Mallar Tanımında Farklı Tanımlar,* Maliye Dergisi, Sayı:155, s. 113.

dolayı küresel kamusal mal olamayacağı savunulmuştur[75]. Bununla birlikte, öğretide küresel kamusal malların tanımına dair açık bir uzlaşı bulunmamaktadır. İnsan eliyle inşa edilse dahi işlevsel açıdan tüm insanlığa mal olması nedeniyle korunmasının gerekliliği yanında, siber savaş hukukuna göre siber uzayın uluslararası hukuka göre yönetimi gereklilik arz ettiğinden dolayı küresel kamusal bir mal olarak değerlendirilmesi faydalı olacaktır.

Ayrıca ifade edilmelidir ki bir görüşe göre deniz alanlarının kontrol edilmesinin zorluğuna benzer bir durum siber uzayda da geçerli olduğundan siber savaşta J. S. Corbett'e ait olan "denizleri kontrol etmenin yolunun, ağırlıklı olarak deniz iletişimini kontrol etmeye bağlı olduğuna" dair tezin uygulanması mümkündür. Bu görüşün temelinde ise, Corbett'in anılan ilkesinin A. D. Altwies tarafından küresel terörizmle mücadelede benimsenmesi yatmaktadır[76]. Bu görüşün temelinde siber uzayın küresel kamusal mallar kategorisinde değerlendirilmesi bulunmaktadır. Zira deniz savaşlarında olduğu gibi, savaş vasıtasıyla siber uzayın tamamen kontrolü olanaklı bulunmamaktadır. Buna paralel olarak deniz savaşlarında geçerli olan deniz kanallarının kontrolünü ele geçirmek ya da deniz iletişimine hâkim olmak suretiyle dost güçlerin kullanım imkânını güvence altına alırken düşman güçlerin kullanımını önlemek hedefi siber savaşta da uygulanmalıdır.

Siber uzayın beşinci veya küresel kamusal mal olarak kabulü hukuki bağlam dışında yararlıdır. Buna karşın, siber uzayın ve siber operasyonların egemenlik ilkesiyle ilişkili fiziki yapısı göz ardı edildiğinden uluslararası uzmanlar grubu tarafından bu tanım kabul görmemiştir[77]. Zira siber uzayda eylemde bulunan kişiler aynı zamanda gerçek dünyada egemen devletlerin ülke sınırları içinde bazı hukuki sorumlulukları taşıyan insanlar oldukları gibi, siber aktivitelerin gerçekleştirilebilmesine olanak sağlayan aygıtları da aynı hukuki statüye sahip olmaktadır.

---

[75] Kanuck, Sean. (2010). *Sovereign Discourse on Cyber Conflict Under International Law*, Texas Law Review, Cilt:88, s. 1579.

[76] Straub, Jeremy / Traylor, Terry. (2018). *Introduction Marytime Model for Cyber and Information Warfare*, International Conference on Computational Intelligence, s. 26-27.

[77] Schmitt, 2017, *Tallinn Manual 2.0.* s. 12.

Önceleri siber saldırıların siber uzayın sınırlı alanıyla kısıtlandığı genel olarak kabul görmüş olsa da[78] siber uzayın uzun dönemde yol açacağı sosyal etkiler ve sonuçlar henüz net değildir. Siber uzay terimi öncelikle internet ve World Wide Web'i ifade etmekle birlikte insan gayretinin pek çok farklı alanında esaslı değişiklikler meydana getirmiştir[79]. Stuxnet saldırısı ile birlikte, ağa bağlı olmayan kapalı devre bir tesisin dahi siber uzay ile bağlantısının önlenemeyeceği ortaya çıkmıştır. Yaşanan süreçte sadece akıllı telefonlar vasıtasıyla ağa bağlılık artmamış; akıllı ev sistemleri, akıllı televizyon, uydudan kontrol edilebilen araç ve yapay zekânın gelişimiyle birlikte insan yaşamında ve devlet faaliyetlerindeki kritik önem arz eden pek çok sistemin siber uzaydaki yerinin artışıyla siber uzayın genişlemesi kaçınılmaz olmuştur. Siber uzayın etkisinin artmasının bir sonucu olarak geleneksel anlamda temel güç faktörleri olarak kabul edilen askeri ve ekonomik güç yanında siber güç[80] faktörü de yerini almıştır[81].

1.2.SİBER SALDIRI VE DİĞER SİBER FAALİYETLER

Siber faaliyetler öğretide alt başlıklarda farklı şekillerde gruplandırılmakta ve bu yeni alanda terimler üzerinde yeknesaklık bulunmamaktadır. Bazı durumlarda bu faaliyetlerin birleşmeleri nedeniyle geniş anlamda siber saldırı kavramının ya da siber zorla girme kavramı altında siber saldırı ve siber casusluk terimlerinin tercih edildiği[82] görülmektedir. Bu konuda benimsenen tanıma göre farklı sınıflandırmalar yapılmakta, siber faaliyetler siber zorla girme (*cyber intrusion*) genelinde siber saldırı (*cyber attack*), siber harekât/operasyon (*cyber operation*), siber casusluk (*cyber espionage*) ve siber suç (*cyber*

[78] Geers, 2009, s.3.

[79] Betz ve Stevens, 2011, s. 125.

[80] Siber gücün, siber ortama hâkimiyet anlamına geldiğine dair bkz: Sağıroğlu ve Alkan, 2018, s. 200.

[81] Korhan, 2017, s. 81.

[82] Bkz.: Kesan ve Hayes, (Spring 2012). s.440.

crime) ya da siber saldırganlık (*cyberaggression*) genelinde siber suç, siber terörizm (*cyberterrorism*) ve siber saldırı şeklinde tasnif edilmektedir[83].

Siber saldırının tanımlanabilmesi için öncelikle siber faaliyetlerin[84] geniş ölçekte ortaya konulması gerekmektedir. Teknolojinin gelişmesi sonucu kendini gösteren zararlı siber faaliyetlerin sınıflandırılması konusunda öğretide ve devlet uygulamalarında farklı yaklaşımlar söz konusudur. Zira bir devlete yönelik gerçekleştirilen zararlı bir siber faaliyetin uluslararası hukuk kapsamında hukuka aykırı bir eylem olarak nitelendirilip nitelendirilmeyeceğinin, bir diğer ifadeyle uluslararası hukuk kurallarına aykırılık teşkil etmeyen casusluk gibi bir eylem olup olmadığının belirlenmesi noktasında siber saldırı kavramının tanımlanması önem arz etmektedir.

Bu bağlamda mevcut savaş hukukunun siber savaşa nasıl uygulanacağı sorusu ancak bir devletin siber saldırı olarak algıladığı şeye karşı hukuki olarak güç kullanabileceğinin belirlenmesi suretiyle cevaplanabilir[85]. Siber faaliyetlerin siber saldırı olarak kabulü kuvvet kullanımı yasağını gündeme getirebilirken, aksi durumda kuvvet kullanma yasağına girmeyen casusluk ya da zorlama eylemlerini de oluşturabilmektedir.

Aynı şekilde BM Şartı ve yapılageliş hukuku gereğince uluslararası hukuk alanında sorumluluğu bulunan uluslararası hukuk kişilerinin siber eylemleri ile sadece ulusal hukuk kapsamında sorumluluk gerektiren siber suç faillerinin eylemlerinin de ayrılması gereklidir. Bahse konu terimler birbirlerine yakın anlamlar taşımakta ve bu faaliyetler birbiriyle iç içe giren eylemlerden oluşabilmektedir. Bir siber faaliyetin hangi durumlarda

---

[83] Stahl, 2011, s. 270.

[84] Tallinn El Kitabı'nda siber faaliyet, siber altyapı tesislerinin işletilmesine etki etmeye yönelen ve siber altyapı unsurlarının kullanımını ya da siber araçların yerleştirilmesini gerektiren eylemler olarak tamınlanmıştır. Ayrıca siber faaliyetlerin siber operasyonları kapsadığı ama bununla sınırlı olmadığı belirtilmiştir. Schmitt, 2017, *Tallinn Manual 2.0.* Glossary, s. 564.

[85] Graham, David E. (2010). *Cyber Threats and the Law of War,* Journal of National Security Law and Policy, Cilt:4:87, s. 87. Erişim: 23.04.2020 https://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf

siber operasyon, siber saldırı, siber casusluk ya da siber zorlama oluşturduğunu tespit etmek eyleme karşı verilecek cevabı da belirleyecektir.

Siber uzayda gerçekleşen eylemlerin çoğunluğunun finansal temelli olduğu görülmektedir[86]. Bu tür eylemler kar amacı elde etmeye yönelik kriminal faaliyetler olduğundan siber suçlar kapsamında değerlendirilmektedir. Siber faaliyetleri gerçekleştirenlerin bazılarının ise politik bir amaçla hareket etmesi nedeniyle bu eylemler hacktivizm olarak adlandırılmaktadır. Bu politik dürtü bir devlet lehine, vatanseverlik içeren bir harekette kendini gösterebileceği gibi, hayvan hakları ve çevrenin korunması gibi kişisel politik bir şekilde ya da sırf holiganizm/vandallık amaçlı da gerçekleşebilmektedir. Siber faaliyetlerin kişilerin ötesinde bir devlet ya da devlet destekli gruplar tarafından gerçekleştirilmesi halinde ise eylemin uluslararası niteliği ön plana çıkmakta ve siber operasyon ya da siber saldırıdan bahsetmek mümkün olabilmektedir.

Burada dikkat edilmesi gereken husus siber saldırı kavramının dar anlamda kullanılarak genel anlamda siber faaliyetlerden ayrılmakta olmasıdır. Genel anlamda bir siber saldırı ya da operasyon, barış dönemini de kapsayan siber casusluk, siber terörizm ve siber suçları da kapsayan tüm siber faaliyetleri de içermekte iken dar anlamda siber saldırı kavramı uluslararası hukuk dâhilinde devlet eylemi olan ya da bir devlete atfedilebilir olan kuvvet kullanma niteliğindeki faaliyetleri kapsamaktadır. Bu bağlamda siber operasyon ile dar anlamda siber saldırı terimlerinin faklı hukuki anlamlar taşıdığı göz önünde bulundurulmalıdır.

[86] Lindsay, Jon R. (2013). *Stuxnet and the Limit of Cyber Warfare*, Security Studies. s. 9. Erişim: 28.06.2022 https://www.scinapse.io/papers/1972914161

Siber operasyon[87], siber saldırı terimini de kapsayan daha geniş bir anlam taşır. Siber operasyon, Uluslararası Kızılhaç Komitesi raporunda, veri akışı yoluyla bir bilgisayara veya bilgisayar sistemine karşı ya da bunlar üzerinden gerçekleştirilen operasyonlar olarak ele alınmıştır[88]. Tallinn El Kitabı'nda ise siber uzay vasıtasıyla ya da siber uzayda amaca ulaşmak için siber kapasitenin kullanılması olarak tanımlanmıştır[89]. Ancak belli bir zarar eşiğine ulaşmış siber operasyonlar siber saldırı olarak nitelendirilmektedir[90]. Siber saldırı, Tallinn El Kitabı Kural 92'de kişilerde yaralanma veya ölüm, nesnelerde hasar ya da yıkıma sebep olması makul şekilde beklenen saldırı veya savunma şeklindeki siber operasyon olarak belirtilmiştir[91]. Burada sebep olunan olumsuz etkiler hedeflenen siber sistemlerle sınırlı olmayıp, siber sistemler üzerinde bir hasar bulunmasa dahi örneğin baraj sularının serbest bırakılmasına sebep olan SCADA (*Supervisory Control And Data Acquisition* / Veri Tabanlı Kontrol ve Gözetleme Sistemi) sisteminin manipüle edilmesi sonucunda çok daha ağır sonuçlar ile karşılaşılması mümkündür[92]. İfade edilmesi gerekli bir diğer husus, siber saldırı olarak kabul edilebilecek savunma niteliğindeki siber eylemin ancak aktif savunma şeklinde gerçekleşmesi gereğidir. Zira pasif savunma niteliğindeki siber güvenlik uygulamaları siber saldırı kapsamına girmemektedir.

Yöntem ve araçların sebep olduğu sonuçlar itibariyle saldırı unsurlarını taşımadıkça, tek başına saldırı olarak kabul edilmeyen siber casusluk konusunda Uluslararası Uzmanlar

---

[87] Tallinn El Kitabı'nda siber operasyon, siber uzaydaki veya siber uzay aracılığıyla hedeflere ulaşılabilmesi için siber yeteneklerin kullanılması olarak tamınlanmıştır. Schmitt, 2017, *Tallinn Manual 2.0.* Glossary, s. 564.

[88] Gül, Yunus Emre. (2021). *Savaş Hukuku 2.0 Siber Saldırılar ve Hukuk*, İstanbul: Hukuk Akademisi, s. 28.

[89] Schmitt, 2017, *Tallinn Manual 2.0.* s. 564.

[90] Gül, Yunus Emre. (2019). *Devletler Düzeyinde Siber Zorlama Faaliyeti*, Düşünce Dergisi, Sayı:11, s. 42. Erişim:18.12.2021 https://www.researchgate.net/publication/351054846_Devletler_Duzeyinde_Siber_Zorlama_Faaliyeti

[91] Schmitt, 2017, *Tallinn Manual 2.0.* s. 415.

[92] Schmitt, 2017, *Tallinn Manual 2.0.* s. 416.

Grubu'nda fikir birliği bulunmaktadır. Buna paralel olarak sivil nüfus üzerinde rahatsızlık yaratma eylemleri konusunda da aynı görüş hâkimdir. Uzmanlar Grubunca "*inconvenience*" kavramı üzerinde uzlaşma bulunmamakla birlikte sivil nüfus üzerinde rahatsızlık oluşturan (*inconvenience*) siber operasyonların saldırı seviyesine ulaşmadığı kabul edilmektedir[93]. Siber casusluk ile benzerlik taşıyan ve belirli durumlarda hukuka aykırı sayılmayan siber zorlama (*cyber coercion*) ise siber zorla girmeden de farklı bir anlam taşır. Kişilerin birbirleri üzerine siber uzayda baskı yapmaları siber zorbalık (*cyber bullying*) olarak adlandırılırken devletler düzeyinde bu durum siber zorlama (*cyber coercion*) olarak ifade edilmektedir[94]. Bazı devletlerce siber zorlama içişlerine karışma yasağı kapsamında değerlendirilmektedir[95].

Siber faaliyetlerden bir diğeri olan propaganda, siyasi amaçlı bilgi yaymaya yönelik olarak gerçekleştirilmektedir. Geleneksel propaganda yöntemlerine nazaran siber propagandanın çok daha kolay ve etkili şekilde uygulanması, siber yöntemleri fazlasıyla cazip hale getirmektedir[96]. Siber propaganda yönteminin kullanılması da sivil halkı ya da savaşçıları ikna etmeye yönelik eylemler olması nedeniyle silahlı saldırı seviyesine ulaşmamaktadır. 2003 yılında ABD tarafından Irak'a gerçekleştirilen işgal harekâtında gerek uçaklar ve gerekse de telefon kısa mesajları vasıtasıyla gerçekleştirilen propaganda faaliyetlerinin Irak askerlerinin çatışmadan teslim olmalarına sebep olduğu görülmüştür. Gelecekte dünyanın herhangi bir yerinde meydana gelebilecek çatışmalarda aynı yöntemin daha kolay ve etkili biçimde siber propaganda vasıtasıyla gerçekleştirilmesine tanık olmamız kaçınılmaz görünmektedir.

---

[93] Schmitt, 2017, *Tallinn Manual 2.0.* s. 418.

[94] Gül, 2019, s. 42.

[95] Position Paper. (2021). *On the Application of International Law in Cyberspace*, s. 5. Erişim: 04.08.2022, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

[96] Hruza, Petr / Cerny, Jiri. (2017). *Cyberwarfare,* International Cenference Knowledge-Based Organization, Cilt:23, Sayı:1, s. 157. Erişim: 25.01.2022 https://www.researchgate.net/publication/318737253_Cyberwarfare

Radyo korsanları olarak bilinen sivil havacılık faaliyetlerine radyo frekansları üzerinden müdahale edilmesi eylemlerinin siber saldırı oluşturup oluşturmayacağı[97] konusuna gelince, bilişim teknolojisi kullanılmaksızın gerçekleşen bu tür eylemler yönünden sivil havacılıkta iletişim amaçlı kullanılan radyo frekanslarının karıştırılması suretiyle uçuşun tehlikeye atılması geleneksel bir müdahale yöntemidir. Genel olarak radyo iletişimine ve televizyon yayınlarına yapılan müdahale eylemlerinin geleneksel olarak silahlı çatışmalar hukuku anlamında saldırı eylemine dâhil edilmemesi nedeniyle Tallinn El Kitabı'nda siber operasyonların bu eylemleri kapsamadığı belirtilmiştir[98].

1.2.1. SİBER SALDIRI

İlk siber saldırı fikrinin kamu bilincine yerleşmesi 1983 tarihli *WarGames* isimli bilim-kurgu filmiyle olmuştur[99]. Filmin konusunu oluşturan, bilgisayar oyunu firması hacklenmek isterken kazara nükleer savaş oyunu için tasarlanmış bir deneysel askeri süper bilgisayara sızılarak neredeyse III. Dünya Savaşı'na sebep olunması, kamuoyunda olası bir nükleer savaş korkusunu tetiklemiş ve ilk ulusal siber güvenlik politikasının ortaya çıkmasına sebep olmuştur[100]. Film çok gerçekçi kurgulanmıştır ve iyi bir araştırmaya dayanmaktadır; filmin ne kadar iyi olduğu da ön gösterisi yapıldıktan sonra bu filmin etkisiyle veri bankalarına giren Ronald Mark Austin'in tutuklanmasından anlaşılabilmektedir[101].

---

[97] Akkutay, Ali İbrahim. (Ekim 2017). *Sivil Havacılığa Yönelik Gerçekleştirilen Siber Saldırılar: Uygulanacak Uluslararası Hukuk Kuralları, Yetki ve Sorumluluk*, Yıl: 8, Sayı: 32, s. 172.

[98] Schmitt, 2017, *Tallinn Manual 2.0.* s. 418.

[99] Betz ve Stevens, 2011, s. 19.

[100] Ayrıntılı bilgi için bkz.; https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html Erişim: 20.03.2020)

[101] Aust ve Ammann, 2018, s.219.

Bunun sonucunda Amerikan toplumunda ortaya çıkan bu siber Pearl Harbor korkusunun[102] gerçek bir tehditten kaynaklanmayıp farkındalığı ve eyleme yönelik motivasyonu arttırmak amacıyla bu korkunun kullanıldığı haklı olarak ileri sürülmüştür[103]. Buna karşın bu güne değin korkulanın aksine dehşete düşüren bir siber saldırı ya da siber operasyon sonucu gerçekleşen bir nükleer bir patlamanın yaşanmaması bu korkutma fikrini akla getirmekte ise de bugüne kadar yaşanmamış olması gelecekte yaşanmayacağı anlamına da gelmemektedir. Bu bağlamda, ulusal ve uluslararası düzeyde siber güvenlik politikalarının geliştirilmesinin hayati bir öneme sahip olduğu söylenebilir. 2005 yılında Amerikan Hava Kuvvetleri'nin görevini yeni bir alana genişleterek "havada, uzayda ve siber uzayda uç ve savaş" sözünü benimsemesi sonrasında, toplam çatışma alanlarındaki birleşik askeri operasyonlar arasında, siber operasyonlar hayati önemde ulusal çıkarlar arasına alınmıştır[104]. Bu durum günümüzde siber tehdidin uzak bir olasılık olarak görülmediğini göstermektedir.

Siber saldırı konusunun uluslararası hukuk ve akademik çevrelerce ilgi ve endişe konusu olması 1990'ların sonlarına rastlamaktadır[105]**.** Gelinen noktada asimetrik çatışmaların ve ekonomi savaşlarının ortaya çıkmasıyla birlikte nükleer güç dengesinin korunması doktrininin de demode olduğu, geleneksel veya nükleer bir güce sahip daha büyük bir ordunun siber savaşı kazanacağının bir garantisinin olmadığı, zira hiçbir silah sisteminin

---

[102] İlk olarak 2000 yılında ABD başkanlık eski özel danışmanı Richard Clarke tarafından ortaya atılan "Dijital Pearl Harbor" fikri üzerine siber suçların ve siber casusluğun şaşırtıcı yükselişi karşısında ulusal güvenlik uzmanlarının bu konudaki cevap arayışı ulusal kritik alt yapı unsurlarına yönelik ağır bir siber saldırnın an meselesi olduğu yönünde olmuştur. Bkz.: Geers, 2009, s.2.

[103] Lawson, Sean. (7 Aralık 2016). Does 2016 Mark the End of Cyber Pearl Harbor Hysteria? *Forbes.* Erişim: 02.05.2020

https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#35dcff0522c2

[104] Convertino, Sebastian M. / DeMattei, Lou Anne / Knierim, Tammy M. (2007). *Flying and Fighting in Cyberspace.* Alabama: Air University Press, s. 1.

[105] Weglinski, Konrad. (2016). *Cyberwarfare and Responsibility of States*, Torun International Studies, Cilt:1, Sayı:9, s. 79.

internete dayalı bir teknoloji olmadan çalışmadığı savunulmaktadır[106]. Buna göre teknolojik üstünlüğün uluslararası güç dengesinde yaratacağı çok önemli sonuçlar bulunmaktadır. Bir devlet için siber kapasitenin geliştirilmesi, en karmaşık silah sistemlerine sahip olmaya eşdeğer bir avantaj sağlayabilecektir.

Bilişim teknolojisinin gelişim sürecinde, ilk dönemde bilgisayar saldırısı (*computer attack*) terimi kullanılmış olup siber saldırı teriminin sonraları ortaya çıktığı görülmektedir. 2015 tarihinde Rusya Federasyonu ile Çin Halk Cumhuriyeti arasında yapılan uluslararası antlaşmada "*computer attack*" kavramı, bilgisayar yazılımı kullanılarak bilişim sistemlerine, bilişim ve telekomünikasyon ağlarına, elektronik iletişim ağlarına ve otomatik işlem kontrol sistemlerine işlenen bilginin emniyet ve güvenliğini tehlikeye atma, işlevini bozma amacıyla gerçekleştirilen kasti müdahale olarak tanımlanmıştır[107].

Benzer şekilde Hava ve Füze Savaşı'na Uygulanabilir Uluslararası Hukuk Kitapçığı'nda, siber saldırı yerine bilgisayar ağ saldırısı (*computer network attack*) terimi kullanılmış ve bilgi operasyonunun bir şekli olduğu belirtilerek, bir bilgisayar veya bilgisayar ağı üzerinde kontrol elde etmek için bilgisayar ağını veya bilgisayar ağı veya bilgisayardaki bilginin manipüle edilmesi, bozulması, engellenmesi, ayrıştırılması veya yok edilmesi operasyonu şeklinde ifade edilmiştir[108]. Ayrıca Hava ve Füze Kitapçığı'nda Tallinn El Kitabıyla uyumlu şekilde, kişi veya nesnelerde hasar, yıkım, yaralama veya ölümle sonuçlanmayan istihbarat toplama, propaganda veya diğer askeri faaliyetler saldırı tanımına dâhil edilmemiştir[109].

---

[106] Aust ve Ammann, 2018, s.341.

[107] Streltsov, 2017, s. 6.

[108] Harvard Program on Humanitarian Policy and Conflict Research, *Commentary on the HPCR Manual on International Law Applicable to Air and Misslile Warfare*, (2010), s. 34. Benzer bir tanımlama için bkz.; Waxman, Matthew C. (2013). *Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions,* US Naval War Collage International Law Studies, Cilt:89, s. 109.

[109] Harvard Program on Humanitarian Policy and Conflict Research, *Commentary on the HPCR Manual on International Law Applicable to Air and Misslile Warfare.* (2010), s. 28.

Geleneksel anlamda silah teriminin saldırı veya savunmaya uygun veya teknik olarak kullanışlı herhangi bir araç manasına gelişinden yola çıkan Rus uzmanlara göre, bilgi ve iletişim teknolojisi silah olmayıp Rusya Federasyonu ile Belarus ve Çin Halk Cumhuriyeti arasındaki bilişim teknolojisi güvenliği antlaşmalarında kullanılan bilgi silahları (*information weapons*) kavramı, bilgi savaşında (*information warfare*) kullanılan yöntem ve araçları ifade eder [110] . Konvansiyonel çatışmalara ait terimlerin yeni teknolojiye ve siber uzaya geleneksel bakış açısıyla uygulanması bu çeşit görüşlere sebep olmaktadır. Bilgi ve iletişim teknolojisinin siber saldırılarda kullanılarak konvansiyonel silahlardan daha etkili sonuçlara ve zararlara sebep olunması nedeniyle bu görüşün gelinen noktada genel kabul görmeyeceği ise açıktır.

Bu noktada saldırı kavramının geleneksel anlamının siber saldırı yönünden nasıl değerlendirildiğine bakmakta fayda bulunmaktadır. 1949 tarihli Cenevre Konvansiyonu'na Ek 1977 tarihli 1. Protokol'ün 49. maddesinde saldırı (*attack*) "savunma (*defence*) ya da taarruz (*offence*) şeklinde rakibe karşı gerçekleştirilen şiddet eylemleri" olarak tanımlanmıştır[111]. Bu tanımlama, siber operasyonların kinetik olmayan doğası itibariyle hangi boyutta şiddet eylemleri olarak değerlendirilebileceği ve buna göre uluslararası insancıl hukuk kapsamında saldırı oluşturabileceği konusunda önemli bir tartışma başlatmıştır[112]. Tallinn El Kitabı'nda, siber saldırı açısından Ek Protokol'deki "şiddet eylemleri" kavramının yalnızca kinetik gücün serbest kalması olarak anlaşılmayacağı, kinetik etki taşımayan kimyasal, biyolojik ve radyolojik saldırılarda olduğu gibi siber saldırıda da yıkıcı sonuçların operasyonun saldırı olarak kabulünü sağlayacağı kabul edilmektedir[113].

---

[110] Streltsov, 2017, s. 6.

[111] International Commitee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (1987), s. 601.

[112] Melzer, 2011, s. 25.

[113] Schmitt, 2017, *Tallinn Manual 2.0.* s. 415-416.

Siber saldırı tanımlarından biri de; *"siber saldırı, bir bilgisayar ağının işlevlerini siyasi ve ulusal güvenlik amacıyla zayıflatmak için yapılan her türlü eylemlerden oluşur"* [114] şeklindedir. Siber saldırının bu tanımı siber savaşın savunma ya da saldırı biçiminde gerçekleşebileceği kabulü ile de uyumludur[115]. Bu tanıma göre eylem aktif olmalı, saldırı veya aktif savunma niteliğinde gerçekleşmelidir. Bir diğer ifade ile antivirüs programların saldırıyı tespiti ve engellemesi faaliyetleri siber saldırı olarak nitelendirilemeyecektir. Aktif savunma söz konusu olduğunda saldırıya uğrayan bir devletin siber saldırıdan korunmak amacıyla ateş duvarı ya da antivirüs programlarını kullanmasından daha öteye gidilerek saldırgana yönelik derhal bir karşı saldırı gerçekleştirilmektedir.

Yine aynı tanımda siber saldırının siyasi ve ulusal güvenliğe yönelik bir amaç taşıması, siber saldırının siber suç ile olan farkını ortaya koymaktadır[116]. Zira siber saldırının altında yatan dürtünün siyasi olmasına karşın siber suçta finansal kaygılar ön plana çıkmaktadır [117] . Roscini siber saldırıyı, siber gücün hasmane kullanımı şeklinde tanımlamakta, bunun münferit bir eylem veya silahlı bir çatışmanın ilk darbesi veya zaten başlatılmış silahlı bir çatışma bağlamında bir saldırı veyahut önceki konvansiyonel veya siber saldırıya karşı bir tepki oluşturabileceğini ifade etmektedir[118]. Bu noktada siber saldırının geleneksel bir saldırının bir parçasını oluşturmasının da mümkün olduğu ifade

---

[114] Hathaway, Oona A. / Crootof, Rebecca / Levitz, Philip / Nix, Haley / Aileen, Nowlan / Perdue, William / Spiegel, Julia. (2012). *The Law of Cyber-Attack.* California Law Review, Cilt:100, s. 826.

[115] Hruza ve Cerny, 2017, s. 157.

[116] Ayrıntılı bilgi için bkz.; Hathaway ve diğerleri, 2012, s. 830.

[117] Mukherjee, Sourav. Cyber warfare and Implications, s.3. Erişim: 27.06.2022 https://deliverypdf.ssrn.com/delivery.php?ID=611103021078106112122000084119065112034072042037055057122116099022104008025122084096028012000000098030047022007074095119104098111025000087019002007009066025112066105066009032027079000123002122091009110077113003030097074107127016097016118005109120097096&EXT=pdf&INDEX=TRUE

[118] Roscini, Marco. (2010). *World Wide Warfare-Jus ad bellum and the Use of Cyber Force*, Max Planck Yearbook of United Nations Law, Cilt:14, s. 96.

edilmelidir. Kinetik bir saldırıda hedef ülke savunmasının bir siber operasyon ile etkisiz hale getirilmesi buna örnek gösterilebilir[119].

Siber saldırının bu farklı tanımlamalarının sebebi, farklı yaklaşımların benimsenmesinden kaynaklanmaktadır. Bu konuda üç farklı yaklaşımdan bahsedilebilir. Bunlar; saldırının ardındaki dürtüyü esas alan "*objective-based approach*", saldırının hedef aldığı nesneleri ölçüt olarak alan "*target-based approach*" ve saldırının sonuçlarına odaklanan "*effect-based approach*"tur[120]. Daha sonra ayrıntılı şekilde bahsedilecek bu yaklaşımlardan etki ya da sonuç odaklı olan sonuncu gerek Tallinn El Kitabı'nda ve gerekse genel olarak öğretide genel kabul görmektedir.

Siber saldırı tanımının, uluslararası silahlı çatışmalarda olduğu gibi, uluslararası olmayan silahlı çatışmalarda da uygulanacağı kabul edilmektedir[121]. Bu bağlamda siber saldırıyı gerçekleştiren aktörün sadece devlet olması gerekli değildir. Bu tür bir saldırı devlet dışı aktörler tarafından da gerçekleştirilebilmektedir[122]. Buna karşın bir devlete atfedilebilir olmayan devlet dışı aktörlerin eyleminden dolayı bireylerin, uluslararası hukuk kapsamındaki sorumluluğuna olanak tanıyan uluslararası cezai sorumluluğu haricinde ancak ulusal hukuk dâhilinde sorumlu olacağı unutulmamalıdır[123].

Siber operasyonların ölüm, yaralanma ve yok etmeye sebep olması durumunda şiddet eylemi ve saldırı olarak kabul edilmesi düşüncesi genel bir destek bulmuş ise de; öldürme, yaralama ve yok etme durumu söz konusu olmaksızın sırf yakalama veya etkisiz hale

---

[119] Schmitt, 2017, *Tallinn Manual 2.0.* s. 419.

[120] Gül, 2021, s. 29-30.

[121] Schmitt, 2017, *Tallinn Manual 2.0.* s. 415.

[122] Ayrıntılı bilgi için bkz.; Hathaway ve diğerleri, 2012, s. 830.

[123] Zira benzer bir görüşe göre; devlet dışı örgütlerin gerçekleştirdiği siber saldırıların kuvvet kullanma yasağı kapsamında değerlendirilmesi BM Şartı'nın suiistimaline yol açacağından ve meşru müdafaa hakkının kullanılabileceği yorumuna sebep olabileceğinden karşıt görüş benimsenmemektedir. Bu konuda bkz.: Erdem, Merve / Özocak, Gürkan. (2019). *Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü.* Ankara Üniversitesi Dergisi, Sayı: 68, s. 136.

getirmeyi (*neutralize*) amaçlayan siber operasyonlar konusunda öğretide farklı görüşler ortaya çıkmıştır[124]. Uluslararası Uzmanlar Grubu, ciddi hastalık ve şiddetli zihinsel acıyı yaralanmaya eşit görerek, insancıl amaçlara dayanan silahlı çatışmalar hukuku ışığında kişilerde yaralanma ve ölüme sebep olan yaralanma tanımına dâhil etmektedir[125]. 1977 tarihli Ek Protokol'ün 51/2 maddesinde ana amacı sivil nüfus üzerinde terörü yaymaya yönelik şiddet eylemi ve tehdidi yasaklanmıştır[126].

Uluslararası Uzmanlar Grubu, siber araçların bir nesnenin işlevselliğini etkilemesinin bozma ya da hasar olarak değerlendirilip değerlendirilmeyeceği konusunda yoğun fikir ayrılıkları taşımaktadırlar. Çoğunluk görüşüne göre, işlevselliğin düzeltilebilmesi için fiziki bileşenlerin değiştirilmesinin gerekmesi halinde siber operasyonun bir saldırı olarak kabulü gerekir[127]. Örneğin, çoğunluğa göre siber araçların kullanılması suretiyle elektrik dağıtım tesisinin işleyişine müdahale edilmesi sonucunda faaliyetin durması nedeniyle kontrol sisteminin ya da hayati bileşenlerin değiştirilmesi gerektiğinden eylem saldırı olarak kabul edilmelidir.

Çoğunluk içinde bazı uzmanlar daha da ileri giderek, işlevselliğe müdahalenin, bu tür sistemlerin işleyişi için gerekli işletim sistemi ya da özel verilerin yeniden kurulumunu gerektirmesi halini de kapsaması gerektiğini ileri sürmektedirler[128]. Diğer bazılarına göre ise, bir nesnenin ne şekilde işlev dışı bırakıldığı önemsizdir. Buna göre, siber altyapı unsurunun kullanılabilirliğinin kaybı saldırının varlığı için yeterli nitelikte bir hasar kabul edilmelidir[129].

---

[124] Melzer, 2011, s. 25.

[125] Schmitt, 2017, *Tallinn Manual 2.0.* s. 417.

[126] International Commitee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, (1987), s. 613.

[127] Schmitt, 2017, *Tallinn Manual 2.0.* s. 417.

[128] Schmitt, 2017, *Tallinn Manual 2.0.* s. 417.

[129] Schmitt, 2017, *Tallinn Manual 2.0.* s. 418.

Bu konuda benimsenecek yaklaşımın siber operasyonun silahlı bir saldırı eşiğine varıp varmadığının tespiti yönünden çok önemli olduğu gözden uzak tutulmamalıdır. "*Titan Rain*" olarak adlandırılan 2003 yılında ABD Savunma Departmanı'ndan veri sızdırılması, 2010 yılında Çin Halk Cumhuriyeti'ndeki bilişim korsanları tarafından Google'dan veri kopyalanması, "*Operation Aurora*" ve Mart 2011 tarihinde ABD Savunma Departmanı'ndan 24.000 Pentagon dosyası sızdırma eylemleri siber casusluk veya siber istismar mahiyetinde olduğundan bazılarınca siber saldırı olarak kabul edilmemektedir[130]. Yine Aramco saldırısı sonucunda yüzlerce dâhili bellekte meydana gelen zararın nitelendirmesine göre saldırının silahlı bir saldırı oluşturup oluşturmadığının tespiti aynı zamanda meşru müdafaa hakkının varlığını da belirleyecektir. Aynı şekilde kritik altyapı tesislerine yönelik olarak gerçekleştirilecek siber faaliyetlerin nitelendirilebilmesi yönünden objektif kıstasların ortaya konulması oldukça önemlidir.

Çatışmaların ilk aşamasında genel olarak siber saldırılar bilişim, iletişim ve kritik altyapı sistemlerini (örn.; enerji endüstrisi, finans, ulaşım, telekomünikasyon ve sağlık sistemleri gibi) hedef almaktadır. Bu doğrultuda siber saldırılar ile bu sistemlerin komuta kontrol sistemlerini bozmak, konvansiyonel askeri kapasitesini ve devletin çatışmaya hazır olma halini azaltmak amaçlanmaktadır [131] . Olası siber saldırı türleri üç kısımda incelenmektedir[132]. Bunlar ilk olarak, iletişim altyapısının hedeflenerek tüm ülkenin internet erişiminin sona erdirilmesidir. İkincisi, hava, kara veya demir yolu ulaşım sistemlerinin hedeflenerek ciddi kazalara sebep olunmasıdır. Son olarak, içme suyu temini, baraj, gıda dağıtım sistemleri, elektrik dağıtım sistemleri, enerji istasyonları ve yakıt veya nükleer güç güvenlik sistemleri gibi hayati öneme sahip altyapı sitemlerine

---

[130] Ayrıntılı bilgi için bkz.; Hathaway ve diğerleri, 2012, s. 829.

[131] Hruza ve Cerny, 2017, s. 156.

[132] Afroditi, Papanastasiou. (2010). *Application of International Law on Cyber Warfare Operations*, s. 9. Erişim: 23.04.2020, https://poseidon01.ssrn.com/delivery.php?ID=904114091001094030071081005075016112117009040087024023014000092108095082074007118117124123020032031057028101069083067090119076109033095005041121095065083018093023067042082017120016093080097114086124070119127120114019021125119085097082001000124123112017&EXT=pdf

saldırıdır. Bu değerlendirmede dikkat çeken nokta bir siber saldırının hedefinin çoğunlukla kritik alt yapı tesisleri olmasıdır.

Daha sonra da belirtileceği gibi bir siber saldırının nitelendirilmesinde en önemli unsur saldırının *etkileri* olsa da siber saldırıların işleniş şeklinin (*modus operandi*) teknik yönden analiz edilmesi tasnif konusunda bize yardımcı olacaktır. Bazı devletler bir siber saldırının işleyişine ilişkin olarak Lockheed Martin adlı bir Amerikan şirketi tarafından geliştirilen "*Cyber Kill Chain*" sistemini benimsemektedir[133]. Bu sisteme göre siber saldırılar 7 adımda gerçekleşmektedir. Bunlar; hedefin belirlenmesine yönelik keşif (*reconnaissance*), zararlı yazılımın üretimi suretiyle silah haline getirme (*weaponization*), zararlı yazılımın hedef sisteme yerleştirilmesi (*delivery*), erişim sağlamak suretiyle zafiyetten yararlanma (*exploitation*), arka kapı açma (*installiation*), uzaktan komuta ve kontrol etme (*command and control*) ve amaca yönelik eylem (*action on objectives*) şeklindedir[134]. Zararlı yazılımın silah haline getirilmesi terimi, tıpkı kinetik silahlarda olduğu gibi, aracın aksama veya yok etme için kullanılmasının amaçlanması manasına gelir[135].

---

[133] Bu konuda bkz.: Rølsåsen, Thea Helen Eriksen. (2016). When do Cyber Operations Amount to Use of Force and Armed Attack, and What Response will They Justify?, Master Thesis, University of Oslo, s. 12. Erişim: 26.06.2020 https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1&isAllowed=y

[134] Sunum için bkz.: Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defence, Lockheed Martin, s. 1-10, Erişim: 27.06.2020 http://cdn2.hubspot.net/hubfs/91979/Gaining_the_Advantage_Cyber_Kill_Chain.pdf?t=1459783725510&utm_campaign=Commercial+Cyber&utm_source=hs_automation&utm_medium=email&utm_content=21881761&_hsenc=p2ANqtz-8cr09K-ZaN2zypp5DVXY61NM8WOUa8WolIWEbmilZIHlySlNuHD7D1cuB8wAoAqDTklkdr2mYB_jz-RhLIlVS_LjK3Zg&_hsmi=21881761

[135] Rølsåsen, 2016, s. 20.

1.2.2. SİBER PROTESTO VE HACKTİVİZM

Tarihi yönden bakıldığında, siber protesto ya da hacktivizmin aktörleri olan siber korsanların gerçek dünyadan etkilendiği ve gerek yöntem ve gerekse semboller itibariyle tarihi olaylardan ilham alındığı görülmektedir. Örneğin, hacktivist ya da web gerillası olarak da adlandırılan Anonymus'un simgesel yüzü olan Guy Fawkes maskesi, 1980'li yıllarda revaçta olan çizgi roman *V for Vendetta'*ya aittir. Guy Fawkes, 05 Kasım 1605 tarihinde 36 adet karabarut fıçısı kullanarak Kral 1. James, hükümet üyeleri, milletvekilleri ve lordlar ile birlikte İngiliz Parlamentosu'nu havaya uçurmayı düşünürken suç ortağının ihaneti nedeniyle başarısız olmuş ve darağacında tabureden bizzat atlayarak ölmeyi tercih etmiştir[136]. Guy Fawkes'in ölüm tarihi İngiltere'de uzun süre bayram olarak kutlanmış ise de 80'li yıllardan itibaren direnişin sembol yüzü haline gelerek kahramanlaştırılmıştır.

Tarihsel süreçte şekil değiştiren korsanlık siber uzayda hacktivizm olarak anılmaya başlamış ve daha eğitimli olan bilişim korsanları meşruiyet kaynağı olarak belirli etik ilkelere dayanma gereği duymuşlardır. "Bilgisayar Devriminin Kahramanları" isimli temel eserinde Amerikalı yazar Steven Levy, bilişim korsanı etiğini yazmış ve kitabında şunları ifade etmiştir:

> *"Dünyadaki olayları anlamaya yardımcı olan tüm bilgilere ve bilgisayara erişim her bir birey için, sınırsız ve kapsamlı olmak zorundadır. İştirakçılık prensibi her yerde geçerlidir. Tüm bilgiler bedava olmalıdır. Otorite olanlara itimat etme! Bilişim korsanlarını diploma, yaş, ırk veya statü gibi eskimiş ölçütlere göre değil, eylemlerine göre değerlendir!"*[137]

Bu etik ilkeler, internetin ve bilginin özgürlüğünü savunmanın yanında, hacktivizmin ve otoriter yaklaşımlara karşı gerçekleştirilen itaatsizliklerin meşruiyetini sağlamaktadır.

---

[136] Ayrıntılı bilgi için bkz.: Aust ve Ammann, 2018, s. 261-262.

[137] Aust ve Ammann, 2018, s. 224.

Siber korsanların gerçekleştirdikleri çeşitli saldırıların temelinde hangi dürtünün bulunduğunu tespit etmek saldırının sınıflandırılmasına olanak sağlamaktadır. Bazı bilişim korsanları siber operasyonları çevre, insan ve hayvan hakları gibi kişisel politik sebeplerden dolayı gerçekleştirmektedir[138]. Saldırganları bu eyleme iten sebepler 2002-2004 yılları arasındaki dönemde araştırılmış ve bu saldırıların sadece eğlence için, web sitelerinden intikam almak için, politik sebeplerden dolayı, meydan okuma amacıyla, en yıkıcı olmak için ya da vatanseverlik adı altında gerçekleştirildiği belirlenmiştir[139]. Siber faaliyetlerin gerçekleştirilmesindeki saik, bu saldırı türlerinin sınıflandırılabilmesini sağlamak yanında eylemin ulusal düzeyde cezalandırmayı gerektiren ya da uluslararası düzeyde devlete atfedilebilir bir saldırı şekli oluşturup oluşturmayacağını da belirlemektedir.

Hacktivizm, sırf kriminal anlamda bilişim korsanlığından farklılık arz etmektedir. Zira hacktivizm, sadece bir sisteme zarar vermek niyetini taşımamaktadır. Hacktivizm ayrıca elektronik sivil itaatsizlik suretiyle protesto şeklinde kamuoyunu ve hükümeti etkilemek niyetiyle politik dürtü içerir[140]. Hactivizmin veya siber protestonun bu dürtü unsuru eylemin niteliğini belirlemekte, ulusal güvenliği veya kritik altyapıları hedef almayan eylemlerin toplum tarafından desteklenmesine bile sebep olmaktadır. Yakın zamanda yaşanmış olan gizli dokümanların ifşası skandallarında, Snowden ve onun Wikileaks ya da Anonymus'un "hacktivistler" olarak da adlandırılan siber korsanları gibi destekçileri, diplomatik krizler yaratabilmekte; ayrıca hükümetleri sarsabilmekte ve bu esnada halk nezdinde enformasyon özgürlüğünün kahramanları olarak itibar görebilmektedir[141].

Hacktivistleri, vatansever bilişim korsanlarından (*patriotic hackers*) ayıran özellikleri ise; vatansever bilişim korsanlarından farklı olarak hacktivistlerin devletlerinin belirli bir

---

[138] Schreier, 2015, s. 9.

[139] Canbek Gürol / Sağıroğlu, Şeref. (2007). *Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme.* Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Cilt:23, Sayı:1-2, s. 3.

[140] Adkins, Bonnie N., Major USAF. (2001). *The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?*, AU/ACSC/003/2001-4, s. 9.

[141] Aust ve Ammann, 2018, s. 19.

konudaki tutumlarına aykırı olabilecek politik konularda tavır takınabilmeleridir[142]. Vatansever bilişim korsanlarının her durumda kendi devletlerinin benimsediği politika ve tutumlar doğrultusunda hareket etmelerine karşın hacktivistlerin kendi devletleri de dâhil baskıcı devlet otoritesine ilke olarak karşı durmaları nedeniyle özgürlük temelli daha farklı bir dürtü ile eylemlerini gerçekleştirdikleri görülmektedir. Bu kapsamda ifade edilmesi gereken bir diğer siber yöntem ise vandalizmdir. Siber vandalizm, hükümet web sitelerini hedef alan yaygın bir saldırı şeklidir[143]. Siber holiganizm olarak da adlandırılan siber vandalizm[144], bilişim korsanlarının internet sitelerine en yıkıcı olmak için ve sadece eğlence için saldırmaları halinde söz konusu olmaktadır[145]. Bu tür olayların etkisi genellikle zaman olarak sınırlıdır. Yine bunlar daha ziyade göreceli olarak zararsız ancak rahatsızlık veren nitelikte faaliyetleri kapsamakta veya betimlemektedir[146].

1.2.3. SİBER CASUSLUK

Kimi zaman siber saldırı ile iç içe geçen ve siber alanda gerçekleştirilen bir diğer faaliyet siber casusluktur. Siber casusluk rakip devletin sırları, niyetleri ve kapasiteleri hakkında bilgi toplamaya dönük geleneksel çabaların uzantısı olan alışılagelmiş olaylardır[147]. Yabancı istihbarat operasyonlarında siber casuslukla ilgili kamusal alanda bulunan bilginin çok az olmasına rağmen hiç şüphe yok ki siber casusluk dünya çapındaki çoğu devlet istihbarat örgütleri arasındaki en yaygın faaliyet biçimidir[148].

Devletlerin istihbari bilgi toplama (espiyonaj) hakkı, 1907 Lahey IV. Konferansı'nda ve 1961 tarihli Viyana Sözleşmesi'nde kabul edilmiştir. Uluslararası hukuka göre her

[142] Kesan ve Hayes, (Spring 2012). s. 441.

[143] Hruza ve Cerny, 2017, s. 157.

[144] Schreier, 2015, s. 9.

[145] Canbek ve Sağıroğlu, 2007, s. 4.

[146] Schreier, 2015, s. 9.

[147] Schreier, 2015, s. 9.

[148] Adkins, 2001, s. 10.

devletin ulusal güvenliğini sağlamaya yönelik casusluk faaliyetlerini gerçekleştirme hakkı bulunmaktadır. Buna karşın, ulusal yasalar tarafından casusluk eylemlerinin suç haline getirilebilmesi hakkı saklıdır. Ayrıca 1907 Lahey Yönetmeliği'ne[149] göre casusluk, savaşan statüsünün kaybedilmesine sebep olmaktadır[150].

Birazdan daha ayrıntılı olarak bahsedilecek olan AB Parlamentosu'na ECHELON sistemiyle ilgili olarak sunulan 2001 tarihli rapora göre, istihbarat birimlerinin görevleri, devlet güvenliğine yönelik tehditleri önlemek amaçlı bilgi toplama, genel olarak karşı casusluk, silahlı güçlere yönelik olası tehditlerin önlenmesi, yurtdışındaki durumlara dair bilgi toplamaktır[151]. İnternet teknolojisinin gelişiminden önce bilgi toplamaya yönelik bu casusluk faaliyetleri ile kinetik saldırı arasındaki ayrım çok belirgin iken siber casusluk faaliyetleri ile birlikte bazı siber istismar eylemleri kuvvet kullanma oluşturabileceğinden bazı siber casusluk faaliyetlerinin uluslararası hukuka uygun olduğu hususu tartışmaya açıktır.

Geleneksel casusluk faaliyetlerinde insan unsurunun ağırlıklı olarak kullanılması söz konusu iken, tarihsel süreç içerisinde yaşanan teknolojik gelişimle birlikte teknik takip veya iletişimin tespiti gibi yöntemler ön plana çıkmış, casusluk faaliyetleri de evrim geçirmiştir. Öncelikle 20. yüzyılın başlarından itibaren ABD ve İngiltere tarafından uluslararası telekomünikasyon altyapı sistemlerinin bu amaçla takibe elverişli hale getirilmesi buna hizmet etmiştir. Bu süreç siber uzayın ortaya çıkması sonrasında çok daha karmaşık bir hal almış, siber uzay teknolojisinin omurgasını oluşturan teknolojik

---

[149] 1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022 http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

[150] Pazarcı, 2021, s. 621.

[151] European Parliament, *REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, (11 Temmuz 2001) Erişim: 02.05.2020 https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

altyapıların ele geçirilmesi konusunda teknolojik olarak gelişmiş devletlerce kıyasıya bir mücadele başlamıştır. Bu bağlamda casusluk faaliyetlerinin siber boyutunun önemli bir yer tuttuğu ifade edilmelidir[152].

"*Related computer network exploitation enabling operation*" (CNE) olarak da ifade edilen siber casusluk operasyonları, örneğin web sitesini tahrif etmek suretiyle propaganda amaçlı bilgi yaymayı veya bilgisayardan hassas bilgileri çalmayı amaçlayabilir[153]. Siber casusluk faaliyetinde bulunan devlet görevlilerinin kullandığı siber istismar (*cyber exploitation*) yöntemi bir sistem veya ağda depolanmış olan ya da buradan geçen, normal şartlar altında sadece yetkili tarafın erişebileceği bilginin gizliliğini hedef alır[154]. Gizli kapı yazılım (*trap doors*) ve dinleyici (*sniffers*) siber casusluk için özellikle kullanışlı araçlar olup ilki, bilgisayarın sahibinin bilgisi dışında, herhangi bir zamanda harici kullanıcıya erişim izni vermekte; ikincisi ise uzaktaki bilgisayar tarafından kullanıcı şifresini veya kimlik bilgilerini ağ üzerinden çalmak için veri kaydeden veya ele geçiren programdır[155].

Siber casusluk, bilişim korsanlığı faaliyeti şeklinde gerçekleştirilmesi ve yakalanmamak için hasar veya zarara sebep olmaktan bilerek kaçınılması nedeniyle tespiti en zor siber tehdit biçimidir[156]. Siber casusluk faaliyetlerinde öne çıkan siber istismardan farklı olarak siber saldırı, bilginin bütünlüğünü (*integrity*), özgünlüğünü (*authenticity*), erişilebilirliğini (*availability*) hedef almaktadır[157]. Siber casusluk faaliyeti bilgi toplamaya yönelik gerçekleştirildiğinden bilginin ve sistemin istismarı şeklinde gerçekleştirilmektedir. Buna karşın siber saldırı anında gerçekleşenin siber casusluk ya

[152] Siber casusluk konusunda popüler olan "*The Cuckoo's Egg*" ve "*Friendly Spies*" adlı kitaplar yabancı istihbarat, siber casusluk operasyonlarının yarattığı potansiyel tehdidi gözler önüne sermiştir. Bkz.; Adkins, 2001, s. 11.

[153] Roscini, 2010, s. 92.

[154] Lin, 2010, s. 67.

[155] Roscini, 2010, s. 93.

[156] Adkins, 2001, s. 10.

[157] Lin, 2010, s. 68.

da siber saldırı faaliyeti olup olmadığının, kaynağının ve failin belirlenmesi oldukça zordur. Bunun sebebi siber casusluk yöntemlerinin çoğunlukla siber saldırılara zemin hazırlayan ön faaliyetler olmasından kaynaklanabilmektedir.

Siber casusluk faaliyeti yapan kişilerin 1907 Lahey Yönetmeliği[158] gereğince savaşan statüsünü kaybetmeleri durumu Tallinn El Kitabı 89. Kural'da düzenlenmiştir[159]. Bu Kural uyarınca silahlı çatışmalar dâhilinde, düşmanın kontrol ettiği bölgede siber casusluk yapan bir silahlı kuvvetler mensubu savaş tutsağı statüsünü kaybedecektir. Bu türden bir faaliyeti gerçekleştiren siviller ise, çatışmaya doğrudan katılanlardan kabul edilerek Kural 97 gereğince yargılanmaları ve cezalandırılmaları mümkündür[160]. Barış döneminde gerçekleştirilen siber casusluk faaliyetleri ise, Kural 32 gereğince uluslararası hukuku ihlal eden bir eylem olarak kabul edilmemektedir[161].

Siber casusluğa imkân tanıyan alt yapı unsurlarının üretimi nedeniyle devletlerarasında rekabet yaşanmaktadır. Çin Halk Cumhuriyeti'nin dünya çapında bir bilişim devi olan Huawei'in, fiber optik kablosundan network ayırıcı aletlerden akıllı telefonlar ve tabletlere varıncaya kadar internet teknik alt yapısına dair her şeyi fiili olarak üretmesi ABD'yi endişeye sevk etmiştir[162]. Anılan şirketin ürettiği donanımlarda oluşturulacak "arka kapılar" sayesinde Çin askeri birimlerinin ve Pekin destekli bilişim korsanlarının hükümet ve şirket sırlarını ele geçireceği endişesiyle gerçekleştirilen "*shotgiant*" operasyonu ile NSA (*National Security Agency*), şirket ile Halkın Özgürlüğü Ordusu arasındaki bağı tespit etmekten öte şirket teknolojisini ele geçirmiştir[163].

---

[158] 1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022 http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

[159] Schmitt, 2017, *Tallinn Manual 2.0.* s. 409.

[160] Schmitt, 2017, *Tallinn Manual 2.0.* s. 428.

[161] Bkz.: Schmitt, 2017, *Tallinn Manual 2.0.* s. 168.

[162] Aust ve Ammann, 2018, s. 296.

[163] Sanger, David E. / Perlroth, Nicole. (22 Mart 2014). N.S.A. Breached Chinese Servers Seen as Security Threat, *The New York Times.* Erişim: 02.05.2020

Edward Snowden olayında ABD; dostu, düşmanı ve kendi halkını casusluk maksadıyla köşe bucak izleyen, Almanya Şansölyesi'ni gizlice dinleyen [164] ve tüm internet mecrasını takip mekanizmasına çeviren, kötülüğü gözetleyici bir aktör konumuna gelmiştir[165]. Büyük Alman şirketlerine yönelik gözetleme faaliyetleri çerçevesinde, dünyanın herhangi bir yerinde Amerikan uyum yasalarına uymamış olan Daimler ve Siemens gibi firmalara karşı açılan bütün davaların NSA'in elde ettiği bilgilere dayandığı[166] iddiasının Edward Snowden ile Alman Devlet Kanalı (ARD) tarafından yapılan bir söyleşide doğrulandığı[167] görülmektedir.

Bu bağlamda küresel casusluk konusunda önemli bir yer tutan ECHELON sistemi incelendiğinde, UKUSA olarak kısaltılan İngiliz ve ABD sistemlerinin ilk olarak 1987 tarihli sözleşmeyle Britanya Devletler topluluğundan üç ülke, Kanada, Avustralya ve Yeni Zelanda dâhil edilerek "*Five Eyes*" olarak adlandırılan oluşum ortaya çıkmıştır[168]. Bu oluşuma ilişkin AB Parlamentosu'na sunulan rapor 11 Temmuz 2001 tarihli oturumda kabul edilmiş ve raporda ECHELON sisteminin varlığı ve bu sistemin yukarıda sayılan beş devlet tarafından işletildiği şüpheden uzak bir biçimde kabul edilmiştir. Raporda ABD

---

https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html

[164] Daha önce belirtilen "Friendly Spies" adlı kitabın konusunu Alman istihbaratının ABD'nin de dâhil olduğu pek çok devletin bilgisayar sistemlerine girmesini konu alırken bu kez kamuoyuna sızan son olayda Alman Şansölyesi'nin Amerikan istihbaratı tarafından dinlemeye alınması Alman kamuoyunda öfke ile karşılanmıştır. Bkz.: Fisher, Max. (29 Ekim 2013). Why America Spies on its Allies (and probably should), *The Washington Post.* Erişim: 09.09.2021

https://www.washingtonpost.com/news/worldviews/wp/2013/10/29/why-america-spies-on-its-allies-and-probably-should/

[165] Aust ve Ammann, 2018, s. 19.

[166] Aust ve Ammann, 2018, s. 303.

[167] Snowden talks industrial espionage, death threats in German interview. (27 Ocak 2014). *France 24.* Erişim: 02.05.2020

https://www.france24.com/en/20140127-snowden-german-interview-industrial-espionage

[168] Aust ve Ammann, 2018, s. 306.

istihbaratının rüşvet ile mücadele gerekçesini bahane etmek suretiyle yalnızca genel ekonomik istihbarat yapmakla kalmadığı, ayrıca özellikle akdin yapıldığı ortam da dâhil olmak üzere firmalar arası iletişimi izlediği belirtilmiştir[169]. Yine AB araştırmacısı Duncan Campbell'in STOA (*Scientific and Technological Options Assessment*) panelinde sunduğu Interception Capabilities 2000 adlı rapora göre,[170] İngiliz-Amerikan istihbarat işbirliği 1947 yılında imzalanan UKUSA adlı gizli bir antlaşma ile başlamış ve taraflar bu antlaşmayı 1999 Mart ayına kadar açıkça kabul etmemişlerdir.

ABD'nin Utah eyaleti, Bluffdale şehrinde NSA'in milyarlarca dolar harcayarak 2013 yılında kurduğu "*Spy Center*" olarak da bilinen "Utah *Data Center*" da yaklaşık 200 kişilik bir uzman ekibinin casusluk faaliyeti yaptığı ileri sürülmektedir[171]. Dünya çapındaki tüm veri trafiğinin beşte dördünün doğrudan Amerika kıtası üzerinden iletilmesinin sağladığı avantaj sayesinde Bluffdale'in dijital dünyanın merkezi olması öngörülmektedir[172]. Buna karşılık, Çin Halk Cumhuriyeti casusluk amacıyla Şangay'da "61398" birimini kurmuştur[173].

---

[169] European Parliament. (11 Temmuz 2001). *REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)).* Erişim: 02.05.2020 https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

[170] Campbell, Duncan, *Development of Surveilliance Technology and Risk of Abuse of Economic Information*, Ekim 1999 Erişim: 02.05.2020 https://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

[171] Aust ve Ammann, 2018, s. 28. Ayrıca daha ayrıntılı bilgi için bkz.; Hogan, Mel. (2015). Data flows and water woes: The Utah Data Center. Erişim: 12.08.2022 https://www.researchgate.net/publication/281807399_Data_flows_and_water_woes_The_Utah_Data_Center

[172] Aust ve Ammann, 2018, s. 29.

[173] Aust ve Ammann, 2018, s. 334.; Ayrıca basın haberleri için bkz.; Sanger, David E. / Barboza, David / Perlroth, Nicole. (18 Şubat 2013). Chinese Army Unitis Seen as Tied to Hacking Against U.S., *The New York Times.* Erişim: 12.08.2028 https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

ABD İstihbarat Servisi Direktörü James Clapper'in 2013 tarihli demecinde istihbarat camiasının ekonomik ve finansal meseleler ile terörizmin finansmanı konularında bilgi topladığının bir sır olmadığına, bu tür istihbarat bilgilerini, küresel ekonomiye olumsuz etkileri olacağından AB ve müttefiklerini uyarmak amacıyla topladıklarına dair ifadeleri [174] istihbarat örgütlerinin ekonomik casusluk faaliyetleri yaptıklarını doğrulamaktadır. Geçmişte NSA'nın, Brezilya Hükümeti'nin e-postalarını incelediği ortaya çıkmış, İngiliz istihbaratı ile işbirliği içinde gerçekleştirilerek birçok Brezilya şirketinin ağlarına erişim sağlandığı, bunlar arasında bankalar ve devlet petrol şirketi olan Petrobras'ın da bulunduğu iddia edilmiştir[175]. Bu konuda Brezilya devlet başkanı Dilma Rousseff'in BM Genel Kurulu'ndaki ABD casusluğuna ilişkin olarak NSA'in uluslararası hukuku ihlal ettiği yönündeki beyanları[176] dikkat çekmiştir.

Tüm bu siber casusluk faaliyetlerinin geleneksel manada bilgi toplama olarak değerlendirilmesi hayatın gerçeklerine uygun düşmemektedir. Zira tüm bu çabalar istihbari bilgi toplamanın ötesine geçmekte ve her alanda kontrol ve yönlendirme isteğini de göstermektedir. Örneğin, ABD'de NSA'in enformasyon hükümranlığı (information superiority)[177] mücadelesinin, bu amaçla dünya çapında kişisel verilerin toplanması ve analizi çabasının toplumları sevk ve idare etmeye yönelik olduğu, "toplumun sibernetik güdümü" olarak adlandırılan bu durumun kontrol amaçlı olduğu[178]**,** güdümbilimi olan sibernetiğin geçmişe ait davranışlardan geleceğin davranışlarının öngörülebilir olduğu

---

[174] *Statement by Director of National Intelligence James R. Clapper on Allegations of Ecomomic Espionage* (08 Eylül 2013) Erişim: 02.05.2020 https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage

[175] Aust ve Ammann, 2018, s. 300.

[176] Borger, Jullian. (24 Eylül 2013). Brazillian president: US Surveillance 'a breach of international law'. *The Guardian.* Erişim: 02.05.2020 https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance

[177] Aust ve Ammann, 2018, s. 13.

[178] Aust ve Ammann, 2018, s. 39.

kanısıyla hareket edildiği ileri sürülmüştür[179]. Yakın geçmişte seçimlere yönelen kitlesel eğilimlerin yapay zekâ sayesinde tespiti ve seçim sonuçlarının Google şirketi tarafından tahmin edilmesi de bu iddiayı desteklemektedir.

Bu noktada tartışılması gereken bir konu olan siber casusluğun geleneksel anlamda uluslararası hukuka uygun olup olmadığı hususudur. Mevcut uluslararası hukuk kurallarına göre, diğer bir devletin bilişim sistemine rıza hilafına girmek suretiyle siber casusluk (espiyonaj) yapmak, tek başına hukuka aykırı kabul edilmemektedir[180]. Bu genel kabule göre siber casusluk, uluslararası hukuka aykırı bir kuvvet kullanma olarak değerlendirilmemekte ise de bazılarına göre hassas askeri ve istihbarat sitelerine karşı uzun bir süre boyunca ve büyük miktarda gerçekleştirilen siber istismarın hasmane niyeti gösterdiği için kuvvet kullanma yasağını ihlal edebileceği ileri sürülmektedir[181].

Siber casusluk yöntemleri ile siber saldırı yöntemlerinin teknolojik anlamda birbirine girmiş olmasından dolayı yukarıda belirtilen görüşün haklılık payının olduğu kabul edilmelidir. Siber casusluk amacıyla gerçekleştirilen siber istismar aracı olan bir programın sadece bilginin gizliliğini ihlal amacını mı yoksa sistemin erişilebilirlik, özgünlük ya da bütünlüğünü hedef alan bir mantık bombası olup olmadığını tespit için karar vericileri beklemek her zaman kabul edilebilir bir durum değildir[182]. Bu halde mağdur devletin ön alıcı (*anticipatory*) meşru müdafaa hakkının doğması için gerekli hasmane sızma niyetinin tespiti önem arz etmektedir[183]. Örneğin, hedef alınan sistemin kritik altyapı tesislerinin bir parçası olması gerçekleşmekte olanın bir siber saldırı olduğunu tespite yönelik olarak saldırgan niyete işaret edebilir.

[179] Aust ve Ammann, 2018, s. 40.

[180] Sharp, 1999, s. 129.; Heinegg, 2012, s. 11.; Schmitt, 2017, *Tallinn Manual 2.0.* s. 168.

[181] Lin, 2010, s. 84.

[182] Lin, 2010, s. 83.

[183] Sharp, 1999, s. 132.

1.2.4. SİBER SABOTAJ

Uluslararası hukuk alanında genel olarak siber saldırı terimi bir devlet tarafından veya devlet dışı bir örgüt tarafından olsa dahi devlete atfedilebilir olması durumunda vuku bulan siber kuvvet kullanma anlamında kullanılmaktadır. Dolayısıyla siber suça ya da siber casusluğa ilişkin faaliyetler, yetkisiz erişim türleri ya da veri hırsızlığı veya sisteme yönelen sabotaj eylemlerinin silahlı saldırı kapsamına girmediği kabul edilir. Siber terörizmin bir türü olarak kabul edilen siber sabotaj ise, siber saldırı yeteneğine sahip teröristler tarafından, siber altyapı unsurlarına yönelik gerçekleştirilen ve bu unsurlarda aksama veya yıkıma sebep olan eylemleri ifade eder[184].

Buradan hareketle bu tür eylemler, hukuka aykırı karışma ya da ulusal hukuka veya uluslararası hukuka aykırı suçları oluşturabilecektir[185]. Örneğin, İran'ın nükleer enerji kaynağının nükleer enerji tesisleri olmadığı, devletin işlevinde ağır bozulmaya sebep olmadığı gerekçesiyle Stuxnet saldırısının silahlı saldırıya erişmeyen bir sabotaj örneği oluşturduğu savunulmaktadır[186]. Stuxnet saldırısının İran'ın kritik altyapı unsurlarını hedef almayan, özellikle çevresel zararlar doğurmaması için tasarlanmış bir siber silah olduğu gözetildiğinde İran'ın gelişmekte olan nükleer faaliyetlerini sabote etmeye, geciktirmeye yönelen ve silahlı saldırı düzeyine erişmeyen bir siber faaliyet olduğu söylenebilir.

1.2.5. SİBER SAVAŞ

Tarihi birikim göstermiştir ki insan türü ne zaman yeni bir alanı ortaya çıkarmış ise kısa bir süre içinde savaşta bu alanı kullanmanın bir yolunu bulmuştur[187]. Son 3.400 yıllık insanlık tarihinde savaşsız geçen dönemin 268 yıl olduğu, kayıtlı tarihin yalnızca küçük

[184] Adkins, 2001, s. 12.

[185] Gill ve Ducheine, 2013, s. 440.

[186] Gill ve Ducheine, 2013, s. 459.

[187] Mačák, 2018, s. 37.

bir kısmının savaşsız geçtiği[188] dikkate alınırsa insanlığın önlenemez savaşma arzusunun ne derece baskın olduğu anlaşılabilir.

Savaş, devletler ya da gruplar tarafından politik etki için zarar, yıkım ya da can kaybına sebep olmak amaçlı kuvvet kullanılması durumunda söz konusu olmaktadır[189]. Kelsen, savaşı uluslararası hukuku ihlal eden devlete karşı sınırsız bir müdahale ve silahlı güç kullanımı olarak tanımlamaktadır[190]. Bu kapsamda karışma ile savaşı ayıran husus müdahalenin yoğunluk derecesidir. Topyekün bir müdahale savaş oluştururken daha düşük yoğunluktaki müdahaleler savaş olarak kabul edilmemektedir.

Savaş terimi, kinetik (geleneksel, fiziki), biyolojik, kimyasal veya gerilla savaşı adlarıyla saldırı araçları temelinde ya da enformasyon, psikolojik, elektronik, ekonomik veya komuta ve kontrol savaşı şeklinde doğrudan hedeflenen amaca göre sınıflandırılabilmektedir[191]. Bu doğrultuda benimsenecek sınıflandırma türüne göre siber savaşın sınırları da çizilecektir. Zira bilgisayar ağı vasıtasıyla bir insansız hava aracı kullanımı suretiyle gerçekleştirilen veya denizaltı ağ kablosuna yönelen kinetik silahlı bir saldırının siber saldırı kabul edilip edilmeyeceği sorusunun cevabı bu yaklaşıma göre değişecektir. Örneğin, amaç temelli yaklaşımın benimsenmesi halinde, yüksek teknolojiye sahip bir İHA'nın uzaktan kumandasının siber operasyonla ele geçirilerek yönetilmesi suretiyle gerçekleştirilen bombalama eylemi siber saldırı olarak kabul edilmezken; denizaltı internet ağı kablolarına gerçekleştirilecek bir konvansiyonel

---

[188] Hedges Chris. (06 Haziran 2003). What Every Person Should Know Abour War, *The New York Times.* Erişim: 07.02.2021 https://www.nytimes.com/2003/07/06/books/chapters/what-every-person-should-know-about-war.html#:~:text=Has%20the%20world%20ever%20been,wars%20in%20the%20twentieth%20century.; Benzer bir tespit için bkz: Sağıroğlu ve Alkan, 2018, s. 181.

[189] Schreier, 2015, s. 68.

[190] Kelsen, Hans. (2012). *Principles of International Law.* New Jersey: The Law Book Exchange, Ltd, Clark, s. 25.; Çeşitli savaş tanımları için bkz: Sağıroğlu ve Alkan, 2018, s. 183-185.

[191] Hathaway ve diğerleri, 2012, s. 826-827.

saldırının siber saldırı olarak kabulü gibi bir sonuca ulaşılabilmektedir ki bu yaklaşımın tartışmaya açık bir görüş[192] olduğu ifade edilmelidir.

Buna karşın öğretide, siber uzayı oluşturan fiziki, mantıki ve sosyal katmanların her birinin saldırıya açık olması nedeniyle bir bilgisayarın veya bilgisayar ağının ya da bilgisayar kullanıcısının çeşitli şekillerde fiziken hedef alınarak yok edilmesinin de siber saldırı oluşturacağı gibi bir sonuca varılmaktadır[193]. Ayrıca siber uzay alanında savaşmak ve savaş alanı olarak bilgi teknolojisini veya siber uzayı kullanmak arasında fark bulunduğu ifade edilmektedir[194]. Buna göre, bilişim teknolojisinin ya da siber uzayın savaş alanı olarak kullanılması aynı şekilde değerlendirilmelidir.

Uygulamada geleneksel savaş, elektronik savaş ya da siber savaşın hibrit savaş adı altında değerlendirildiği görülmekte ise de siber uzayın fiziki dünyadan ayrı bir sanal alan olarak değerlendirilerek sınıflandırılması kanaatimizce daha uygun olacaktır. Zira geleneksel savaşa göre hazırlanmış uluslararası hukuk normlarının siber savaşa uygulanabilmesi için siber uzayın ve siber savaşın sınırlarının ortaya konulması, hibrit savaş kapsamında dahi ayrılması gereklidir. Siber savaş, siber uzayda ya da siber uzay vasıtasıyla gerçekleşen siber saldırı eylemleriyle sınırlı olmalıdır. Buna göre, siber faaliyetleri gerçekleştiren kişilere ya da nesnelere yönelen kinetik saldırıların siber saldırı olarak değerlendirilmemesi gerekir. Örneğin, bir hibrit savaşta faaliyet gösteren bilişim korsanının düşman güç mensubu bir keskin nişancı saldırısıyla vurulması, siber saldırı olarak kabul edildiğinde uygulayıcılar açısından kavram ve yorum kargaşası ortaya çıkabilecektir.

---

[192] Bkz.: Hathaway ve diğerleri, 2012, s. 827.

[193] Bkz.; Singh, 2022, s. 3290.

[194] Liles, Samuel / Rogers, Marcus / Dietz J. Eric / Dean, Larson. (2012). *Applying Traditional Millitary Principles to Cyber Warfare*, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, s. 169.

Siber savaşın evrensel düzeyde kabul edilmiş bir tanımı bulunmamaktadır[195]. Rusya, Belarus ve Çin Halk Cumhuriyeti arasında imzalanan siber güvenlik antlaşmalarında tercih edilen ve günümüzde siber savaş terimini de kapsayan "bilgi savaşı" (*information warfare)*[196], bir veya birden fazla devletin bilişim alanında (siber uzayda) bilişim sistemlerine, işleme sürecine, kaynaklarına, kritik derecede önemli ve diğer yapılara zarar vermeyi, muhalefet partisinin çıkarları hakkında devleti karar vermeye zorlamak yanında kitlesel biçimde ahalinin beynini yıkamak suretiyle toplumu ve hükûmeti istikrarsızlaştıran, politik, ekonomik ve sosyal sistemlerin altını oymayı amaçlayan karşılaşmalar olarak tanımlanmıştır[197]. Bu tanımı benimseyen devletlerin interneti tehdit olarak algılayan yapısı ve düşünce ve ifade özgürlüklerini sınırlandırmaya yönelik tutumları gözetildiğinde tanımlamanın hedef temelli olduğu görülmektedir. Saldırı ya da

[195] Schreier, 2015, s. 16.

[196] Öğretide bilgi savaşının, siber savaştan daha geniş bir faaliyet alanını kapsadığı kabul edilmekte ve çoğu devlet siber savaşa bilgi savaşının (information warfare) bir alt bölümü olarak bakmaktadır. Ayrıntılı bilgi için bkz.; Schreier, 2015, s. 19.; Bununla birlikte zamanla her iki terimin aynı anlamda kullanıldığı görümektedir. Bkz.: Sağıroğlu ve Alkan, 2018, s. 197.; Ayrıca ifade edilmesi gereken bir konu da, radyo dalgaları (hertzler) üzerinden gerçekleştirilen elektronik harp ile bilgi sinyalleri (bitler) vasıtasıyla gerçekleştirilen siber savaş farklı düzlemlerde ortaya çıkmaktadır. Bkz.; Akgül, Fatih (Ed.: Yıldız, Gültekin / Ateş, Barış). (2022). *Hibrit Tehditleri Anlamak.* Ankara: Milli Savunma Üniversitesi Yayınları, s. 96-97.

[197] Streltsov, 2017, s. 6.; "Information war" terimi Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması'nın Ek 1'de tanımlanmıştır. Bunun için bkz.: Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması, s.9. Erişim: 17.12.2021

Agreement_on_Cooperation_in_Ensuring_International_Information_Security_between_the_Member_States_of_the_SCO.pdf ; Benzer bir tanımlama için bkz.: Taddeo, Mariarosaria. (2011). *Information Warfare: A Philosophical Perspective*. Philopsophy and Geography, Cilt:25(1), s. 114. Erişim: 12.08.2022

https://www.researchgate.net/publication/234627039_Information_Warfare_A_Philosophical_Perspective; Ayrıca, bilgi savaşının bileşenlerinin elektronik savaş, psikolojik operasyonlar ve siber savaş olduğu kabul edilmektedir. Bkz.; Bakshi, Bipin. (2018). *Information Warfare: Concepts and Components*, International Journal of Research and Analytical Reviews, Cilt:5, Sayı:4, s. 184.

savunma amaçlı olarak gerçekleştirilen bilgi savaşı, düşmanın kaynaklarına sızma, bu kaynakları bozma ya da kontrol etme amacını taşımaktadır[198].

Genel nitelikte bir tanıma göre siber savaş, bir devlet ya da büyük bir insan topluluğu tarafından diğer bir devlete yönelen büyük boyutta ve koordine edilmiş dijital saldırıdır[199]. Bu tanımda siber savaşı oluşturan en önemli unsur saldırının dijital nitelikte olmasıdır. Fiziki, ekonomik ya da psikolojik saldırıdan farklı olarak dijital sistemler üzerinden gerçekleştirilmesi bu niteliği sağlamaktadır. Ancak her türlü dijital saldırı siber savaş boyutuna erişmemekte ve siber savaşın mevcut olması için uluslararası bir boyut taşıması, saldırının belirli bir boyuta ulaşması ve taraflarının devlet ya da devlet dışı organize örgüt olması gerekli görülmektedir. Bir dijital saldırının ortaya çıkardığı zarar eşiği konusunda kabul edilen ölçüt ise, silahlı saldırı düzeyine erişmesi ile benzerlik göstermektedir[200].

Buradan hareketle savaş, genel olarak silahlı çatışma durumunda askeri düşmanlık eylemi olarak anlaşılırken siber savaş terimi, siber araç ve yöntemler vasıtasıyla siber uzayda gerçekleştirilen savaş olarak tanımlanmaktadır[201]. Siber savaşın daha geniş bir tanımına göre ise, bir devlet ya da devlet benzeri bir aktör tarafından gerçekleştirilen kritik ulusal altyapı unsurlarına ve askeri tesislere yönelik tehdit içeren simetrik ya da asimetrik saldırı ya da savunma dijital ağ faaliyetleri siber savaşı oluşturmaktadır[202]. Tüm bu tanımlamalarda en temel unsur olan siber saldırıların taraflarının devlet ya da organize örgütlerden oluşması, eylemin belirli bir düzeye ulaşması ve devlet için kritik kabul edilen tesislerin hedef alınması aranmaktadır. Bu haliyle siber savaş kavramının tam olarak neyi anlattığı, siber saldırıdan farkının ne olduğu konusunda bir takım tereddütler oluşabilecektir.

---

[198] Taddeo, 2011, s. 110.

[199] Schreier, 2015, s. 16.

[200] Schreier, 2015, s. 76.; Schmitt, 2017, *Tallinn Manual 2.0.* s. 332-333.

[201] Melzer, 2011, s. 4.

[202] Schreier, 2015, s. 17.

Bu noktada ifade edilmelidir ki siber faaliyetler gelecekteki askeri operasyonların ayrılmaz bir parçasını oluşturmaktadır[203]. 2008 yılında gerçekleşen Gürcistan olayında olduğu gibi, siber saldırıların konvansiyonel savaş dâhilinde gerçekleşmesi de mümkün olup siber savaşın fiziki çatışmalardan ayrı düşünülmemesi gerekir. Bu nedenle silahlı çatışma ya da savaş kavramıyla bütünleşmiş bir siber saldırı teriminin çoğu zaman daha yaygın biçimde kullanıldığı görülmektedir. Uygulamada bu iki savaş türünün birlikte gerçekleşmesi halini ifade etmek için hibrit savaş [204] kavramı tercih edilmektedir. Örneğin, hibrit savaşlar düşman devletin hava savunma sisteminin siber saldırılarla çökertilmesi sonrasında hava kuvvetlerinin tespit edilmeksizin ve direnişle karşılaşmadan saldırması şeklinde gerçekleşebilmektedir.

Bu bağlamda siber savaşın geleneksel anlamda savaş kavramı içerisine dâhil edilerek tamamen siber saldırı kavramıyla belirtilmesi de hibrit savaşları ifade etmek yönünden yetersiz kalmaktadır. Bir diğer ifade ile konvansiyonel silahlarla gerçekleştirilen geleneksel savaşlar ile siber savaşın birleşmesi sonucunda yeni bir kavram ortaya çıkmaktadır. Bu nedenle yeni ve ayrı bir savaş alanını oluşturan siber uzayda gerçekleşen çatışmaların, geleneksel savaş dâhilindeki bazı siber operasyonlara indirgenmesi siber tehdidin ya da gücün küçümsenmesine sebep olabileceği dikkate alınmalıdır.

---

[203] Hruza ve Cerny, 2017, s. 156.

[204] Hibrit savaş, ilk kez 2006 yılında gerçekleşen Lübnan savaşıyla ABD'li Frank Hoffman tarafından kavramlandırılmış ve Rusya'nın Kırım ve Donbas müdahaleleri sonrası 2014 Galler Zirvesinde NATO tarafından benimsenmiştir. Bkz.; Akgül, 2022, s. 92-93. Hibrit savaşta asıl amacın karşı tarafın siyasi yönetimini ve devlet kurumlarını dengesiz hale getirmek, yönetim boşluğu oluşturmak ve kargaşa yaratmak olduğu, bu suretle hedef ülkenin güçlü yanlarını bir kenara atarak, çatışma koşullarını onun zayıf taraflarına odaklamaya çalışmak olduğu kabul edilmektedir. Bkz.: Sağıroğlu ve Alkan, 2018, s. 214. Hibrit savaş kavramı genel olarak konvansiyonel savaşlar ile terörizm, vekâlet savaşları, asimetrik savaşlar, kriminal aktiviteler ya da siber savaşın birlikte gerçekleştirilmesi suretiyle düzenli birliklerce gerçekleştirilen savaşların ötesinde gerçekleştirilen yoğun çatışmaları ifade etmektedir. Bu çalışmada siber savaşlar ile konvansiyonel savaşların birlikte gerçekleştirilmesi hali olarak hibrit savaş terimi kullanılmaktadır.

Bu nedenle bu çalışmada bağımsız bir kavram olarak benimsenen siber savaşın sınırlarının belirlenmesi ve diğer siber faaliyetlerden farkının ortaya konulması gerekmiştir. Kuvvet kullanma düzeyine varmayan diğer faaliyetler uluslararası hukukta savaş kapsamında değerlendirilmezler. Siber uzaydan kaynaklanan ancak silahlı saldırı eşiğine varmayan güvenlik tehditleri siber suç, siber operasyon, siber terörizm, siber polisiye faaliyetleri ve siber korsanlık olarak ifade edilmektedir[205]. Siber suç, ulusal ya da uluslararası hukuka göre suç olarak kabul edilen eylemlerin devlet dışı aktörler tarafından gerçekleştirilmesi halinde[206] söz konusudur. Bu haliyle siber suç, siber saldırı ve siber savaş kavramından daha farklı bir alanı kapsamaktadır. Daha önce de izah edildiği üzere siber casusluk ya da siber istismar ise genel olarak siber saldırı olarak kabul edilmemektedir. Buna göre, barış döneminde gerçekleşen her siber operasyonun siber savaş olarak adlandırılmaması gerektiği ve silahlı saldırı eşiğinin aşılması ya da silahlı bir çatışmanın varlığı halinde siber savaştan bahsedilebileceği söylenebilir.

Roscini, 2006 tarihli Siber Operasyonlar için ABD Ulusal Askeri Strateji Belgesi'nde bilgisayar ağı operasyonlarının (*computer network operations* [CNO]), bilgisayar ağ saldırısı (*computer network attacks* [CNA]), bilgisayar ağ savunması (*computer network defence* [CND]) ve operasyonu mümkün kılan ilgili bilgisayar ağı istismarını (*related computer network exploitation enabling operations*)[CNE]) kapsamına aldığını ifade etmekle birlikte CNE'yi siber operasyonlara dâhil etmemektedir[207]. Daha açık bir tespite göre bir bilgisayar ağı veya sistemine zarar verme eyleminin siyasi veya ulusal çıkarlara yönelik bir amaçla gerçekleştirilmesi halinde siber saldırı eylemi gerçekleşmekte, buna ilaveten siber saldırı eyleminin etkilerinin silahlı saldırı eşiğine erişmesi halinde ya da eylemin silahlı çatışma kapsamında gerçekleşmesi halinde saldırının siber savaşa dönüşmesi söz konusu olmaktadır[208].

[205] Melzer, 2011, s. 22.

[206] Hathaway ve diğerleri, 2012, s. 834.

[207] Roscini, 2010, s. 93.

[208] Hathaway ve diğerleri, 2012, s. 833.

Sonuç olarak, uluslararası hukukun ne ölçüde siber uzaya uygulanacağı konusunda ortaya çıkan soruya öğretide verilecek cevap hiç şüphesiz yer sınırlamasına bakılmaksızın uygulanması yönündedir. Buna göre, devletlerin faaliyetleri, siber uzay dâhil nerede gerçekleştirilirse gerçekleştirilsin mevcut uluslararası hukuk, bu faaliyetlere prensip olarak uygulanacaktır[209]. Saldırıyı gerçekleştirenin niyeti eylemin özellikle siber uzay ile sınırlı olması yönünde ise de bunun siber uzay dışında kinetik veya elektronik olmayan diğer etkiler üretebilmesi mümkündür[210]. Siber savaşın siber uzayın dışında etkiler doğurması halinde dahi saldırı, siber savaş kapsamında değerlendirilir. Buna göre klasik savaş teorisinin, günümüzdeki teknolojik gelişimin gerektirdiği yeni savaş biçimlerine de uygulanabildiği, eylemin yoğunluk derecesinin belirleyici olduğu görülmektedir.

1.3. SİBER SALDIRI YÖNTEM VE ARAÇLARI

Siber saldırılar, bilgisayarın işletim sistemini bozmasına veya işletim sistemi etkilenmeden yalnızca sistemdeki verilerin doğruluğunun değiştirilmesine sebep olmasına göre sırasıyla söz dizimsel (*syntactic)* veya anlamsal (*semantic)* saldırı olarak çeşitlendirilmektedir[211]. Anlamsal saldırılar genellikle casusluk ya da elektronik dolandırıcılık (*phishing*) gibi kriminal faaliyetlerin icrasında kullanılmaktadırlar[212]. Hedeflenen zarar veya sonuç yerine, bu saldırıda kullanılan saldırı yöntemine göre yapılacak bir sınıflandırma ise, saldırı yöntem ve araçlarını ortaya koymaktadır. Ancak bazı durumlarda bir bilgisayarın işletim sistemi ya da veriler hedef alınmadan da siber saldırıların gerçekleştirilmesi olanaklıdır. Dağınık hizmet blokajı saldırısında olduğu üzere, ne işletim sistemine ne de verilere saldırı gerçekleştirilmeden de internet hizmetinin başka yöntemlerle aksatılması suretiyle siber saldılar gerçekleştirilebilir.

[209] Melzer, 2011, s. 3.

[210] Melzer, 2011, s. 4-5.

[211] Hathaway ve diğerleri, 2012, s. 828.

[212] Singh, 2022, s. 3290.

Buradan hareketle siber saldırı yöntem ve araçlarının sınıflandırılmasında yukarıda bahsedilen söz dizimsel ve anlamsal saldırı ayrımının amaca hizmet etmeyeceği sonucu çıkarılabilir. Zira teknolojik gelişmeye paralel şekilde, siber saldırıların gerçekleştirilmesinde yeni yöntemlerin uygulanması her zaman söz konusu olacaktır. Farklı yöntem ve araçların uygulanması muhtemel olmakla birlikte, uygulamada yaygın şekilde gerçekleşen saldırı yöntem ve araçlarından bazılarının kötücül yazılımlar ve dağınık hizmet blokajı yöntemleri olduğu öncelikle ifade edilmelidir.

1.3.1. KÖTÜCÜL YAZILIM (MALWARE)

İngilizcede "*malicious veya malevolent software*" kelimelerinin kısaltılmasından türetilen "*malware*" terimi[213], bir sistemi çoğunlukla kötüye kullanmakta ve bozmakta kullanılan, düşmanca program kodu olarak tanımlanabilecek kötücül yazılım; işleyiş şekline göre virüs, solucan, truva atı, casus yazılım (*spyware*), *adware, root kit, bots* ve *ronsomware* olarak adlandırılabilmektedir [214] . Kötücül yazılımın temel amacı, özel bilgisayar sistemlerine erişim sağlama, hassas bilgileri toplama veya bilgisayarın işleyişini bozma olarak özetlenebilir[215]. Bu kötücül bilgisayar programlarından bazıları daha yaygın görülür.

Brain A. olarak bilinen ve disketi kopyalama özelliği gösteren bir virüs olan ilk kötücül yazılım 1986 yılında iki kardeş tarafından Pakistan'da geliştirilmiştir[216]. Virüs, kendini kopyalayan zararlı bir program olup aktarılmaları gerektiğinden, pasif nitelikteki virüsler yerleştirildikleri bilgisayar ya da ağa zarar vermek için diğer zararlı faaliyetler yanında

---

[213] Milosevic, Nikola. (2013). *History of Malware, Digital Forensics Magazine,* 1/16, s. 58. Erişim: 24.04.2021 https://www.research.manchester.ac.uk/portal/files/32297162/FULL_TEXT.PDF

[214] Namanya, Anitta Patience / Cullen, Andrea / Awan, Irfan U. / Disso, Jules Pagna. (2018). *The World of Malware: An Overview,* IEEE 6th International Conference on Future Internet of Things and Cloud, s. 420. Erişim: 04.04.2021 https://www.researchgate.net/publication/327665678_The_World_of_Malware_An_Overview

[215] Milosevic, 2013, s. 58.

[216] Milosevic, 2013, s. 58.

bilgi çalma, botnetler oluşturma, reklam verme ya da para çalma gibi amaçlarla da kullanılabilirler[217]. Virüs genellikle hedef bilgisayardaki meşru bir programa ilişerek onu değiştiren, çoğunlukla diğer programları ve eğer bir ağa bağlı ise diğer bilgisayarları da etkileyen, kendi kendini kopyalayan bir programdır[218].

Kendini kopyalama özelliğini taşıyan ancak virüsten faklı olarak insan müdahalesi olmadan bir ağa yayılabilmesi nedeniyle aktif nitelikteki solucanlar, sistemi istikrarsızlaştırmak ya da sistemin çökmesine sebep olmak yanında veri çalma, dosya silme ya da bulaştığı sistemi bir botnetin parçası haline getirmeye kadar varan bot oluşturma amacıyla kullanılabilmektedirler[219]. Solucanların virüsten farklılık arz eden bir yönü de diğer programları değiştirmeyip hedef bilgisayardaki adresleri ele geçirip tüm sistemdeki mesajları tekrar gönderip genel bir yavaşlama ve olası bir çökmeye sebep olmasıdır[220]. İlk solucan 1988 yılında MIT öğrencisi olan Robert Tappan Morris tarafından birçok bilgisayarı ağa bağlamak isterken tesadüfen geliştirilmiştir. Morris önemli ölçüde ağ veri akışına ve bunun neticesinde dönemin internetinin neredeyse çökmesine sebep olmuştur. Bu fiillerden dolayı Morris tutuklanmış ve bu suçtan mahkûm edilen ilk kişi olmuştur[221].

Virüsler ve solucanlar, gerçekte zararlı bir programı gizleyen veya dışardan bir kullanıcının bilgisayara uzaktan erişimine izin veren, görünüşte zararsız bir kod parçası olan truva atı içinde saklanabilirler[222]. Bu noktada ifade edilmesi gereken bir başka kötücül yazılım türü ise truva atıdır. Görünürde faydalı ve yasal şekilde sisteme yüklenen ve işletilen ancak arka planda çalışmakta olan zararlı bir dosya içeren ve bu suretle sisteme virüs yerleştirme veya sadece uzaktan kontrol imkânı sağlayan truva atı programı,

[217] Namanya ve diğerleri, 2018, s. 420.

[218] Roscini, 2010, s. 93-94.

[219] Namanya ve diğerleri, 2018, s. 420.

[220] Roscini, 2010, s. 94.

[221] Milosevic, 2013, s. 61.

[222] Roscini, 2010, s. 94.

kendi kendini kopyalayamadığından sistem işleticisinin harekete geçirmesine ihtiyaç duyar[223]. Zaman veya mantık bombaları ise sırasıyla belirli bir zamanda veya belirli şartlarda harekete geçmek için tasarlanmış bir truva atı tipidir[224].

Bir diğer kötücül yazılım olan ve Stuxnet saldırısında kullanılan *Rootkit*, saldırgana sistemin tam kontrolünü veya sistemde yüklü diğer zararlı yazılımlar arasında en yüksek ayrıcalık elde etme yeteneği sağlamak için tasarlanmıştır[225]. 2010 yılı itibariyle kötücül yazılım teknolojisi artık sadece kişisel finansa, dosyalara veya iş hayatına tehdit olmaktan çıkmış; askeri veya polis gücü ve istihbarat örgütleri tarafından da kullanılmaya başlanmıştır. Bunun en iyi örneği olarak da "süper kötücül" yazılım olarak adlandırılan Stuxnet gösterilmektedir[226].

Bu sayılan kötücül yazılım türlerinden başka daha az zararlı faklı yöntemler de bulunmaktadır. Bu tür kötücül yazılım türlerine kısaca değinmek gerekirse sırasıyla *spyware, adware* ve *ransomeware* sayılabilir. Adından da anlaşılacağı üzere casus yazılım (*spyware*), kullanıcı davranışlarını, klavye kullanım hareketlerini, internet kullanım alışkanlıklarını izleme ve saldırgana bilgi gönderme niyetiyle oluşturulmuş programlardır[227]. *Adware* ise, özellikle web sitesi *pop-up* reklamlarıyla otomatikman ekrana gelen reklam destekli kötücül yazılımdır[228]. Son olarak *ransomware* ya da fidye yazılımı[229] olarak bilinen yazılım, kullanıcının hard diskini şifreleyip, masa üstünde değişiklik yaparak şifrenin kırılması için gerekli kod karşılığı belli bir meblağ isteme

---

[223] Namanya ve diğerleri, 2018, s. 420.

[224] Roscini, 2010, s. 94.

[225] Namanya ve diğerleri, 2018, s. 421.

[226] Milosevic, 2013, s. 65.

[227] Namanya ve diğerleri, 2018, s. 421.

[228] Namanya ve diğerleri, 2018, s. 421.

[229] Ayrıntılı bilgi için bkz.; Çelik, Soner / Çeliktaş, Barış. (2018). *Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar,* Cyberpolitik Journal. Cilt:3, Sayı:5. Erişim: 04.11.2022 https://dergipark.org.tr/en/download/article-file/536201

şeklinde kendini göstermektedir[230]. İstenilen bedel ödenmediği takdirde verilerin ya da operasyonel uygulamaların seçilip yayınlanması, verilere erişimin şifrelenmesi ve kalıcı şekilde engellenmesi gibi tehditler ile karşı karşıya kalınmaktadır[231].

1.3.2. HİZMET DIŞI BIRAKMA (DENIAL OF SERVİCE [DoS)]) ve DAĞINIK HİZMET BLOKAJI (DISTRIBUTED DENIAL OF SERVICE [DDoS] ATTACKS)

Bir bilgisayarı veya bilgisayar ağını etkisiz hale getirmek için en çok kullanılan yöntemler, fiziksel olarak yok edilmesinin yanı sıra donanımının veya yazılımının bozulmasına veya çökmesine neden olacak kadar çok bilgi sağanağına maruz bırakmaktır[232]. Hizmet dışı bırakma ya da hizmet aksattırma saldırıları (DoS) olarak da ifade edilen bu saldırı yöntemi, yetkisiz erişim veya sistem kontrolünü ele geçirmeye yarayan saldırılardan farklı bir amaç için gerçekleştirilmekte, bir bilgisayar, sunucu veya ağın kaldırabileceğinden çok daha fazla yük bindirilmesi sağlanarak söz konusu sistemin kullanılmaz hale getirilmesi amaçlanmaktadır[233]. Bir DoS eylemi, doğrudan saldırı olarak gerçekleştirilebileceği gibi, saldırıya uğrayan tarafın saldırıyı geri yönlendirmek suretiyle karşı saldırı olarak saldırgana yönelik olarak da gerçekleştirilebilir[234].

DoS saldırısı önemli sayıda bilgisayar tarafından gerçekleştirildiğinde DDoS saldırı olarak adlandırılır[235]. Bu saldırıların gerçekleştirilme şekli şöyledir:

> *"Böyle bir saldırıda bulunmak isteyen kişi, sadece özel bir programı bilgisayarına indirmek zorundadır. Yükü arttırmak için, saldırıda bulunan*

---

[230] Milosevic, 2013, s. 65.

[231] Bkz.: Fidye yazılımı nedir? Erişim: 04.11.2022, https://www.oracle.com/tr/security/what-is-ransomware/

[232] Roscini, 2010, s. 93.

[233] Canbek ve Sağıroğlu, 2007, s. 8.

[234] Kesan ve Hayes, (Spring 2012). s. 434.

[235] Roscini, 2010, s. 94.

> *bilgisayarlar, dünya çapında devasa botnetlere (bunlar robot tarafından yönlendirilir) bağlanır; virüs bulaşmış bu bilgisayar, otomatik olarak milyonlarca istekte bulunur. Bu şekilde botnetler, yüz binlerce bilgisayarın evrensel ağları halini alabilir: bilgisayar kullanıcıları ise bu saldırıya dair hiçbir şey fark etmezler. En fazla, bilgisayarlarının biraz yavaşlamasına şaşırırlar. Virüslü bir maili açarak, virüs bulaşmış bir yazılımı indirerek veya buna uygun hazırlanmış olan internet sayfasında dolanarak böyle bir botnete takılabilirsiniz. Bilişim korsanlarının dediği gibi, bilgisayarlar "zombilere" dönüşür: İnternet üzerinden uzaktan kontrol edilebilirsiniz ve bir komut üzerine DDoS saldırılarına iştirak edebilirsiniz..."*[236]

İnternet sitelerine saldırı yapmanın en kolay ve aynı zamanda en etkili silahı, Dağınık Hizmet Blokajı olarak tercüme edilebilecek DDoS (*Distrubuted Denial of Service*) adı verilen saldırılardır[237]. Bu saldırı yönteminin uygulandığı Estonya'da 2007 yılında acil durum aramaları servisi bir saat kadar devre dışı kalmış, 2008 yılında Gürcistan'ın dış dünya ile internet bağlantısı kesilmiştir[238]. 2009 yazında Japonya ve Güney Kore tarafından yapılan "siber akım" tatbikatı sırasında Kuzey Kore'nin denize füze göndererek meydan okuması sonrasında ABD ve Güney Kore web sitelerine yönelik gerçekleşen siber saldırılarda, çok yoğun şekilde, saniyede bir milyondan fazla sayfa çağırma eyleminden sonra ABD hükümeti internet sayfaları ve New York Borsası sunucuları çökertilmiştir[239]. Kısa bir süre sonrasında ise, Seul'a yönelik gerçekleştirilen ikinci ve üçüncü saldırı dalgasında 74 ülke üzerinden 166.000 bilgisayarlık bir botnet, Güney Kore banka ve hükümet kuruluşlarının web sayfalarına saldırmıştır[240].

Yaşanan bu saldırılar göstermektedir ki bu saldırı yönteminin sonuçlarının geniş bir alana yayılması ve özellikle de hedeflenen ülkedeki kamusal ve özel kritik hizmetleri aksatması

---

[236] Aust ve Ammann, 2018, s. 267.

[237] Aust ve Ammann, 2018, s. 267.

[238] Erdem ve Özocak, 2019, s. 130.

[239] Aust ve Ammann, 2018, s. 342.

[240] Aust ve Ammann, 2018, s. 342.

nedeniyle yaygın şekilde tercih edilmektedir. Özellikle konvansiyonel bir savaş öncesinde psikolojik üstünlük sağlaması nedeniyle de etkili bir saldırı aracı olarak kullanılmaya elverişlidir. Bu hizmet dışı bırakma eylemleri göstermektedir ki daha önce de belirtildiği gibi, bilgisayarların işletim sistemi ya da veriler hedef alınmadan da sadece internet hizmetinin aksatılması suretiyle de çok geniş ölçekte ve etkili biçimde siber saldırı gerçekleştirilebilmektedir. Bu tür saldırıların bireysel olarak gerçekleştirilemeyeceği ve belli bir siyasal dürtünün varlığı da bir gerçektir. Bu bağlamda siber saldırıları gerçekleştiren aktörlerin tespiti zor olsa da saldırı yöntem ve araçlarının incelenmesi ve sınıflandırılması süreç içerisinde önemli bir basamak oluşturmaktadır.

1.4. BAŞLICA SİBER SALDIRI OLAYLARI

Siber saldırı olaylarının ilk örneği olan 1982 yılında Sibirya'da gerçekleşen, Sovyet boru hatları patlaması ile başlayan siber saldırı olayları 1991 Körfez Savaşı, 1994 ve 1997-2001 yılları arasında Çeçen-Rus savaşı, 1999 Kosova ve 1999-2002 arası İsrail-Filistin çatışmalarıyla devam etmiştir[241]. Daha sonraları siber saldırıları olaylarına yenileri eklenmiş ve saldırılar nitelik değiştirmiş, siber uzayın kapsam alanı genişledikçe ve teknolojik gelişim arttıkça bu saldırıların etkisi de artmıştır. Bu saldırı olaylarından öne çıkan bazılarının aşağıda daha ayrıntılı olarak incelenmesi gerekli görülmüştür.

1.4.1. SLAMMER SOLUCANI

Safir olarak da adlandırılan Slammer solucanı, tarihin en hızlı yayılan bilgisayar solucanı olup 2003 yılında 10 dakika içinde savunmasız sunucuların %90'ına yayılmış, ulaşım, finans ve hükümet hizmetlerinde önemli aksamalara sebep olmuş, ağ kesintileri yanında uçuş iptalleri, seçim müdahalesi ve ATM arızaları gibi öngörülemeyen sorunlara neden olmuştur[242]. Bu solucan nedeniyle ABD'nin Seattle eyaletinde 911 acil yardım servisi

[241] Schreier, 2015, s. 107-109.

[242] Inside the Slammer Worm, *Center for Applied Data Analysis.* Erişim: 28.06.2020, https://www.caida.org/publications/papers/2003/sapphire2/sapphire.xml

birkaç gün kapalı kalmış, Bank of America'nın ATM ağı çökmüş, birkaç havaalanında uçuş kontrol sistemleri etkilenmiş ve uçuş iptallerine sebep olmuş ve daha da önemlisi Ohio eyaletinde bir nükleer güç tesisinde bu solucandan kaynaklı sorunlar yaşanmıştır[243]. Slammer solucanı bilgisayar solucanlarının evriminde önemli bir dönüm noktası oluşturmaktadır[244]. Bu nedenle sonradan gerçekleştirilen siber saldırıların anlaşılabilmesi için bahsedilmesi gereken bir siber olaydır.

1.4.2. ESTONYA SİBER SALDIRISI

Öncesinde Sovyetler Birliği üyesi olan Estonya'da yönetim, Sovyet işgalinin izlerini silmek amacıyla çıkardığı "Yasak Anıtlara Karşı Kanun" ile II. Dünya Savaşı'nda ölen bir Rus Kızıl Ordu askerinin, Tallinn merkezinde bulunan ve kanun kapsamına giren bronz anıtının kaldırılmasına karar vermiştir. Yerel Ruslar tarafından bu karara karşı konulmuş[245] ve 2007 yılı Nisanı'nda, Sovyet savaş anıtının Tallinn şehir merkezinden kent dışına taşınması kararı üzerine Estonya bir dizi DoS, web sitesi bozma, yoğun e-posta ve spam saldırılarına maruz kalmıştır[246]. Bu olay siber saldırıların devlet hizmet alanlarında ne derece etkili sonuçlar doğuracağını göstermesi açısından önemlidir.

1.3 milyon nüfusa sahip Estonya internete erişim konusunda çok yüksek bir seviyeye erişmiş olup, Estonya hükümeti faaliyetlerini 2005 yılı Kasım ayından itibaren sanal ortama taşımıştı[247]. Modern altyapısıyla "E-stonya"[248] dünyanın en iyi ağ donanımına sahip ülkesi olması nedeniyle bu özelliği bumerang etkisi göstermiş, erişim taleplerinden

---

[243] Nikola, 2013, s.63.

[244] Inside the Slammer Worm. (2003). *Security and Privacy Magazine*. Erişim: 13.08.2022, https://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf

[245] Aust ve Ammann, 2018, s. 337.

[246] Betz ve Stevens, 2011, s. 29.

[247] Schreier, 2015, s. 109.

[248] Bu nedenle E-Stonia olarak da bilinir. Ayrıca internete erişim hakkı Parlamento tarafından temel bir insan hakkı olarak kabul edilmiştir. Bu konuda bkz.; Afroditi, 2010, s. 4.

dolayı ülkenin en önemli sunucularına aşırı yüklenilmiş ve sunucular bu yükü kaldıramamıştır[249]. Saldırı sonucunda dış işleri ve adalet bakanlığı web siteleri, bankalar ve acil yardım servisi hizmet dışı kalmış ve başbakanın partisinin web sitesinde başbakanın resmi hitlervari bıyıklı olarak değiştirilmiştir[250].

Bu siber saldırılar nedeniyle devlet aygıtının çaresiz kalmasına ve saldırıların NATO'dan (*North Atlantic Treaty Organization* / Kuzey Atlantik Antlaşması Örgütü) yardım talep edilecek kadar ciddi boyutlara ulaşmasına rağmen saldırıların herhangi bir devlete isnat edilebilmesi mümkün olmamıştır[251]. Estonya Dışişleri Bakanı Urmas Paet siber saldırılara doğrudan karıştığı gerekçesiyle Kremlin'i suçlamış ise de saldırılarla Rus otoritelerinin bağlantısına dair delil bulunmadığını daha sonra kabul etmiştir[252].

Estonya siber saldırısının, *jus ad bellum* bakımından haklı bir sebebe dayanmadığı ve bir son çare (*ultima ratio*) oluşturmadığı kabul edilmektedir. Bunun yanında, *jus in bello* bakımından ayrım gözetmeyen ve orantısız olduğu ileri sürülmesine rağmen[253] NATO tarafından kolektif meşru müdafaa gerektiren bir eylem olarak kabul edilememiş olup genel olarak da kuvvet kullanma niteliğinde değerlendirilmemektedir. Ülkede Rus azınlık tarafından internetten yapılan isyan çağrısı olarak nitelendirilen bu siber saldırı Tallinn El Kitabı'nda uluslararası olmayan bir silahlı çatışma seviyesine erişmemiş kabul edilmektedir[254].

[249] Aust ve Ammann, 2018, s. 337.

[250] Schreier, 2015, s. 109.

[251] Gül, 2021, s. 24.

[252] Weglinski, 2016, s. 80.

[253] Schreier, 2015, s. 110.

[254] Schmitt, 2017, *Tallinn Manual 2.0.* s. 387.

1.4.3. GÜRCİSTAN SİBER SALDIRISI

Bu saldırı bir devletin diğer bir devlete karşı gerçekleştirdiği kara, deniz ve hava saldırılarıyla aynı zamanda gerçekleştirilen ilk siber saldırı örneği olarak kabul edilmektedir[255]. 2008 yılında Özerk Güney Osetya bölgesinden kaynaklanan Rus-Gürcistan anlaşmazlığı sırasında Rus siber güçleri tarafından başlatılan saldırıda, Gürcistan, Rus ve Türk yönlendiriciler (*router*) üzerinden dünya çapındaki ağlara bağlandığı için, bunlar önce yoğun DDoS saldırılarına maruz kalmış, Gürcistan'da e-posta gönderme faaliyetleri durmuş, banka sunucuları kapatılmıştır[256]. Gürcistan siber saldırısı, hibrit savaş döneminin başladığına işaret etmektedir[257]. Bununla birlikte yeni savaş kavramının önemi ortaya çıkmış, devletler bu yeni savaş modeline uygun ulusal güvenlik ve harp politikaları belirlemişlerdir.

Saldırı nedeniyle sadece mali kayıplar yaşanmakla kalınmamış, ayrıca iletişimde önemli aksamalar yaşanmıştır[258]. Botnetler, DDoS saldırıları vasıtasıyla Moskova'nın askeri kampanyasına *çarpan etkisi* sağlamak suretiyle bu saldırıda anahtar bir rol oynamış, Gürcistan hükûmetinin web sitelerini ve bağımsız medyayı devre dışı bırakmış, hükûmetin halkıyla iletişim kapasitesini işlevsiz kılmıştır[259]. Bu siber saldırı kampanyasının öncelikli amacı Rusya'nın Gürcistan'ı işgalini desteklemek olup siber saldırı askeri tarzda işgal planına uygun olarak gerçekleştirilmiştir[260]. Saldırının arkasında Rusya'nın olduğuna dair iddialar Rus hükümetince kabul edilmemiştir[261].

---

[255] Schreier, 2015, s. 112.

[256] Aust ve Ammann, 2018, s. 338-339.

[257] Güleç, Özge / Kişman, Zülfükar Aykaç. (2021). *Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri*. Akademik Açı Dergisi, Cilt:1, Sayı:1, s. 143.

[258] Weglinski, 2016, s. 80.

[259] Farwell, James P./ Rohozinski, Rafal. (2011). *Stuxnet and the Future of Cyberwar*, Survival, Cilt:53:1, s. 26.

[260] Schreier, 2015, s. 112.

[261] Weglinski, 2016, s. 80.

1.4.4. STUXNET SALDIRISI

Göründüğü kadarıyla, yarısından fazlası İran'da olmak kaydıyla dünyanın değişik bölgelerinde bulunan 60.000'den fazla bilgisayara bulaştığı tespit edilen ve 2010 yılı Haziran ayında fark edilen[262] bir siber solucan İran'a ait Natanz nükleer tesislerini vurmuştur[263]. Resmi olarak kabul edilmemiş olsa da ABD Başkanı George W. Bush'un 2006'da "*Olimpic Games*" adlı operasyonun emrini vermesi ve Başkan Barrack Obama'nın da operasyonu devam ettirmesiyle İran'ın Natanz uranyum zenginleştirme tesislerine karşı gerçekleştirilen[264], sonradan solucan programının bazı anahtar kelimeleri olan ".stub ve mrxnet. sys" den türetilmiş[265] ve stuxnet adını almış bu siber saldırı pek çok ilke imza atan özellikleri ile çok sayıda çalışmaya konu olmuştur.

Amerikan-İsrail ortak yapımı olduğu tahmin edilen virüs, İran'ın Natanz'daki uranyum zenginleştirme tesisine herhangi bir internet bağlantısı olmaması nedeniyle bir flaş bellek yardımıyla sokulmuştur. Bu zararlı yazılım, on beş bin satır koddan oluşmakta olup sisteme girdiği andan itibaren on beş gün boyunca kuluçkada bekleyerek sistemin olağan akışını kaydetmiştir[266]. Yazılım, Siemens türü SCADA sistemiyle işletilen santrifüjlere saldırarak tescilli yazılımları baskılamakta ve santrifüjlere aşırı yükleme yaparak, hasar oluştururken geri dönülmez noktaya gelinceye kadar gözlemciler tarafından durumun fark edilmemesini de başarmaktadır[267].

---

[262] Virüsün varlığı ve saldırıya ilişkin ayrıntılı bilgi yaklaşık bir sene sonra ortaya çıkmıştır. Bkz.; Çelik, Şener. (2013). *Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme*. DEÜ Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, s. 145.

[263] Farwell ve Rohozinski, 2011, s. 23.

[264] Aust ve Ammann, 2018, s. 322-323.

[265] Aust ve Ammann, 2018, s. 326.

[266] Gül, 2021, s. 7.

[267] Schreier, 2015, s. 114.

Stuxnet solucanının en önemli özelliğinin "hassaslığı" (*precise*) olduğu, bu sayede hedeflenen santrifüjün dışında çevresel zararın ortaya çıkmamasının sağlandığı ifade edilmektedir[268]. Çevresel zararlara sebep olmasa da tesisin yaklaşık beşte birine tekabül eden 1000 adet santrifüj bu saldırıda işlevsiz hale gelmiştir[269]. Bu haliyle "ateşle ve unut" kötücül yazılımının (stuxnet), "ateşle ve unut füzesinin" (*fire-and-forget missile*) siber uzayda seçilmiş bir hedefe yönelik yeni nesil bir temsilcisi olduğu kabul edilmektedir[270].

Stuxnet'in bir diğer özelliği o güne kadarki en gelişmiş ve karmaşık siber saldırı aracı olmasıdır. Özel bir amaç için tasarlandığı ve çevresel zararlara sebep olmamasının hedeflendiği, diğer su ve elektrik tesislerine zarar vermeyip sadece Natanz uranyum geliştirme faaliyetlerini geciktirmeyi hedeflediği anlaşılmaktadır. İran devleti aksini iddia etse de bunun gerçeği yansıtmadığı[271], saldırının başarıya ulaştığı ve iki yıllık bir süre için İran uranyum zenginleştirme programının gecikmesine sebep olduğu bilinmektedir.

Stuxnet saldırısının sebep olduğu bir sonuç da bir zamanlar sadece vizyonerlerin aklını meşgul eden siber devrim fikrinin savunma politikası çevrelerinde geniş bir etki yaratmasıdır[272]. Bu saldırının silahlı saldırı düzeyine erişip erişmediği konusunda yapılan değerlendirmelerde, İran'ın nükleer enerjiye bağlı olmaması nedeniyle kritik altyapı tesisleri niteliğinde olmadığı gerekçesiyle silahlı saldırı oluşturmadığı, tam bir sabotaj örneği oluşturduğu kabul edilmektedir[273]. Zira yukarıda siber sabotaj başlığı altında

---

[268] Rølsåsen, 2016, s. 18.

[269] Gümüşbaş, Ahmet, *Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları,* s.185. Erişim: 30.11.2020 https://tasam.org/Files/Icerik/File/Stuxnet_ve_Aramco_Saldırıları_pdf_1acfbb35-785b-4de4-8d9a-850a695d45ac.pdf

[270] Farwell ve Rohozinski, 2011, s. 24.

[271] Çelik, 2013, s. 146.

[272] Lindsay, 2013, s. 3.

[273] Gill ve Ducheine, 2013, s. 459.; Aksi yönde görüş için bkz.; Çelik, 2013, s. 159-160.

açıklandığı üzere, devlete atfedilebilir olmayan ulusal ya da uluslararası suç oluşturan eylemler ile kritik altyapı tesisi olarak kabul edilmeyen tesislere yönelen casusluk, yetkisiz erişim, veri hırsızlığı ya da sabotaj faaliyetleri silahlı saldırı olarak kabul edilmemektedir.

1.4.5. ARAMCO SALDIRISI

Stuxnet saldırısının arkasında ABD'nin ve İsrail'in olduğuna dair New York Times'da 01 Haziran 2012 tarihinde yayınlanan yazı[274] sonrasında Suudi Arabistan devletine ait petrol şirketi olan Suudi Aramco'nun yaklaşık 30 bin bilgisayarlarına virüs bulaşmıştır. Bu olayda kayıtlı verilerin yaklaşık dörtte üçünü silinmiş ve yanar durumda bir ABD bayrağı yerleştirilmiştir[275]. Günlük cirosu bir milyar doların üzerinde olan şirketin petrol üretimi durma noktasına gelmese de bilgisayar ve e-posta sistemlerinin yenilenmesi gerektiğinden bu saldırı şirket içi iletişimin 10 gün boyunca aksamasına sebep olmuştur[276].

Bu siber saldırıyı incelenmeye değer yönü ise, siber saldırı sonucunda fiziki zarar ortaya çıkmadığından uzmanlar arasında sistemin işlevselliğinin bozulmasının ya da verilerin silinmesinin tek başına silahlı saldırı düzeyine erişmeye yeterli kabul edilip edilmeyeceği konusuna ilişkin olmasıdır. İlerleyen kısımlarda daha ayrıntılı olarak izah edileceği üzere, bu konuda işlevin bozulmasının da önemli düzeye erişmesinin ya da fiziki bileşenlerin değiştirilmesinin gerekliliğine dair farklı görüşler bulunmaktadır.

---

[274] Sanger, David E. (01 Haziran 2012). Obama Order Sped Up Wave of Cyberattacks Against Iran, *The New York Times.* Erişim: 03.05.2020 https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[275] Aust ve Ammann, 2018, s. 342-343.

[276] Gümüşbaş, s.186.

1.5. ULUSLARARASI ALANDA YAPILAN ÇALIŞMALAR

Uluslararası hukuk ilkelerinin ve geleneksel kuralların siber uzaya uygulanabilirliği konusu 20. yüzyılın sonundan itibaren ABD'de tartışılmakta ise de Avrupa hükümetleri Stuxnet ve Gürcistan saldırılarından sonra konuya ilgi göstermeye başlamışlardır[277]. Süreç içerisinde siber uzaydaki kurallara yönelik olarak çeşitli uluslararası örgütler tarafından bazı çalışmalar yapılmıştır. Bunların en başında NATO gelmekte olup BM ve Avrupa Konseyi gibi uluslararası örgütler tarafından benzer çalışmaların yapıldığı görülmektedir. Ayrıca bu amaçla yapılan çalışmalar sadece örgütler nezdinde yapılmamakta ve siber uzaya bağlılığı çok önemli düzeyde bulunan ABD gibi devletlerin siber güvenlik politikaları da uluslararası örgütlere rehber olmaktadır.

Siber uzaya ilişkin kurallar konusunda uluslararası angajman ve işbirliği 3 kategoride incelenmektedir. Bunlar: İnternet yönetimi, çok taraflı kamu politikası ve internet güvenliğidir [278] . Bu kapsamda uluslararası örgütlerce gerçekleştirilen çalışmalara geçmeden önce siber uzayın yönetiminde en etkili güç olan ABD'nin uluslararası işbirliğini öne çıkaran siber güvenlik politikasından[279] bahsetmek gerekir. 2003 tarihli Amerikan siber uzay ulusal güvenlik strateji belgesinde 5 önceliğin altı çizilmiştir[280]. Bunları kısaca; ulusal siber güvenlik tepki sistemi, ulusal siber tehdit ve hassasiyet azaltma programı, ulusal siber güvenlik farkındalık ve eğitim programı oluşturma, hükümete ait siber alanı güvenli kılma ve son olarak ulusal ve uluslararası siber güvenlik işbirliğini sağlamak olarak listeleyebiliriz. Gelinen noktada tüm ülkeler için ulusal alanda farkındalık yaratma, teknik ve kurumsal altyapı oluşturma ve uluslararası alanda işbirliği kurma en temel güvenlik stratejileri olarak belirginleşmektedir.

[277] Heinegg, 2012, s. 7.

[278] Kanuck, 2010, s. 1580.

[279] Daha ayrıntılı bilgi için ayrıca bkz.; Güleç ve Kişman, 2021, s. 144-145.

[280] Convertino ve diğerleri, 2007, s. 30-31.

1.5.1. KUZEY ATLANTİK ANTLAŞMASI ÖRGÜTÜ (NATO) TARAFINDAN YAPILAN ÇALIŞMALAR

NATO üyesi ülkeler tarafından kabul edildiğine göre, örgütün siber savunma politikası kapsamında uluslararası insancıl hukuk da dâhil olmak üzere uluslararası hukuk siber uzaya uygulanabilecektir. Bu husus 4-5 Eylül 2014 tarihinde gerçekleştirilen Galler Zirvesi Bildirisi'nde de örgüte üye devletler tarafından teyit edilmiştir[281]. NATO üyesi devletlerden Almanya'nın bu konuya ilişkin tutum belgesinde BM Şartı ve insancıl hukuk da dâhil uluslararası hukukun çekincesiz şekilde siber uzaya uygulanacağına dair kanısını ortaya koymuştur[282].

NATO'nun bu tutumu 2007 yılına kadar uzanmaktadır. 2007 yılında gerçekleşen Estonya siber saldırısı sonrasında destek amaçlı olarak Estonya'nın Tallinn kentinde Siber Savunma Mükemmeliyet Merkezi kurulmuştur. Bu merkez tarafından silahlı çatışmalar hukukunun silahlı çatışmalar süresince siber operasyonlara uygulanabilirliği yanında, BM Şartı'na ve yapılageliş hukuku kapsamında kuvvet kullanma terimini ilgilendiren durumları düzenleyen uluslararası hukukun siber uygunluğunu değerlendiren çok yıllık bir proje başlatılmıştır[283]. 2013 tarihli Siber Savaşa Uygulanacak bahse konu Uluslararası Hukuk El Kitabı (Tallinn Manual 1.0) sonrasında ise 2017 yılında aynı merkez tarafından siber operasyonlara ilişkin barış zamanı rejimine yönelik[284] 2. el kitabı olan Tallinn Manual 2.0 yayınlanmıştır.

Her iki çalışma da Michael N. Schmitt başkanlığında küresel bir uzman grubu tarafından hazırlanmıştır. İlk grup silahlı çatışmalar alanında uzman olan ve münhasıran batı

---

[281] Hruza ve Cerny, 2017, s. 156.

[282] Position Paper, 2021, s. 1.; Ayrıca Almanya'nın siber güvenlik stratejisine dair bkz.; Güleç ve Kişman, 2021, s. 144-145.

[283] Schmitt, Michael N. (2017). *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, Harvard National Security Journal, Cilt:8, s. 242.

[284] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law*. s. 242.

dünyasından gelen kişilerden oluşurken, eleştiriye cevaben ikinci uzman grubu hem daha geniş bir kaynaktan (Tayland, Japonya, Çin Halk Cumhuriyeti ve Belarus üyeleri dâhil) hem de daha geniş bir uzman gurubu (insan hakları, uzay hukuku, uluslararası telekomünikasyon hukuku alanları dâhil) tarafından hazırlanmıştır [285] . Böylece çalışmanın hem coğrafi temsil kabiliyeti arttırılmış, hem de hukukun çeşitli dalları içinde konu ele alınmıştır. Ayrıca ilk baskıda siber savaşta özel sektöre dair tespit yapılmamışken, ikinci baskıda devletler yanında özel sektörün de siber saldırılara karşı koyabilmeleri üzerinde durularak örneğin, bir devletin egemenliğinin ihlali niteliğinde bir saldırı halinde kritik altyapı tesislerini işleten özel sektörün de geri hackleme (hack back) olanağı ortaya konulmuştur[286]. Son olarak, 2021 yılında El Kitabı'nın 3. versiyonun (Tallinn Manual 3.0) hazırlanmasına ilişkin 5 yıllık çalışma başlatılmıştır[287].

Tallinn El Kitabı'nın amacı hukuk yaratmak ya da hukuki yaptırım gücünü haiz bir kitapçık oluşturmak değildir. El Kitabı'nın tanıtım kısmında açıkça ifade edildiği üzere uluslararası uzmanlar gurubunun fikirlerinin açıklanması hedeflenmiştir[288]. Siber savaşa uygulanacak uluslararası hukukun yardımcı kaynakları arasında yargı kararları, akademik çalışmalar ve Uluslararası Hukuk Komisyonu çalışmalarından sonra Tallinn El Kitabı 4. sırada gösterilmekte[289] ya da bağlayıcı nitelikli olmayan uluslararası hukuk metinlerini ifade etmek için kullanılan "*soft law"* olarak ifade edilmektedir[290]. Anılan çalışmanın ayrı bir kaynak olarak ifade edilmesi doğru görülmemekle birlikte, devlet uygulamalarının ve yapılageliş kurallarının oluşması için dünyanın farklı bölgelerinden uzmanların ortaya

---

[285] Jensen, Eric Talbot. (2017). *The Tallinn Manual 2.0: Highlights and Insights*, Georgetown Journal of International Law, Cilt:48, s. 738.

[286] Garrie ve Simonova, 2020, s. 517-518.

[287] The NATO Cooperative Cyber Defence Centre of Excellence. *The Tallinn Manual*. Erişim: 22.01.2023. https://ccdcoe.org/research/tallinn-manual/

[288] Jensen, 2017, s. 738.

[289] Bu konuda bkz.: Rølsåsen, 2016, s. 10.

[290] Ayalew, Yohannes Eneyew. (2015). *Cyber Warfare: A New Hulloballoo under International Law.* Beijing Law Review, Cilt:6, s. 221.

Erişim: 21.01.2023 https://www.scirp.org/pdf/blr_2015101514533777.pdf

çıkaracağı uzman hukukçu görüşlerinin faydalı olduğu söylenebilir. Zira siber savaşa ilişkin uluslararası bir antlaşma bulunmamakta ve zorunlu görünmemektedir. Bunun yerine doktrin görüşü kapsamında uluslararası uzmanlardan oluşan bir grubun gerçekleştirdiği çalışmanın geliştirilmesi, çalışmamızın "yorum" konusundaki yaklaşımına uygun düşmektedir.

Henüz hiç bir devlet Tallinn çalışmasına itiraz etmemiş, aksine 50'nin üzerinde devlet Lahey sürecinde bu El Kitabı'nın ikinci baskısı taslağına gözlemlerini sunmuştur[291]. Tallinn El Kitabı siber operasyonlara uygulanacak hukuku ifade etmeye yönelik ilk ciddi çalışma olması nedeniyle önemli bir yer tutmakta olup Rusya'nın raporun meşruiyetine yönelik itirazları olsa da çoğu devlet tarafından desteklenmiştir[292].

NATO nezdinde konuyla ilgili olarak yapılan son çalışma olan 2030 gündemi belgesi NATO 2022 Liderler Zirvesi'nde kabul edilmiştir. Bu belgenin özellikle Asya'da ortaya çıkan küresel riskler nedeniyle örgütü askeri ve politik yönden güçlendirmek ve güvenlik alanındaki ya da stratejik ve politik değişikliklere uyum sağlamak amacıyla hazırlandığı belirtilmektedir. Bu girişimin başlatılmasına, Rusya'nın askeri faaliyetleri, Çin Halk Cumhuriyeti'nin yükselişi, pandemi, bilgi kirliliğinin yaygınlaşması, demokrasi ve insan haklarına yönelik artan tehditler gerekçe olarak gösterilmiştir. Belgede politik istişareden, caydırıcılığa, savunmadan iklim değişikliğine ilişkin 8 öneride bulunulmuştur[293]. Bu kapsamda hazırlanan siber uzay 2030 strateji belgesinde Rusya ve Çin Halk Cumhuriyeti'nin artan siber etkinliği karşısında siber operasyonların yoğunlaşacağı öngörülmektedir. Geleneksel güç kullanımının ve caydırıcılık kavramının değişmesi ve

[291] Bkz.; Mačák, 2018, s. 23.

[292] Rølsåsen, 2016, s. 10.

[293] Therrien-Tremblay, Anne-Marie. (2022). *The NATO 2030 Initiative: Overview and Implications for Canada*. Ottowa: Library of Parliement. Erişim: 24.01.2023. https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/HillStudies/PDF/2022-16-E.pdf

siber operasyonlarla birlikte gerçekleşen hibrit savaşların sebep olduğu risk karşısında NATO'nun yeni bir strateji belirlemesi gerekli görülmektedir[294].

1.5.2. BİRLEŞMİŞ MİLLETLER (BM) TARAFINDAN YAPILAN ÇALIŞMALAR

BM nezdinde 1995 yılında siber suçlarla mücadeleye yönelik olarak yayınlanan Bilgisayar Kaynaklı Suçların Kontrolü ve Önlenmesine dair BM Kitapçığı bu alana ilişkin ilk çalışma olarak gösterilebilir[295]. Daha sonra o dönemdeki adıyla bilgisayar kaynaklı suçlara yönelik kapsamlı iç politika geliştirilmesi çağrısını içeren 55/59 sayılı ve 2000 tarihli karar BM Genel Kurulu tarafından kabul edilmiştir[296].

Siber suçlar yanında siber güvenlik konusu da uluslararası toplumun genel olarak ilgisini çekmekte olup BM'nin himayesinde Cenevre'de 1999 yılında gerçekleştirilen uluslararası uzmanlar toplantısı[297] gelişen bilişim teknolojisi güvenliğine dair ilk çalışmadır. Bu tarihten itibaren BM Genel Kurulu'nca tüm uluslararası toplumun çıkarlarını etkileyen bilgi teknolojileri ve araçlarının kullanılması ve yayılmasına ilişkin bir dizi karar verilmiş, bir dizi Genel Kurul Kararı[298] yayınlanmıştır. BM nezdinde

---

[294] Pernik, Piret (Ed.). (2022). *Cyberspace Strategic Outlook 2030 Horizon Scanning and Analysis.* Tallinn: CCDCOE Publication. Erişim: 24.01.2023. https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_v2_170x240_220513.pdf

[295] Stahl, William M. (2011). *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, GA. J. INT'L & COMP. L., Cilt:40, s. 265.

[296] Stahl, 2011, s. 265.

[297] Hathaway ve diğerleri, 2012, s. 860.

[298] BM Genel Kurulu kararları: 58/32 sayılı ve 08.12.2003 günlü kararı; 59/61 sayılı ve 03.12.2004 günlü kararı; 60/45 sayılı ve 06.06.2006 günlü kararı; 61/54 sayılı ve 19.12.2006 günlü kararı; 62/17 sayılı ve 08.06.2008 günlü kararı; 63/37 sayılı ve 09.06.2009 günlü kararı; 64/25 sayılı ve 14.06.2010 günlü kararı. Ayrıntılı bilgi için bkz.: Hathaway ve diğerleri, 2012, s. 860, dipnot 179.

gerçekleştirilen Bilgi Toplumuna İlişkin Dünya Zirvesi iki aşamalı olarak 2003'de Cenevre'de ve 2005'te Tunus'ta gerçekleştirilmiştir[299].

BM Genel Kurulu tarafından verilen 2004 tarihli ve 58/199 sayılı küresel siber güvenlik kültürü yaratma ve siber kritik altyapı unsurlarının korunmasına yönelik karar ve 2010 tarihli 64/211 sayılı küresel siber güvenlik kültürü oluşturma ve kritik altyapı unsurlarının korunmasına ilişkin ulusal çabaların değerlendirilmesine yönelik karar bu konuda dikkate değer diğer kararlardır[300].

Bu alanda gerçekleştirilen bir diğer çalışma olan ve aralarında; Çin Halk Cumhuriyeti, ABD ve Rusya gibi başlıca siber güçlerden oluşan 15 devlet uzmanlarından oluşan bir grup tarafından hazırlanan tavsiye kararı Haziran 2010 tarihinde BM Genel Sekreterine sunulmuş, devletlerarası diyalog ve güven oluşturulmasına dair birtakım önerilerde bulunulmuştur[301].

1.5.3. AVRUPA KONSEYİ TARAFINDAN YAPILAN ÇALIŞMALAR

23 Kasım 2001 tarihinde imzalanan Siber Suçlara İlişkin Avrupa Konseyi Konvansiyonu[302] 1 Temmuz 2004 tarihinde yürürlüğe girmiş, Konsey üyeleri yanında üye olmayan 14 devletin katılımıyla Konvansiyon evrensel bir boyut kazanmıştır[303]. 2002 tarihli G8 Sınıraşan Suçlara İlişkin Tavsiye kararında siber suçların soruşturulması, cezalandırılması konusunda uluslararası işbirliği ve Siber Suçlara ilişkin Avrupa Konseyi

[299] Roscini, 2010, s. 88.

[300] Afroditi, 2010, s. 34.

[301] Ayrıntılı bilgi için bkz.: Hathaway ve diğerleri, 2012, s. 860.

[302] Sözleşme için bkz.: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[303] Erdem ve Özocak, 2019, s. 156.

Konvansiyonu'nun benimsenmesi tavsiye edilmiştir[304]. Siber saldırıların, bilgisayar veri ve sistemlerine erişilebilirlik, mahremiyet ve bütünleşme, özellikle de yasa dışı erişim, veri ve sisteme müdahale ile ilgili suçları kapsaması nedeniyle Konvansiyon, uluslararası siber saldırıları düzenleyen kapsamlı bir hukuki alt yapı oluşturmaktadır[305].

Konvansiyon'un siber savaş operasyonları için yasaklayıcı bir taslak oluşturabileceği önerilerine karşılık, dolandırıcılık ve çocuk pornografisi gibi suçları düzenleyen Konvansiyon'un geniş ölçekli, devlet destekli siber savaş operasyonlarıyla mücadelede kullanılamayacağı, ancak uluslararası siber antlaşma taslağı için bir başlangıç noktası oluşturabileceği savunulmaktadır[306]. İlk bakışta Konvansiyon'un devlet dışı aktörler ve iç hukukla sınırlı şekilde suç ile mücadeleye yönelik olması nedeniyle uluslararası siber savaş hukukuna önemli bir katkısının olmayacağı düşünülebilir ise de siber saldırılara karşı devletlerin başvurabileceği aktif savunma tedbirlerinin olumsuz yanlarından dolayı yeknesak ve etkin ulusal ceza mevzuatı caydırıcılık açısından oldukça önemlidir. Ayrıca silahlı saldırı düzeyine ulaşmayan siber saldırganlık suçları ve atfedilebilirlik unsuru yoksunluğundan kaynaklı olarak devletlerin sorumluluğuna gidilememesi ve saldırgan bireylerin yargılanması yoluna gidilmesi halinde Konvansiyon'un önemli bir boşluğu doldurduğu söylenebilir. Konvansiyon'un 3. bölümünde yer alan soruşturmada uluslararası işbirliğine, suçluların iadesine ve geçici tedbirlere ilişkin yardımlaşmaya dair düzenlemeler uluslararası toplumu ilgilendiren sınıraşan siber suçlarla mücadelede ve siber güvenliğin sağlanmasında devletlere imkânlar sunmaktadır[307].

Siber Suçlar Konvansiyonu yanında Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol 28 Ocak 2003 tarihinde imzaya açılıp, 1 Mart 2006 tarihinde

[304] Stahl, 2011, s. 265.

[305] Hathaway ve diğerleri, 2012, s. 863.

[306] Afroditi, 2010, s. 33.

[307] Erdem ve Özocak, 2019, s. 157.

yürürlüğe girmiştir[308]. Bu alanda AB nezdinde yapılan diğer bir çalışma ise 2004 yılında Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) kurulmasıdır[309]. ENISA tarafından 2017 tarihinde yayınlanan Ağ ve Bilgi Güvenliği Direktifi ile siber saldırılara karşı üye devletlerarasındaki iş birliği teşvik edilmiştir[310]. Ayrıca kritik bilgi altyapısının korunmasına yönelik Avrupa Toplulukları nezdinde yapılan ilk girişim[311] 2009 yılında başlatılmış, Birleşik Krallık Lordlar Kamarası AB Komitesi tarafından hazırlanan "Avrupa'yı Geniş Ölçekli Siber Saldırılara Karşı Koruma" başlıklı 2010 tarihli rapor[312] ise bu alanda yapılan ikinci çalışmadır[313].

1.5.4. AMERİKA DEVLETLERİ ÖRGÜTÜ TARAFINDAN YAPILAN ÇALIŞMALAR

Temelini 1969 tarihli Amerikan İnsan Hakları Sözleşmesi'nin oluşturduğu ve Amerika Kıtası'ndan 35 devleti temsil eden örgüt[314], Nisan 2004 tarihinde Avrupa Konseyi Siber Suç Sözleşmesi prensiplerinin uygulanması tavsiyesinin değerlendirilmesine yönelik bir karar almış, ayrıca Amerika Devletleri Arasında Kapsamlı Siber Güvenlik Stratejisi'ni kabul etmiştir[315]. Bu strateji kapsamında siber suçların cezalandırılması ve bilişim sistemlerinin korunması konusunda yasal düzenleme yapma ve uygulamaya geçirme

---

[308] Erdem ve Özocak, 2019, s. 156.

[309] ENISA'nın web sayfası için bkz.: https://www.enisa.europa.eu/

[310] Kadıoğlu Kumtepe, Cemre. (2021). *Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliği,* s. 4. Erişim: 11.09.2022 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4083156

[311] Çalışma için bkz.: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[312] Rapor için bkz.: https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf

[313] Afroditi, 2010, s. 33

[314] Doğan, İlyas. (2016). *Devletler Hukuku*. Ankara: Astana Yayınları, s, 440.

[315] Hathaway ve diğerleri, 2012, s. 864.

konusunda teknik yardım sağlamak amacıyla Uzmanlar Grubu uluşturulmuş ancak siber saldırı konusunda genel düzeyde daha aktif bir program ortaya konulamamıştır[316].

1.5.5. ŞANGAY İŞBİRLİĞİ ÖRGÜTÜ TARAFINDAN YAPILAN ÇALIŞMALAR

Çin Halk Cumhuriyeti, Kazakistan, Kırgızistan, Rusya, Tacikistan ve Özbekistan tarafından 2001 yılında kurulmuş bulunan hükümetler arası karşılıklı güvenlik organizasyonu olan Şangay İşbirliği Örgütü'nün (ŞİÖ) kurumları 2004 yılında faaliyete geçmiştir. ŞİÖ'nün beş temel organı bulunmakta olup bunlar; Devlet Başkanları Konseyi, Hükümet Başkanları Konseyi, Dışişleri Bakanları Konseyi, Bakanlar Konferansı ve Ulusal Koordinatörler Konseyi'nin yanı sıra Sekretaryası ve Bölgesel Anti-Terörizm Merkezi'dir[317].

Terör, aşırılık ve ayrıkçılık yanında yeni nesil suçlarla da mücadele merkezi[318] olmayı amaçlayan ŞİÖ tarafından açıklanan 16 Haziran 2009 tarihli Yekaterinburg Deklarasyonu [319] ile üye devletlere uluslararası ortak güvenlik sisteminin temel unsurlarından biri olan uluslararası bilgi güvenliğini sağlama konusunun önemini vurgulamıştır[320]. Aynı örgüt tarafından aynı yıl imzalanan Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması'nda [321] ise uluslararası bilgi güvenliği için öncelikle

---

[316] Hathaway ve diğerleri, 2012, s. 865.

[317] Altundağ, Zehra. (2016). *Geçmişten Günümüze Şangay İşbirliği Örgütü*. Avrasya Etüdleri, Cilt: 49, Sayı:2016/1, s. 111. Erişim: 24.01.2023 https://dergipark.org.tr/en/download/article-file/422162

[318] Altundağ, 2016, s. 109.

[319] Deklerasyon metni için bkz.: Erişim: 17.12.2021

Yekaterinburg_Declaration_by_the_Heads_of_the_Member_States_of_the_SCO.pdf

[320] Hathaway ve diğerleri, 2012, s. 865.

[321] Antlaşma metni için bkz.: Erişim: 17.12.2021)

Agreement_on_Cooperation_in_Ensuring_International_Information_Security_between_the_Member_States_of_the_SCO.pdf

devletlerarasında karşılıklı güvenin derinleştirilmesi ve devletlerarasında işbirliğinin geliştirilmesinin gerekli olduğu ifade edilmiştir[322]. Örgüt ayrıca üye devletlerine, belirtilen bölgesel antlaşma kapsamında bilgi içerikleri üzerinde egemenlik kontrolü sağlanmasının meşru kabul edilmesini önermiştir[323].

Antlaşmanın 2. maddesinde uluslararası bilgi güvenliğine tehdit oluşturan başlıca eylemler belirtilmiştir. Bunlar sırasıyla: bilgi savaşına (siber savaş) hazırlık yapmak ve gerçekleştirmek için bilgi silahı (siber silah) geliştirmek ve kullanmak, bilgi terörizmi (siber terörizm), siber suç, diğer devletlerin güvenliğine ve çıkarlarına zarar vermek için siber uzaydaki baskın konumu kullanmak; diğer devletlerin manevi ve kültürel çevrelerine, sosyo-politik ve sosyo-ekonomik sistemlerine zararlı bilgi yayma; insan yapımı ya da doğal olan küresel ve ulusal bilgi altyapı sistemlerinin istikrarlı ve güvenli çalışmasına tehdit eylemleridir.

Antlaşma'nın 3. maddesinde uluslararası bilgi güvenliğini sağlamada temel işbirliği alanları ortaya konulmuş, siber suçlarla mücadele, tehditlere cevap verme ve ortak izleme sistemi oluşturma, uzmanlık ve bilgi alış verişi gibi hususlar vurgulanmıştır. Antlaşma'nın 4. maddesinde temel insan haklarına saygı ve uluslararası hukuk normları ve ilkeleri ile uyumluluk işbirliğinin temel prensibi olarak kabul edilmiştir. Antlaşma'nın 5. maddesinde ise işbirliğinin şekli ve mekanizması düzenlenmiştir.

1.6. SİBER SALDIRIYI DOLAYLI ŞEKİLDE DÜZENLEYEN ULUSLARARASI HUKUK ALANLARI

Siber saldırı, sadece kuvvet kullanma yasağı ve silahlı çatışmalar hukuku içinde uygulama yeri bulan bir husus olmayıp aynı zamanda uluslararası hukukun hemen diğer bütün alt başlıklarında karşımıza çıkma potansiyeli olan bir konudur. Bu alt başlıklar arasında uluslararası telekomünikasyon hukuku, uluslararası sivil havacılık hukuku,

[322] Erdem ve Özocak, 2019, s. 161.

[323] Kanuck, 2010, s. 1575.

uluslararası uzay hukuku ve uluslararası deniz hukuku yer almaktadır. Bu alanlarda geçerli mevcut hukuk kurallarının siber saldırı konusunda ne şekilde uygulanacağının özellikle Tallinn El Kitabı çerçevesinde incelenmesi gerekli görülmüştür.

1.6.1. ULUSLARARASI TELEKOMÜNİKASYON HUKUKU

Uluslararası kablolu ve radyo frekansı iletişimini içeren siber saldırılar telekomünikasyon hukukuna konu olabilmektedir [324] . Telekomünikasyon konusunda 1973 Malaga-Torremolinos Uluslararası Telekomünikasyon Sözleşmesi gereğince haberleşme toplum için bir hak olarak görülmekte ve haberleşme serbestliği ilkesi kabul edilmektedir[325]. Haberleşme serbestliği ilkesi geçerli olmakta ve gökyüzünün tek başına sahiplenilmesi mümkün değilse de kablosuz iletişime ve medya yayınlarına Uluslararası Telekomünikasyon Birliği (UTB) himayesinde yasal kısıtlamaların getirilebileceği kabul edilmektedir[326].

UTB'nin amacı, yeterli iletişim hizmetleri vasıtasıyla tüm devletlerarasında barışın, ekonomik ve sosyal gelişmenin korunması olarak ifade edilmiştir[327]. UTB çerçevesinde 1959 tarihinde imzalanan Radyo Yönetmeliği, bir devletin ülkesi dışında, açık denizde, kurulan gezici istasyonlar aracılığıyla yayın yapılmasını yasaklamış ve bunu sağlama görevini ilgili devletlere bırakmıştır [328] . Uluslararası telekomünikasyon kurallarını düzenleyen UTB Kurucu Antlaşması da taraf devletlere birtakım sorumluluklar yüklemiştir. Uluslararası iletişimin siber alanı da kapsaması nedeniyle uluslararası telekomünikasyon kurallarının devletlere yüklediği sorumluluklar siber alan üzerinden gerçekleştirilen iletişim yönünden de geçerlidir. Buna karşın, UTB Antlaşması uyarınca

[324] Hathaway ve diğerleri, 2012, s. 866.

[325] Pazarcı, 2021, s. 320-321.; Toluner, Sevin. (1996). *Milletlerararası Hukuk Dersleri Devletin Yetkisi*. İstanbul: Beta, s. 48.

[326] Kanuck, 2010, s. 1574.

[327] Hathaway ve diğerleri, 2012, s. 867.

[328] Pazarcı, 2021, s. 321.

bazı kısıtlamaların uygulanması mümkün ise de siber saldırılar gibi askeri amaçlı kullanımların özellikle yasaklanamayacağı kabul edilmektedir[329].

Tallinn El Kitabı'na bakıldığında UTB Kurucu Antlaşması'nın 33. maddesi gereğince devletler telekomünikasyon altyapı tesislerini kurma, 37. maddesinde düzenlenen iletişimin gizliliği ve 38. maddesinde düzenlenen hızlı ve kesintisiz iletişimi sağlama yükümlülüklerini taşırlar. Aynı Antlaşma'nın 34 ve 35. maddelerinde, kamu düzeni ve ulusal güvenliğin tehlike altında olması durumunda devletlere, siber iletişimin durdurulması ya da askıya alınabilmesi olanağı tanınmaktadır. Kamu düzeni ve ulusal güvenlik kavramlarının kötüye kullanılması halinde ise, UTB mevzuatına aykırılık söz konusu olacaktır.

1.6.2. ULUSLARARASI SİVİL HAVACILIK HUKUKU

Hava ulaşımı konusunda, deniz ulaşımının aksine, yerleşik uluslararası yapılageliş kuralları bulunmamaktadır[330]. Hava taşımacılığı konusunu düzenleyen 1919 tarihli Paris Hava Ulaşım Sözleşmesi[331], 1929 Varşova Sözleşmesi ve onu değiştiren 1955 Lahey Protokolü ile hava araçlarının vereceği zararlar nedeniyle sorumluluk konusunu düzenleyen 1933 Roma Sözleşmesi ve onu değiştiren 1952 Sözleşmesi bu alanda hayata geçen ilk sözleşmelerdir[332]. Uluslararası havacılık alanında gerçekleşen saldırılara yönelik hükümler içeren diğer uluslararası antlaşmalar ise, 1963 tarihli Hava Araçlarında İşlenen Suçlar ve Diğer Bazı Eylemlere İlişkin Sözleşme (Tokyo Sözleşmesi) ve 1970 tarihli Hava Araçlarına Hukuka Aykırı El Konulmasının Önlenmesine dair Sözleşmedir (Lahey Sözleşmesi)[333]. Bunlardan başka siber saldırı durumunda uygulanabilecek uluslararası hukuk kurallarını düzenleyen sözleşmeler arasında en başta gelen Şikago

[329] Hathaway ve diğerleri, 2012, s. 868.

[330] Sur, 2022, s. 426.

[331] Sur, 2022, s. 425.

[332] Pazarcı, 2021, s. 311.

[333] Akkutay, Ekim 2017, s. 156.

Sözleşmesi olarak adlandırılan 1944 Uluslararası Sivil Havacılığa dair Şikago Konvansiyonu [334] yanında Montreal Sözleşmesi olarak anılan 1971 tarihli Sivil Havacılığa Karşı Yasadışı Eylemlerin Bastırılmasına İlişkin Konvansiyon yer alır. Ayrıca 1988 yılında düzenlenen Ek Protokol ile Montreal Sözleşmesi'nde bazı hususlarda ilave düzenlemeler yapılmıştır. 1944 tarihli Şikago Sözleşmesi, 1971 tarihli Montreal Sözleşmesi ve 1988 tarihli Ek Protokol'ün askeri olmayan havacılığı hedefleyen siber operasyonlar ile ilgili düzenlemeler olduğu kabul edilmektedir[335].

1919 Paris Antlaşması ile Uluslararası Ulaşım Komisyonu kurulmuştu[336]; 1944 Şikago Sözleşmesi ile uluslararası hava trafiğini düzenlemek ve koordine etmekle görevli bir özel BM ajansı (Uluslararası Sivil Havacılık Örgütü) kurulmuş, ayrıca hava sahası, hava araçları, seyrüsefer, kayıt ve güvenlik konularında bir kurallar seti oluşturmuştur[337]. Dört bölümden oluşan Uluslararası Sivil Havacılık Sözleşmesi'nin ilk bölümünde ulusal hava sahası üzerinde uçuş, hava araçlarının tabiiyeti, hava ulaşımını kolaylaştırıcı önlemler, uçuş sırasında uyulacak kurallar ve havacılığa ilişkin uluslararası standartlar düzenlenmiş, diğer bölümlerde bahse konu örgütün kuruluşu ve diğer kurallar düzenlenmiştir[338].

Hava sahası, ulusal hava sahası ve uluslararası hava sahası olarak ikiye ayrılmaktadır[339]. Şikago Sözleşmesi'nin ilk iki maddesi gereğince devletler ulusal hava sahalarında tam egemenlik hakkını haizdir[340]. Bu nedenle hava sahasında bulunduğu devletin ülkesini,

---

[334] Şikago Konvansiyonu 4 antlaşmadan oluşur. Bunlar: Uluslararası Sivil Havacılık Geçici Antlaşması; Uluslararası Sivil Havacılık Sözleşmesi; Uluslararası Hava Servisleri Transit Antlaşması; Uluslararası Hava Ulaşım Antlaşması. Bkz.; Pazarcı, 2021, s. 311.

[335] Hathaway ve diğerleri, 2012, s. 868.

[336] Sur, 2022, s. 431.

[337] Hathaway ve diğerleri, 2012, s. 869.

[338] Pazarcı, 2021, s. 312.

[339] Pazarcı, 2021, s. 313.; Sur, 2022, s. 428-429.

[340] Türk Sivil Havacılık Kanunu'nun 4. Maddesi uyarınca "Türkiye Cumhuriyeti, Türk hava sahasında tam ve münhasır egemenliği haizdir. Sur, 2022, s. 426.; Toluner, 1996, s. 40.

hukuk düzenini ve ulusal güvenliğini etkileyen, uçuş güvenliğini veya havacılık düzenlemelerini ihlal eden suçların bir hava aracında işlenmesi halinde yetkili devletin belirleyeceği havaalanına iniş emri vermesi hukuka uygundur[341]. Hava sahasının kullanıldığı devleti belirtilen şekilde etkilemeyen diğer siber faaliyetlerde ise, kayıtlı devletin yargı yetkisinin bulunduğu kabul edilmektedir[342].

Tokyo, Lahey ve Montreal Sözleşmelerinin tamamı Uluslararası Sivil Havacılık Örgütü (*International Civil Aviation Organization*/ICAO) tarafından gerçekleştirilen çalışmalar sonucu oluşturulmuştur[343]. Sivil havacılık konusunda yetkili beş havacılık örgütü Uluslararası Sivil Havacılık Örgütü, Uluslararası Hava Taşımacılığı Derneği (IATA), Uluslararası Havaalanları Konseyi (ACI), Sivil Hava Ulaştırma İşletmeleri Birliği (CANSO) ve Uluslararası Havacılık Sanayi Birlikleri Koordine Konseyi (ICCAIA) 10 Aralık 2014 tarihinde Montreal'de siber tehditlere karşı gerçekleştirecekleri eylemler konusunda gösterecekleri işbirliğine ilişkin ortak bir yol haritası üzerinde uzlaşmışlardır[344].

Montreal Sözleşmesi, sivil havacılığın güvenliğini tehlikeye sokan bazı yasadışı eylemlerin çerçevesini çizmektedir[345]. Montreal Sözleşmesi'nin siber saldırılara uygulanabilirliği, Sözleşmenin 1. maddesi gereğince bir hava aracının uçuşunun engellenmesi veya hava aracının uçuş güvenliğinin ciddi şekilde tehlikeye sokulmasıyla sınırlı olup Montreal Protokolü'nün 2. maddesi ile havalimanlarının güvenliğinin zaafa uğratacak eylemler yasaklanmıştır[346]. Şikago Sözleşmesi'nin 3. maddesinde ise devletlerin sivil havacılığı tehlikeye düşürecek silah kullanımından kaçınma zorunluluğu

[341] Schmitt, 2017, *Tallinn Manual 2.0.* s. 263.

[342] Schmitt, 2017, *Tallinn Manual 2.0.* s. 263.

[343] Akkutay, Ekim 2017, s. 157.

[344] Akkutay, Ekim 2017, s. 168.

[345] Hathaway ve diğerleri, 2012, s. 869.

[346] Hathaway ve diğerleri, 2012, s. 869-870.

söz konusu olduğundan, Tallinn El Kitabı Kural 57'de silah olması nedeniyle sivil havacılığı tehlikeye düşürecek siber operasyonlar yasaklanmıştır[347].

1.6.3. ULUSLARARASI UZAY HUKUKU

Teknik olarak uzaydan uydular aracılığıyla haberleşme ve yayın olanaklarının doğması üzerine, daha önce bu konuyu hava sahası bakımından düzenleyen Uluslararası Telekomünikasyon Birliği kurucu antlaşmaları ve eklerinin uygulanabilirliği uzay için de kabul edilmiştir[348]. Buna paralel olarak öğretide, BM Şartı 2/4 maddesinde düzenlenen kuvvet kullanma yasağının yer bakımından (*ratione loci*) uzayı da kapsadığı kabul edilmektedir[349]. İnsanlığın ilk kez uzaya gittiği 1961 yılında BM Genel Kurulu kararıyla "uzayın serbestliği ilkesi" ilan edilmiştir[350]. Ayrıca BM Genel Kurulu'nun 13.12.1963 gün ve 1962 sayılı kararıyla kabul ettiği Uzayın Araştırılması ve Kullanılması Konusunda Devletlerin Faaliyetlerini Yöneten Hukuksal İlkeler Bildirisi bu alandaki temel belgelerdendir[351]. Bunu, uzay hukukunun siber saldırıları ilgilendiren alanları dış uzayın ve uyduların barışçıl amaçlarla kullanımını öngören 1967 tarihli Dış Uzayın Kullanımı ve İşletilmesi Faaliyetleri Yöneten İlkelere İlişkin Antlaşma [352] ile 1971 tarihli

---

[347] Schmitt, 2017, *Tallinn Manual 2.0.* s. 268.

[348] Pazarcı, Hüseyin. (2003). *Uluslararası Hukuk Dersleri.* 2. Kitap (7. bs.). Ankara: Turhan Kitabevi, s. 445.

[349] Erkiner, Hakan Hakkı. (2020). *Uluslararası Hukukta Kuvvet Kullanma Yasağının Kişi bakımından (Ratione Personae), yer Bakımından (Ratione Loci) ve Konu Bakımından (Ratione Materiae) Uygulanabilirliği,* Karadeniz 3. Uluslararası Sosyal Bilimler Kongresi, s. 285. Erişim: 11.09.2022 https://www.researchgate.net/publication/352826229_Uluslararasi_Hukukta_Kuvvet_Kullanma_Yasaginin_Kisi_Bakimindan_Ratione_Personae_Yer_Bakimindan_Ratione_Loci_Ve_Konu_Bakimindan_Ratione_Materiae_Uygulanabilirligi

[350] Sur, 2022, s. 435.; Hava sahasından farklı olarak, uzay ve gök cisimlerinin hukuki statüsü konusunda, egemenlik ilkesinden hareket edilmemiştir. Bkz.: Toluner, 1996, s. 49.

[351] Pazarcı, 2021, s. 322.

[352] 1967 Uzaya İlişkin İlkeler Antlaşmasıolarak da bilinen bu antlaşmada yer alan bir kısım ilkeler şimdiden genel uluslararası örf ve adet kuralı niteliğini almıştır. Bkz.; Sur, 2022, s. 435.

Telekomünikasyon Uydu Örgütüne İlişkin Antlaşma ve 1979 tarihli Uluslararası Denizcilik Uydu Örgütü Antlaşması izlemiştir[353].

Tallinn El Kitabı'nda uluslararası uzay hukukunun siber operasyonlarda iki şekilde uygulama yeri bulabileceği belirtilmektedir[354]. İlk olarak, uzay konumlu siber altyapı tesisleri haricinde uzayla da az ilişkili olan uydudan yere veya uyudular arası iletişimlerde uzay vasıtasıyla siber operasyonlar bu kapsamda değerlendirilmektedir. Bu ilk siber operasyonların uzayda bulunan uydular ya da uzayda konuşlu siber altyapı sistemleri vasıtasıyla gerçekleştirilen Dünyaya ait iletişimin siber operasyonlarda hedef alınması söz konusudur. İkinci olarak ise, siber teknolojinin olanaklı kıldığı uzay operasyonları ifade edilmektedir. Uzayın olanaklı kıldığı siber operasyonlarda, uzay araçları ile uzay üslerine yönelik olarak siber araçlar kullanılarak operasyon gerçekleştirilmektedir.

Uzay boşluğunda bulunan uydular vasıtasıyla gerçekleştirilen iletişime yönelen siber saldırılara yönelik yukarıda belirtilen telekomünikasyon hukuku kapsamında UTB Kurucu Antlaşması'nın 33-38. maddelerinde devletlere görevler yükleyen hususların uygulama yeri bulduğu anlaşılmaktadır. Mevcut hükümlerin gelişen teknolojiye göre yorumlanması kaçınılmaz olduğundan uzay boşluğu ile ilişkili olmayan telekomünikasyon yanında, uzayda bulunan vasıtalar üzerinden sağlanan iletişimin de belirtilen sözleşme içerisinde değerlendirilmesi zorunludur.

Uluslararası telekomünikasyon hukukunun uzay hukuku ile kesişen düzenlemelerinden başka uzay hukukunun kendi içinde barındırdığı bazı ilkeler, siber araçlar ile uzayda gerçekleştirilen operasyonlarda da uygulama yeri bulmaktadır. Tallinn El Kitabı 58. Kural'da Ayda ya da diğer uzay cisimlerinde gerçekleştirilecek siber operasyonların

---

[353] Hathaway ve diğerleri, 2012, s. 871. Astronotların kurtarılması, uzay cisimlerinin tescili ve bunlardan kaynaklı zarar ve gök cisimlerine ilişkin devlet faaliyetleri konularına ilişkin diğer antlaşmalar için bkz.; Sur, 2022, s. 435-436.

[354] Schmitt, 2017, *Tallinn Manual 2.0.* s. 270.; Genel olarak uzayın araştırılması ve kullanılmasına ilişkin faaliyetlerle ilgili kurallar uzaya yönelik ve uzaydan dünyaya yönelik faaliyetler şeklinde düzenlenmektedir. Bkz.: Pazarcı, 2021, s. 325-326

barışçıl olması gerektiği belirtilmiştir. Bu kuralda belirtilen bir diğer durum ise, dış uzayda gerçekleştirilen siber operasyonların uluslararası kuvvet kullanma sınırlandırmalarına tabi olmasıdır. Uzayda gerçekleştirilecek faaliyetlerin barışçıl olması gerekliliği, öğretide her türlü askeri amacı dışarıda bıraktığı şeklinde yorumlanmaktadır. Zira 1963 Bildirisi ve 1967 Antlaşması'na bakıldığında uzayın askeri amaçlı araştırılması ve kullanılmasının "bütün ülkelerin yarar ve çıkarlarına" uygun olamayacağı değerlendirilmektedir[355].

Tallinn El Kitabı'nda belirtilen, uzay hukuku kapsamında gerçekleştirilebilecek siber operasyonları düzenleyen diğer birtakım kurallar şunlardır; diğer devletlerin uzaydaki siber faaliyetlerine saygı ve diğer devletlerin barışçıl siber faaliyetlerine müdahale etmeme (Kural 59), hükûmet dışı varlıkların uzaydaki siber faaliyetlerinin devletler tarafından yetkilendirilmesi, denetlenmesi ve devletlerin yükümlülükleri ve sorumlulukları taşımasıdır (Kural 60).

1.6.4. ULUSLARARASI DENİZ HUKUKU

Uluslararası deniz hukukunun siber savaşta uygulama yeri bulması mümkündür. Deniz Hukukuna İlişkin 1982 tarihli BM Konvansiyonu'nun 19., 109. ve 113. maddeleri denizde siber saldırılarla ilgilidir[356]. Sözleşmenin 19. maddesi zararsız geçişi[357], 109. maddesi açık denizlerde yapılan yetkisiz yayını ve 113. maddesi ise denizaltı kablolarını düzenlemektedir. Tallinn El Kitabı'nda uzmanların kabulüne göre uluslararası deniz hukuku, okyanuslar da dâhil olmak üzere denizde konumlu siber altyapı tesislerinden ya

[355] Pazarcı, 2021, s. 324-325.; Sur, 2022, s. 437-438.

[356] Hathaway ve diğerleri, 2012, s. 872.

[357] Kıyı devletinin zararsız geçiş hakkını kullanan gemiler üzerindeki hukuki ve cezai yargı yetkisi sınırlıdır. Aksar, Yusuf. (2021). *Teoride ve Uygulamada Uluslararası Hukuk II.* Ankara: Seçkin, s. 50.; Bununla birlikte bir devletin karasularından zararsız geçiş hakkını kullanırken kıyı devletine yönelik siber casusluk faaliyetinin gerçekleştirilmesi halinde kıyı devletinin hukuka aykırı faaliyette bulunan bu gemiyi karasularından çıkarma hakkı gündeme gelmektedir.

da bu tesisler vasıtasıyla gerçekleştirilen siber operasyonlara uygulanabilmektedir[358]. Siber altyapı tesislerinin denizin altında ya da üzerinde konumlanması önem arz etmeksizin denizin üzerinde seyreden gemi ya da denizaltı aracından gerçekleştirilen bir siber operasyona uluslararası deniz hukuku kurallarının uygulanması her iki durumda da söz konusu olabilecektir.

Tarihten gelen açık denizlerin serbestliği ilkesi[359] siber operasyonlarda uluslararası hukukun aksini öngörmemesi halinde açık denizlerde siber operasyonların ancak barışçıl amaçla gerçekleştirilmesini zorunlu kılmaktadır[360]. Tallinn El Kitabı Kural 45'de bu husus üzerinde durulmuştur. Açık denizlerde veya münhasır ekonomik bölgede siber araçlardan yararlanılarak korsanlık, köle ticareti ve yetkisiz yayın eylemlerinin gerçekleştirilmesi halinde bayrak devletinin rızası olmaksızın diğer devletlerin gemiyi sanal ya da fiziki ziyaret haklarının bulunduğu kabul edilmektedir[361]. Buna göre sosyal medyada köle ticareti yapıldığına dair önemli kanıtların tespiti halinde herhangi bir devlet tarafından ilgili gemiye fiziki ziyaret yapılması[362] ve sanal ortamda gerekli önleyici önlemlerin alınması mümkündür.

Benzer şekilde karasularında, takımadalarda, bitişik bölge deniz alanlarında ve uluslararası boğazlarda gerçekleştirilen ve bu bölgelere ilişkin uluslararası rejime aykırı

---

[358] Schmitt, 2017, *Tallinn Manual 2.0.* s. 232.

[359] BMDHS madde 88. Tarihi süreç için bkz.; Sur, 2022, s. 401-402.; Bu ilke kapsamında 1958 tarihli Açık Deniz Sözleşmesi'nin 2. maddesi ile seyrüsefer serbestisi, uçuş serbestisi, sualtı kablo ve boru hattı döşeme serbestisi ve balıkçılık serbestisi tanınmış; 1982 tarihli Deniz Hukuku Sözleşmesi'nin 87. maddesi ile bunlara bilimsel araştırma ve yapay ada ve diğer tesis serbestisi ilave edilmiştir. Bkz.: Aksar, 2021, (2. Kitap), s. 91.

[360] Schmitt, 2017, *Tallinn Manual 2.0.* s. 233.; Açık deniz serbestisi ilkesi mutlak ve sınırsız değildir. BMDHS'nin 88. maddesi gereğince "açık denizin barışçı faaliyetlere konu olması" kuralı yanında, açık denizde ulaşımının güvenliği, doğal veya canlı kaynaklar ile çevrenin korunmasına ilişkin kısıtlayıcı kurallar söz konusudur. Bkz.; Sur, 2022, s. 402-403.

[361] Schmitt, 2017, *Tallinn Manual 2.0.* s. 235-239.; Uluslararası hukukta kural olarak açık denizlerde seyir halindeki gemilere ilişkin yargı yetkisini bayrak devletine tanımıştır. Aksar, 2021, (2. Kitap), s. 91.

[362] BMDHS madde 110.

siber faaliyetlerden dolayı sonuçlarının uzandığı kıyı devletinin birtakım yetkileri kullanması mümkündür. Tallinn El Kitabı 54. Kural'da kabul edilen bir başka husus ise denizaltı kablolarına ilişkin uluslararası hukuk rejiminin denizaltı telekomünikasyon kablolarına uygulanacağı yönündedir. Netice olarak, deniz hukukuna ait yapılageliş kuralları, uygun düşmesi halinde ilgili deniz alanlarında gerçekleştirilen siber faaliyetlere de uygulanabilecektir.

2. BÖLÜM: SİBER UZAYDA DEVLETİN YETKİ VE SORUMLULUĞU

2.1. SİBER UZAY VE EGEMENLİK

Egemenlik ilkesi, tarihi süreç içerisinde Avrupa'daki monarşilerin papalık ve Roma-Cermen İmparatorluğu arasındaki güç mücadelesi sonucunda ortaya çıkmıştır. Bu ilke, Fransa kralları tarafından ülke içinde kendi iktidarlarına rakip olabilecek bir iktidar, ülke dışında da kendilerinden üstün bir kudret tanınmadığını ifade etmekteydi[363]. Jean Jaques Rousseau'ya göre, doğanın herkese bütün organları üzerinde mutlak bir erk vermesi gibi, toplumsal sözleşme de siyasi gövdeye kendi organları üzerinde mutlak bir hak sağlamaktadır ki genel iradenin yönettiği bu erk egemenlik adını alır[364].

Devletin temel ölçütü olarak kabul edilen[365] ve devlete ulusal ve uluslararası alanda birtakım yetki ve yükümlülükler sunan egemenlik ilkesi, günümüzde de devletin kendisinden başka hiçbir öğeye bağımlı olmamasını ifade etmektedir[366]. Ancak küreselleşme, kalkınma, nüfus artışı, teknolojik ilerleme ve demokratikleşme hususları, uluslararası hukukun karşılayabileceği küresel kamusal mallara olan talebi ve yerel hükûmetler üzerindeki baskıyı artırmıştır[367]. Soğuk savaş sonrası, devletlerin egemen eşitliği ilkesi büyük değişimlere uğramıştır[368]. Bu bağlamda, klasik egemenlik teorisinin

---

[363] Kapani, Münci. (1992). *Politika Bilimine Giriş.* Ankara: Bilgi Yayınevi, s. 55-56.

[364] Rousseau, Jean Jaques. (2008). *Toplum Sözleşmesi* (Çev. Ali Alper). İstanbul: Oda Yayınları, s. 31.

[365] Sur, 2022, s. 120.

[366] Pazarcı, 2003, (2. Kitap), s. 18.; Sur, 2022, s. 121.

[367] Trachtman, Joel P. (2013). *The Future of International Law Global Government*. New York: Cambridge University Press, s. 83-84. Ulus devletin klasik egemenlik hakkının dönüşümüne dair ayrıca bkz.; Aybudak, Utku. (2017). *Modern Devlet Bağlamında Ortaya Çıkan Egemenlik Kavramı ve Egemenliğin Dönüşümü.* Uluslararası Sosyal Araştırmalar Dergisi, Cilt:10, Sayı:54, s. 226-237.

[368] Aksar, 2021, (1. Kitap), s. 27.

günümüzde değerini ve geçerliliğini kaybettiği kabul edilmekte[369] ve bu nedenle küreselleşme ve teknolojik dönüşümün devlet egemenliğinin düşüşüne işaret etmekte olduğu müjdelenirken; görünen gerçeklik bunun aksi yönde gerçekleşmiştir[370]. Egemen eşitlik ilkesinin gerçek anlamda eşitlik olmadığı bazı devletlerin "daha eşit olduğu" yönündeki genel eleştiriler bir yana, uygulanan uluslararası hukukta halen devletin temel unsuru kabul edilen egemenlik ilkesinin devletlere içsel[371] ve dışsal alanda sağladığı hak ve yükümlülükler siber uzayın hukuki statüsünde de en belirleyici unsur olmuştur.

Uygulanan uluslararası hukukta halen belirleyici unsur olarak kabul edilen egemenlik hakkına bağlı bazı önemli ilkeler söz konusudur. Bunlar; egemen eşitlik ilkesi, içişlerine karışmama ilkesi ve doğal kaynakların üzerinde sürekli egemenlik ilkesidir[372]. Bu ilkelerin ilki olan egemen eşitlik ilkesinin devletlere öncelikle sağladığı en temel yetki ulusal alanda kendini gösterir. Bu ilke, devlete içsel alanda münhasıran iktidar ve yetki sağlar ki bu durum *Palmas Adası Davası*'nda teyit edilmiştir[373]. Kısaca ifade etmek gerekirse bu ilke, devletin egemenlik yetkisini kullanırken uluslararası hukukun öngördüğü yükümlülükler dışında başka hiçbir otoriteye bağımlı olmaması ve devletin ülkesi üzerinde egemenlik yetkisini münhasır bir şekilde kullanmasını sağlar[374]. İkinci sırada belirtilen iç işlerine karışmama ilkesinin bir sonucu ise müdahale yasağıdır[375]. Doğal zenginlikler üzerinde daimi egemenlik ilkesi gereği, kamu yararı, yabancılar

[369] Kapani, 1992, s. 61.

[370] Betz ve Stevens, 2011, s. 55.

[371] İçsel egemenlik iki farklı anlam taşımaktadır. İlk ve asıl anlamı, devlet iktidarının en üstün olma, sınırsız ve mutlak, bölünmez ve devredilemez olmasını ifade ederken, ikinci olarak devlet iktidarının niteliği değil fakat doğrudan doğruya kendisini, onun içeriğini ve kapsamını ifade eder. Bkz.; Kapani, 1992, s. 58.

[372] Pazarcı, 2003, (2. Kitap), s. 22. ; Devletlerin egemenliği aynı zamanda uluslararası hukukun bir temel ilkesidir. Bkz.: Sur, 2022, s. 120.

[373] Sur, 2022, s. 120.; Jensen, 2015, s. 283.

[374] Pazarcı, 2003, (2. Kitap), s. 20. Yetkinin münhasır olması uygulamada özellikle yabancıların durumu bakımından kendini göstermektedir. Yabancılara vize verilmesi, iltica, sınır dışı etme, suçluların iadesi ülke devletinin takdirindedir. Sur, 2022, s. 122.

[375] Sur, 2022, s. 129.

arasında ayrım gözetmeme ve bedel ödenmesi şartıyla yabancıların mallarının millileştirilmesi mümkün kabul edilmektedir[376].

Buna karşın, Rousseua'ya göre, egemenlik ne kadar mutlak, dokunulmaz olursa olsun genel uzlaşmanın sınırlarını aşamaz[377]. Bu bağlamda mutlak yetki sağlayan egemen eşitlik ilkesinin devletlere yüklediği bazı yükümlülüklerden de bahsetmek gerekir. Egemen eşitlik ilkesinden kaynaklanan yükümlülükler, egemenlik hakkını kullanılırken diğer devletlerin egemenlik hakkına saygı gösterme ve uyuşmazlıkların barışçıl yollarla çözülmesidir[378]. Diğer bir önemli yükümlülük, UAD'nın *Korfu Kanalı Davası*'nda ortaya konulan devletlerin bilerek ülkelerini diğer devletlere zarar verecek şekilde kullandırmamak zorunda olmasıdır[379]. Bundan başka, UAD'nın *Tahran Rehineler Davası*'nda[380] ortaya koyduğu üzere, ülkesinde bulunan diğer devlet vatandaşlarını koruma yükümlülüğü[381], bir diğer ifade ile diğer devletlerin haklarını koruma konusunda gerekli adımları atma yükümlülüğü, yine Hakemlik *Trail Smelter* Hakemlik Kararı'nda[382] ortaya konulan başka devletlere zarar doğuracak biçimde ülke topraklarını kullandırmama yükümlülüğü[383] ülkesel egemenlikten kaynaklanan yükümlülüklerdir. Zira egemen eşitlik ilkesi aynı zamanda tüm devletlere diğer devletlerin ülkesel egemenliğine saygı gösterme yükümlülüğü getirmektedir ki UAD *Nikaragua Davası*'nda ülkesel egemenliğe saygının uluslararası ilişkilerin esaslı bir dayanağı olduğu

---

[376] Sur, 2022, s. 125.

[377] Rousseau, 2008, s. 34.

[378] Jensen, 2015, s. 286-287.

[379] Jensen, 2015, s. 293.

[380] UAD, "*Case Concerning United States Diplomatic and Consular Staff in Tehran*", 24 Mayıs 1980, Erişim: 16.07.2022 https://www.icj-cij.org/public/files/case-related/64/064-19800524-JUD-01-00-EN.pdf

[381] Devlet, "due diligence" ilkesi gereği genel olarak ülkesindeki yabancıları korumakla yükümlüdür. Bkz.: Sur, 2022, s. 129.

[382] Hakemlik Kararı, "*Trail Smelter Case*", 16 Nisan 1938 ve 11 Mart 1941, Erişim: 16.07.2022 https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf

[383] Jensen, 2015, s. 293.

vurgulanmıştır[384]. Birbirini tamamlayıcı olan bu ilkeler, egemen devletlerin eşitliğini, birbirlerinin içişlerine karışmamalarını ve ülke kaynakları üzerindeki hakların kullanılabilmesini teminat altına almaktadır. Buna paralel olarak egemenlik ilkesinin, kendi kaynak ve arzularına göre her devlete siber kapasitesini geliştirme hakkını da sağladığı kabul edilmektedir[385].

Tallinn El Kitabı'nda 1 ila 3. kurallar arasında genel olarak egemenlik ve egemenliğin içsel ve dışsal yönleri incelenmiş, 4. kural olarak egemenliğin ihlali başlığı altında devletlerin diğer devletlerin egemenliğini ihlal edecek siber operasyonları gerçekleştirmeme yükümlüğü ifade edilmiştir. Devletlerin siber operasyonlarının diğer devletlerin egemenlik haklarının ihlalini oluşturmasının istisnasını, genel hükümler çerçevesinde Güvenlik Konseyi'nin yetkilendirmesi ve doğal meşru müdafaa hakkının kullanılması olarak ifade etmek mümkündür. Tallinn El Kitabı'nda bu, 71. ve 76. kurallarda ifade edilmiştir.

Bir devletin kendi ülkesinde sahibi olduğu içsel egemenlik yetkisi iki uluslararası hukuki hak sağlamaktadır. Bu hakların ilki siber altyapı unsurları ve aktiviteleri devletin iç yasal ve düzenleyici kontrolüne tabi olmasıdır[386]. Bunun sonucu olarak bir devlet ülkesinde konumlanmış siber altyapı tesisleri diğer devletlerin müdahalesine karşı koruma altındadır[387]. Ülkesel egemenlik olarak da ifade edilebilecek içsel egemenliğin siber uzayı kapsayabilmesi için öncelikle siber altyapı tesislerinin ilgili devletin kara ülkesinde, iç sularında ve kara sularında ya da uygulanabildiği ölçüde takımada suları ya da ulusal hava sahasında konumlu olması gereklidir[388]. Siber altyapı tesislerinin, özel ya da kamuya ait olması bu sonucu değiştirmemektedir. Örneğin, egemen bir devletin ülke üzerinde

[384] Jensen, 2015, s. 293.

[385] Jensen, 2015, s. 287.

[386] Schmitt, 2017, *Tallinn Manual 2.0.* s. 13.

[387] Heinegg, 2012, s. 11.

[388] Heinegg, 2012, s. 11.

konumlanmış bir özel internet servis sağlayıcısı (ISP), yurt dışında merkezli olsa dahi konumlandığı egemen devletin hukukuna tabi olacaktır[389].

Siber uzayın fiziki katmanında egemenlik ilkesinin geçerli olduğu dikkate alındığında, devletin kıta sahanlığı üzerindeki denizaltı telekomünikasyon kabloları üzerinde egemen devletin yargı yetkisinin söz konusu[390] olduğu da kabul edilmelidir. Bunun yanında bir devletin egemenliği altındaki bir hava ya da deniz aracı ya da diğer bir platformda bulunan siber altyapı unsurları da bu devletin egemenliği koruması altındadır[391]. Fiziki ortama ilaveten, egemenlik prensibi devlete ülkesi üzerinde siber uzayın mantıksal katmanı açısından kontrol yetkisi de bahşetmektedir[392].

Tüm devletlerin antlaşmalara dayalı olarak egemenlik hakkını birlikte paylaştıkları, münhasır egemenlik imkânı tanımayan Antarktika, derin deniz yatakları ve Ay gibi küresel ortak alanlara[393] siber uzayın dâhil edilip edilmeyeceği konusunda henüz bir uzlaşı bulunmamaktadır. Siber uzayın bu türden bir ortak alan olarak kabulü halinde siber uzayın yönetimi ve veri akışı üzerinde devletlerin egemenlik haklarını ne şekilde kullanacakları da belirsizliğini korumaktadır. ABD'nin bu konudaki yaklaşımı şirketler, teknik uzmanlar, sivil toplum örgütleri, topluluklar ve hükümetlerin katılımıyla oluşturulan özel bir yönetim tarafından internetin yönetileceği yönündedir. Çin Halk Cumhuriyeti tarafından 2017 yılında yayınlanan Siber Uzayda İş Birliği Hakkında Strateji Belgesi'ne göre, siber uzay tüm insanlığın etkinliklerini gerçekleştirdiği bir alan olarak tüm devletler tarafından yönetilmelidir[394].

---

[389] Schmitt, 2017, *Tallinn Manual 2.0.* s. 13-14.; Heinegg, 2012, s. 12.

[390] Schmitt, 2017, *Tallinn Manual 2.0.* s. 14.

[391] Heinegg, 2012, s. 12.

[392] Schmitt, 2017, *Tallinn Manual 2.0.* s. 14.

[393] Jensen, 2015, s. 284.

[394] Kadıoğlu Kumtepe, 2021, *Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliği,* s. 3.

Siber uzayın gerek fiziken ve gerekse de kontrol mekanizması olarak tek bir devletin egemenlik alanında bulunmaması nedeniyle bir devletin, egemenlik alanında bulunan siber uzaya bağlı siber altyapılar üzerindeki egemenlik hakkından feragat etmiş sayılıp sayılmayacağı konusunda Tallinn El Kitabı'nda bunun feragat şeklinde yorumlanamayacağı ifade edilmiştir[395]. Zira egemenlik prensibinin bir uzantısı olarak, devletlerin internet bağlantısını sonlandırma hakkını haiz olduğu gibi, siber altyapı unsurları uluslararası antlaşma ve yapılageliş hukuku sınırlamalarına ve özellikle de uluslararası insan hakları hukukuna tabidir[396]. Silahlı çatışmalar hukukunun geçerli olduğu bir dönemde ise, savaşanlar açısından meşru hedef oluşturan siber altyapı unsurları üzerinde içsel egemenlik koruması söz konusu değildir[397].

İçsel egemenlik yetkisinin devlete sağladığı ikinci hak, siber uzayın sosyal katmanına ilişkindir. Bu hak devlete, gerçek ya da tüzel kişilerin egemen devletin ülkesi üzerindeki siber faaliyetlerini düzenleme yetkisi tanımaktadır. Örneğin, bir devlet uluslararası insan hakları hukukuna tabi olmak kaydıyla ülkesi üzerindeki çocuk pornografisi veya çevrimiçi şiddeti teşvik eylemlerini suç haline getirebilme hakkını taşır[398]. Uygulamada buna örnek olarak Avustralya'da Dow Jones ve Kanada'da Washington Post davaları yanında Nazi ürünlerinin internette satışına ilişkin olarak Fransız ulusal mahkemesinin yasaklama kararı alması gösterilebilir. Bu konuda Amerikan Yüksek Mahkemesi tarafından küresel alanda çevrimiçi faaliyet gösteren Amerikan şirketlerinin yerel yasalara daha fazla uyum sağlaması gerekliliği yönünde karar verilmiştir[399]. Daha önce de ifade edildiği üzere Şangay İşbirliği Örgütü'nün üye devletlere tavsiyesi de bu yönde olup Çin Halk Cumhuriyeti ve Katar, bilgi akışı serbestisinin ulusal egemenlik ve her

[395] Aynı görüş için bkz.; Heinegg, 2012, s. 14.

[396] Schmitt, 2017, *Tallinn Manual 2.0.* s. 12-13.

[397] Heinegg, 2012, s. 13.

[398] Schmitt, 2017, *Tallinn Manual 2.0.* s. 14.

[399] Haber için bkz.: Wathers, Richard. (13 Ocak 2006). Yahoo loses Nazi memorabilia case. *The Financial Times.* Erişim: 04.10.2020 https://www.ft.com/content/81127f12-83cb-11da-9017-0000779e2340

devletin siber uzay alanlarını iç hukukuyla uyumlu şekilde yönetmesi ilkeleri kapsamında güvence altına almaktadırlar[400].

Dışsal egemenlik konusuna gelince, bu yetkinin bir devletin dış politikasını şekillendirme özgürlüğünü taşıması ve uluslararası antlaşma yapabilmesi anlamını taşıdığı görülmektedir[401]. Dışsal egemenliğin kaynağı, BM Şartı'nın 2 (1) maddesinde ifade edilen egemen eşitlik ilkesinden kaynaklanmaktadır. Siyasal bağımsızlık olarak ifade edebileceğimiz bu ilke gereği devletler siyasal, sosyal, ekonomik ve kültürel sistemlerini serbestçe belirleyebilmektedirler[402]. Bu bağlamda siber faaliyetler açısından devletler, özel siber antlaşma rejimini benimsemekte veya herhangi bir siber devlet uygulamasının uluslararası yapılageliş hukukunun doğasına ilişkin *opinio juris* ifadesinde bulunmakta serbesttir[403].

Tallinn El Kitabı Kural 12'ye göre, dışsal egemenlik devlet bağışıklığının da kaynağıdır[404]. Buna göre, bir devletin ülkesi dışında bulunan siber altyapı unsurlarının yargı bağışıklığından ve dokunulmazlığından yararlanabilmesi için söz konusu siber altyapı platformunun münhasıran hükümet faaliyetine adanmış olması gereklidir[405]. Bir devletin insansız hava aracına yönelik DOS saldırı gerçekleştirmek veya aracın kontrolünü ele geçirmek devletin egemen bağışıklığının ihlali anlamına gelir[406]. Aynı şekilde devlete ait bir savaş gemisinin siber faaliyet gerçekleştirmesi zararsız geçiş hakkının ihlali sonucunu doğurur[407].

---

[400] Kanuck, 2010, s. 1575.

[401] Schmitt, 2017, *Tallinn Manual 2.0.* s. 16.

[402] Position Paper, 2021, s. 3.

[403] Schmitt, 2017, *Tallinn Manual 2.0.* s. 17.

[404] Schmitt, 2017, *Tallinn Manual 2.0.* s. 17.

[405] Schmitt, 2017, *Tallinn Manual 2.0.* s. 28.

[406] Schmitt, 2017, *Tallinn Manual 2.0.* s. 28.

[407] Schmitt, 2017, *Tallinn Manual 2.0.* s. 28.; Zararsız geçiş hakkında daha ayrıntılı bilgi için bkz.: Ünal, Şeref. (2005). *Uluslararası Hukuk*. Ankara: Yetkin, s, 133.

Siber uzaydaki bir veri örneğinde olduğu üzere kötücül yazılımın naklinin kontrol edilememesi yanında, geçtiği devletler tarafından da kontrolü olanaklı değildir. Bu demektir ki bir kötücül yazılım hedef devlete varmadan önce pek çok devleti geçebilmekte ve transit geçiş yapılan devlet sorumlu olmak istememektedir[408]. Bu noktada ifade etmek gerekir ki kablosuz sinyallere, hedef devletin ülkesi dışından sırf sızmak suretiyle gerçekleşen siber casusluk faaliyetleri, hedef devlet ülkesinde bulunan siber altyapı unsurları üzerinde sonuç doğurmadığından egemenliğin ihlali olarak kabul edilememektedir[409]. Zira siber operasyonların devletlerin egemenlik haklarını ihlal etmesi için siber altyapı unsurlarında önemli sayılabilecek zararlara sebep olması gerekmektedir[410].

Uzaktan gerçekleştirilen ve hedef devlet ülkesi üzerindeki siber alt yapı unsurları üzerinde etki gösteren uzaktan siber operasyonların hukuki durumu değişken olup Uluslararası Uzmanlar Grubu bu eylemlerin iki durumda yasal olacağını kabul etmektedir. Bunlar; hedef devletin ülkesel bütünlüğünü bozma derecesi ve içkin yönetim işlevlerinin gaspı veya karışılmasının söz konusu olup olmamasıdır[411].

Uzmanlar ilk durumu, fiziki zarar, işlev kaybı ve işlev kaybı eşiğinin altında kalan işlev bozulması seviyeleri olarak analiz etmektedir[412]. Fiziki zarar, eşyaya verilen maddi hasar ya da yaralanma halinde söz konusu olabilir. İkinci duruma örnek olarak, Aramco Tesisleri'nde meydana gelen binlerce hard disk değişimi gösterilebilir. Böyle bir durumda, fiziki zarar ve yaralanmaya yakın sonuçları olan bir ihlale eşit fiziki siber alt yapı işlev bileşenlerinin tamiri veya değişkenliğini gerektiren işlev kayıpları söz

[408] Jensen, 2015, s. 280.

[409] Schmitt, 2017, *Tallinn Manual 2.0.* s. 19-20.

[410] Heinegg, 2012, s. 11.

[411] Schmitt, 2017, *Tallinn Manual 2.0.* s. 20.

[412] Schmitt, 2017, *Tallinn Manual 2.0.* s. 20.

konusudur[413]. Alman devletinin bu konudaki tutumu, siber operasyon fiziki zarar ile sonuçlanmasa da meydana gelen işlevsel bozulmanın önemli düzeyde olması halinde ülkesel egemenliğin ihlali söz konusu olabileceği, önemsiz fiziki zararların ve gerekli eşiğin altında kalan işlevsel bozuklukların ise ülkesel egemenliğin ihlalini oluşturmayacağı yönündedir[414]. Üçüncü olasılık ise işlev kaybına sebep olmayan ancak DDoS saldırısı gibi siber altyapının veya programın farklı şekilde çalışmasına sebep olan, kötücül yazılım (*malware*) yerleştirmek gibi durumlar olup bu konuda uzmanlar arasında görüş birliği bulunmamaktadır[415].

Bu bahiste ifade edilmesi gereken bir diğer husus; devletin yargı yetki alanının bir şekilde egemenlik ile ilgili olmasıdır[416]. Siber uzayın ise doğası gereği egemenliğe aykırı olduğu[417] iddiasının doğru olmadığı, hatta devletin teknolojik kontrolü ve normatif rejimi düzenlemek suretiyle egemenliğini savunacak çeşitli yöntemler kullandığı savunulmaktadır[418]. Bu konuda uluslararası kamu hukukunda iki farklı yaklaşım bulunmaktadır[419]. İlk olarak *Lotus&Bozkurt Davası*'nda[420] olduğu şekilde, yasaklayıcı bir hüküm bulunmaması halinde devletin ülkesel yargı yetkisini kullanabileceği ya da günümüzde ağırlıklı olarak benimsendiği biçimde, izin verici kural bulunmadıkça ülkesel yargı yetkisinin kullanılamayacağı durumudur. Buna karşın bir sonraki başlık altında açıklanacağı üzere *Lotus&Bozkurt Davası*'nda kabul edilen kuralın etki doktrini üzerinden siber uzay için yeniden gündeme geldiği görülmektedir.

---

[413] Schmitt, 2017, *Tallinn Manual 2.0.* s. 20.

[414] Position Paper, 2021, s. 4.

[415] Schmitt, 2017, *Tallinn Manual 2.0.* s. 21.

[416] Ryngaert, Cedric. (2008). *Jurisdiction in International Law.* Oxford: Oxford University Press, s. 5.; Aksar, 2021, (1. Kitap) s. 297.

[417] Betz ve Stevens, 2011, s. 56.

[418] Betz ve Stevens, 2011, s. 58.

[419] Ryngaert, 2008, s. 21.

[420] Uluslararası Daimi Adalet Divanı (UDAD), "*The Case of the S.S. Lotus*", 27 Eylül 1927, Erişim: 04.11.2022 The Case of the S.S. Lotus, France v. Turkey, Judgment, 7 September 1927, Permanent Court of International Justice (PCIJ) (worldcourts.com)

2.2. SİBER UZAY VE DEVLETİN YETKİ ALANI

Siber saldırıların silahlı saldırı düzeyine ulaşması halinde meşru müdafaa hakkını kullanabilen devletlerin, silahlı saldırı eşiğine varmayan saldırıları gerçekleştirenlere karşı yargı yetkisini kullanabilip kullanamayacağı konusu da uluslararası hukuk kapsamında ele alınmaktadır. Siber uzayın tüm devletlerin yetki alanlarından bağımsız yapısından dolayı devletin ülkesi sınırları dışında yargı yetkisini kullanabilmesi uygulamada karşılaşılan en önemli zorluklardan biridir.

Siber uzayda, dünyanın herhangi bir yerinden bir internet kullanıcısı tarafından gerçekleştirilen bir siber faaliyete yönelik olarak bu eylemden dolayı zarara uğradığını iddia eden devletlerin hangi yargı yetkisine başvuracakları sorununa karşı öğretide yeni öneriler getirilmektedir. Siber saldırganlık olarak ifade edilen siber faaliyetlere karşı BM Deniz Hukuku Sözleşmesi'nin (BMDHS) ülkesel yargı yetkisi ile evrensel yargı yetkisini dengeleyen hükümlerinin rehber olacağı, açık denizlerde işlenen korsanlık ya da suçların siber saldırganlık eylemleriyle benzerlik gösterdiği ileri sürülmektedir[421]. Buna karşın, etki doktrinine göre ülke sınırları dışında da işlense, etkilerinin görüldüğü ülke devletinin yargı yetkisini taşıdığı savunulmaktadır[422]. *Lotus&Bozkurt Davası*'na konu olaya benzer bir durumun söz konusu olduğu böylesi bir durumda, zarar gören devletin yargı yetkisini kullanması hukuka uygun kabul edilmelidir. 1982 tarihli BMDHS'nin yürürlüğe girmesiyle değişikliğe uğrayan bu görüşün siber uzay yönünden değiştirilerek benimsenmesi, siber uzayda gerçekleştirilen ve diğer bir devlet ülkesinde etki doğuran eylemlerden dolayı zarar gören devletin yargı yetkisinin tanınması isabetli olacaktır.

Kara savaşında değerli toprakların ele geçirilmesi ve elde tutulması ana strateji iken, hava ve deniz savaşlarında bu hedef hava ve deniz kanalları ile iletişim hatlarının dost güçler

[421] Stahl, 2011, s. 265.

[422] Heinegg, 2012, s. 14-15.

için kullanım güvenliği sağlamaya ve düşman güçlerin kullanımının önlenmesine yöneliktir. Siber savaşta ana strateji ise, sunucular gibi fiziki varlıklar ile yazılım ve bilgi kaynakları gibi fikri varlıkları korumayı amaçlar[423].

Denizlerde olduğu üzere siber alanın büyüklüğünden dolayı tamamen kontrol edilmeye elverişli olmaması nedeniyle çabaların ve beklentilerin küresel kamusal mallar dâhilinde siber sanal bölgedeki ve buna karşı gerçekleştirilen eylemle sınırlı olması gerekmektedir[424]. Buna karşın, evrensel yargı yetkisinin kullanılabildiği açık deniz alanlarında gerçekleşen birtakım suçlardan farklı olarak diğer kaynağının tespiti çok zor olan ve bir devlet ülkesinde gerçekleşen bu tür eylemlerde evrensel yargı yetkisinin uygulanabilmesi farklılık arz etmektedir. Bu halde bir devlet ülkesinde gerçekleşen siber faaliyetlerden zarar gören devletin başka bir devlet ülkesinde bulunan saldırganı ele geçirmesi, *Adolf Eichman Davası*'nda ileri sürülen[425] ilgili devletin egemenlik hakkının ihlal edilmesi anlamına gelecektir.

Başka bir devlet ülkesinde bulunan internet kullanıcılarının zararlı siber faaliyetlerinden zarar gören devletlerin evrensel yargı yetkisini kullanabilmesinin zorluğu ortadadır. Bu nedenle BM nezdinde Uluslararası Denizcilik Organizasyonu benzeri bir örgütün siber saldırganlık suçlarında evrensel yargı yetkisinin kullanılabilmesinde ve siber güvenliğin sağlanabilmesinde uluslararası işbirliğinin sağlanabilmesi için kurulması ve ileri vadede örgütün uluslararası bir siber suçlar mahkemesine dönüştürülmesi önerilmektedir[426].

Mevcut uluslararası hukuk kurallarına bakıldığında yargı yetkisi ilk olarak devlete sivil, idari ve cezai konularda otorite olma hakkı tanıyan yetki alanı ve ikinci olarak ülkesel ve

---

[423] Straub ve Traylor, 2018, s. 26.

[424] Straub ve Traylor, 2018, s. 27.

[425] Nazi Almanya'sında soykırımdaki rolü nedeniyle İsrail devleti tarafından sorumlu tutulan Eichman, İsrail gizli servisi tarafından Arjantin ülkesinde bulunduğu halde kaçırılarak İsrail'e götürülüp yargılanmış ve idam edilmiştir. İsrail devletinin bu kaçırma operasyonunun Arjantin'in egemenlik hakkını ihlal ettiği itirazları yargılama üzerine gölge düşürmüştür.

[426] Stahl, 2011, s. 270-272.

ülke dışındaki yetki alanı şeklinde ikiye ayrılır. Devletin ülkesi dâhilinde gerçekleşen bir suça ilişkin olarak gerçekleştirdiği bu yargılama faaliyeti devletin ülkesel yetkisini kullanması suretiyle gerçekleşebilir. Devlet bu yetkisini düzenleme (*prescriptive*/ kural koyucu), uygulama (*enforcement*) ve yargısal (*judicial*) olarak üç farklı şekilde kullanır[427]. Somutlaştırmak gerekirse, Türk Ceza Kanunu'nda (TCK) düzenlenen bir siber dolandırıcılık suçunun ceza yasasında düzenlenmesi işlemi devlet için kural koyma yetkisi dâhilinde gerçekleştirilen bir yetkidir. Bu ceza normuna aykırı davranan bir kişinin eyleminin suçun kanunda tanımlanan ve cezai müeyyide gerektiren bir suç oluşturup oluşturmadığının değerlendirilmesi ise devletin yargısal yetkisini ifade eder. Ayrıca suç konusu oluşturan eylemi gerçekleştiren kişinin yakalanması ve hakkında yaptırım uygulanması ise devletin uygulama yetkisini kullanması anlamına gelmektedir.

Devletin yetkileri ilke olarak ülkesi ile sınırlı olmakla birlikte, mevcut uluslararası hukuk kuralları birçok konuda bir devlete ülkesi dışında da birtakım yetkiler kullanma hakkını tanımaktadır[428]. Bu yetkilerin bir bölümü ülkesel nitelikli yetkiler olup, bir devletin ülkesel yetkisinin belirli bir süreklilik içerisinde ülke dışına uzanması biçiminde ortaya çıkmaktadır[429]. Örneğin, devletin bayrağını taşıyan bir deniz aracı ya da devlet adına kayıtlı bir hava aracında gerçekleşen eylemler yönünden de devletin ülkesel egemenlik yetkisi söz konusudur[430]. Bu örnekte belirtilen araçlarda gerçekleşen eylemlerde olduğu gibi devletin ülkesini oluşturmayan bitişik bölge, münhasır ekonomik bölge, balıkçılık bölgesi ya da açık deniz gibi uluslararası alanlarda da devletin ülkesel yetkisinin kullanılabilmesi mümkündür[431].

Bazı durumlarda ise, devlet ülkesi dışındaki bir failin gerçekleştirdiği eylemin neticesinin ülke sınırları içinde ortaya çıkması halinde ya da ceza politikası gereğince yurtdışında

---

[427] Schmitt, 2017, *Tallinn Manual 2.0.* s. 51.; Position Paper, 2021, s. 2.; Heinegg, 2012, s. 13.

[428] Pazarcı, 2021, s. 167.

[429] Pazarcı, 2021, s. 167.

[430] Heinegg, 2012, s. 13.

[431] Pazarcı, 2021, s. 168.

işlenen suçlara karşı korunması gerekli görülen üstün bir hakka yönelik suçların yargılanması gerekli olabilmektedir. Devletin ülkesi dışında düzenleme yetkisini sağlamaya yönelik olarak uluslararası hukukun tanıdığı diğer bazı yetkiler, istisnai olarak aktif kişisellik prensibi, pasif kişisellik prensibi, koruma prensibi veya evrensellik prensibine dayanabilmektedir[432].

Belirtilen şekillerde ülkesel nitelikli yetkilerin ülke dışına uzanması halinde birden çok devletin yetki alanlarının çatışması olasıdır. Uluslararası hukuk çerçevesinde özellikle uluslararası alanlarda aynı türden yetkilerin bütün devletlere eşit olarak tanındığı durumlarla giderek artan bir biçimde karşılaşılmaktadır[433]. Özellikle aynı siber faaliyetten dolayı birden çok devletin ortak ve yarışan yetkiler taşıması söz konusudur. Örneğin, bir devletin vatandaşının başka bir ülke topraklarında gerçekleştirdiği siber saldırı eyleminden dolayı saldırıyı gerçekleştirenin vatandaşı olduğu devlet, aktif kişisellik prensibi temelinde ülke dışı düzenleme yetkisini kullanırken, saldırının gerçekleştiği ülke devleti ise ülkesel nitelikli yetki kullanma hakkını taşımaktadır[434].

Yargısal yetkinin uygulanması açısından, uluslararası hukukta, iç hukuktan farklı olarak, siber suç faillerinin cezai kovuşturma öncesinde yargı makamları önünde fiziken hazır bulundurulmasının gerekip gerekmediği henüz çözüme kavuşmamıştır[435]. Buna ilişkin olarak Türk hukukunda Ceza Muhakemeleri Kanunu'nun (CMK) 247. maddesinde[436] yoklukta yargılama yapılabilmesi usulü düzenlenmiştir.

---

[432] Ryngaert, 2008, s. 85.

[433] Pazarcı, 2021, s. 181.

[434] Schmitt, 2017, *Tallinn Manual 2.0.* s. 28.

[435] Schmitt, 2017, *Tallinn Manual 2.0.* s. 53.

[436] Yasa metni için bkz.: CMK 247/3 "Kaçak sanık hakkında kovuşturma yapılabilir. Ancak, daha önce sorgusu yapılmamış ise, mahkûmiyet kararı verilemez" Erişim: 01.10.2022 https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

2.2.1. ÜLKESEL YETKİ

Ülkesel yargı yetkisi prensibi uluslararası hukukta en temel yetki prensibi olup özellikle Kıta Avrupası'nda ülkesellik prensibi temel yetki prensibiyken, Anglo-Sakson yapılageliş hukukunda olduğu şekilde kişisel ve evrensel yargı yetkisi genel kabul görmüştür[437]. Devletin ülkesel yetkileri her türlü yasama, yürütme ve yargı işlemlerini kapsamaktadır[438]. Devletin yetki alanı ülkesiyle yakın bir ilişki içinde bulunduğundan uluslararası hukukta ülkesellik prensibi ağır basmaktadır[439]. Devletin egemenlik emarelerinin en önemlilerinden bir tanesi cezai yargılama yetkisi olup devlet ülkesi üzerinde işlenen suçlardan dolayı cezai yargılama yetkisini kullanmaktadır[440]. Bu prensibe göre, devletin egemenlik hakkının uzantısı olarak bir devlet ülkesi üzerinde bulunan kişiler, nesneler ve gerçekleşen eylemlere ilişkin yetki kullanımı söz konusudur. Türkiye açısından bakıldığında yine ülkesellik prensibinin benimsendiği görülmektedir. TCK'nın 8. maddesinde[441] düzenlenen yer bakımından yetki ilkesine göre, Türkiye'de işlenen suçlar bakımından Türk kanunları uygulanmaktadır.

Suçu oluşturan eylemin bir devlette başlayıp başka bir devlette sonuçlanması halinde, bir diğer ifade ile sınıraşan suçlarda, uluslararası hukukta iki yaklaşım söz konusudur. Subjektif ülkesellik ilkesi, suçun işlenmeye başladığı yeri esas alırken objektif ülkesellik ilkesi suçun tamamlandığı, zararın ve mağduriyetin ortaya çıktığı yeri yetkili kabul

---

[437] Ryngaert, 2008, s. 42-43.

[438] Pazarcı, 2021, s. 157.

[439] Ryngaert, 2008, s. 49.

[440] Aksar, 2021, (1. Kitap) s. 300.

[441] Yasa metni için bkz.: "Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır." Erişim: 01.10.2022 https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

etmektedir[442]. Uluslararası hukukta objektif ülkesellik ilkesinin uygulandığı en önemli yargı kararı *Lotus&Bozkurt Davası*'dır[443].

Tallinn El Kitabı Kural 9'da belirtilen bu ilke, devletin ülkesinde gerçekleşen siber faaliyetler ile kişi ve siber altyapı unsurları üzerinde; devletin ülkesinden kaynaklanan veya burada tamamlanan; yine ülkesi üzerinde önemli etkilerini taşıyan siber faaliyetlere ilişkin olarak kullanılabilir[444]. Ülkesellik temellinde bir yetkinin bir devletin ülkesinde bulunan siber altyapı unsuruyla en düşük düzeyde bağlantısı durumunda, örneğin sadece verinin transit aktarımı halinde, kullanılıp kullanılamayacağı konusunda Uluslararası Uzmanlar Grubu'nda fikir ayrılığı oluşmuştur[445]. Siber uzayın tüm devletlerin ülke sınırlarını da kapsayan bir alan üzerinde inşa edildiği açıktır. Buna göre siber uzayda gerçekleşen eylemler yönünden zararın meydana geldiği devletlerin ülkesel yetkiyi haiz olduğu görüşünün ağır bastığı görülmektedir. Örneğin, Tallinn El Kitabı'nda bir devletin ülkesinde bulunan bir terörist grup tarafından diğer bir devletin ülkesindeki elektrik dağıtım tesisine karşı gerçekleştirilen siber bir saldırı halinde her iki devletin de eşit düzeyde yetkili olduğu kabul edilmiştir. Bu durumda eylemin başladığı ilk devletin yetkisinin sübjektif ülkesel yetki, saldırının gerçekleştiği siber alt yapı tesisinin bulunduğu ikinci devletin yetkisinin ise objektif ülkesel yetki olduğu kabul edilmektedir[446].

Yine Tallinn El Kitabı'na göre, yabancı devlet vatandaşının bir devletin ülkesini etkileyen siber faaliyetlerine ilişkin olarak, başka bir devlet vatandaşının siber faaliyetleri, ülke devleti için önemli düzeyde etki göstermedikçe ülke devletinin diğer ülke vatandaşı üzerinde ülkesel yetkisi söz konusu olmayacaktır[447]. Bu durumda, önemli etkiler söz

---

[442] Aksar, 2021, (1. Kitap) s. 300.; Eylemi veya durumu oluşturan bir unsurun neticelendiği ülkenin yetkili kabul eden görüş için bkz.; Ryngaert, 2008, s. 75.

[443] Aksar, 2021, (1. Kitap) s. 301.

[444] Schmitt, 2017, *Tallinn Manual 2.0.* s. 55.

[445] Schmitt, 2017, *Tallinn Manual 2.0.* s. 56.

[446] Schmitt, 2017, *Tallinn Manual 2.0.* s. 56.

[447] Schmitt, 2017, *Tallinn Manual 2.0.* s. 59.

konusu olduğunda ülke dışında gerçekleştiği halde siber faaliyetin etkilerinin ülke içerisinde ortaya çıkmasından kaynaklı olarak ülkesel nitelikli yetki kabul edilmektedir. Siber uzayın açık deniz gibi ortak bir uluslararası alan olarak kabulü ile ülkesinde önemli zararlar doğan devletlerin ülkesel yetkisinin kabul edilmesinde uluslararası hukuka aykırı yönün bulunmadığı kanaatindeyiz. Buna karşın Tallinn El Kitabı'nda belirtilen önemlilik kıstasının ise ülkeden ülkeye değişebilmesi nedeniyle muğlak olduğu değerlendirilmektedir.

2.2.2. ÜLKE DIŞI DÜZENLEME YETKİSİ

Devletin egemenlik hakkı ya da yargısal yetkisi sadece ülkesiyle sınırlı değildir[448]. Devlet her türlü konuyu veya meseleyi, ulusal hukuk düzeni çerçevesinde ele alarak düzenleme yetkisine sahiptir[449]. Bir devletin ülkesi üzerinde bulunan kişiler, nesneler ve eylemlere ilişkin olan ülkesel yetkisinin bazı durumlarda ülke sınırlarının dışına uzanması mümkün olabilmektedir. Örneğin, TCK'nun 8. maddesi uyarınca suç oluşturan bir eylemin ülke sınırları dışında işlenmesine karşın bazı durumlarda Türk devletinin yargı yetkisinin geçerli olduğu kabul edilmiştir[450]. Buna göre, yasada belirtilen şekilde gerçekleşen siber suçlara ilişkin olarak ulusal yargı yetkisi uygulanacaktır. Türkiye'nin Somali açıklarında deniz haydutlarıyla mücadele için Türk Silahlı Kuvvetleri'ne yetki veren hukuki düzenleme ülke sınırları dışına yönelik düzenle ve hatta uygulama yetkisi örneğidir[451].

---

[448] Heinegg, 2012, s. 13.

[449] Aksar, 2021, (1. Kitap) s. 298.

[450] Belirtilen husus TCK'nun 8. maddesinde şu şekilde düzenlenmiştir: "Suç; a) Türk kara ve hava sahaları ile Türk karasularında, b) Açık denizde ve bunun üzerindeki hava sahasında, Türk deniz ve hava araçlarında veya bu araçlarla, c) Türk deniz ve hava savaş araçlarında veya bu araçlarla, d) Türkiye'nin kıt'a sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı, işlendiğinde Türkiye'de işlenmiş sayılır" Yasa metni için bkz.: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf (Erişim: 01.10.2022)

[451] Aksar, 2021, (1. Kitap) s. 298.

Küreselleşme nedeniyle ülke dışı düzenleme yetkisi kullanımı yaygınlaşırken internet gibi teknolojilerin gelişmesiyle bu konudaki tartışmalar da artmıştır[452]. Siber uzayın ülke sınırlarının ötesine geçmesine ve verilerin ışık hızıyla dünyayı dolaşmak suretiyle aktarımına karşın siber altyapı tesislerinin ülke sınırlarında bulunmasından dolayı devletlerin siber uzay üzerindeki egemenlik hak ve yetkileri konusunda belirsizlikler söz konusudur. Siber uzaya ilişkin devlet egemenliği ile birey hak ve özgürlüklerinin çatışması da bu sorunu daha karmaşık bir hale sokmaktadır.

Bir devletin ülkesel yetkisi, ülkesi içerisinde siber altyapı unsurları, siber faaliyetler ve bu tür faaliyetlerle meşgul olan kişiler bakımından uygulanırken, bu yetki kuralı ülke dışında belirtilenler yönünden düzenleyici devlet yetkisini ifade eder[453]. Bu durumda devletler, diğer sınıraşan hukuki meselelerde olduğu gibi yurt dışında bulunan siber altyapı tesisleri hakkında ulusal çıkarlara ilişkin mülkiyet hakkının korunması amacıyla ülke dışı yetki kullanma yoluna başvurabilecektir[454]. Devletler ayrıca, kişiler üzerinde egemenlik yetkisini kullanmak için yöntem yaratan uluslararası antlaşmalar da oluşturabilirler ki bunlar Avrupa Siber Suç Sözleşmesi gibi çok taraflı antlaşmalar olabileceği gibi suçluların iadesi gibi iki taraflı antlaşmalar da olabilir[455].

Ülke dışı düzenleme yetkisi, Tallinn El Kitabı'nda 10 nolu Kural olarak düzenlenmiştir. Buna göre, bir devletin vatandaşı tarafından; devlete ait gemi veya hava aracında işlenen; yabancı bir devlet vatandaşı tarafından işlenen, devletin temel çıkarlarını ciddi şekilde baltalamak için planlanmış; yabancı bir devlet vatandaşı tarafından bahse konu devlet vatandaşına karşı belirli sınırlar dâhilinde işlenen veya evrensellik prensibine bağlı olarak uluslararası suçların oluşturduğu siber suçlar bakımından söz konusu olabilir[456]. Kural

---

[452] Kadıoğlu Kumtepe, Cemre. (2021). *Uluslararası Veri Aktarımının Kısıtlanmasına İlişkin Veri Uygunluğu İlkesinin Devletlerin Egemenliğine Etkisi,* s. 5. Erişim: 11.09.2022 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4083162

[453] Schmitt, 2017, *Tallinn Manual 2.0.* s. 61.

[454] Kanuck, 2010, s. 1574.

[455] Jensen, 2015, s. 295.

[456] Schmitt, 2017, *Tallinn Manual 2.0.* s. 60.

10'da düzenlenen bir gemi veya hava aracının tabiiyeti, kayıtlı olduğu devlet temeline dayanır. Bayrak devleti olarak da adlandırılan kayıtlı olunan devlet, gemi veya hava aracında gerçekleşen siber faaliyetler veya siber faaliyetlerle meşgul olan kişiler üzerinde yetki sahibi olacaktır[457].

Kural 10'un son kısmını oluşturan ulusal güvenlik temelli yetki, diğer bir ifade ile koruma prensibi, bir devletin ulusal güvenliği ile ilgili hayati devlet çıkarlarına dair devlete sınırları dışında yetki kullanma imkânı sağlar. Kritik devlet görevlilerinin can güvenliği veya fiziki güvenliği, hükümetin zorla devrilmesi veya terörizm gibi ulusal güvenliğin ve devletin ana fonksiyonlarına ciddi müdahale, para sahteciliği veya banka sisteminin ciddi şekilde gizliliğinin bozulması gibi devletin finansal ödeme gücü veya istikrarını tehdit eden eylemler genellikle bu kategoride değerlendirilir[458]. Mevcut uluslararası hukuk kurallarına bakıldığında, başka bir devletin vatandaşı tarafından devlet güvenliğine karşı ülke dışında işlenen suçlar ile uzay araçlarına karşı işlenen suçlar bakımından devletin ülke dışı yetkisinin bulunduğu kabul edilmektedir[459]. Zira devletlerin, ülkesi dışında bulunan vatandaşları üzerinde yetkisinin bulunduğu; soykırım, savaş suçları ve insanlığa karşı suçlar gibi bazı suçlar bakımından evrensel yetkiye sahip olduğu kabul edilmektedir[460]. Bir devletin vatandaşı tarafından yurt dışında işlenen suçları vatandaşı olduğu devletin yargılaması halinde aktif vatandaşlık prensibi söz konudur. Bu prensibe uygun düzenleme TCK'nun 11. maddesinde[461] düzenlenmiştir. Koruma prensibinin

---

[457] Schmitt, 2017, *Tallinn Manual 2.0.* s. 63.

[458] Schmitt, 2017, *Tallinn Manual 2.0.* s. 64.

[459] Pazarcı, 2021, s. 178.

[460] Kadıoğlu Kumtepe, 2021, *Uluslararası Veri Aktarımının Kısıtlanmasına İlişkin Veri Uygunluğu İlkesinin Devletlerin Egemenliğine Etkisi,* s. 4.

[461] Yasa metni için bkz.: TCK 11 "(1) Bir Türk vatandaşı, 13 üncü maddede yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı bir yıldan az olmayan hapis cezasını gerektiren bir suçu yabancı ülkede işlediği ve kendisi Türkiye'de bulunduğu takdirde, bu suçtan dolayı yabancı ülkede hüküm verilmemiş olması ve Türkiye'de kovuşturulabilirliğin bulunması koşulu ile Türk kanunlarına göre cezalandırılır.103 (2) Suç, aşağı sınırı bir yıldan az hapis cezasını gerektirdiğinde yargılama yapılması zarar görenin veya yabancı hükûmetin şikâyetine bağlıdır. Bu durumda şikâyet, vatandaşın Türkiye'ye girdiği tarihten itibaren altı ay içinde yapılmalıdır" Erişim: 01.10.2022

karşılığını bulduğu TCK'nun 12/1. fıkrasında[462] ise Türkiye zararına karşı yabancı ülkede işlenen suçlara ilişkin ulusal yargı yetkisi kabul edilirken, anılan yasanın 13. maddesinde ise önemli görülen suçlar ile ilgili olarak evrensel yargı yetkisi öngörülmüştür.

Ülke dışı düzenleme yetkisi dâhilinde incelenen bir diğer konu pasif vatandaşlık veya pasif kişilik prensibidir. Bu prensip bir devletin cezai yasama yetkisinin, kendi devleti vatandaşına karşı yurtdışında uçak kaçırma veya terörist saldırı gerçekleştirme gibi suçları işleyen yabancı devlet vatandaşına uzanması anlamına gelir[463]. TCK'nun 12/2. fıkrası[464] uyarınca Türk vatandaşının aleyhine yabancı ülkede işlenen bir suça ilişkin yargılama yetkisi kabul edilmiştir.

Yurt dışında bulunan silahlı gücün diğer bir devlet vatandaşı bireylerini içermesi mümkün olup devletin silahlı güçleri, bu güce dâhil olan bireylerin uyruğuna bakılmaksızın, *ipso facto* bu devlete ait olarak değerlendirilir[465]. Bu kişilerin işlediği siber suçlar bakımından silahlı güçlerin bağlı olduğu devletin cezai kural koyucu yetkisi söz konusu olmaktadır. Başka bir devletin ülkesi içerisinde bulunan bir devletin vatandaşları üzerinde ikinci devlet düzenleme yetkisi taşımakta ise, bu vatandaşın ürettiği veri üzerinde aynı şekilde

https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

[462] Yasa metni için bkz.: TCK 12/1 *"*Bir yabancı, 13 üncü maddede yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı en az bir yıl hapis cezasını gerektiren bir suçu yabancı ülkede Türkiye'nin zararına işlediği ve kendisi Türkiye'de bulunduğu takdirde, Türk kanunlarına göre cezalandırılır. Yargılama yapılması Adalet Bakanının istemine bağlıdır" Erişim: 01.10.2022

https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

[463] Schmitt, 2017, *Tallinn Manual 2.0.* s. 64.

[464] Yasa metni için bkz.: TCK 12/2 *"*Yukarıdaki fıkrada belirtilen suçun bir Türk vatandaşının veya Türk kanunlarına göre kurulmuş özel hukuk tüzel kişisinin zararına işlenmesi ve failin Türkiye'de bulunması halinde, bu suçtan dolayı yabancı ülkede hüküm verilmemiş olması koşulu ile suçtan zarar görenin şikayeti üzerine fail, Türk kanunlarına göre cezalandırılır*"* Erişim: 01.10.2022

https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

[465] Schmitt, 2017, *Tallinn Manual 2.0.* s. 63.

bir yetkiyi haiz olup olmadığı konusunda uzmanlar, veri üzerinde ilk devletin ülkesel yetki taşıdığını kabul etmiştir[466].

Son olarak evrensel yetki prensibi gereğince uluslararası yapılageliş ve antlaşmalar hukukuna göre tanınan deniz haydutluğu, köle ticareti, soykırım, insanlığa karşı suçlar, savaş suçu ve işkence suçları hakkında devletin düzenleme yetkisi söz konusu olmaktadır[467]. Belirtilen bu suçlar ile uçak kaçırma, deniz ve sivil havacılık güvenliğini ihlal, uluslararası koruma altındaki kişilere saldırı, terör amaçlı rehin alma, terör finansmanı ve terörist bombalama gibi birçok yetkiye temel sağlayan çok taraflı uluslararası antlaşma tarafından düzenlenen suçları ayrı tutmak gerekir[468].

2.2.3. ÜLKE DIŞI UYGULAMA YETKİSİ

Uluslararası hukuka göre devletlerin düzenleme yetkisinin kullanılacağı yer kural olarak kendi ülkesidir ve aksine herhangi bir yükümlülük altına girilmediği müddetçe, hiçbir devletin, askeri veya polis gücü veya mahkemesi, başka bir devletin ülkesi üzerinde yetki kullanamaz[469]. Devletin ülkesel egemenlik yetkisi gereğince koruma altında bulunan verinin ülke sınırlarına tabi olmayan siber uzayda aktarımı nedeniyle ülke kurallarının yurtdışında uygulanması meselesinde olduğu üzere kuralların yurt dışında uygulanması da sorunlu alanlardan biridir. Bu konuda bir devletin yurt dışında düzenleme yetkisine sahip olduğu kabul edilse de uygulama yetkisini ancak ülkesel yetkiyi haiz devletin rızası gereğince kullanabileceği savunulmaktadır[470]. Bu görüş Tallinn El Kitabı'nda benimsenmiş ve silahlı çatışmalar hukuku içinde askeri işgal boyunca işgal gücü tarafından yargısal yetkinin kullanılması istisna olmak üzere, siber saldırı faaliyeti

[466] Schmitt, 2017, *Tallinn Manual 2.0.* s. 63.

[467] Schmitt, 2017, *Tallinn Manual 2.0.* s. 66.

[468] Schmitt, 2017, *Tallinn Manual 2.0.* s. 66.

[469] Aksar, 2021, (1. Kitap) s. 298-299.

[470] Kadıoğlu Kumtepe, 2021, *Uluslararası Veri Aktarımının Kısıtlanmasına İlişkin Veri Uygunluğu İlkesinin Devletlerin Egemenliğine Etkisi,* s. 7.

gerçekleştiren kişi üzerinde uygulanan yargısal yetkinin diğer bir devletin ülkesinde fiziksel olarak gerçekleştirilmesi ülke devletinin iznine bağlı olduğu belirtilmiştir[471].

Ayrıca Tallinn El Kitabı'nın 11. Kuralı uyarınca; bir devlet sadece uluslararası hukukta özel bir yetkinin tahsisi veya yabancı bir devletin bölgesinde yetki uygulanmasına rıza göstermesi halinde kişi, obje ve siber faaliyet ile ilgili ülke dışında uygulama yetkisi kullanabilir[472]. Uluslararası yapılageliş veya antlaşmalar hukuku altında özel bir yetki tahsisinin açık olması gerekli olup genel uluslararası hukukun diğer kuralları temelinde ima edilmiş olamaz[473]. Anılan kural uyarınca yabancı bir devlet ülkesinde uygulama yetkisi bulunduğunu ileri süren devletin, bu yetkinin açıkça tanındığını ortaya koyması gerekir. Örneğin bir devlete yönelen terör tehdidinden kaynaklı sınırlı operasyon yetkisi tanınması, ilgili devlete ülke dışında kendi yasalarını uygulama ve yargı yetkisini taşıdığını göstermez.

2.3. SİBER UZAY VE ULUSLARARASI SORUMLULUK

Uluslararası hukuk kişilerinin fiilleri ve diğer faaliyetleri sonucunda diğer hukuk kişilerinin menfaatlerinin ihlal edilmesi durumunda ortaya çıkan zararın tazmin edilebilmesi için eylemi gerçekleştiren hukuk kişisi ile sonuç arasındaki bağın ortaya konulması gerekir. Bununla birlikte uluslararası hukuk kişilerinin fiil ve faaliyetlerinin diğer hukuk kişilerinin menfaatlerini ihlal etmesi de bu kişilerin tek başına sorumlu tutulmasını gerektirmez. Zira devletlerin bazı fiil ve faaliyetleri uluslararası hukuka uygun şekilde gerçekleştirmesine karşın diğer bazı devletlerin bundan zarar gördüğünü iddia etmesi halinde sorumluluk kurumunun işletilip işletilemeyeceği ortaya konulmalıdır.

---

[471] Schmitt, 2017, *Tallinn Manual 2.0.* s. 53.

[472] Schmitt, 2017, *Tallinn Manual 2.0.* s. 66.

[473] Schmitt, 2017, *Tallinn Manual 2.0.* s. 67.

Bunun yanında bir devlet ya da uluslararası örgüt[474] tarafından gerçekleştirilen fiil ya da faaliyetin uluslararası hukuka aykırı kabul edilmesi halinde dahi ortaya çıkan sonucun zarar tanımı üzerinden ne şekilde nitelendirileceği sorun oluşturabilmektedir. Ayrıca uluslararası bir yükümlülüğün ihlalini oluşturan bir fiil ve faaliyetin icrai bir eylem ikası suretiyle gerçekleştirilmesinin zorunlu olup olmadığı, ihmalin söz konusu olması halinde sorumluluğa sebebiyet verip vermeyeceği bu konu dâhilinde tartışıp açığa çıkarılmalıdır[475].

Geleneksel anlamda bakıldığında fiziki kuvvet kullanımının söz konusu olduğu durumlarda kuvvet kullanan devletin sorumluluğuna başvurmakta büyük bir zorluk yaşanmamaktadır. Buna karşın, siber saldırı gibi eylemin nereden kaynaklandığının belirsiz olması halinde ya da hukuka aykırı eylemin kuvvet kullanımını içermemesi durumunda eylemi gerçekleştiren devletin uluslararası sorumluluğuna ne şekilde başvurulacağı konusunda açık bir uluslararası kaynak da bulunmadığından bu konuda yapılageliş hukuku kurallarının yazılı hale getirilmesi bir gereklilik olarak kendini göstermiştir.

Bu konuda önemli bir yer tutan Uluslararası Hukuka Aykırı Fiiller için Devletin Sorumluluğuna Dair Taslak Çalışma[476], 2001 yılında BM Uluslararası Hukuk Komisyonu tarafından yaklaşık 40 yıllık bir çalışması sonunda, 53. oturumda kabul edilmiştir. Bu çalışma bir antlaşma olmasa ve bağlayıcı bir yönü bulunmasa da BM Genel Kurulu'nun 12 Aralık 2001 tarihli 56/83 nolu kararıyla hükümetlere tavsiye edilmesi ve 2012 tarihi itibariyle uluslararası mahkemeler tarafından 154 kez atıf yapılması nedeniyle Tallinn El

[474] UAD'nın *BM Hizmetinde Uğranılan Zararların Giderilmesi* konusundaki 11.04.1949 tarihli danışma görüşü ile uluslararası örgütlerin uluslararası kişiliği onun amaçlarıyla ve kurucu devletlerin kendisine tanıdığı yetkiyle sınırlı olduğu ifade edilmekle bunların uluslararası hukuk kişiliğine sahip oldukları kabul edilmiştir. Pazarcı, 2021, s. 143.

[475] Örneğin, devlet bakımından yasama organı açısından uluslararası yükümlülüklerine aykırı bir yasa çıkarılması nedeniyle, yargı organı açısından ise adaletten kaçınma (denial of justice) durumunda uluslararası sorumluluk söz konusu olabilmektedir. Ayrıntılı bilgi için bkz.: Pazarcı, 2021, s. 449-451.

[476] Bundan sonra "Taslak Çalışma" olarak ifade edilecektir.

Kitabı'na esas alınmıştır[477]. Ayrıca Taslak Çalışma'nın uluslararası sorumluluk mekanizmalarındaki uluslararası yapılageliş hukuku kurallarını yansıtmasından dolayı *Soykırım Suçunun Önlenmesi ve Cezalandırılması Sözleşmesi'nin Uygulanmasına İlişkin Dava*'da[478] (*Bosna-Hersek v. Sırbistan ve Karadağ*) olduğu şekilde uyuşmazlıkların çözümünde bu çalışmaya atıf yapılmıştır[479].

Uluslararası sorumluluk konusunda zihinlerde oluşabilecek soru işaretlerine genel çizgileriyle yukarıda değindikten sonra uluslararası sorumluluk konusunda temel bir çalışma olan Taslak Çalışma ve Tallinn El Kitabı temelinde uluslararası sorumluluk konusunun öncelikle geleneksel anlamda ve akabinde siber uzay zemininde gerçekleşen fiil ve faaliyetler yönünden incelenmesi gereklidir. Bu amaçla genel anlamda sorumluluk koşullarının ortaya konulması ve sonrasında uluslararası hukuk kişilerinin hangi siber faaliyetlerden dolayı uluslararası sorumluluğunun doğabileceği konusunun daha ayrıntılı şekilde ele alınması uygun görülmektedir.

2.3.1. Uluslararası Sorumluluğun Doğması Koşulları

Devletler tarafından az sayıda esaslı itirazın söz konusu olduğu[480] ve yukarıda bahsedilen Taslak Çalışma'nın 1. maddesinde her uluslararası hukuka aykırı fiilin sorumluluk

---

[477] Schmitt, 2017, *Tallinn Manual 2.0.* s. 79.

[478] UAD, "*Case Concerning Application of The Convention on the Prevention and Punishment of the Crime of Genocide*", 26 Şubat 2007, Erişim: 16.07.2022 https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf

[479] Erkiner, Hakkı Hakan. (2010). *Uluslararası Hukukta Uluslararası Topluluk Kavramının Başlıca Görünümleri*, s. 20. Erişim: 07.04.2020. https://www.academia.edu/33296812/HAKKI_HAKAN_ERK%C4%B0NER_MAKALE_ULUSLARARASI_HUKUKTA_ULUSLARARASI_TOPLULUK_KAVRAMININ_BA%C5%9ELICA_G%C3%96R%C3%9CN%C3%9CMLER%C4%B0

[480] Jensen, Eric Talbot / Watts, Sean. (2017). *A Cyber Duty of Due Dilience: Gentle Civilizer or Crude Destabilizer?* Texas Law Review, Cilt:95:1555, s. 1560.

gerektirdiği belirtilerek [481], 2. maddesinde bir devletin icra veya ihmal suretiyle gerçekleştirilen uluslararası hukuka aykırı fiilinden sorumluğu için iki unsur öngörülmüştür. Bunlar; ilk olarak belirtilen eylemin bir devletin uluslararası yükümlülüğünün ihlalini oluşturması, ikinci olarak bu eylemin uluslararası hukuka göre bir devlete atfedilebilir olması hususlarıdır[482]. Bu sayılanlar dışında eylemin zarara sebep olması ya da uluslararası sorumluluğu ortadan kaldırıcı ya da etkilerini silici bir nedenin bulunmaması hususları da öğretide şart olarak ifade edilebilmekte[483] ise de biraz ileride açıklanacağı üzere zarar hususu bazı durumlarda bir ön şart olarak kabul edilmemektedir.

Buna göre, uluslararası hukuka aykırı bir fiilin ya da sorumluluk öngörülen belirli bir faaliyetin uluslararası sorumluluk doğurabilmesi için bu fiilin ya da faaliyetin bir uluslararası hukuk kişisine ait olması gerekmektedir[484]. Uluslararası hukuk kişisinin sorumluluğu, uluslararası hukuk kurallarına aykırı bir fiilden kaynaklanabileceği gibi hukuka aykırı olmayan ancak sorumluluk gerektiren diğer bir faaliyetten de kaynaklanabilir. Ancak uluslararası hukuka aykırılık oluşturmayan diğer bir faaliyetten dolayı bir uluslararası hukuk kişisinin sorumluluğunun kabulü, uluslararası hukukta kusursuz sorumluluğun kabul edildiği anlamına gelmemektedir[485]. Bir diğer ifade ile uluslararası hukukta sorumluluk için kusur şartı aranmamaktadır[486].

---

[481] International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, (12 Aralık 2001), Yearbook of the International Law Commission, 2001, Cilt:2. s. 32.

[482] International Law Commission, 2001, s. 34.

[483] Pazarcı, 2021, s. 444.; Bozkurt ve Erdal ve Poyraz, 2017, s. 306.

[484] Pazarcı, 2021, s. 449.

[485] Uluslararası hukukta devlet sorumluluğunun doğması için kusurun gerekli olup olmadığı konusunda fikirbirliği bulunmamaktadır. Öğreti, devlet görevlilerinin kusurlu davranışının gerektiğini savunanlar (sübjektif görüş) ile böyle bir duruma gerek bulunmadığını savunanlar (objektif görüş) olarak ikiye ayrılmaktadır. Aksar, 2021, (2. Kitap), s. 301.; Bu konuda kusursuz sorumluluğu savunan görüş için bkz.: Doğan, 2016, s, 482.

[486] Uzun, 2007, s. 33.

Uluslararası hukuka aykırı fiile en uygun örnek olarak öğretide işaret edilen *Korfu Kanalı Davası*'nda yaşandığı üzere kara sularına mayın döşediği halde bunu öteki devletlere bildirmeyen Arnavutluk'un bildirmeme eylemi, UAD tarafından pasif nitelikli bir fiil olarak değerlendirilmiştir[487]. Bu olayda Arnavutluk devletinin sorumluluğu, uluslararası hukukun bir gereği olarak mayın tehlikesinden diğer devletleri haberdar etmemesi ve bu suretle diğer devletlerin zararına olmayacak bir biçimde davranma yükümlülüğünü ihlal etmesinden kaynaklanmaktadır. Uluslararası hukuka aykırı bir fiil oluşturmamakla birlikte bir uluslararası hukuk kişisinin sorumluluğunu doğuran diğer hal ise, diğer devletlerin uğradığı zarara sebep olan bir faaliyetten dolayı bir uluslararası hukuk kişisinin sorumlu tutulabilmesidir. Örneğin, sınıraşan çevre kirliliği doğuran eylemler yönünden bir devletin uluslararası hukuka aykırı bir eylemi bulunmasa dahi sorumluluğuna gidilebilmektedir[488].

Buna paralel olarak diğer devletler açısından zarar doğuran bir faaliyetin uluslararası hukuka aykırılık oluşturmaması ve eylemi gerçekleştiren uluslararası hukuk kişisine atfedilebilir bir kusur bulunmamasına rağmen nükleer enerjinin barışçıl kullanımı, uzay faaliyetleri ya da denizlerin hidrokarbürle kirletilmesi gibi tehlikeli faaliyet alanlarında ortaya çıkan bir zarardan dolayı sorumlu tutulabileceği kabul edilmektedir[489]. Bu bağlamda uluslararası hukuk kişisine ait olduğu kabul edilen bir fiil ya da faaliyet nedeniyle ortaya çıkan zarardan fiili gerçekleştiren hukuk kişisinin sorumlu tutulabilmesi için kusurlu olması gerekli ise de bir önceki cümlede belirtilenler gibi bazı durumlarda kusur atfedilemese dahi uluslararası hukuk kişisinin sorumluluğu söz konusu olabilecektir. Uluslararası hukukun gelişen bir hukuk dalı olmasının da etkisiyle gelinen son aşamada zararın aranmaması[490] ya da nimet külfet dengesi bağlamında bu şekilde sorumluluk halinin kabul görmesi mümkün olmuştur.

---

[487] Pazarcı, 2021, s. 445.

[488] Uzun, 2007, s. 15.

[489] Pazarcı, 2021, s. 446.

[490] Gelinen noktada zararın aranmadığı konusunda bkz.; Uzun, 2007, s. 35-36. Zararın bulunması gerektiği görüşü de manevi hukuksal çıkarların ihlali şeklinde kabul edilmektedir. Bkz: Doğan, 2016, s, 484.

Uluslararası hukuk kişisi kavramının ise, günümüzde sadece devlet ve uluslararası örgüt ile sınırlı olacak biçimde dar şekliyle ele alınmamakta, kavramın uluslararası toplum çerçevesinde faaliyet gösteren değişik nitelikteki ve güçteki birimlerin de dâhil edildiği, uluslararası hukuk kurallarının yöneltildiği bütün birimleri kapsadığı kabul edilmektedir[491]. Uluslararası sorumluluk doğuran bir fiil ya da faaliyeti gerçekleştiren uluslararası hukuk kişisinin tespit edilmesi halinde zarar gören devletin diğer bir hukuk kişisinin uluslararası sorumluluğuna başvurabilmesi için öncelikle hukuka aykırı eylemden sorumlu olan tarafı bilgilendirmesi, ihlalin sona erdirilmesini istemesi ve barışçıl çözüm yollarına başvurması gerekir. İhlalin durdurulması halinde uzlaşma ya da dava yoluyla zararın giderilmesi beklenirken, ihlalin durdurulmaması durumunda mağdur devletin kuvvet kullanma içermeyen karşı önlemlere başvurma hakkı gündeme gelebilmektedir. [492]

Devletin sorumluluğu için bir eylemin yalnızca zararlı olması da yeterli olmayıp ayrıca eylemi gerçekleştiren devletin uluslararası yasal yükümlülüklerinin ihlali seviyesine erişmesi gereklidir [493]. İcra ya da ihmal suretiyle ihlal edilebilen bu yükümlülük, antlaşmalar hukuku ya da yapılageliş hukukundan kaynaklanabileceği gibi her ikisinden de kaynaklanabilir[494]. Uluslararası hukukun devletlere olumlu bir eylem yükümlülüğü getirdiği durumlarda bu yükümlülüğe uymamak ihmal oluşturur ve özen yükümlülüğünün ihlali buna örnek gösterilebilir[495]. Böylesi bir durumda uluslararası yasal bir yükümlülükten kaynaklı bir zarar bulunmasa dahi devletin sorumluluğuna başvurmak mümkün görünmektedir[496].

---

[491] Pazarcı, 2021, s. 143.

[492] Doğan, 2016, s, 440.

[493] Jensen ve Watts, 2017, s. 1560.

[494] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 256.; Hukuka aykırı olarak kabul edilen fiilerin yapmama şeklinde gerçekleştirilebileceğine dair Meksika ile ABD arasında görülen *Janes* ve *Massey* Davaları ile *Korfu Boğazı Davası* örnek gösterilebilir. Bkz.; Uzun, 2007, s. 38.

[495] Schmitt, 2017, *Tallinn Manual 2.0.* s. 85.

[496] Aksar, 2021, (2. Kitap), s. 302.

Devletin uluslararası yükümlülüğünün ihlali konusu, Taslak Çalışma'nın 12. maddesinde belirtilmiştir. Buna göre uluslararası yükümlülüğün ihlali, kaynağına ve karakterine bakılmaksızın bir devletin antlaşma yükümlülüğünü, uluslararası yapılageliş hukukunu veya hukukun genel prensibini çiğnemek suretiyle gerçekleşebilir[497]. Buna örnek olarak, tek başına hukuka aykırı olmayan siber casusluk eyleminin bir başka devletin karasularından zararsız geçişi sırasında gemide bir devlet tarafından gerçekleştirilmesi halinde zararsız geçiş ile uyumlu olmayan bu eylem nedeniyle deniz hukukuna aykırı davranışın gündeme gelmesi gösterilebilir[498].

BM Şartı 2/4 maddesinde ifade edilen "devletlerin uluslararası ilişkilerinde" güç kullanımının yasaklanması kuralı, kullanılan kuvvetin veya tehdidin esas olarak bir veya diğer birkaç devlete yönlendirilmiş olmasını ve ayrıca bu eylemin hukuken bir devlete atfedilebilir olmasını gerektirmektedir[499]. Uluslararası hukuka aykırı fiilin atfedilebilirlik unsuru Taslak Çalışma'nın 4. maddesinde düzenlenmiş olup devletin bir organının eylemi tek başına devlete atfedilebilir bir eylem olarak kabul edilmektedir[500]. Aynı maddede devletin yasama, yürütme ve yargı veya diğer herhangi bir işlevini yerine getiren organ tanımlanmıştır. Maddenin ikinci bendinde organ, iç hukukla uyumlu bir durum taşıyan kişi veya varlık olarak ifade edilmiştir. 4. maddenin ikinci bendinde kullanılan bu ifadeden, kişi veya varlığın iç hukukta açıkça organ olarak tanımlanmasının gerekmediği[501], iç hukuka göre organ kavramıyla uyumlu bir durum sergilemesinin yeterli olacağı anlaşılmaktadır. Zira Taslak Çalışma'nın 4/2. paragraf şerhinde devlet organı durumunda olmayan kişi veya varlıkların eyleminin uluslararası hukuka göre devlete atfedilebileceği açıklanmaktadır. Devletin iç hukukuna göre organ olarak kabul

[497] Schmitt, 2017, *Tallinn Manual 2.0.* s. 84.

[498] Tallinn El Kitabı'nın 48. Kuralı'na göre karasularında siber operasyonlar hukuka aykırı kabul edilmektedir. Bkz.: Schmitt, 2017, s. 79.; Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law*. s. 256.

[499] Melzer, 2011, s. 10.

[500] International Law Commission, 2001, Art. 4/1, s. 40.

[501] Schmitt, 2017, *Tallinn Manual 2.0.* s. 88.

edilmeyen kişi veya varlıkların eyleminin devlete atfedilebilir kabul edilmesine örnek olarak UAD'nın önemli derecede kontrolün bulunması gerektiğine karar verdiği 2007 tarihli *Bosna-Hersek v. Sırbistan-Karadağ* Kararı[502] örnek gösterilmektedir[503].

Kural olarak, uluslararası hukukta eylemlerin devlete atfedilebilmesi ve kişilerin davranışlarına devlet adına uluslararası hukuki sonuç bağlanabilmesi için bir devletin onayı, yetkilendirmesi veya devlet adına hareket eden varlık veya kişiler tarafından gerçekleştirilmesi gereklidir[504]. Devletin uluslararası sorumluluğu kapsamında yerini bulan bu atfedilebilirlik şekli[505], Tallinn El Kitabı'nda yasal atfedilebilirlik (legal attribution) olarak nitelendirilmekte, siber eylemler söz konusu olduğunda ise ana kurala göre devlete atfedilebilirlik imkânı her zaman mümkün olamayacağından ayrıca olgusal atfedilebilirlik (*factual attribution*) kavramı kullanılmaktadır[506]. Bunun sebebi, siber uzayın dinamik ve karmaşık yapısından dolayı mevcut normların uygulanabilir olmaması yanında atfedilebilirliği kesin şekilde sağlayan bir "siber DNA"nın söz konusu olmamasıdır[507]. Bir devletin, organları tarafından gerçekleştirilen hukuka aykırı

---

[502] UAD, "*Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide*", 27 Şubat 2007, Erişim: 05.11.2022 https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf

[503] Schmitt, 2017, *Tallinn Manual 2.0.* s. 88.; Soykırım davası olarak da adlandırılan 2007 tarihli Bosna-Hersek v. Sırbistan-Karadağ kararına ilişkin ayrıntılı bilgi için bkz.; Değer, Ozan. (Yaz 2009). *Soykırım Suçu ve Devletin Uluslararası Sorumluluğu: Uluslararası Adalet Divanı'nın Bosna-Hersek v. Sırbistan-Karadağ Kararı*, Uluslararası İlişkiler, Cilt:6, Sayı:22, s. 61-95.

[504] Melzer, 2011, s. 10.

[505] Atfedilebilirlik konusunda bazı kaynaklarda üç ana test bulunduğu kabul edilmektedir. Bunlar kurumsal test, işlevsel test ve kontrol temelli testtir. Stokes, Paul. (2014). *State Responsibility for Cyber Operations: International Law Issues, Event Report,* British Institute of International and Comperative Law, s. 2. Erişim: 29.08.2022, https://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf

[506] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 254.

[507] Garrie ve Simonova, 2020, s. 525.

eylemlerden yasal olarak sorumlu olmasına karşılık, belirlilik derecesini ifade eden olgusal atfedilebilirlikte, eylemi gerçekleştiren devletin belirlenmesi konusunda "makuliyet" ölçütü uygulanmaktadır[508].

Bir devlet organının eylemi olmakla birlikte yetki aşımı (*ultra vires*) durumunda dahi devlete atfedilebilirlik söz konusu olabilmektedir. Yetki aşımına ilişkin olarak 1927 tarihinde Meksika ve ABD arasında görülen *Mallén Davası*'nda[509] devlet görevlisinin resmi görevi adına gerçekleştirdiği yetkisini aşan eylem devlete atfedilebilir kabul edilmiş ancak kendi adına gerçekleştirdiği eylem egemen devlete atfedilebilir bulunmamıştır[510]. Bu konuda öğretideki son zamanlardaki eğilime bakıldığında, yetkilerini aşan devlet görevlileri yönünden, yetkisini aşan görevlinin fiilinin de eğer durum iç hukuk çerçevesinde düzeltilmemişse, ilgili devletin bu kez ihmali nedeniyle uluslararası sorumluluğunun gerekeceği görülmektedir[511].

Devlet adına hareket etmeyen veya ilgili devletin uluslararası sorumluluğunun doğması için yeterli bağ bulunmayan kişi veya varlıklar ise devlet ajanı olarak değerlendirilmeyip devlet dışı aktörler olarak kabul edilir[512]. Ayrıca devlet organının bir parçası olmamakla birlikte devlete ait yönetimsel otorite unsurlarını kullanmakla yetkilendirilmiş bir kişi veya varlığın eylemi, Taslak Çalışma'nın 5. maddesinde uluslararası hukuk tarafından devlete atfedilebilir kabul edilmiştir[513]. Bütün bu ihtimallerin ötesinde devlet adına hareket etmeyen bir grubun eyleminin devlet tarafından kabullenilmesi veya

---

[508] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 254.

[509] *Mallen Davası* için bkz.: Francisco Mallén (United Mexican States) v. U.S.A., Reports of International Arbitral Awards, UN General Claims Commission, Cilt:5, 1927, s. 170-190. Erişim: 27.02.2021, https://legal.un.org/riaa/cases/vol_IV/173-190.pdf

[510] International Law Commission, 2001, Art. 4/13, s. 42.

[511] Pazarcı, 2021, s. 450.

[512] Melzer, 2011, s. 10.

[513] International Law Commission, 2001, Art. 5, s. 42.

benimsenmesi halinde *Tahran Rehineler Davası*'nda UAD'nın kabul ettiği üzere atfedilebilirlik unsuru gerçekleşebilmektedir[514].

Devlet dışı bir aktör tarafından gerçekleştirilen bir eylemin devlete atfedilebilmesi için devletin yönlendirme ve kontrolü altında gerçekleştirildiğinin belirlenmesi hayati bir öneme sahiptir [515] . Taslak Çalışma'da belirtildiği üzere yönlendirme ve kontrol kavramlarının sınırlarının belirlenmesi karışık bir durumdur. Bu nedenle bu kavramların tanımına dair değerlendirme işi mahkemelere bırakılmıştır [516] . UAD, *Nikaragua Davası*'nda kontrol kavramı üzerinden yaptığı değerlendirmede ABD'nin kontralar üzerinde "etkin kontrolünün*"* (*effective control*) bulunmaması nedeniyle kontraların gerçekleştirdiği uluslararası silahlı çatışmalar hukukuna aykırı eylemlerin ABD'ye atfedilebilir olmadığına karar vermiş, ayrıca eylemin atfedilebilir olabilmesi için devletin fiili katılımının ve devlet tarafından verilmiş bir talimatın bulunmasının gerektiği belirtilmiştir[517]. Diğer bir ifadeyle devlete "tam bağlılık" (*complete dependence)* koşulu aranmaktadır[518]. Divan, *de jure* nitelikte olmayan kişileri ve oluşumları; tamamen yabancı devlete bağımlı olan kişiler ve oluşumlar (ekonomik, lojistik ve plan/yönlendirme konularında: *Unilaterally Controlled Latino Assets/UCLA*) ile görece bağımlı, bağımsız hareket edebilme yetisine sahip kişiler ve oluşumlar (kontralar) olarak ele almıştır. İlk kategori kapsamında değerlendirilen grupların devletin sorumluluğuna sebep olabilecekken, ikinci kategorideki grupların doğrudan devletin sorumluluğuna yol açabilmesinin güç olduğu dile getirilmiştir[519].

---

[514] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 255.

[515] Weglinski, 2016, s. 82.; Bu yöntem kontrol temelli test olarak da adlandırılmaktadır. Bkz.; Stokes, 2014, s. 2.

[516] Shackelford, Scott J. (2010). *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Conference on Cyber Conflict, CCD COE Publications, Tallinn, s. 201.

[517] International Law Commission, 2001, Art. 8, s. 47.

[518] Shackelford, 2010, s. 201.

[519] Değer, 2009, s. 87.

Bu kararın 15 yıl sonrasında, devlet dışı aktörlerin eylemlerinden kaynaklanan devletin sorumluluğu konusunda uygulanacak etkin kontrol testinde esaslı değişiklikler meydana gelmiştir. Eski Yugoslavya Uluslararası Ceza Mahkemesi'nde (EYUCM) görülen *Tadi´c Davası*'nda, yönlendirme ve kontrol nedeniyle devlete atfedilebilme konusunda kabul edilen yaklaşım, askeri operasyonların denetim ve planlanmasında sırf finansal ve donanım desteğinin ötesinde "genel kontrol" (*overall control*) kavramı üzerinde şekillenmiştir[520]. Bu teste göre bir grubun devlet tarafından desteklenmesine ilaveten organizasyon ve koordinasyon faaliyetlerinde devletin rolü bulunmalıdır[521]. Grubun askeri faaliyetlerinin genel planlamasına devlet tarafından yardım edilmesi ve koordine edilmesi halinde askeri grubun eyleminden devletin sorumlu olabileceğinin kabul edilmiş olmasının farz edilen sorumluluk anlamına geldiği ileri sürülmüştür[522].

Belirtilen iki karar arasındaki fark UAD'nın devletin bir eylemden doğan sorumluluğunu belirlemek için etkin kontrol şartını benimsemesi, EYUCM'nin ise sadece çatışmanın türünün belirlenmesi adına bundan daha düşük bir eşiği temsil eden genel kontrol testinden yararlanmasıdır[523]. Etkin kontrol testi, bir grup ile devlet arasında bağlılık ve sadakat ilişkisini gerektirmekte olup[524] daha yüksek bir seviyede eşik oluşturmaktadır. 2007 yılında görülen *Bosna Soykırımı Davası*'nda UAD'ye göre, bir çatışma türünün belirlenmesinde genel kontrol standardının kullanılması uygun olabilirken, bir devletin bir silahlı çatışma esnasında belirli bir eylemden kaynaklanan sorumluluğunun belirlenmesinde yapılacak incelemede kullanılamayacaktır[525]. Genel (*overall*) kontrol

---

[520] International Law Commission, 2001, Art. 8, s. 48.; Weglinski, 2016, s. 83. Ayrıca dava için bkz.; EYUCM, "*Tadi´c Case*", 07 Mayıs 1997, Erişim: 16.07.2022 https://www.icty.org/en/press/tadic-case-verdict

[521] Shackelford, 2010, s. 201.

[522] Graham, 2010, s. 95.

[523] Gül, 2021, s. 54.

[524] Padmanabhan, Vijay M. (2013). *Cyber Warriors and the Jus in Bello*, Int'l L. Stud., Cilt:89, s. 294.

[525] Gül, 2021, s. 54-55.

standardı yerine etkin kontrol standardını benimseyen UAD, belirtilen davada soykırım suçu için gereken özel kastın bulunmadığı sonucuna varmıştır[526].

2.3.2. Siber Faaliyetlerden Kaynaklı Uluslararası Sorumluluk

Bir önceki alt başlıkta genel olarak bahsolunan sorumluluğun oluşabilmesi için aranan koşulların siber faaliyetlere uygulanmasında ne tür bir yaklaşımın benimseneceği hususu önem arz etmektedir. Taslak Çalışma metinlerinin, yapılageliş kurallarının ve emsal yargı kararlarının siber uzayın yapısına uygun şekilde değerlendirilmemesi halinde istenilen sonuca varılamayacağı gözetilmelidir. Bu noktada karşılaşılabilecek en önemli zorluklardan ilkinin atfedilebilme unsuru olduğu söylenebilir. Siber faaliyetlerin kaynağını doğru şekilde tespit etmenin zorluğu dikkate alınırsa bunun sebebi kolaylıkla anlaşılabilecektir. Atfedilebilirlik konusunun kapsamlı olması nedeniyle öncelikle fiil ve zarar konusundan bahsedilecektir.

Daha önce de bahsedildiği üzere bir devletin ya da uluslararası örgütün uluslararası sorumluluğunun doğabilmesi için fiil veya faaliyetin uluslararası hukuk kurallarına aykırılık oluşturması gerekir. Devlet ya da uluslararası örgütün fiilinin hukuka aykırılık oluşturabilmesi ise uluslararası yükümlülüklerin ihlali şeklinde gerçekleşmektedir. Siber uzayda gerçekleştirilen barış zamanı kurallarına ve silahlı bir çatışmada uygulanabilir olanları ihlal mahiyetindeki eylemlere örnek olarak, barış zamanı karasularından geçen gemiden zararsız geçiş hakkının ihlali suretiyle gerçekleştirilen siber saldırı eylemleri ve silahlı çatışma esnasında sivil hedeflere yönelik gerçekleştirilen siber saldırı eylemleri gösterilmektedir[527]. Bu bağlamda uluslararası yükümlülüklere aykırılık; uluslararası antlaşmalara aykırı davranmanın yanı sıra egemenliğe saygı, karışmama yükümlülüğü veya kuvvet kullanma yasağı gibi yapılageliş kurallarına aykırı davranış suretiyle de gerçekleşebilir[528].

---

[526] Shackelford, 2010, s. 201.

[527] Schmitt, 2017, *Tallinn Manual 2.0.* s. 85.

[528] Schmitt, 2017, *Tallinn Manual 2.0.* s. 84.

İfade edilmesi gereken bir diğer unsur olan zararın varlığı konusunda da genel uygulamalardan ayrık durumlar hemen kendini göstermektedir. Örneğin, devletin sorumluluğu kapsamında uluslararası hukuka aykırı bir fiil olarak siber saldırının nitelendirilmesinde fiziki zarar veya yaralanma, zararın ana kuralın ihlalinin unsuru olmadıkça, bir ön şart değildir[529]. Tallinn El Kitabı'nda buna örnek olarak; taraflardan birinin Avrupa Konseyi Siber Suç Sözleşmesi'nin 20. maddesine uygun şekilde gerçek zamanlı (*real-time data*[530]) trafik verisi toplama konusunda yasal ve diğer gerekli önlemleri almasında başarısız olması halinde zarar doğmasa dahi uluslararası sorumluluk doğması gösterilmektedir. Bununla birlikte bir devlet tarafından diğer bir devlete karşı gerçekleştirilen siber eylem zararlı, itiraz edilebilir veya dostça olsa dahi uluslararası bir yükümlülüğe aykırı olmadığı takdirde devletin sorumluluğuna sebep olmaz[531]. Aynı şekilde zarar verme niyeti de uluslararası hukuka aykırı bir fiilden bahsetmek için bir gereklilik değildir. Ancak Soykırımın Önlenmesi ve Cezalandırılması Sözleşmesi'nde olduğu şekilde belirli bir gurubu kısmen veya tamamen yok etme niyeti gerektiğinden olay bazında değerlendirme yapılmalıdır [532].

Siber faaliyetlere özgü ayrık durumlardan ilk olarak değinilen atfedilebilirlik konusuna dönüldüğünde görülmektedir ki siber saldırılar açısından uluslararası hukuka aykırı bir fiilin devlete atfedilebilirliği konusunda geleneksel uygulamadan bariz farklılık arz eden durumlar bulunmaktadır. Örneğin, geleneksel olarak tank ve savaş gemisi gibi devlete ait varlıkların devlet organı dışında bir çalışan tarafından kullanılması olanak dâhilinde

---

[529] Schmitt, 2017, *Tallinn Manual 2.0.* s. 86.; International Law Commission, 2001, Art. 2, para. 9, s. 36.

[530] Seyrüsefer ya da izleme faaliyetlerinde sıklıkla kullanılan gerçek zamanlı veri, elde edildiğinde anında paylaşılması gereken bilgi anlamına gelmektedir. Daha ayrıntılı bilgi için bkz.: Wikipedia The Free Encyclopedia. Erişim: 05.11.2022. https://en.wikipedia.org/wiki/Real-time_data

[531] Schmitt, 2017, *Tallinn Manual 2.0.* s. 85-86.; International Law Commission, 2001, General Commentary, para. 4, s. 32.

[532] Özarslan, Bahadır Bumin. (2014). *Soykırım Suçunun Önlenmesi ve Cezalandırılması Sözleşmesi Açısından Hocalı* Katliamı, Hacettepe HFD, Cilt:4, Sayı:1, s. 196.; Schmitt, 2017, *Tallinn Manual 2.0.* s. 86.; International Law Commission, 2001, Art. 2, para. 10, s. 36.

bulunmadığından, bu araçlar ile gerçekleşen eylemlerin devlete atfedilebilirliğinin aksi ispatlanamaz kabul edilirken, bu yaklaşımın siber bağlama kolaylıkla aktarılamayacağı söylenebilir[533]. Zira siber faaliyetlerin bir devlet ya da devlet dışı unsurlar tarafından başka bir devletin siber altyapı unsurları kullanılarak gerçekleştirilebilmesi nedeniyle görünen bağlantı atfedilebilirlik yönünden tek başına yeterli olamamaktadır.

Ayrıca bir devletin ülkesi üzerinden gerçekleştirilen her siber faaliyet, zorunlu olarak ülke devletinin sorumluluğuna sebep olmamakta, bunun için ayrıca siber faaliyetin ülke devletine atfedilebilir olması aranmaktadır[534]. Atfedilebilirlik koşulu sağlanmadıkça karşı önlemlere ya başvurulamamakta ya da en azından olağanüstü düzeyde risk söz konusu olmaktadır[535]. Atfedilebilirlik unsurunun varlığının kabul edilmesi için gereken saldıranın kimliğinin hangi düzeyde ya da netlikte tespiti konusu önemli olduğu kadar da tartışmaya açıktır. Zira masum bir ülkeye karşı gerçekleştirilecek bir karşı saldırı meşru müdafaa kapsamında değerlendirilemeyecek, aksine saldırı eylemi (*act of aggression*) oluşturacaktır[536].

Bir devlete uluslararası sorumluluk atfedilebilmesi konusunda siber saldırıların kaynağının tespiti çok önemli olsa da kaynağın tespiti bir o kadar sorunludur. Örnek vermek gerekirse, 2009 yılında yaşanan bir olayda birtakım Güney Kore ve Amerikan web sitelerinde iletişim kanallarının tıkanmasına sebep olan bir DoS ya da yoğun spam saldırısı gerçekleşmiştir. İlk tespitlere göre saldırının kaynağı Kuzey Kore iken birkaç hafta sonra saldırının kaynağının Miami olduğu ve Kuzey Kore üzerinden yönlendirildiği anlaşılmıştır. Ayrıca saldırının kaynağının Miami'den önce başka bir yer olup olmadığı hala kesin olarak bilinememektedir[537]. Bu örnekten de anlaşılacağı üzere atfedilebilirlik unsurunun tespitinde bazı durumlarda gelinen teknik seviye yetersiz kalmakta ve hatta

[533] Schmitt, 2017, *Tallinn Manual 2.0.* s. 91.

[534] Jensen ve Watts, 2017, s. 1560.

[535] Jensen ve Watts, 2017, s. 1564.

[536] Farwell ve Rohozinski, 2011, s. 35.

[537] Goldsmith, 2013, s. 132.

yukarıda belirlenen karineler vasıtasıyla da atfedilebilirlik sorununun çözümü mümkün olmayabilmektedir. Böylesi durumlarla karşılaşan devletler için sorumlu devletin zaman içinde tespitini sağlama yerine, saldırı anında aktif savunma saldırısı kurallarına göre cevap vermeyi tercih etme olasılığı daha yüksektir.

Siber faaliyetlerden kaynaklı uluslararası sorumluluk hususunda hemen yukarıda bahsedilen ayrık durumlar ve zorluklar gözetilerek atfedilebilirlik özelinde, dolaylı kuvvet kullanma, yardım, yetki aşımı, *de facto* görev konusu ve farz edilen atfedilebilirlik konularında yeni değerlendirmeler ve tespitlerin yapılması gerekmektedir. Bir önceki alt başlıkta ifade edilen devlet görevlileri tarafından gerçekleştirilen fiillerin devlete atfedilebilir kabul edilmesi asıldır. Buna karşın siber operasyonları icra eden devlet ajanları sadece silahlı kuvvetler veya istihbarat elemanları gibi devlet görevlilerinden (*de jure* devlet ajanı) oluşmayıp ayrıca devlet adına hareket etmeye yetkilendirilmiş özel akit tarafı (*de facto* devlet ajanı) gibi diğer personelleri de içerebilir[538]. Özel sektörün yasa ile hükümet adına siber faaliyetlerde bulunmakla yetkilendirilmesi halinde bu kişiler *de jure* devlet görevlisi kabul edilmektedir[539]. Uygulamada pek çok devletin siber güvenlik stratejileri gereği oluşturdukları siber hızlı reaksiyon ekipleri bu kapsamda *de jure* devlet görevlisi olarak kabul edilmelidirler.

Devletler adına hareket etmekte olan *de facto* görevlilerin eylemleri ile devlet tarafından dolaylı kuvvet kullanılması durumları farklılık arz etmektedir. *De facto* devlet ajanı tarafından kuvvet kullanma ile dolaylı kuvvet kullanılması arasındaki fark, ilkinde devlet adına hareket eden ajanın eyleminden devlet doğrudan sorumlu iken, ikincisinde devlet dışı aktörün kendi adına kuvvet kullanmasından dolayı devlet sadece yardım eylemiyle sınırlı ve dolaylı şekilde sorumlu tutulmaktadır[540].

---

[538] Melzer, 2011, s. 10.; Schmitt, Michael N.. (2013). *Classification of Cyber Conflict*. US Naval War Collage International Law Studies, Cilt:89, s. 241.

[539] Schmitt, 2013, *Classification of Cyber Conflict*. s. 242.

[540] Melzer, 2011, s. 11.

Sorumluluğu ileri sürülen bir devletin, adli bilişim gibi bazı durumlarda teknik imkânlarının sınırlı olmasından dolayı siber faaliyetlerde özel sektörden hizmet sağlaması mümkündür. Bu çeşit bir hizmet alan devlet, atfedilebilirlik yönünden fiilin devlet organının eylemi olmadığını gerekçe göstererek sorumluluktan kaçınamaz[541]. Buna göre, devlet ile iş yapan ve siber faaliyette bulunan şirketin (*de facto* görevli) uluslararası yükümlülüklere aykırı eylemlerinin devlet adına gerçekleştirilmesi halinde devlete atfedilebilir bir hukuka aykırı fiilden, kendi adına hareket etmesi halinde ise atfedilemez bir eylemden bahsedilebilir. Devlete atfedilebilmesi için ise, özel şirketin eyleminin yönetimsel niteliği haiz olması ve şirketin yetkilendirilmiş olması gerekir.

Dolaylı şekilde kullanılan devlet dışı aktöre bir devletin genel olarak destek vermesi veya cesaretlendirmesi, atfedilebilirlik için yeterli değildir. Siber faaliyetler yönünden kıyas yapılacak olursa, bir devletin devlet dışı bir aktöre kötü amaçlı yazılım temin etmesi tek başına atfedilebilirliği sağlamaz[542]. UAD *Nikaragua Davası*'nda, etkin kontrol eşiğine ulaşma açısından, bir devletin devlet dışı bir aktöre finansal açıdan ya da organizasyon, eğitim, donatım ve ikmal konularında baskın ve belirleyici desteğini ve askeri-yarı askeri hedeflerin seçimi, tüm harekâtın planlanması eylemlerini yeterli bulmamıştır. Buna karşın, devlete atfedilebilir bulunmayan siber faaliyetlerin uluslararası hukukun ihlali manasına gelmeyeceği, bir gruba kötücül yazılım sağlamanın Kural 66'da düzenlenen karışma durumuna sebep olabileceği kabul edilmektedir[543].

Roscini, özellikle eğer zarar gören devletin meşru müdafaa hakkını ileri sürmesi halinde, devletlerin önemsiz bir şekilde suçlanmasını önleyeceği için siber faaliyetlerle bağlantılı sorunlarda kimlik saptama konusunda genel kontrol standardına nazaran etkin kontrol standardının daha uygun olduğunu savunmaktadır[544]. Zira UAD, genel kontrol standardını sadece organize ve hiyerarşik yapılı bir grupla ilgili olaylarda

[541] Schmitt, 2017, *Tallinn Manual 2.0.* s. 90.

[542] Schmitt, 2017, *Tallinn Manual 2.0.* s. 97.

[543] Schmitt, 2017, *Tallinn Manual 2.0.* s. 97.

[544] Roscini, 2010, s. 100.; Aynı şekilde etkin kontrol testinin benimsendiğine dair bkz.: Jensen ve Watts, 2017, s. 1562.

kullanmaktadır[545]. Buna karşın, siber uzayın kendine özgü mimarisinden dolayı devlete atfedilebilirlikte genel kontrol standardının kullanılmasının daha doğru olacağı ileri sürülmüştür. Bu görüşe göre, atfedilebilirlik konusunda etkin kontrol standardının benimsenmesi, devlet destekli siber saldırılara serbest geçiş imkânı sağlayacaktır[546]. Buna karşın, siber saldırıları gerçekleştiren grupları destekleyen bir devlete atfedilebilirlik konusunda genel kontrol standardının uygulanması halinde ise, her türlü şüphenin ötesi kıstası yerine makul şüphenin ötesinde yeterli kanıtların varlığı kıstası uygulanacağından devletin sorumluluğu söz konusu olabilecektir[547]. Kanaatimizce, siber faaliyetler konusunda etkin kontrol standardının benimsenmesi, devlete atfedilebilirlik konusunda daha zor ispat kurallarının işletilmesini gerektireceğinden ve bunun teknik zorlukları nedeniyle genel kontrol standardının siber faaliyetlere daha uygun olduğu kolaylıkla söylenebilir. Meşru müdafaa konusu ise, kendi kuralları dâhilinde olayın gerçekleşme koşullarına göre değerlendirilmelidir.

Estonya saldırısında olduğu üzere anlık gelişen bir hacktivist siber saldırı kampanyası durumunda, bu saldırının bir devlete yaraması ya da yoğun şekilde ilgili devlet vatandaşlarının eylemleri olması atfedilebilirlik hususunda tek başına yeterli kabul edilmemektedir. Ancak ilgili devletin gerçekleştirilen saldırı kampanyasının sürdürülmesini onaylaması ve cesaretlendirmesi halinde, gerçekte yönlendirme bulunmasa da bu kişiler *de facto* devlet organı olarak kabul edilebilecektir[548]. Devletin bu onay ve cesaretlendirme tutumu, *Tahran Rehineler Davası*'nda olduğu üzere, saldırının bir yönüyle benimsenmesi düzeyinde değerlendirilirse bu durum söz konusu olabilecektir. Zira devletin siber operasyonu planlama ve yönetme, bir diğer ifade ile genel kontrol söz konusu olmasa da benimsemesi, sorumluluğuna sebep olabilecek bir husustur.

---

[545] Jensen ve Watts, 2017, s. 1560.

[546] Shackelford, 2010, s. 202.

[547] Shackelford, 2010, s. 205-206.

[548] Schmitt, 2013, *Classification of Cyber Conflict.* s. 242.

Devlet dışı aktörlerin gerçekleştirdiği *ultra vires* eylemlerin devlete atfedilebilirliği konusu Tallinn El Kitabı'nda üç ihtimalde ele alınmıştır[549]. İlk olarak, bir devletin özel bir şirkete, diğer bir devlete olan uluslararası yükümlülüklerini siber faaliyette bulunarak ihlal eden silahlı güce destek vermesi talimatına dayanarak gerçekleştirilen, örneğin diğer bir devletin SCADA sistemine yıkıcı mantık bombası yerleştirmek gibi bir eylemin ilk devlete atfedilebilir olduğu kabul edilmektedir. İkinci halde, devletin yasal karşı önlem mahiyetinde diğer devletin SCADA sistemine karşı siber saldırı gerçekleştirmesi için özel şirkete talimat vermesi, ancak sonuç olarak üçüncü bir devletin karşı saldırıdan olumsuz etkilenmesi durumunda, talimatın parçası olmamasına rağmen, karşı önlem konusunda talimat veren devlete atfedilebilir bir eylem söz konusudur. Son durumda ise, devletin diğer bir devletin hükümet ağına kötü amaçlı yazılım yerleştirmesi talimatına karşın, talimat alan özel şirketin yetkiyi suiistimal ederek kötü amaçlı yazılımı üçüncü bir devletin ağına bulaştırması halinde, *ultra vires* nedeniyle haksız eylem ilk devlete atfedilemeyecektir.

Bir devletin etkin kontrolü altındaki devlet dışı bir aktör tarafından gerçekleştirilen *ultra vires* siber operasyonunun devlete atfedilebilir olup olmadığının tespiti için, operasyonun göreve özgü olup olmadığının ve açıkça onun ötesine geçip geçmediğinin [550] değerlendirilmesi gereklidir. Uluslararası Uzmanlar Komisyonu, eğer *ultra vires* siber operasyon devletin etkin kontrolü altındaki operasyonun amacıyla ilgisiz ve konu dışı ise hukuka aykırı fiilin, kontrol eden devlete atfedilemeyeceği konusunda fikir birliği içindedir. Bu, eylemin devletin etkin kontrolü altındaki operasyonun esaslı bir parçası olması bakımından bütüncül olduğu sürece devlete atfedilebilir olduğu manasına gelir[551].

Tallinn El Kitabı'nda, uluslararası yükümlülüğün ihlalinin devlet organı tarafından görünüşe göre (*appearently official capacity*) veya yetkinin arkasına saklanarak görev bahanesiyle (*under the colour of autority*) resmi görev adına gerçekleştirilmesi halinde

[549] Schmitt, 2017, *Tallinn Manual 2.0.* s. 97-98.

[550] International Law Commission, 2001, Art. 8, para. 8, s. 48.

[551] Schmitt, 2017, *Tallinn Manual 2.0.* s. 98.

yetki aşımı söz konusu olduğunda devlete atfedilebilirlik kabul edilmiştir[552]. Yetki aşımı veya yetkisiz eylem, Taslak Çalışma'nın 7. maddesinde düzenlenmiştir. Buna göre, bir devlet organının yetkisiz şekilde gerçekleştirdiği ya da devletin yönetimsel otorite unsurlarını kullanmakla yetkilendirilmiş devlet organı dışındaki bir varlığın yetki aşımı mahiyetindeki eylemi devlete atfedilebilir bir durumdur[553]. Buna karşın yasal yetkili şirketin yükümlülükleriyle ilgisi bulunmayan örneğin çalışanların siber suç oluşturan zararlı fiilleri devlete atfedilemez[554].

Uluslararası hukuka aykırı bir siber operasyonun bir devlete atfedilebilmesi için gereken ilk koşulun, operasyonun bir devlet organı tarafından gerçekleştirildiğinin tespiti olduğu, bunun sağlanamaması halinde ise *Rehineler Davası*'nda gerçekleştiği üzere devletin benimsemesi halinin arandığı[555] yukarıda açıklanmıştı. Bu operasyonun devlet dışı bir aktör tarafından gerçekleştirilmesi ve genel kontrol testinin de bazı durumlarda uygulanamaması halinde atfedilebilirlik konusunda yeni kavramlar ortaya çıkmıştır. Zira siber saldırıların izi sürüldüğünde, saldırıların tamamında esasen devlet dışı aktörlere varılması gerçeği karşısında dikkatler "farz edilen atfedilebilirlik" kavramı üzerinde toplanmıştır[556]. Öğretide "sanal kontrol" testi olarak da ifade edilen bu yeni kavram ile devlet dışı aktörlerin siber faaliyetleri nedeniyle genel kontrol testinden de daha geniş ölçekli yeni bir standart önerilmektedir[557]. Tallinn El Kitabı'nda olgusal atfedilebilirlik olarak ele alınan bu kavram yasal atfedilebilirlik kurallarının özellikle siber eylemler söz konusu olduğunda çoğunlukla devlet dışı örgütler tarafından gerçekleştirilen eylemler ile ilgili devlet arasında bağ kurulması mümkün olamadığında uygulama yeri bulmaktadır. Zira devletin uluslararası sorumluluğunda geleneksel anlamda geçerli olan ve uluslararası hukuka aykırı fiilin devlete kesin olarak atfedilebilirliğinin gerekliliği unsuru, siber saldırılarda kaynağın tespit edilmesi halinde dahi zombi saldırıda bilgisayar

[552] Schmitt, 2017, *Tallinn Manual 2.0.* s. 89.

[553] International Law Commission, 2001, Art. 7, para. 1, s. 45.

[554] Schmitt, 2017, *Tallinn Manual 2.0.* s. 91.

[555] Shackelford, 2010, s. 203.

[556] Graham, 2010, s. 93.; Garrie ve Simonova, 2020, s. 534.

[557] Weglinski, 2016, s. 83.

kullanılabilmesi ihtimali söz konusu olduğundan siber saldırıların doğası gereği tam olarak uygulanamamaktadır.

Devletin siber saldırıları için farz edilen sorumluluğu, devletlerin ülke topraklarının böylesi bir saldırıda fırlatma rampası olarak kullanılmasını önleme görevinin bulunduğu ön kabulüne dayanır[558]. Devletlerin yükümlülüğünde olan önleme görevi ise, sırasıyla; ulusal sınırları içerisinden uluslararası siber saldırı gerçekleştirilmesi halinde etkili ceza yasaları oluşturmak; siber saldırıların esaslı ve detaylı şekilde soruşturulması; bu saldırıları işleyenlere dava açılması; bu saldırılardan sorumlu olanların mağdur devletçe soruşturulması ve dava açılması konusunda işbirliğinden oluşmaktadır[559]. Devletlerin engelleme yükümlülüğünün kaynağı konusunda Avrupa Siber Suç Sözleşmesi önemli bir yer tutmaktadır. Ayrıca devletlerin uygulamaları açısından BM Genel Kurulu Kararları (BM GK. 45/121[560] ve 55/63[561] sayılı) bu konuda devletlere açıkça yükümlülükler öngören dayanak normları olarak ifade edilebilir[562]. Devletin farz edilen sorumluluğu 11 Eylül saldırıları sonrasında dolaylı sorumluluk olarak vücut bulmuş, Taliban hükümetinin El Kaide terör örgütü üzerinde ne etkin ne de kapsamlı kontrole sahip olmamasına rağmen Afganistan'a sorumluluk atfedilmiştir. Buna gerekçe olarak ise, devlet dışı aktörlerin devletin ülkesini başka devletlere saldırıda üs olarak kullanmasını önlemeye yönelik

---

[558] Graham, 2010, s. 93.; Devletin önlem yükümlülüğüne dair UAD'nın *Korfu Kanalı Davası*'nda verdiği karar belirtilen ilkenin dayanağını oluşturmaktadır. Bkz.: Schmitt, 2013, *Classification of Cyber Conflict*. Dipnot 36, s. 244.

[559] Graham, 2010, s. 94.; Sklerov, Matthew J. (2009), *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent*. Erişim: 27.04.2020 https://www.hsdl.org/?view&did=12115

[560] BM Genel Kurulu. "Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (A/RES/45/121)" Erişim: 05.11.2022 https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/565/10/IMG/NR056510.pdf?OpenElement

[561] BM Genel Kurulu. "Combating the Criminal Misuse of Infirmation Thecnology (A/RES/55/63)" Erişim: 05.11.2022 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement

[562] Graham, 2010, s. 94.

uluslararası yükümlülüklerde başarısız olunması gösterilmektedir [563] . Uluslararası kamuoyunda tartışmalı olan bu yaklaşımın siber saldırılara uygulanması durumunda yeterli soruşturma ve kovuşturma yapmayan ya da uluslararası yükümlülüklerini yerine getirmede başarısız kabul edilen bir devletin devlet dışı aktörlerin eylemlerinden dolayı sorumluluğu söz konusu olabilecektir.

Tallinn El Kitabı 14. Kural'da, uluslararası hukuka aykırı siber-bağlantılı fiilden dolayı bir devletin sorumlu olabilmesi için Taslak Çalışma'da yer alan iki unsurun[564] varlığının gerektiği belirtilmiştir. Siber-bağlantılı fiil terimi, devlet tarafından gerçekleştirilen veya ona atfedilebilir siber saldırı dışındaki sorumluluk gerektiren eylemleri belirtmek için kullanılmaktadır. Buna örnek olarak bir devletin siber altyapı unsurlarını devlet dışı grup veya başka bir devlete açması, kendi topraklarından gerçekleşen siber saldırıyı önlemeye yönelik tedbirleri almaması (Kural 6-7), siber saldırı için yazılım ve donanım sağlanması gösterilmiştir[565].

Devletin uluslararası hukuka aykırı fiilden sorumluluğuna dair Taslak Çalışma'nın 6. maddesinde belirtilen bir devletin sorumluluğu altında bulunan başka bir devlet organının eyleminden sorumluluk durumu ise, Tallinn El Kitabı'nda 16. Kural'da siber eylemler yönünden değerlendirilmiştir. Bir devlet organının belirli bir yönetimsel faaliyeti gerçekleştirmek amacıyla diğer bir devletin sorumluluğunda olduğu sırada gerçekleştirilen siber eylemlerden dolayı kabul eden devletin, "münhasırlık kontrolü" ve "kabul eden devlet adına ve amaçlarına yönelik eylemler" olgusal ön şartları söz konusu olduğu takdirde sorumlu olduğu kabul edilmiştir[566]. Kabul eden devletin bahse konu organ üzerinde münhasır kontrol yetkisini taşıması, gönderen devletin kontrol yetkisinin

---

[563] Graham, 2010, s. 96.

[564] Bunlar; ilk olarak belirtilen eylemin bir devletin uluslararası yükümlülüğünün ihlalini oluşturması, ikinci olarak bu eylemin uluslararası hukuka göre bir devlete atfedilebilir olması hususlarıdır. Bkz.; International Law Commission, 2001, s. 34.

[565] Schmitt, 2017, *Tallinn Manual 2.0.* s. 84.

[566] Schmitt, 2017, *Tallinn Manual 2.0.* s. 93.

olmamasını gerektirmektedir. Aksi takdirde gönderen devletin yetkisinin devam etmesi halinde bu kuralın uygulanması söz konusu olmayacaktır.

Münhasır yönetim ve kontrol terimleri, gönderen devlet ile kabul eden devletin sorumluluk ayrımının yapılmasında kullanılmaktadır. Gönderen devletin sadece talimatının (*instructions*) bulunması sorumluluk için yeterli değildir. Sorumluluğu, münhasır yönetimi (*exclusive direction*) ve kontrolü elinde bulunduran devlet üstlenmekte ve fiil bu devlete atfedilebilmektedir. Daha açık ifade ile gönderen devletin kabul eden devlete gönderdiği siber uzmanlar için başta verdiği görevlendirme talimatı tek başına gönderen devleti sorumlu kılmamakta, ancak olaysal temelde gönderen devletin münhasır yönetiminin ve kontrolünün olması durumunda sorumluluk ilk devlete atfedilebilir olmaktadır.

Diğer bir devletin sorumluluğunda, münhasır yönetimi ve kontrolü altında olmakla birlikte, siber faaliyetlerin buna imkân sağlamasından dolayı, uzmanların fiziken kendi ülkelerinde konumlanmış olmaları halinde siber faaliyetlerden kaynaklı sorumluluk genel kurala uygun biçimde kabul eden devlete atfedilebilir. Buna karşın, siber faaliyetlere karşılık olarak, gönderen ve kabul eden devlete yönelik gerçekleştirilen siber operasyonlar söz konusu olduğunda, Tallinn El Kitabı'nda bahse konu uzmanların eyleminden bu uzmanların organı olduğu devletin doğrudan yararlanacağı gözetilerek bu kuralın uygulanamayacağı kabul edilmektedir[567].

Bir devletin siber hızlı reaksiyon ekibini başka bir devletin tam sorumluluğu altında görevlendirmesi ve kabul eden devlet tarafından pasif savunma halinde ve söz konusu siber saldırının zararlarını hafifletmeye yönelik talimatları kapsamında faaliyet halinde olması mümkündür. Böyle bir durumda, ekibin kendi isteğiyle DoS saldırısı ve karşı hackleme gibi bir aktif savunma eylemini gerçekleştirmesi örneğinde olduğu şekilde bir *ultra vires* söz konusu olduğunda genel kural gereği kabul eden devletin sorumluluğundan

[567] Schmitt, 2017, *Tallinn Manual 2.0.* s. 94.

bahsedilecektir[568]. Bu noktada, kabul eden devletin sorumluluğundan bahsedilebilmesi için eylemin göreve özgü olması ve eylemin operasyonun esaslı bir parçasını oluşturması gerektiği de dikkate alınmalıdır.

Tallinn El Kitabı 17. Kural'da devlet dışı aktörler tarafından gerçekleştirilen siber faaliyetlerin devlete atfedilmesi konusu incelenmiş ve iki halde devlete atfedilebileceği kabul edilmiştir[569]. İlki, devletin talimatları doğrultusunda veya devletin yönlendirme ve denetimi altında gerçekleşen siber faaliyetler; ikinci olarak devletin söz konusu siber faaliyetleri kabul veya benimsemesi halidir. Devletin sorumluluğuna dair Taslak Çalışma'da talimat, yönlendirme ve kontrol kavramlarının ayırıcı bir özelliğe sahip olduğu ve bunlardan birinin gerçekleşmesi halinde atfedilebilirlik unsurunun ortaya çıkacağı ifade edilmiştir[570].

Bu kural Uluslararası Hukuk Komisyonu Taslak Çalışması'nın 8. maddesinde yer bulmuş ve genel olarak özel kişi veya varlıkların eylemin devlete atfedilebilir kabul edilmese de özel kişi veya varlık ile devlet arasında belirli, gerçek bir ilişki bulunması halinde eylem devlete atfedilebilecektir. Bunun için ilk olarak, özel kişinin uluslararası hukuka aykırı fiili gerçekleştirdiğinde devletin talimatı üzerine hareket ediyor olması ve ikinci ihtimalde daha genel bir durum olarak özel kişinin devletin yönlendirme ve kontrolünde eylemi gerçekleştirmesi gerekir. Her iki durumda da uluslararası hukukta etkililik prensibi göz önünde bulundurularak devlet mekanizması ile özel kişi veya varlık arasında gerçek bir bağlantının varlığı söz konusu olmalıdır[571].

Devlet dışı aktörler kişi veya gruplardan oluşabileceği gibi, gruplar birleşik veya bağımsız, hiyerarşi içinde ya da değil, organize ya da teşkilatsız, iç hukukta yasal bir kişiliğe sahip ya da sahip olmamış olabilir. Tallinn El Kitabı'nda bahse konu kavramın,

---

[568] Schmitt, 2017, *Tallinn Manual 2.0.* s. 94.

[569] Schmitt, 2017, *Tallinn Manual 2.0.* s. 94.

[570] International Law Commission, 2001, Art. 8, para. 7, s. 48.

[571] International Law Commission, 2001, Art. 8, s. 47.

diğerleri arasında, münferit bilişim korsanlarını, Anonymus gibi gayri resmi grupları, siber suçlar ile meşgul olan suç örgütleri, ticari bilgi teknolojileri, yazılım ya da donanım şirketleri gibi yasal varlıklar ve siber teröristler veya direnişçileri kapsadığı ifade edilmektedir[572].

Taslak Çalışma'nın 16, 17 ve 18. maddelerinde düzenlenen[573] üçüncü devletin yardımı, yönlendirme ve kontrolü veya zorlaması ile gerçekleştirilen hukuka aykırı fiilden sorumluluk konusu Tallinn El Kitabı Kural 18'de tek bir maddede düzenlenmiş olup siber operasyonlar bakımından bir devletin üç durumda da diğer bir devletin eyleminden sorumlu olacağı belirtilmiştir. İlk olarak, diğer bir devletin uluslararası hukuka aykırı fiilin işlenmesine maddi destek veya diğer yardımından dolayı; ikinci olarak, diğer bir devletin uluslararası hukuka aykırı fiilinden, hukuka aykırı fiilin koşulları hakkında bilgi sahibi olduğu haliyle yönlendirme ve kontrolü altında işlenmesinden; son olarak, diğer bir devleti zorlaması neticesinde oluşan hukuka aykırı fiilden devletler sorumlu olacaktır[574].

Bu kurala göre yardım eden devletin sorumlu olabilmesi için uluslararası yasal bir yükümlülüğün ihlal edildiğinin bilincinde olması kritik bir unsurdur. Yardım eden devletin kendi kontrolü altındaki ISP gibi bir siber alt yapı unsurunu bilerek, fiilin gerçekleştirilmesinde kullanılmak üzere diğer bir devlete izin vermesi buna örnek gösterilebilir[575]. Devletin devlet dışı aktöre dikkate değer yardımı halinde, devlet dışı aktörlerin siber operasyonlarından dolayı devlet doğrudan sorumlu tutulamaz. Devlet yardımı bizatihi BM Şartı 2/4 aykırı şekilde dolaylı güç kullanımına veya içişlerine karışmama prensibine aykırılığa eşit olabilir[576].

---

[572] Schmitt, 2017, *Tallinn Manual 2.0.* s. 95.

[573] International Law Commission, 2001, Art. 16, 17, 18, s. 65-69.

[574] Schmitt, 2017, *Tallinn Manual 2.0.* s. 100.

[575] Schmitt, 2017, *Tallinn Manual 2.0.* s. 101.

[576] Melzer, 2011, s. 11.

Kural 18'de düzenlenen diğer bir devlet bağlantılı hukuka aykırı fiilden sorumluluk konusunda, ilk fıkrada öngörülen yardım eylemi halinde yardım eden devletin sorumluluğu yalnızca yardım eyleminin sonuçlarıyla sınırlı iken, diğer iki fıkrada gerçekleşen eylemlerin sonuçlarından diğer bir devlet tamamen sorumludur[577]. Buna karşın, Uzmanlar Grubu devletin maddi destek veya yardımı yardım edilen devletin siber operasyonunun esaslı ve ayrılmaz bir parçası olması halinde yardım eden devletin tüm uluslararası hukuka aykırı fiilden sorumlu olacağı kabul etmektedir[578]. Sırf donanım ve yazılım sağlama eyleminin atfedilebilirlik hususunda gerekli şartları karşılamadığı kabul edilmektedir[579]. Zorlama halinde ise zorlama sonucu uluslararası hukuka aykırı fiili gerçekleştiren devletin mağdur devlete karşı sorumluluğu bulunmamaktadır[580].

Siber saldırıların içişlerine karışma yasağına aykırı olduğunu kabul eden Roscini, içişlerine karışmama konusunda 1981 tarihli BM Genel Kurulu Deklarasyonu'nun tam olarak siber saldırılara uyduğunu, zira Deklarasyonun bilgiye serbest erişim ve müdahale olmaksızın bilgi sistemlerini, kitlesel medyayı ve politik, ekonomik sosyal ve kültürel çıkarlarını ve arzularını geliştirmek için bilgi medyasını kullanmada kendini tamamen geliştirme konusunda insanlara ve devletlere çağrıda bulunduğunu ifade eder[581]. Devletin uluslararası sorumluluğuna ilişkin Uluslararası Hukuk Komisyonu (UHK) çalışmasında tahrik (*incitement*) ile ilgili açık bir düzenleme bulunmamakta, ancak tahrik edici eylemin Madde 8'e göre yönlendirme ve kontrole eşit olması halinde sorumluluğun bulunacağı öngörülmektedir[582].

Devletin uluslararası sorumluluğu ile bireylerin savaş suçu, barışa karşı ve insanlığa karşı suç ya da soykırım gibi suçlardan cezai sorumluluğu ile bahse konu devletlerin ve

[577] Schmitt, 2017, *Tallinn Manual 2.0.* s. 102.

[578] Schmitt, 2017, *Tallinn Manual 2.0.* s. 102.

[579] Schmitt, 2013, *Classification of Cyber Conflict*. s. 243.

[580] International Law Commission, 2001, Art. 18, para. 4, s. 70.

[581] Roscini, 2010, s. 103.

[582] Roscini, 2010, s. 101.

uluslararası örgütlerin geleneksel uluslararası sorumluluğu aynı değildir[583]. Uluslararası sorumluluk konusu dışında kalmakla birlikte son olarak siber faaliyetleri gerçekleştiren kişilerin bireysel sorumlulukları konusuna bu bahiste değinmek gerekli görülmüştür. "Saldırı" suçuna eşit düzeydeki siber saldırıların faillerinin uluslararası cezai sorumluluk taşıdıkları konusuna Roscini kuşkuyla yaklaşmaktadır. Uluslararası Ceza Mahkemesi Statüsü'nün 8/2. maddesinde belirtilen durumlara kinetik saldırılarla benzerliği bulunan belirli siber saldırı eylemlerinin uyduğu düşünülebilirse de Roscini bu derece geniş yorumu kabul etmemektedir[584].

Kanaatimizce, gerek genel kabul gören etki temelli test uyarınca ortaya çıkan sonuç üzerinden değerlendirme yapıldığında ve gerekse de mevcut normların siber saldırılara uygun şekilde yorumlanması halinde, geniş yorum ya da aşırı yorum söz konusu olmadan da sonuca varılabilecektir. Örneğin, soykırım suçunun kanunilik, maddi ve manevi unsurlarını karşılayan bir siber saldırı eylemi sonucunda ortaya çıkan sonucun kinetik ya da siber silahlarla gerçekleştirilmesi arasında fark bulunmamaktadır. Böyle bir durumda, siber saldırılar ile kinetik saldırılar arasında benzerlik konusunda uygulanmakta olan uluslararası hukuk normlarının geniş yorum yöntemiyle değerlendirilmesi söz konusu değildir. Zira kullanılan silahın türüne bakılmaksızın iddia olunan eylemin hareket ve netice kapsamında ceza normuna uygunluğu ve failin özel kastı haiz olup olmadığı değerlendirilecektir.

Genel olarak devlete atfedilemedikçe gerçek ve tüzel kişilerin uluslararası hukuku ihlal edemeyeceği, ancak devletin ihlal edebileceği kabul edilmektedir[585]. Ancak uluslararası ceza hukuku rejimine göre bir gerçek kişinin savaş suçundan dolayı uluslararası hukuku ihlalden sorumlu tutulabilmesi olanaklıdır[586]. Bu noktada 1949 tarihli Cenevre Konvansiyonları'na Ek Protokol'ün 90. maddesi gereğince kurulan Gerçekleri Araştırma

[583] Pazarcı, 2021, s. 444.

[584] Roscini, 2010, s. 112.

[585] Schmitt, 2017, *Tallinn Manual 2.0.* s. 17.

[586] Schmitt, 2017, *Tallinn Manual 2.0.* s. 35.

Komisyonu'nun, Konvansiyonlarda ve Ek Protokollerde tanımlanan ağır suçlar ile silahlı çatışmalar hukukunun diğer ağır ihlallerini araştırma üzere kurulduğu[587] dikkatten kaçırılmamalıdır. Tallinn El Kitabı'nın 84. Kuralı'nda da savaş suçuna eşit olan siber operasyonların uluslararası hukuk kapsamında bireylerin cezai sorumluluğuna sebep olabileceği kabul edilmiştir.

2.3.3. Devletin Gereken Özeni Gösterme Yükümlülüğü

Devletin uluslararası hukuka aykırı siber faaliyetlerinden sorumluluğu konusunda sorunlu bir unsur olan atfedilebilirliğe dair yeni yaklaşımların kabulü bir gerekliliktir. Bu konuda var olan boşluğu doldurabilmek için geleneksel uluslararası hukuk öğretilerinin gelişen teknolojiye farklı şekilde uyarlanması söz konusu olmaktadır. Bu noktada uygulama alanı bulan devletin özen gösterme yükümlülüğü ve bu ilkenin siber alana uygulanması konusunda uluslararası uzlaşı eksikliği söz konusudur[588]. Bununla birlikte özen gösterme yükümlülüğü ilkesi, devletlerin ülkesinden kaynaklanan siber faaliyetlere daha geniş ölçekte uygulanması nedeniyle atfedilebilme boşluğunu doldurmada yardımcı olabilecek[589] bir yaklaşım olarak kabul edilmektedir[590].

---

[587] Streltsov, 2017. s. 9.

[588] Corn, Gary / Jensen, Eric Talbot. (2018). *The Use of Force and Cyber Countermaesures*. 32 International & Comperative Law Journal 127, s. 8. Erişim: 17.01.2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3190253; Ayrıca siber uzay söz konusu olduğunda bu yükümlülüğün uygulanmasının zorluğu konusunda bkz.; Dal, Ufuk. (2019). *Uluslararası Sorumluluk Hukukunda Uluslararası Hukuka Aykırı Eylemin Devlete Atfedilmesi*. Doktora Tezi, İstanbul, İstanbul Üniversitesi, s. 147.

[589] Jensen ve Watts, 2017, s. 1565.

[590] Taslak Çalışma'nın 25. Maddesinin Türkçe metni için bkz.; Erkiner, Hakkı Hakan. (2008). *Devletin Haksız Fiilinden Kaynaklanan Milletlerarası Sorumluluğu*. Doktora Tezi, İstanbul, Marmara Üniversitesi, s. 195. Alman devleti tarafından yayınlanan tutum belgesinde devletin özen gösterme yükümlülüğü benimsenmiştir. Bkz.; Position Paper, 2021, s. 3.

Özen gösterme yükümlülüğünün kaynağının ne olduğu, devletlerin bu yükümlülüğünün nereden kaynaklandığı sorusunun cevabı, uluslararası hukukun dayanağı konusundaki teorik tartışmalara varmaktadır. Bu yükümlülüğün doğal hukukun bir gereği olduğu ya da devlet iradesinden kaynaklandığı veya ahde vefa ilkesinin sonucu olduğu savunulabilir. Zira antlaşma hükümleri kural olarak, sadece bu antlaşmaya taraf olan devletlerarasında hukuki sonuç doğurur (*pacta tertiis nec nocent nec prosunt*). Viyana Antlaşmalar Hukuku Sözleşmesi'nin (VAHS) Üçüncü Devletlerle İlgili Genel Kural başlığını taşıyan 34. maddesinde bu durum ortaya konulmuştur[591]. Buna karşın, bazı antlaşmaların taraf olmayan devletleri de bağlayacak şekilde objektif hukuki durum yaratması mümkündür. Özen gösterme yükümlülüğünün kaynağını, böylesi antlaşmada bulmak olanaklı değil ise de bazı uluslararası yargı kararlarında temel ilkelerden yola çıkılarak bu ilkeye atıf yapıldığı görülmektedir.

Bu yükümlülük, egemenlik prensibinin bir uzantısı olarak Latincede "*sic utere tuo ut alienumnon laedas*" olarak ifade edilen "mülkiyetini başkasının mülküne zarar vermeyecek biçimde kullan" ilkesini kapsamaktadır[592]. Mülkiyetten kaynaklanan yükümlülük konusunda Hugo Grotious'a kadar giden[593] bu ilkeyi teyit eden *Trail Smelter* Kararı'nda devletin ülkesini diğer bir devlet ülkesine zarar vermeyecek şekilde kullanma yükümlülüğü vurgulanmıştır[594]. Bu yükümlülük ayrıca bazı durumlarda "ihtiyat yükümlülüğü" (*Korfu Kanalı Davası*'nda olduğu üzere), "önleme yükümlülüğü" ve "önleme görevi" ne işaret etmektedir[595]. Bugüne değin siber güvenlik bağlamında UAD tarafından verilen bir karar bulunmasa da daha önceki kararlar devletlere siber güvenlik politikasının belirlenmesinde yol gösterici olabilir[596]. Gelinen noktada siber özen

---

[591] Tütüncü, Ayşe Nur / Arıkoğlu, Enver / Akün, Verda Neslihan / Başkaracaoğlu, Elif. (2017). *Milletlerarası Hukuk.* İstanbul: Beta, s. 203.

[592] Schmitt, 2017, *Tallinn Manual 2.0.* s. 30.

[593] Bkz.; Grotius, Hugo. (2001). *On the Law of War and Peace* (Çev. A.C. Campbell). Kitchener: Batoche Books, s. 107.

[594] Jensen ve Watts, 2017, s. 1565.

[595] Schmitt, 2017, *Tallinn Manual 2.0.* s. 31.

[596] Weglinski, 2016, s. 84.

gösterme yükümlülüğünün yukarıda belirtilen ilkeler yanında insan haklarını çevrim içi koruma ve insancıl hukuk kapsamında da uygulama alanı bulduğu kabul edilmektedir[597].

Tallinn El Kitabı'nda Kural 6'da belirtilen özen gösterme yükümlülüğü, uluslararası hukukun genel bir prensibi olarak, bir devletin kendi ülkesinin veya egemenliği altında bulunan diğer bir bölgenin veya siber altyapı unsurlarının diğer bir devletin haklarını etkileyecek veya ciddi olumsuz sonuçlar doğuracak biçimde kullanılmasına izin vermemesini gerektirmektedir[598]. Tallinn El Kitabı'nda düzenlenen siber özen gösterme yükümlülüğü, yukarıda bahsedilen başkasına zarar vermeme ve ihtiyat yükümlülüğü ilkelerini tek bir ilkede birleştirmiştir[599]. Bu bağlamda bir devletin ülkesinden kaynaklı ve diğer devletlere zarar getiren siber saldırıları önlemeye yönelik gerekli önlemleri alması zorunludur[600]. Bu önlemler bir devletin siber faaliyetlerden kaynaklanan zararı önleme, durdurma ve gidermeye yönelik olarak elinden gelenin en iyisini gerçekleştirmesini kapsamaktadır [601] . Bununla birlikte, devletin ülkesini veya egemenliğini kullandığı yer veya siber alt yapı tesislerinin diğer devletlerin zararına kullanılmaması konusunda gerekli özeni göstermesi beklenir ise de Tallinn El Kitabı'nda Uzmanlar Grubu bunu somut önleyici adım atılmasını kapsayan bir önleyici yükümlülük olarak kabul etmemektedir[602].

Benzer şekilde, ülkesinden başka bir devlete yönelik zararlı siber saldırı gerçekleştirilen devletin önleme kapasitesinin yetersiz olmasına karşın başka bir devletten yardım alması halinde özen gösterme yükümlülüğünü yerine getirebileceğinden bahisle sorumlu tutulamayacağı, zira özen yükümlülüğünün egemenlikten kaynaklandığı kabul

---

[597] Coco, Antonio / Dias, Talita de Souza. (2021). '*Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*, EJIL, Cilt:32, Sayı:3, s. 783.

[598] Schmitt, 2017, *Tallinn Manual 2.0.* s. 30.

[599] Coco ve Dias, 2021, s. 786.

[600] Dal, 2019, s. 147.

[601] Coco ve Dias, 2021, s. 774.

[602] Schmitt, 2017, *Tallinn Manual 2.0.* s. 52.

edilmektedir[603]. Özen yükümlülüğü kuralının yardım etmekten farkı ise, ilkinin ihmal temeline dayalı iken ikincisinde bilerek yardım etme halinin ağır basmasıdır[604]. Özen prensibi, hukuki bir yükümlülük olup ihmal suretiyle işlenebilir. İhmal ise, sadece eylemsizliği değil, ayrıca diğer daha uygun tedbirler mümkün olduğu takdirde, yani makul şekilde erişilebilir ve uygulanabilir olduğunda, etkisiz ve yetersiz önlemlerin alınmasını da kapsar[605].

Devletin özen gösterme yükümlülüğünün kendi ülkesinden kaynaklı zarar vermeme yükümlülüğü yanında diğer devletleri uyarma yükümlülüğünü de kapsadığı kabul edilmektedir[606]. Bu kapsamda bir devletin kendi ülkesinden kaynaklı siber saldırıyı önlemesi gerektiği halde istihbarat paylaşımını sınırlandıran iç hukukunu bahane ederek eylemsiz kalması hukuka uygun kabul edilmemektedir[607]. Ayrıca, ülkesinde zararlı siber faaliyet gerçekleştirilen devletin, örneğin yasa gereği mahkeme kararının gerekmesi gibi iç hukuk sınırlandırmalarının, saldırıyı engellemek için gereken tedbirin alınmaması uluslararası hukuka uygun düşmedikçe, özen yükümlülüğüne uyulduğuna dair bir mazeret olamayacağı kabul edilmektedir[608]. Zira ülkesinde siber altyapı unsurları kullanılarak diğer bir devlete siber saldırı gerçekleştirilen devletin özen yükümlülüğü kapsamında saldırının önlenebilmesini, hızlı ve etkili bir şekilde, Tallinn El Kitabı Kural 6'ya uygun biçimde, sağlayacak lüzumlu yasal düzenlemeyi yapması gereklidir[609]. Uluslararası hukuka aykırı siber eylemin ülke devleti tarafından öğrenilmesine karşın kendi siber kapasitesi ortaya çıkabileceğinden veya istihbarat paylaşımı gibi hassas konular nedeniyle bilgi paylaşımda bulunmayabilirse de önleme kapsamında anılan

[603] Schmitt, 2017, *Tallinn Manual 2.0.* s. 50.

[604] Schmitt, 2017, *Tallinn Manual 2.0.* s. 42.

[605] Schmitt, 2017, *Tallinn Manual 2.0.* s. 43.

[606] Dal, 2019, s. 148.

[607] Schmitt, 2017, *Tallinn Manual 2.0.* s. 44.

[608] Schmitt, 2017, *Tallinn Manual 2.0.* s. 48-49.

[609] Schmitt, 2017, *Tallinn Manual 2.0.* s. 49.

kurala uygun tedbirlere dair uygulanacak araçlar konusunda bir takdir hakkı olduğu kabul edilmelidir[610].

Devletin uyarıda bulunabilmesi için ülkesinden kaynaklı siber saldırının varlığından haberdar olması gerekir [611] . Devletin ülkesinin siber saldırılarda kullanıldığını bilmesinden ne anlaşılacağı ise tereddüt oluşturmaktadır. Zira bu yönde bir izleme yükümlülüğü bulunduğu varsayılan devletin bildiğini kanıtlamak da kolay olmayacaktır. Bu nedenle bilgi, özen gösterme yükümlülüğü kuralının esaslı bir unsuru olarak kabul edilmektedir. Bilginin "bilmesi gerektiğinin varsayılması" (*constructive knowledge*) kavramını da içerdiği, örneğin kamu tarafından bilinen bir saldırıda bu prensibin geçerli olduğu kabul edilmektedir[612] . Buna karşın, bilmesi gerektiği varsayımının önleyici tedbirler alma yükümlülüğünü gerektirmediği, daha ziyade aynı veya benzer durumdaki makul bir devlet gibi davranması gerektiği yönündedir. Eğer olgusal koşullara göre hayatın olağan akışına uygun şekilde konumlanmış ve donanımlı bir devletin söz konusu siber altyapı unsurlarının kullanımını keşfedecek olmaması halinde bilgi kıstasının gerçekleştiği kabul edilmektedir[613].

Devletin bilmesi gerektiği varsayımı, devlete ait siber altyapı yönünden mümkün görülebilir ise de özel bir internet ağı altyapısı söz konusu olduğunda devletin özen yükümlülüğü kapsamında, varsayılan bilme kıstası uygulanamayacaktır[614]. Bu noktada devletin ülkesinde bulunan siber altyapı tesislerinin özel teşebbüse ya da kamuya ait olmasının egemenlikten kaynaklanan bu yükümlülüğün uygulanmasında etkili olamayacağı, ancak yurtdışındaki altyapı tesisleri yönünden böyle bir ayrımın yapılabileceği değerlendirilmektedir. Tallinn El Kitabı'nda, devletin kontrolü altındaki yurtdışı siber alt yapı tesisleri üzerindeki özen gösterme gerekliliğinin, özel teşebbüse ait

[610] Schmitt, 2017, *Tallinn Manual 2.0.* s. 44.

[611] Weglinski, 2016, s. 84.

[612] Schmitt, 2017, *Tallinn Manual 2.0.* s. 41.

[613] Schmitt, 2017, *Tallinn Manual 2.0.* s. 41-42.

[614] Dal, 2019, s. 148.

tesisler dışında kalan devlete ait, yurtdışında bulunan askeri yerleşimdeki ulusal görev ağını, uzay üssü veya açık denizlerdeki yurtdışı bağımsız siber alt yapı platformları ya da diplomatik mülkiyetlerdeki siber altyapı tesislerini kapsadığı kabul edilmiştir[615]. Buradaki kontrol kavramı ile yargı yetkisinin zorunlu olarak eş anlamlı olmadığı, gerçek bir kontrolün varlığının gerektiği kabul edilmektedir. Zira bir devletin yurt dışındaki özel firmaların faaliyetleri üzerinde düzenleme/kural koyucu yetkisinin söz konusu olabilmesine karşın firmaların işlettiği siber altyapı üzerinde devletin kontrol yeteneği eksikliğinin bulunabilmesi mümkündür[616].

İki devletin iş birliği halinde işlettiği siber faaliyet tesislerinde olduğu şekilde, birden fazla devletin yarışan kontrolünün söz konusu olması halinde ise, tüm devletlerin özen yükümlülüğünün bulunduğu kabul edilmektedir[617]. Başka bir devlete ait fiber optik kablosunun vasıta kılınması durumunda olduğu üzere, bir devlet ülkesinin yalnızca veri transit geçişinde kullanılması halinde özel siber alt yapının, botneti içermesi durumunda olduğu gibi, kötü niyetle kurulup kurulmadığına göre bir ayrım yapılması gerekir[618]. Böyle durumlarda ülkesi transit veri geçişinde kullanılan devletin zararı önleme veya durdurma kapasitesi ve pozisyonuna göre değerlendirme yapması uygun olacaktır[619]. Ayrıca üçüncü taraf devletinin ülkesinden hedef devlete karşı gerçekleşen siber saldırı eyleminin, ülkesi kullanılan üçüncü devlete 17. ve 18. Kural uyarınca atfedilebilmesi halinde özen gösterme yükümlülüğü söz konusu olmayacak, bunun yerine doğrudan uluslararası hukuka aykırı eylemin gerçekleştiğinden bahsedilebilecektir[620].

Bu noktada cevaplanması gereken bazı sorular karşımıza çıkmaktadır. Örneğin, “A” devletinin “B” devletine ait siber altyapı unsurlarını kullanmak suretiyle “C” devletine

---

[615] Schmitt, 2017, *Tallinn Manual 2.0.* s. 33.

[616] Schmitt, 2017, *Tallinn Manual 2.0.* s. 33.

[617] Schmitt, 2017, *Tallinn Manual 2.0.* s. 33.

[618] Schmitt, 2017, *Tallinn Manual 2.0.* s. 33.

[619] Coco ve Dias, 2021, s. 787.

[620] Schmitt, 2017, *Tallinn Manual 2.0.* s. 42.

yönelik gerçekleştirdiği bir siber saldırının, "B" devleti tarafından bilinmesi halinde önlenmesi gerekir. Ancak siber altyapının özel bir ISP tarafından hükûmete bildirilmesi yasal olarak zorunlu değilse özen yükümlülüğüne aykırılık söz konusu olacak mıdır?

Benzer bir şekilde "A" devletinin, "B" devletinin siber alt yapısını kullanarak gerçekleştirdiği siber saldırının yasaya uygunluk sebeplerinden birine girip girmediğinin, denetiminin nasıl yapılacağı ve örneğin bir meşru müdafaa durumunda "B" devleti tarafından siber saldırının önlenmesi gerekip gerekmediği sorunu üzerinde de durulmalıdır.

Örnek olarak verilen durumda, "A" devletinin faaliyetinin, siber casusluk gibi tek başına uluslararası hukukun ihlali nedeniyle sorumluluk doğuran bir eylem olmadığı takdirde "B" devletinin özen gösterme yükümlülüğü gündeme gelmeyecektir[621]. Bu bağlamda, "A" devleti ile "C" devleti arasında siber casusluk yapılmamasına ilişkin bir antlaşmanın bulunması halinde, siber alt yapı unsurlarının kullanıldığı "B" devleti sözleşmenin tarafı olmadığı için özen gösterme yükümlülüğünün bulunmadığı söylenebilir[622].

Devletlerin ülkesi kullanılarak gerçekleştirilen her türlü zararın özen yükümlülüğünü ihlal anlamına geleceği söylenemez. Örneğin, devlet dışı aktör tarafından gerçek bir bilginin, bulunulan devletin ülkesi üzerinden geçirilmesi sonucunda hedef devlette ciddi ekonomik sonuçlar doğurması halinde ülkesi kullanılan devletin özen yükümlülüğünden bahsedilemez[623].

Özen yükümlülüğü gerektiren zarar eşiği konusu uluslararası hukukta belirsizliğini korumaktadır. Uzmanlar arasında "ciddi olumsuz sonuçlar doğurma konusunda" fikir birliği bulunsa da bu sonuçların tanımlanması konusunda net bir eşik çizgisi belirlenememiştir. Bu konuda uluslararası çevre hukukunda geçerli kabul edilen

[621] Schmitt, 2017, *Tallinn Manual 2.0.* s. 35.

[622] Schmitt, 2017, *Tallinn Manual 2.0.* s. 35.

[623] Schmitt, 2017, *Tallinn Manual 2.0.* s. 36.

ilkelerden kıyas yapılarak "ciddi" kelimesi yerine "anlamlı/önemli" ya da "azımsanmayacak (miktarda/sayıda)" terimleri önerilmiştir[624]. Uluslararası Uzmanlar Grubu tarafından sadece sıkıntı verici, küçük aksamalara veya önemsiz masrafa sebep olan düzeyde hedef devletin çıkarlarını etkileyen zarar tiplerinin ve olumsuz etki doğuran her türlü devletin ülkesini kullanma eyleminin özen yükümlülüğüne sebep olmayacağı benimsenmiştir[625]. Buna göre, belirli bir sayıya ulaşmayan siteye erişim engellemelerinin ya da kritik olmayan alt yapı sistemlerinde olumsuz etki doğurmanın özen yükümlülüğünden dolayı sorumluluk doğurmayacağı söylenebilir[626].

Siber faaliyetin maddi hasar veya kişisel yaralanma doğurmasa dahi, çevrimiçi bankacılık ve medya faaliyetlerinde, kamu hizmetleri ve ticari faaliyetlerde vahim aksaklık doğuran kritik altyapı operasyonuyla ya da ekonomide önemli bir etkiyle ilgili olması ve yeterli düzeyde sürdürülmesi halinde özen yükümlülüğü bağlamında ciddi olumsuz sonuçlar söz konusu olacaktır[627].

Bir bilişim korsanı grubunun botnet vasıtasıyla birden fazla devlet ülkesi üzerinden diğer bir ülkeyi hedefleyen siber saldırı gerçekleştirmesi durumunda tek bir botnetin kullanıldığı tek bir ülke açısından özen yükümlülüğünün söz konusu olup olmayacağı konusunda Uluslararası Uzmanlar Grubunda fikir ayrılıkları oluşmuştur[628]. Azınlık görüşüne göre, saldırılar birleşik silahlı saldırı olarak değerlendirilerek dağınık her bir botnetin kümelenmesiyle gereken ciddiyet eşiği aşıldığından her devletin özen yükümlülüğünü üstlenmesi gerekmektedir. Çoğunluk görüşüne göre ise, özen gösterme yükümlülüğü devletin ülkesel egemen ayrıcalıklarından kaynaklandığından kümelenme uygun görülmemekte, botnetin işletildiği diğer devlet ülkesinden kaynaklanan

[624] Schmitt, 2017, *Tallinn Manual 2.0.* s. 37.

[625] Schmitt, 2017, *Tallinn Manual 2.0.* s. 37.

[626] Coco ve Dias, 2021, s. 786.

[627] Schmitt, 2017, *Tallinn Manual 2.0.* s. 37-38.

[628] Schmitt, 2017, *Tallinn Manual 2.0.* s. 38.

uluslararası hukuka aykırı eylemden dolayı daha ağır bir sonuçtan ülke devletinin sorumluluğu kabul edilmemektedir.

Özen gösterme yükümlülüğünün ihlali durumunda devletlerin başvurabilecekleri karşı önlemler, uluslararası hukuk sisteminde *self-help* paradigmasının önemli bir boyutunu oluşturmaktadır[629]. Bununla birlikte, bir devlet aleyhine siber özen yükümlülüğünü ihlal eden başka bir devlete karşı gerekli önlemleri almayan bu devlet ülkesinde bulunan özel hukuk kişilerinin karşı siber saldırı gerçekleştirmesi halinde tarafların hukuki durumunu belirlemek kolay değildir.

Tallinn El Kitabı'nda belirtilen ve özen gösterme yükümlülüğüne ilişkin bir örnek olayda özel hukuk kişisine karşı gerçekleştirilen bir siber saldırı nedeniyle egemenliği ihlal edilen ülke devletinin sorumluluğu üzerinde durulmaktadır[630]. Bu örnek olay, bir devlet ülkesinde bulunan özel hukuk kişisine karşı gerçekleştirilen bir siber saldırıya, ülkesinde bulunulan devletin çeşitli sebeplerle cevap vermemesi nedeniyle, saldırı altındaki özel hukuk kişisinin uluslararası hukuka göre karşı önlem alma yetkisi bulunmadığı halde savunma saldırısı gerçekleştirmesine ilişkindir. Zira bu durumda karşı saldırıdan zarar gören diğer bir devlet, uluslararası hukuka göre özel hukuk kişisinin karşı önleme başvurma yetkisi bulunmadığı ve ülke devletinin de özen yükümlülüğü kapsamında saldırının durdurulması için gerekli önlemleri alması gerektiğinden bahisle karşı bir siber saldırı gerçekleştirmesi söz konusu olmaktadır.

Böylesi bir durumda ülke devletinin özen gösterme yükümlülüğü uyarınca özel hukuk kişisinin savunma saldırısını durdurması beklenemez. Her ne kadar özel hukuk kişisinin bir devlete yönelik karşı saldırı gerçekleştirme hakkı bulunmamakta ise de ilk saldırıyı gerçekleştiren devletin eylemi uluslararası hukuka aykırı eylem niteliğinde olduğundan, özel hukuk kişisinin bulunduğu ülke devletinin eylemsizliği hukuka uygun olmaktadır. Bir diğer ifadeyle, ilk saldırıyı gerçekleştiren devlet kendi uluslararası hukuka aykırı

[629] Jensen ve Watts, 2017, s. 1568.

[630] Schmitt, 2017, *Tallinn Manual 2.0.* s. 39-40.

eyleminden yararlanamayacağından özel hukuk kişisinin bulunduğu ülke devletinin özen yükümlülüğünün ihlalini gerekçe gösteremez.

2.4. HUKUKA UYGUNLUK SEBEPLERİ

2.4.1. Genel Olarak

Ortada bir uluslararası hukuk kişisinin sorumluluğunu gerektiren hukuka aykırı bir fiil ya da sorumluluk gerektiren faaliyet söz konusu olmasına rağmen sorumluluğun ortadan kalkmasına sebep olan durumlar söz konusu olabilmektedir. Bu durumlarla ilgili olarak Tallinn El Kitabı Kural 19'da hukuka uygunluk sebepleri düzenlenmiştir. Bu kurala göre siber operasyonlarla ilgili fiilin hukuka aykırılığı rıza, meşru müdafaa, karşı önlem, zorlayıcı neden (mücbir sebep), zaruret hali ve tehlike hali durumları söz konusu olduğunda ortadan kalkmaktadır. Bununla birlikte, söz konusu hukuka uygunluk sebeplerinden dolayı sorumluluğun ortadan kalkabilmesi için fiilin uluslararası hukukun emredici kurallarından birisini ihlal etmemesi gerekmektedir[631].

Hukuka uygunluk sebeplerinin en yaygın olanlarından meşru müdafaa ve karşı önlemlerin, kuvvet kullanma hakkı ile doğrudan ilişkisi gözetilerek bunların kuvvet kullanmanın incelendiği üçüncü bölümde daha ayrıntılı şekilde ortaya konulması uygun görülmüştür. Yine zaruret halinin siber operasyonlarda daha özel bir yer tutması nedeniyle ayrı bir alt başlık altında incelenmesi ve diğer hukuka uygunluk sebeplerinin ise genel hatlarının çizilmesi uygun görülmektedir.

2.4.2. Bazı Hukuka Uygunluk Sebepleri

Hukuka uygunluk sebeplerinin başında yer alan rıza bir fiilden zarar görenin bu zararı kabul etmesi manasına gelmektedir[632]. Devlet görevlisinin rıza beyanının geçerli

[631] Uzun, 2007, s. 47.

[632] Pazarcı, 2021, s. 456.

olabilmesi için ise bu görevlinin görevleri nedeniyle özel yetki gerekmeyen biri ya da yetkili kılınan biri olması ve bu beyanın serbest iradeye dayanması bir diğer ifade ile zorlama sonucu oluşmaması gereklidir[633]. Ayrıca şekli anlamda geçerli olsa da razı olunan durumun *jus cogens* niteliğindeki bir kurala aykırılık teşkil etmesi halinde hukuka uygunluk sebebi oluşturmamaktadır[634].

Hukuka uygunluk sebeplerinden bir diğeri olan zorlayıcı neden, öngörülemeyen ya da karşı konulamayan ve zarara neden olan kişinin iradesi dışındaki bir olayı belirtmektedir[635]. Zorlayıcı neden, deprem ve sel felaketi şeklinde doğal olaylar olabileceği gibi, herhangi bir malın ithalatının yasaklanması ve bu sebeple sözleşmenin ifa edilememesi anlamında bir hukuki olay da olabilir[636]. Tüm önlemlerin alınmasına rağmen meydana gelen kazalardan sorumlu tutulmamak amacıyla zorlayıcı neden ileri sürülebilecek ise de bazı tehlikeli faaliyetler bakımından zorlayıcı nedenlerin dahi hukuka uygunluk hali oluşturmadığı kabul edilmektedir[637]. Bu hukuka uygunluk sebebinin zaruret halinden ve tehlike halinden farkını ise istemeyerek dahi olsa diğer bir seçeneğe başvurma imkânının bulunmaması oluşturmaktadır[638].

Tehlike hali ise, başka şekilde davranılması halinde eylemi gerçekleştiren kişinin ya da bu kişinin sorumluluğu altında bulunanların hayatlarının tehlikede olmasını ifade etmektedir[639]. Taslak Çalışma'nın 24. maddesinde düzenlenen tehlike hali, belirtilen kişilerin hayatlarının kurtarılması için daha uygun bir yolun bulunmaması durumunda

[633] Uzun, 2007, s. 49.

[634] Bozkurt ve Erdal ve Poyraz, 2017, s. 324.

[635] Pazarcı, 2021, s. 457.

[636] Aksar, 2021, (2. Kitap), s. 305.

[637] Bozkurt ve Erdal ve Poyraz, 2017, s. 326.

[638] International Law Commission, 2001, Art. 23, s. 76.

[639] Uzun, 2007, s. 54.

ortaya çıkmaktadır[640]. Tehlike hali ile zaruret hali arasındaki temel farklılık, tehlike halinde insan hayatının kurtarılmasının amaç edinilmesinden kaynaklanmaktadır[641].

2.4.3. Zaruret Hali

Meşru müdafaa konusunda bahsedilen gereklilik hususundan faklı olarak zaruret hali (*plea of necessity*) hukuka aykırılığı kaldıran durumlara ilişkindir[642]. Zaruret hali, koşulların bir hukuk kişisinin yükümlülüklerini yerine getirmesini çok ağır ya da olanaksız kıldığı durum olarak tanımlanmaktadır[643]. Ayrıca zaruret hali, sadece devletlerin temel çıkarlarına ağır ve yakın bir tehlikenin varlığı halinde söz konusudur[644].

Taslak Çalışma'nın 25. maddesinde düzenlenen bu hukuka uygunluk sebebine dayanılabilmesi için uluslararası yükümlülüğe aykırı olan bir fiilin ilk olarak devlet için esaslı bir menfaati pek yakın ve ağır bir tehlikeye karşı korumak için başvurulacak yegâne imkân olması gereklidir. İkinci olarak yükümlülük altında bulunulan devletin ya da devletlerin veyahut milletlerarası toplumun bütününün esaslı bir menfaatine ağır bir şekilde zarar getirmemelidir. Bu koşulların bulunması halinde dahi uluslararası yükümlülüğün zaruret haline başvuru olanağını engellememesi ve zaruret halini ileri süren devletin bunda katkısının bulunmaması gerekir[645].

---

[640] International Law Commission, 2001, Art. 24, s. 78.

[641] Aksar, 2021, (2. Kitap), s. 305.

[642] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 251.

[643] Pazarcı, 2021, s. 458.

[644] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 251.

[645] Taslak Çalışma'nın 25. Maddesinin Türkçe metni için bkz.; Erkiner, 2008, s. 195.; Aksar, 2021, (2. Kitap), s. 306.

Bir devletin temel çıkarlarına ağır ve yakın bir tehlikenin varlığı söz konusu olduğunda ve bu devletin uluslararası yükümlülüklerini yerine getirmesinin çok ağır durumlara sebep olması ya da bunun olanaksız olması halinde, devletin yükümlülüklerine aykırı bu fiillerin hukuka uygun kabul edilmektedir. Bununla birlikte diğer hukuka uygunluk sebeplerinden farklı olarak zaruret halinde tazminat yükümlülüğünün ortadan kalkmamaktadır[646]. Zaruret halinin siber uzaya nasıl uygulanacağı konusu ise, devletin neredeyse bütün kritik altyapı tesislerinin siber uzaya bağlantısı bulunduğundan ayrı bir öneme sahiptir.

Kritik altyapı tesislerine yönelen bir tehlikenin silahlı saldırı düzeyine erişmesi halinde meşru müdafaa hakkı evleviyetle doğacaktır. Buna karşın, saldırıyı gerçekleştiren devletin belirlenememesi halinde meşru müdafaa hakkı kapsamında kuvvet kullanma olanağının bulunmaması söz konusudur. Bu halde, diğer devletlere veya uluslararası topluma karşı sahip olduğu yükümlülüklerin aksine devlet bazı tedbirler alabilir. Bu tedbirlerin hukuka uygun hale gelmesi için ise, diğer hukuka uygunluk sebeplerinin ya da yukarıda belirtilen temel çıkarlara yönelik ağır ve yakın bir tehlikenin varlığı ve uluslararası yükümlülüklerin yerine getirilmesinin çok ağır durumlara sebep olması ya da bunun olanaksız olması koşulları karşılanmalıdır.

Bir devletin temel çıkarlarının bulunduğu şüphesiz olan kritik altyapı tesislerine yönelen yakın bir tehlikenin varlığı halinde bazı durumlarda devletin uluslararası yükümlülüklerini ihlal etmeden bu tehlikeyi bertaraf etmesi söz konusu olmayabilir. Zira bu tehlikeyi bertaraf etmek için başvurulacak yöntem uluslararası yükümlülüklerin ihlalini oluştursa dahi başka bir seçeneğin bulunmaması durumunda ve yükümlülüğün yerine getirilmesinin, bir diğer ifade ile devletin saldırıyı kabullenmesinin devlet için çok ağır sonuçlara sebep olması ya da olanaksız olması halinde hukuka aykırılıktan bahsedilemeyecektir.

[646] Bozkurt ve Erdal ve Poyraz, 2017, s. 327.

Kritik altyapı tesisleri örneğinden gidildiğinde bir devletin siber altyapının "kritik altyapı" olduğuna dair resmi tanımlanması zaruret haline esas kabul edilmesi için yeterli görülmemektedir [647] . Zaruret hali bulunduğundan bahisle diğer devletlere ya da uluslararası topluma olan yükümlülükleri ihlal eden fiilleri gerçekleştiren devletin kendi diğer altyapı tesisleri tanımı ile zaruret haline dayanılarak gerçekleştirilen fiilden zarar gören devletin tanımının çelişmesi halinde uluslararası yargı mercilerinden danışma görüşü alınması ve buna göre değerlendirme yapılması uygun olacaktır.

Kuvvet kullanma eşiğine varmayan siber saldırılara cevaben kinetik saldırılar zaruret hali kapsamında elverişli bir çare olarak kabul edilmemekle birlikte karşı siber saldırıların zaruret hali kapsamında faydalı bir hukuki argüman olarak başvurulabileceği savunulmaktadır[648]. Bu savın gerekçesinde, ABD'nin balistik füze savunma sistemini etkisiz hale getiren ve Kuzey Kore'den kaynaklanan siber saldırıların önlenmesi amacıyla yapılacak bir karşı saldırının Kuzey Kore'nin kritik altyapı sistemlerine vereceği hasar ile ABD'nin olası bir saldırı halinde karşılaşabileceği tehlike bağlamında her iki ülkenin menfaatler dengesinin gözetilmesi bulunmaktadır.

Siber operasyonlar açısından zaruret hali Tallinn El Kitabı'nda bağlamsal veya içeriksel olarak değerlendirilmekte olup, örneğin bir sağlık sisteminin işleyişini sağlayan bir siber altyapıya yönelen siber saldırı söz konusu olduğunda, şayet sağlık hizmetinin devamını sağlayacak yeterli boşta kalan yedek sistemleri var ise karşı saldırı için zaruret halinin bulunmadığı kabul edilmektedir[649]. Bu haliyle saldırıya uğrayan bir sistemin sırf kritik altyapı tesisi olarak nitelendirilmesi tek başına bu tesislerin zaruret unsuru açısından devletin temel çıkarlarının tehlikeye girmesi unsurunu karşılamamaktadır.

---

[647] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 252.

[648] Rienks, Captain Katharina J. (2020). The Plea of Necessity and Cyber Warfare, Army Lawyer, Issue:5, s. 79.

[649] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 252.

Son olarak belirtilmelidir ki gelecekteki olası bir saldırının önlenmesine yönelik önleyici (*pre-emptive self defence*) meşru müdafaa ve devletin bekasının korunmasına yönelik kendini koruma (*self preservation*) durumlarının karışımından oluşan *Caroline* olayının UAD'nın kabulünden farklı olarak zaruret hali ilkesine örnek olmadığı kabul edilmektedir[650]. Ayrıca öğretide 1967 *Torry Canyon* olayında olduğu üzere sırf kendini koruma hali dışında da zaruret halinin söz konusu olabileceği ifade edilmektedir[651].

[650] Rienks, 2020, s. 79.

[651] Rienks, 2020, s. 79.

3. BÖLÜM: KUVVET KULLANMA YASAĞI VE JUS AD BELLUM PARADİGMASINDA SİBER SAVAŞ

BM Şartı'nın amaç ve ilkeler kısmında belirtildiği üzere bu Şart ile amaçlananın barışı sağlamak olduğu, devletlerarası uyuşmazlıkların barışçıl yollarla çözülmesi ve egemen devletlerin içişlerine karışmamasının gerektiği, ayrıca kuvvet kullanımının yasaklandığı görülmektedir. Anılan metinde asıl amaç; barışın ve güvenliğin sağlanması olsa da devam eden maddelerde kuvvet kullanımına başvurulacak durumlar da öngörülmüştür. Bunların dışında, devletlerarasında bir şekilde başlayan silahlı çatışmaların belirli kurallara bağlanması Lahey ve Cenevre Konvansiyonları ile düzenlenmiştir. Buna göre, devletlerarası ilişkilerde kuvvet kullanımı ya da silahlı çatışma öncesi ve sonrasında farklı hukuk kurallarının uygulanması söz konusu olmaktadır.

Uluslararası hukukta kuvvet kullanımının ve silahlı bir saldırıyı neyin oluşturduğunun analiziyle ilgili üç kategori söz konusudur. Bunlar; uluslararası hukukta barış rejimi, çatışma yönetimi hukuku (*jus ad bellum*) ve silahlı çatışmalar hukukudur (*jus in bello*)[652]. Bir diğer ifadeyle savaş hukuku, *jus ad bellum* ve *jus in bello* kurallarından oluşmakta; ilki, kuvvete başvurulmasını sınırlayan ve düzenleyen esasları belirlemekte iken ikincisi, silahlı çatışmalar esnasında uyulacak kurallar bütününü teşkil etmektedir[653].

Bu bağlamda siber operasyonların kuvvet kullanma yasağı merkezinde incelenmesi ve geleneksel silahlı çatışmaların parçasını oluşturup oluşturmamasına göre nitelendirilmesi uygun olacaktır. Zira siber operasyonların kuvvet kullanma düzeyine ulaşmamakla birlikte uluslararası hukuka aykırı bir eylem oluşturması halinde devletin sorumluluğu gündeme gelebilecektir. Bu operasyonların kuvvet kullanma düzeyine erişmesi halinde, kuvvet kullanma yasağı kapsamında *jus ad bellum* gereğince devletlerin karşı önlemler ve zorlama araçları gibi uluslararası hukuka uygun yaptırımlara başvurabileceği gibi, diğer hukuki yollara başvurması da mümkündür. Bir siber operasyonun silahlı çatışma

[652] Sharp, 1999, s. 6-7.

[653] Sur, 2022, s. 296.

düzeyine varması halinde ise, meşru müdafaa hakkı doğacak ve silahlı çatışmalar hukuku hükümleri uygulanacaktır.

Bu doğrultuda tezin konusunu oluşturan siber savaş yönünden merkezi bir konumda bulunan uluslararası hukukta kuvvet kullanımı konusu, tarihsel ve hukuki yönleriyle ortaya konulacak ve kuvvet kullanma yasağı ile kuvvet kullanımı düzeyine erişen siber operasyonların silahlı saldırı düzeyine varması halinde ortaya çıkan meşru müdafaa hakkı ele alınacaktır. Bu bölümde ayrıca siber saldırıların genellikle hedefini oluşturabilecek kritik altyapı tesislerinin tanımlanması ve kapsamının belirlenmesi, meşru müdafaa hakkı bakımından gerekli görülmüştür.

3.1. ULUSLARARASI HUKUKTA KUVVET KULLANIMI

Tarihsel süreç içerisinde devletlerarası uyuşmazlıkların çözüm aracı olarak başvurulan kuvvet kullanımı farklı dönemlerde farklı biçimde uygulanmıştır. Kuvvet kullanmanın kesin olarak yasaklandığı BM Şartı, bu konuda kritik bir yol ayrımı oluşturmuştur. BM öncesi dönemde savaşa başvurma konusunda moral değerler açısından bir sınırlandırma olabilse de bu döneme ait hukuk öğretisinde devletlerin istediği zaman savaş yoluna başvurabilme hakkı olduğu kabul edilmiştir[654]. Geleneksel savaş teorisi haklı savaş kavramıyla şekillenmiş, güç kullanımına başvurulmasının haklı olabilmesi için bazı unsurların gerçekleşmesi gerekli görülmüştür. Genel olarak ifade edilirse bu unsurlar; savaşın haklı sebebe dayanması, devletin savaşma niyetinin haklı bir sebebe yönelik olması, savaşın uygun otorite tarafından gerek kendi kamuoyuna ve gerekse de karşı tarafa duyurulması, barışçıl görüşmeler tüketildikten sonra savaşa son çare olarak başvurulması, savaşmakta başarı olasılığının bulunması ve son olarak orantılılığın gözetilmesidir[655]. Savaşın nedenlerine göre savaşı haklı kılan sebepler ise; kendini

[654] Ayrıntılı bilgi için bkz.; Arend, Anthony Clark / Beck, Robert J. (1993). *International Law the use of Force.* London New York: Routledge, s. 17.

[655] Orend, Briand. (September 2000). *Michael Walzer on Resorting to Force*, Canadian Journal of Political Science, Cilt:33 (3). s. 526.

savunmak, mallarını korumak, sözleşmeyle ya da başka sebeplerle borçlu olunan ama haksız olarak yerine getirilmeyen şeyi elde etmeye çalışmak, şayet onarımda bulunulmamışsa, yapılan kötülükleri veya haksızlıkları cezalandırmak[656] olarak kabul edilmiştir.

Egemenliğin bir uzantısı olarak görülen savaş ilan etme hakkı *just war,* bir diğer ifade ile savaşın haklı sebepten kaynaklanması halinde devletlerin doğal bir hakkı olarak kabul edilmekteydi[657]. Kuvvet kullanma yoluna başvurmanın hak olarak kabul edildiği dönemlerden büyük yıkımların yaşandığı 20. yüzyılda devletlerin herhangi bir bahaneyle kuvvet kullanımına başvurma yoluyla dünya barışını tehdit etmesi önlenmek istenmiş ve kuvvet kullanmanın yasaklanması süreci yaşanmıştır. I. Dünya Savaşının sona ermesiyle yeni bir bilinç yerleşmiş, artık savaşın sadece savaşan taraflar arasındaki ilişkiyi ilgilendirmeyip uluslararası toplumun tümünün savaştan etkilendiği görülmüş ve bir devletin savaşa başvurmasının "hak" olmadığı kabul edilmiştir[658]. Bu sürecin incelenmesine geçmeden önce uluslararası hukukun iç hukuktan farklı olarak yaptırım uygulayan bir üst otoriteye sahip olmamasından kaynaklı olarak devletlerin kendi haklarını kendilerinin koruması anlamına gelen *self-help* rejimi açıklanacak ve sonrasında kuvvet kullanma yasağı incelenecektir.

3.1.1. Uluslararası Hukukta *Self-Help* Rejimi

17. yüzyıldan itibaren hukukun kaynağı olarak, olması gerekene değil olana, yani devletlerin uygulamasına dayanan yaklaşımın ortaya çıkmasıyla, artık gerek görüldüğünde savaşa başvurmak devletlerin egemenlik hakkının bir parçası olarak kabul edilmiştir[659]. BM dönemi öncesinde savaş ilanı, egemenliğin bir sonucu olarak

---

[656] Mutlu, Erdem İlker. (2016). *Savaşın ve Barışın Hukuku.* Ankara: Turhan Kitabevi, s. 80-81.

[657] Aksar, 2021, (2. Kitap), s. 130.; Ünal, 2005, s, 313.

[658] Sur, 2022, s. 297.

[659] Keskin, Funda. (1998). *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve BM.* Ankara: Mülkiyeliler Birliği Vakfı Yayınları, s. 23.

görülmekle birlikte daha yüksek bir hukuk kuralı ya da otoritenin bulunmaması nedeniyle *self-help* rejimi de yasal kabul edilmekteydi[660]. Milletler Cemiyeti (MC) Misakı'nda savaş yoluna başvurmak hiçbir durumda yasaklanmamış, *self-help* ise üyeler arası ilişkilerde tam olarak dışlanmamıştır[661]. *Self-help* rejimi, bu haliyle egemen eşitlerin üzerinde bir otoritenin yaptırım uygulama olanağı bulunmayan uluslararası hukukta, devletlerin kendi haklarını korumasına imkân sağlayan bir çare olarak ifade edilebilir.

Bir hukuk sistemini töre ve ahlak kurallarından ayıran en önemli unsur olan yaptırım konusunda iç hukuk ile uluslararası hukuk arasında önemli farklılıklar bulunmaktadır. Uluslararası alanda hukuk kurallarına uyulmasını sağlayacak devletlerin üstünde bir siyasi organın tam olarak oluşturulamamasından dolayı bu gereklilik günümüzde kısmen egemen devletler ve kısmen BM Güvenlik Konseyi tarafından yerine getirilmektedir. Bu alanda kendini gösteren kurumsal eksiklik nedeniyle devletlerin kendi haklarını istisnai durumlar dışında ilke olarak kuvvet kullanmamak kaydıyla kendilerinin koruması, bir diğer ifade ile *self-help* rejiminin işletilmesi suretiyle yerine getirilmektedir. Örneğin, Türkiye'nin Körfez Savaşı'ndan sonra 1991 Eylül'ünden başlayarak Irak'ın kuzeyindeki otorite boşluğu ya da Irak'ın bu bölgede etkili olamaması nedeniyle Irak'tan özel bir izin almadan, kendi güvenliğini savunma ilkesine dayanarak Irak'ta izleme operasyonları gerçekleştirmesi[662] bu kapsamda değerlendirilmektedir.

Kelsen'e göre *self-help* rejimi, gerçekleşmekte olan bir saldırının mağduru olmayan bir süje tarafından mağdurun saldırgana yönelik gerçekleştirdiği tepki hareketine yardım amaçlı gerçekleştirilen ve hukuk düzeni tarafından yetkilendirilen bir durumda söz konusu olmaktadır. Hukuki düzenin yaptırımın ifasını özel bir organa tanıdığı durumlarda *self-help* geçerli kabul edilmemektedir[663]. S*elf-help* rejiminin sebebi ve kapsamı

[660] Ayrıntılı bilgi için bkz.; Arend ve Beck, 1993, s. 17.

[661] Kelsen, 2012 s. 39.

[662] Pazarcı, 2021, s. 169.

[663] Kelsen, 2012 s. 15.

konusunda benzer bir görüşe göre[664], bu paradigma, uluslararası hukukta merkezi bir siyasi otoritenin bulunmamasından kaynaklanmakta ve bunun kapsamına meşru müdafaa, misilleme, zararla karşılık, tanımama, diplomatik ilişkilerin kesilmesi, abluka, sözleşmelerin sona erdirilmesi gibi önlemler dâhil edilmektedir.

Uluslararası hukukun kaynaklarından birinin de yerleşik uygulamalar olması nedeniyle devletler tarafından *self-help* rejimine göre, kuvvet kullanma yasağı ana ilkesi veya *jus cogens* [665] kuralları kapsamında, kendi haklarını koruma faaliyeti, uygulamadan kaynaklanan bir zorunluluk halini almaktadır. Kelsen, genel uluslararası hukukun merkezi olmayan ve gelişmekte olan yapısı nedeniyle yasa, yürütme ve yargısal organlarının kurulmaması ve bu işlevi meşru uluslararası toplum üyeleri olarak ilgili uluslararası hukuk kişisine bırakmasından dolayı *self-helf* rejimi açısından hukuku ilgili devletlerin kendi elinde tuttuğunu ifade etmiştir[666].

Bu sebeplerden dolayı öğretide, BM sonrası uluslararası hukuk düzeninde yaptırım konusunda istenilen başarının elde edilememesi ve ortak müdahalenin yetersizliğinden dolayı kuvvet kullanma yasağına uyulmadığı ve devletlerin kendi önlemlerini aldıkları ifade edilmektedir [667] . Daha önce de açıklandığı üzere kuvvet kullanma yasağının devletler tarafından bazı bahanelerin arkasına sığınılarak esnetildiği, kuvvet kullanmanın bir yolunun bulunduğu görülmektedir[668]. Zararla karşılık önlemi de bunlardan biri olup, bu önlemin genel olarak kuvvet kullanma yasağına aykırı olması nedeniyle silahlı zararla karşılık önlemi uluslararası hukuka aykırılık teşkil etmektedir[669]. Öğretinin bu konudaki

---

[664] Bkz.; Keskin, 1998, s. 89.

[665] Jus Cogens, ihlal edilmesine izin verilmeyen, uluslararası toplum tarafından uluslararası hukuk düzeninin sürdürülmesi için temel olarak kabul edilen buyruk kurallar bütünüdür. Hukuk sözlüğü için bkz. https://legal-dictionary.thefreedictionary.com/Jus+Cogens Erişim: 05.05.2018

[666] Kelsen, 2012 s. 22-23.

[667] Keskin, 1998, s. 90.

[668] Bkz.; Aksar, 2021, (2. Kitap), s. 132.

[669] Pazarcı, 2021, s. 553.

eğilimine bakıldığında, genel olarak güç kullanımını içeren zararla karşılık eyleminin BM Şartı gereğince yasaklandığı konusunda fikir birliği bulunmaktadır[670].

Bahse konu sistemin daha iyi anlaşılabilmesi için iç hukuk uygulamalarına bakıldığında, ulusal hukuklarda hukuka uygunluk halleri haricinde kişilerin hakkını bizzat almaları, bir diğer ifadeyle ihkak-ı hakkın yasaklandığı görülmektedir. Bunun en önemli sebebi ise, her bireyin kendi hakkını bizzat almaya çalışmasının yaratacağı çatışmaların şiddetin daha da artmasına sebep olmasıdır. Bu nedenle iç hukuklarda hakkın zorla elde edilmesi hakkı bazı istisnalar dışında bir üst yasal organa devredilmiştir.

Bu bağlamda, uluslararası kurumsal yapıdaki eksikliğin sonucu olarak ortaya çıkan bu sistemin uygulamada bazı sorunlara sebep olması beklenebilir bir durumdur ki öğretide II. Dünya Savaşı'nın çıkmasına *self-help* rejiminin sebep olduğu savunulmuştur. Zira pek çok devlet adamının, yıkımın bir devletin saldırgan tutumundan kaynaklanmadığını, daha ziyade birtakım yanlış hesaplama ve yorumlamanın sonucu olarak savaşa başvuru konusunda prosedürel sınırlandırma eksikliğinin durumu daha da kötüleştirdiğini düşündükleri, bu inancın sonucu olarak BM Şart'ında kuvvet kullanımını sınırlandırmaya yönelik düzenlemeler yapıldığı ileri sürülmüştür[671]. Bu görüş aynı zamanda meşru müdafaa dışında kuvvet kullanımının meşru kabul edilmesi halinde varılabilecek sonuçları göstermesi açısından önemlidir.

3.1.2. Uluslararası Hukukta Yaptırım Sorunu ve Eleştirel Görüşler

İç hukuktan farklı olarak eşitler arası ilişkileri düzenleyen hukuk kurallarını uygulayacak bir üst siyasi otoritenin ve ayrı bir yaptırım sisteminin bulunmaması uluslararası hukuka yönelik en önde gelen eleştiri sebeplerini oluşturmaktadır[672]. Öğretide ileri sürülen; uluslararası hukukta tüm devletlerin uyması gereken hukuk kurallarının bulunmayıp daha

[670] Arend ve Beck, 1993, s. 42.

[671] Arend ve Beck, 1993, s. 19.

[672] Ayrıntılı bilgi için bkz.; Bozkurt ve Erdal ve Poyraz, 2017, s. 22-23.; Sur, 2022, s. 8-9.

çok ikili antlaşmalar, ekonomik birlikler ve askeri paktlar mevcut olsa da eşitliğe dayalı bir uluslararası hukuk sisteminin bulunmaması nedeniyle uluslararası hukukun çıkar ve güç dengelerine göre oluşan bir eşitsizlik hukuku olduğu ifadesi eleştirel bir hukuk felsefesi yaklaşımıdır[673]. Uluslararası hukukun en önemli köşe taşını oluşturan bu konudan kaynaklı eleştirilerin genel olarak incelenmesi uygun olacaktır. Siyasi bir üst otorite ve yaptırım sorunu bulunan uluslararası ilişkiler sisteminin bir güç düzenini mi, yoksa bir hukuk düzenini mi oluşturduğu konusunda farklı görüşler ortaya atılmaktadır.

Bu noktada öncelikle uluslararası hukuk düzenine ilişkin farklı bakış açıları ortaya konulacak ve sonrasında yaptırım sorununu incelenecektir. Egemen eşitlik paradigmasının bir mit olarak kabul edilir hale gelmesi ve değişen dünyada güç dengelerine göre yeni bir paradigmanın ortaya çıkmasıyla oluşan devletlerarası ilişkilerde realist görüş uzun süre genel kabul görmüş, daha sonra gücün hukukuna karşı ortaya çıkan tepkiler ve bazı toplumsal hareketlerin de etkisiyle idealist bir akım ortaya çıkmıştır. Her iki akıma yönelik eleştirel bir yaklaşım geliştiren bir diğer görüş ise eleştirel hukuk yaklaşımıdır.

Nasıl olması gerektiğine yönelen idealist görüşe göre, dünyada barışın tesisi ancak liberalizm ve demokrasinin yaygınlaştırılmasıyla sağlanabilecektir[674]. Liberal batı dünyasının bakış açısını yansıtan bu görüşe göre; "*Westphalia dünya düzeni egemenlik anlayışının devletlerin iç ilişkilerine karışılmaması ilkesine dayanmasına karşın Westphalia sonrası yeni liberal dünya düzeninin insan haklarını koruduğu sürece sorumlu şekilde egemenlik anlayışını benimsediği ve liberal demokrasi temelinde bir dünya düzeni için barışçıl operasyonların gerekliliği"*[675] benimsenmektedir. İdealist görüşün insancıl hukukun gelişmesine katkısı bu noktada kendisini göstermektedir.

---

[673] Ökçesiz, Hayrettin. (1997). *Çağdaş Hukuk Felsefesi ve Hukuk Kuramı İncelemeleri.* İstanbul: Alkım, s. 100.

[674] Lawson, Stephanie. (2012). "*International Relation".* Cambridge / Malden: Polity Press, s. 39-41.

[675] Bellamy, Alex J. / Williams, Paul D. (2010). *Understanding Peacekeeping. Cambridge / Malden:* Polity Press, s. 13.

Eleştirel görüşleri iki başlık halinde sınıflandıran ve meseleye meta-biçim teorisi[676] kapsamında ekonomi politik yaklaşım üzerinden bakan görüş ise bunları, kaynağını Amerikan Realizmi akımlarına özgü pragmatizminde bulan Eleştirel Hukuk Çalışmaları Ekolüne dayanan[677] eleştirel görüş veya bir diğer ifadeyle iyileştirici yaklaşım ve ikinci olarak kaynağını devletlerarası ilişkiden alan[678] ekonomi politik yaklaşım olarak ifade etmektedir. Bu farklı görüşlerde dikkati çeken ayrım, ilkinin sonuç odaklı bir çözümü hedeflerken, ikincisinde üst yapı olarak kabul edilen hukuk düzeninin temelini oluşturan altyapının gözden kaçırılmamasına yönelik bir çabayı ifade etmekte olmasıdır.

Buna göre iyileştirici yaklaşım;

> *"...öncelikle, dünya sisteminin ürettiği toplumsal etkilerin kural olarak istenilebilir, katlanılabilir ya da kaçınılmaz olduğunu ön varsayar. Diğer yandan, yine bu yaklaşıma göre, savaş, açlık, göç gibi toplumsal felaketler bu sistemin ürettiği patolojilerdir. Sistemin ürettiği patolojilerle yine sistemin sağladığı imkânlarla mücadele etmek mümkündür. Eleştirel düşüncenin süzgecinden geçirilmiş hukuk kuralları, anılan imkânlar seti içerisinde ayrıcalıklı yeri haizdir. Böylelikle, iyileştirici yaklaşımın penceresinden uluslararası hukuk, patolojilerin giderilmesi için esaslı bir araç haline gelir. Burada, hukukun biçimi, içeriğinden*

---

[676] Meta kavramı, kapitalist bir ekonomide üretilen tüm mal ve hizmetleri kapsar. Bir ürünün meta halini alması, diğer bir ifade ile metalaşması ise meta-biçimi teorisi kapsamında değerlendirilmektedir. Meta-biçimi teorisi ya da meta-form kuramı, Evgeny Pasukanis, Isaac D. Balbus ve China Mieville gibi teorisyenler tarafından geliştirilmiş ve bu teoriye göre hukuk, kapitalizm için kölelik etmektir. Ayrıntılı bilgi için bkz.; Chandler, William M.A. (2017). *Evgeny Pasukanis: Hukukun Meta-Form Kuramı* (Çev. Furkan Yılmaz). Hukuk Kritik. Erişim: 05.11.2022 https://www.hukukkritik.com/projects/evgeny-pasukanis%3A-hukukun-meta-form-kuram%C4%B1; Sarıca, Şermin. (2008). *Farklı Refah Devleti Modellerinde Sosyal Harcamaların Niteliği: Emekgücünün Meta Niteliği Açısından Bir Değerlendirme*. Doktora Tezi, İstanbul, İstanbul Üniversitesi.

[677] Bkz.; Çelebi, Hakan / Özdemir, Ali Murat. (Bahar 2010). "Uluslararası Hukukta Eleştirel Yaklaşımlar", Uluslararası İlişkiler, Cilt:7, Sayı:25, s. 71-72.

[678] Bkz.; Çelebi ve Özdemir, 2010, s. 80.

> *(hukuk kavramlarının içinde anlamını bulduğu ilişkiler, bu kavramların içerdiği emirlerden) soyutlanmış halde ele alınır."*[679]

İyileştirici görüşte asıl olan şey, mevcut güç düzeninin meşrulaştırılmasında bu görüşün bir araç görevi görmesidir. Ekonomi politik yaklaşıma göre ise önemli olan husus, uluslararası hukukun kaynağının ne doğal hukuktan ne de devlet iradesinden kaynaklanmıyor olması nedeniyle çatışmanın maddi temeline inme gerekliliğidir[680].

Uluslararası hukuk alanında pozitivizm ve doğal hukuk teorisi ya da realizm ile egemenlik arasındaki tercih konusunda gösterilmesi gereken dengenin önemi öğretide şu şekilde ifade edilmektedir:

> *"bir uluslararası hukuk politikası saptarken doğal hukuku pozitivizme ya da dünya düzenini egemenliğe tercih ederseniz bu durumda, doğal bir ahlakiliği ön varsaymak durumunda kalıp, uluslararası hukukun normatif içeriğini anlaşılmaz hale getirmek sorunu ile yüz yüze gelebilirsiniz. Diğer yandan, pozitivizmi öne çıkardığınızda da, egemen davranışın eleştirel bir yorumundan mahrum kalıp, her türlü egemen davranışı onaylar duruma düşebilirsiniz"*[681] .

Bu yaklaşımlar kapsamında ve mevcut uluslararası hukuk kuralları açısından bakıldığında eleştirel yaklaşımları destekleyen pek çok sebebin olduğu görülmektedir. BM Şartı'nın genel yaklaşımının müdahaleci olmadığı, bir bütün olarak ele alındığında, BM Şartı'nın temel olarak devletlerin kuvvet kullanma hakkını, uluslararası alanda bireysel veya ortak meşru müdafaa ve BM tarafından yetkilendirilmiş veya kontrol edilen askeri operasyonlara yardım ile sınırlandırdığı[682] gerçeği dikkate alınırsa BM'nin mevcut

---

[679] Bkz.; Çelebi ve Özdemir, 2010, s. 71-72.

[680] Bkz.; Çelebi ve Özdemir, 2010, s. 82.

[681] Çelebi ve Özdemir, 2010, s. 75.

[682] Welsh, Jennifer M. (2004). *Humenitarian Intervention and International Relations*, Oxford: Oxford University Press, s. 72.

yapısıyla amaçlanan hedefin tam olarak yerine getirilemediği ortadadır. Oysaki II. Dünya Savaşı sırasında meydana gelen ölüm sayısı nedeniyle müttefik güçleri, uluslararası çatışmaların yönetimiyle görevli bir evrensel uluslararası örgütün kurulması konusunda daha fazla çaba gösterilmesi gerekliliğine ikna olmuştur. MC'nin görevinde başarısız olması nedeniyle yeni örgütün faklı olması öngörülmüştür[683].

MC sisteminde MC Misakı'na aykırı şekilde savaşa başvuran devletlere karşı zorlama önlemi öngörülürken, BM sisteminde barışa yönelik tehdit, barışın bozulması ve saldırı eylemlerine karşı zorlama önlemi alınabileceği kabul edilmiştir[684]. Bu noktada BM sisteminin daha pasif bir duruş öngördüğü, barış ve güvenliğin sağlamasına ilişkin olarak etkin bir işlev üstlenmediği söylenebilir. Güvenlik Konseyi'nin barışın bozulduğunu sadece 1950 yılında Kore, 1982 yılında Falkland ve 1990 yılında Kuveyt için toplam üç kez saptamış[685] olması da bunu göstermektedir.

BM'nin barış ve güvenliğin sağlanmasında etkin olma konusundaki başarısızlığının sebebi olarak, BM'nin kurulduğu 1945 yılı itibariyle BM'nin barışı koruma görevinin öngörülemediği ve bundan dolayı BM Şartı'nda buna ilişkin bir hüküm bulunmadığı, bunun yerine Güvenlik Konseyi'nin savaşın galibi olan daimi üyelerinin işbirliği içinde dünya polisi olarak barışı sağlamasının benimsendiği ifade edilmektedir[686]. Sonraki yıllarda ortaya çıkan ekonomik anlamda küreselleşme, neoliberalizmin yükselişi ve kapitalizmin zaferi olarak değerlendirilmiş ise de[687] Güvenlik Konseyi'nin oluşumu öncesinde SSCB'nin (Sovyet Sosyalist Cumhuriyetler Birliği) hariç tutularak imzalanan Bretton Woods Antlaşması'yla ekonomik ve siyasal altyapının merkez kapitalist batı devletleri tarafından oluşturulan yeni dünya düzeni, tam olarak barışın ve güvenliğin geçerli olduğu bir dünya olmamıştır. Anılan dönemde barışı koruma çalışmalarının ilk

---

[683] Arend ve Beck, 1993, s. 29.

[684] Keskin, 1998, s. 139.

[685] Keskin, 1998, s. 142.

[686] Hill, Stephen M. (2004). *United Nation Disarmament Process in Intra-State Conflict.* New York: Palgrave Macmillan, s. 1.

[687] Lawson, 2012 s. 141.

olarak ABD ile SSCB arasındaki çatışmaların küresel boyuta ulaşmasını önlemeye yönelik olması[688] iki kutuplu bir dünyada soğuk savaş dönemi içerisindeki BM'nin işlevinin ne şekilde evrildiğini de göstermektedir. Buna bağlamda Uluslararası Para Fonu (*International Monetary Fund*/IMF) ve Dünya Bankası (*The World Bank*) tarafından uygulanan neoliberal politikaların başarılı olmadığı, durumu daha da kötüleştirdiğine dair görüş[689] oldukça yerinde bir tespittir. Ulus devletin denetimi dışında kalan ve uluslararası yatırım olanaklarını güvence altına almayı amaçlayan bu düzen önceleri IMF ve Dünya Bankası gibi uluslararası kapitalist yapılar tarafından kontrol edilirken, kapitalist ekonomik sistemin giderek büyüyen uluslararasılaşması nedeniyle devletler üzerindeki baskı artmıştır[690].

Ayrıca BM Şartı'nın imzalandığı dönem sonrasında uluslararası çatışmaların yapısında meydana gelen değişikliklerin BM'nin görevlerini yerine getirmesinde bazı sorunlara sebep olduğu görülmektedir. Zira II. Dünya Savaşı sırasında Almanya, Japonya ve İtalya'nın açık işgalleri söz konusuyken günümüzdeki çatışma biçimleri karmaşık bir hal almış, silahlı çatışmalar hukuku kurallarından sorumlu olmamak amacıyla çatışmalar daha kapalı, vekâlet savaşları şeklinde ve terör eylemleriyle kendini göstermiştir.[691] Bu bağlamda BM'nin bu sorunlarla eski yöntemlerle baş etmesi pek de kolay olmamış, belirtilen çatışmaların uluslararası barış ve güvenliği tehdit eden eylemler olarak kabul edilip edilmeyeceği ve bu sorunlara karşı ne şekilde kuvvet kullanılabileceği konularında fikir ayrılıkları sistemin beklenen işlevi yerine getirememesine yol açmıştır. Özellikle de bu tür sorunların BM üyesi devletlerin emperyal faaliyetlerinin bir sonucu olduğu gözetildiğinde sorunların çözümü daha bir karmaşık bir hal almaktadır.

Durum uluslararası hukuktaki işleyiş sorunu bağlamında değerlendirildiğinde BM Şartı'nın 106. maddesi gereğince BM'nin daimi üyeleri tarafından ortak güç kullanımında

---

[688] Hill, 2004 s. 2.

[689] Lawson, 2012 s. 135.

[690] Jessop, Bob. (2008). *Devlet Teorisi* (Çev. Ahmet Özcan). Ankara: Epos Yayınları, s. 242-243.

[691] Arend ve Beck, 1993, s. 37.

başarılı olunamaması, öğretide bazı sebeplere dayandırılmaktadır. Bunlar veto, resmi bir kolektif eylem mekanizmasının kurulamaması ve sınırlı kolektif güvenliğin reddi olarak ifade edilmektedir[692]. Veto konusu en temel ve en yaygın bilinen sorun olarak kabul edilse de yaptırım mekanizmasının yokluğu, bu alanda kurulan bir ordu bulunmaması diğer önemli etkenlerdir. Diğer bir sebep ise, ulusal çıkarların ön planda tutulması nedeniyle devletlerin kendilerini doğrudan ilgilendirmeyen barış ve güvenliğin bozulması olaylarına nazaran kendilerini doğrudan ilgilendiren tehditlere daha farklı yaklaşmalarıdır.

Sistemin başarısının sorgulanmasında bir diğer etken ise sistemin kendi içinde çelişkili bir yapıyı barındırması olarak ifade edilebilir. Zira BM'nin insani müdahalesine ilişkin yaşadığı zorlukların merkezinde yer alan BM'nin ilk 45 yılında hâkim olan egemen devletlerin iç ilişkilerine karışmama prensibinin BM'nin müdahale kabiliyetiyle çelişmesinin yattığı iddiası[693] kabule şayandır.

Sürece bakıldığında bir BM kuvveti oluşturulması çabalarının sonuç vermemesi üzerine uluslararası barışı ve güvenliği tehdit eden ya da bozan her durumda *ad hoc* çözümler aranması yoluna gidilmiştir. Bu *ad hoc* çözüm yaklaşımı çerçevesinde ilk kez karşılaşılan ve kuvvet kullanmayı gerektiren durum Kore ile ilgilidir[694]. Bölgesel organizasyonlar, bazı olaylarda yaptırım uygulamış olsa da BM kolektif güvenlik sistemi soğuk savaş döneminde genel olarak etkisiz kalmıştır. BM Şartı'nın VII. kısmının silahlı güç gerektiren tek uygulaması Kore operasyonu olup tek olay olmasıyla olumsuz bir şekilde bilinir[695]. İkinci olarak bu kez BM adına değil, fakat BM'nin izniyle silahlı kuvvet kullanılması Körfez olayı sırasında Irak'a karşı gerçekleştirilmiştir [696] . Bölgesel organizasyonlar konusunda ise en dikkat çekici örnek NATO tarafından yapılan Kosova

[692] Arend ve Beck, 1993, s. 57-58.

[693] Welsh, 2004 s. 71.

[694] Pazarcı, 2012, s. 446.

[695] Gray, 2008 s. 27.

[696] Pazarcı, 2012, s. 446.

müdahalesidir. Bazılarına göre bu bir insani bir müdahale iken bazılarınca da BM Şartı'nın açık bir ihlali olarak kabul edilmektedir[697].

BM döneminde gelişmiş ve gelişmekte olan devletlerarasında kuvvet kullanmanın kapsamı ve kuvvet kullanımının silah kullanımı yanında ekonomik yaptırımı da kapsayıp kapsamadığı konusunda görüş ayrılıkları bulunmaktadır[698]. Uluslararası hukukun en tartışmalı alanları kuvvet kullanımının ekonomik baskı, iç savaşa karışma konularını kapsayıp kapsamadığına ve meşru müdafaa hakkı ve kendi kaderini belirleme hakkının kapsamına ilişkindir[699]. *Jus ad bellum,* BM Şartı'nda münhasıran düzenlenmemiştir. Buna karşın, BM Şartı'nın kuvvet kullanma yasağını düzenleyen 2/4. maddesinde, Güvenlik Konseyi'nin barışı tehdit, barışın bozulması veya saldırganlık eyleminin varlığını tespitte alınacak önlemlere ilişkin 39., 41. ve 42. maddelerinde ve meşru müdafaayı düzenleyen 51. maddesinde *Jus ad bellum* ile ilgili düzenlemeler bulunmaktadır[700]. Bu bağlamda kuvvet kullanımı konusunda devletlerarasındaki fikir ayrılığının sebebi olarak BM Şartı'nda bu konuda açık hükümlerin bulunmaması yanında ulus devletlerin II. Dünya Savaşı'nın yıkımlarına rağmen müşterek çıkarlara nazaran hala ulusal çıkarlarına öncelik vermelerinden kaynaklandığı söylenebilir.

3.1.3. Kuvvet Kullanma ve Tehdit Etme Yasağı

Westfalya Barışı'nın bir sonucu olarak uluslararası hukukun yegâne aktörü kabul edilen devletlerin, 1856 Paris Antlaşması ile egemenlik hakkının uzantısı olan kuvvet kullanma hakkından ilk kez taviz verdikleri ve deniz hukukunun belirsizliğinden kaynaklı tarafsız devletler ile çatışan taraflar arasındaki görüş farklılıkları nedeniyle ortaya çıkabilecek yeni çatışmalar veya önemli sorunlardan kaçınma çabası kapsamında devletlerin bu

[697] Gray, 2008 s. 31.

[698] Gray, 2008 s. 30.

[699] Gray, 2008, s. 7.

[700] Graham, 2010, s. 88.

haktan vazgeçtikleri kabul edilmektedir[701]. Egemen devletlerin kuvvet kullanma hakkının sınırlandırılmasının ilk örneği olan bu antlaşma sonrasında uluslararası hukuk alanında kuvvet kullanma yasağı konusundaki tarihi gelişime baktığımızda, MC Misakı'nda kuvvet kullanımının açıkça yasaklanmadığı görülmektedir.

MC döneminde 1925 yılında bir kısım Avrupa devletleri tarafından imzalanan Lokarno Antlaşması ile saldırı savaşları hukuk dışı ilan edilmiş fakat yaptırım ve meşru müdafaa savaşlarının mümkün olduğu belirtilmiştir[702]. Kuvvet kullanımını kesin şekilde yasaklayan ilk antlaşma[703] olan 1928 tarihli Briand-Kellogg Paktı hükümlerine göre ise, ulusal bir politika aracı olarak savaş yasaklanmış olup, karşı saldırı olarak değil ama Pakt'ın ihlali olarak kuvvet kullanımı mümkün kabul edilmiştir. Buna göre, kendisine saldırı yapılmamış olsa dahi Paktı ihlal eden tarafa savaş açmak meşru kabul edilirken[704] uluslararası anlaşmazlıkları çözmek için savaşa girmek yasaklanmıştır[705]. Pakt'ın ilk iki maddesine göre, taraf devletlerarasında çıkabilecek tüm ihtilafların çözümü ancak barışçı yollarla olacaktır[706]. BM Şartı'nın kuvvet kullanma ve tehdidi yasaklaması ile ilk kez Briand-Kellogg Paktında kabul edilen savaşın hukuka aykırılığı kavramına küçük çaplı kuvvet kullanımını dâhil ederek, kuvvet kullanma tehdidi kadar silahlı misillemeyi de etkili şekilde yaptırıma bağlayarak genişletmiştir[707].

---

[701] Jensen, Eric Talbot. (2002). *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Right of Self-Defense*, Stanford Journal of International Law, Cilt:38, s.214.

[702] Aksar, 2021, (2. Kitap), s. 130.; Hoş, H. Serdar. (2013). *Haklı Savaş ve İnsancıl Hukuk. İstanbul:* On İki Levha Yayıncılık, s. 100.

[703] Pazarcı, 2021, s. 551.; Pakta göre devletler, askeri güçlerini saldırı amaçlı değil, yalnızca savunma amaçlı kullanabilecekleridir. Bu antlaşma ile klasik devletler hukukundaki *jus ad bellum* ortadan kaldırılmıştır. Bkz.: Mutlu, 2016, s. 96.; Aksar, 2021, (2. Kitap), s. 130.

[704] Kelsen, 2012 s. 29-30.

[705] Mutlu, 2016, s. 96.

[706] Sur, 2022, s. 297.

[707] Ruys, Tom. (2010). *Armed Attack' and Article 51 of the UN Charter.* Cambridge: Cambridge University Press, s. 54.

Madde metninde açıkça belirtilmese de öğretide, doğal meşru müdafaa hakkı ve Güvenlik Konseyi'nin Şart'a göre kuvvet kullanımı bağlamında, BM Şartı 2/4. maddesiyle yasaklanan kuvvet kullanma ve tehdit, "saldırgan kuvvet kullanımı" nın yasaklanması[708] olarak yorumlanmaktadır. İleride bahsedileceği üzere bu husus kuvvet kullanma yasağının dar yorumlanmasının bir sonucudur. Ayrıca BM Şartı'nda bilinçli olarak "savaş" yerine "kuvvet kullanma" kavramı tercih edilmiş, ancak kuvvet kullanma yasağı ve meşru müdafaa düzenlemeleri II. Dünya Savaşı'na tepki olarak ortaya çıktığından, bu doğrultuda devletlerarası çatışmalara yönelik olmuştur[709]. BM Şartı'nın yürürlüğe girmesinin ardından yaşanan soğuk savaş döneminde ise kuvvet kullanma yasağını düzenleyen Şart'ın 2/4 maddesinin öldüğünün, hükümsüz kaldığının ileri sürülmesine karşın bazı yazarlarca bunun tam olarak değilse de kısmen doğru olduğu itiraf edilmiştir[710].

Sorunlu da olsa kuvvet kullanımını kesin olarak yasaklayan bir sistem öngören BM döneminde, BM Şartı'nın 2/3 fıkrasında tüm üye devletlerin uluslararası nitelikteki uyuşmazlıkları uluslararası barış ve güvenliği ve adaleti tehlikeye düşürmeyecek biçimde, barışçı yollarla çözmelerinin gerekliliği düzenlenmiştir. Bu da iyi niyet ve işbirliği ruhu içinde gerçekleştirilmelidir. BM Şartı'nın 33. maddesi uyarınca bu barışçıl çözüm yolları görüşme, soruşturma, arabuluculuk, uzlaşma, hakemlik ve yargısal çözüm yolları ile bölgesel kuruluş veya antlaşmalara başvurarak veya kendi seçecekleri bir diğer çözüm yoluna başvurmak olmalıdır. Bu maddeye göre Güvenlik Konseyi, tarafları bu maddede sayılan barışçıl çözüm yollarına başvurmaya çağırabileceği gibi, 38. madde uyarınca uyuşmazlığın taraflarına tarafların tümünün istemesi halinde uyuşmazlığın barışçıl yollarla çözülmesi için tavsiyelerde bulunabilir. Güvenlik Konseyi Şart'ın 39. maddesi uyarınca barışın tehdit edildiğini, bozulduğunu veya bir saldırı eylemi olduğunu

---

[708] Sharp, 1999, s. 33.

[709] Gray, Christine. (2008). *International Law and the use of Force*. Oxford New York: Oxford University Press, s. 7.; Savaş yerine kuvvet kullanmanın yasaklanması BM Şartı 2/4 maddesinin konu bakımından ne şekilde uygulanabileceğini belirlemektedir. Bkz.; Erkiner, 2020, s. 286.

[710] Waxman, Matthew C. (2011). *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* The Yale Journal of International Law, Cilt:436, s. 441.

saptaması halinde ise gerekli tavsiyede bulunabilir veya önlemlerin alınmasına karar verebilir.

Devletlerin uyuşmazlıkları barışçıl yöntemle çözmesi gerekliliğinin bir istisnası olarak uyuşmazlığın tarafı olan bir devletin hukuka aykırı eyleminin buna sebep olması halidir ki bu durumda zarar gören taraf zararla karşılık ya da misilleme yoluna başvurabilir[711]. Ayrıca BM Şartı'nın 2/4. maddesi uyarınca devletlerin kuvvet kullanması yasaklanmış ve sorunların barışçıl yollarla çözümü esas alınmış ise de hukuka aykırı fiilin silahlı saldırı boyutuna varması halinde başvurulabilecek hukuki önlemler yanında BM Şartı'nın 51. maddesi gereğince meşru müdafaadan kaynaklı geçici önlemlere başvuru imkânı saklıdır. İç işlerine karışma yasağı da yapılageliş hukukundan kaynaklanan ve Şart'ın 2/7. maddesi gereği kuvvet kullanma yasağını tamamlayan bir ilkedir.

Öğretide devletlerin BM Şartı'nın 2/3. maddesine aykırı eylemlerine örnek olarak şunlar gösterilmektedir:

- devletlerin uyuşmazlığın çözümü görüşmeleriyle ilgili kötü niyetli eylemleri,
- devletin kendi ihtilafının barışçıl çözümünü diğer tehdit eylemleri,
- diğer bir devletin uyuşmazlığının çözümünü önleyecek veya geciktirecek bir biçimde diğer bir devletin ihtilafıyla çatışan eylemler ve
- devletlerarasında uluslararası barış ve güvenliği tehdit eden ihtilaflar yaratmak gösterilebilir[712].

Buna göre, uyuşmazlıkların barışçıl yöntemlerle çözülmesi gerekliliğine aykırı eylemler Şart'a aykırı olsa da tek başına kuvvet kullanma olarak değerlendirilemez. Siber faaliyetler açısından bakıldığında, bir devletin kendi bilgisayar veri tabanında tahrifat yapması ve uyuşmazlığın çözümü görüşmelerinin aksaması için veri tabanını başka bir devletin kullanmasına izin vermesi veya belirtilen biçimde iki veya daha fazla devlet

[711] Sharp, 1999, s. 85.

[712] Sharp, 1999, s. 86.

arasında uyuşmazlık meydana getireme çabası barış zamanında BM Şartı'nın 2/3. Maddesine aykırılık oluştursa da fiziki yıkım veya diğer faktörler gerektirmedikçe, tek başına uluslararası hukukta kuvvet kullanma oluşturmaz[713].

Buna karşın, başka bir devletin egemenlik alanında yıkıcı etkiler doğuran ve siber uzayda gerçekleşen kasti herhangi bir devlet eylemi hukuka aykırı bir kuvvet kullanma oluşturur. Bununla birlikte, kasti olmadan başka bir devletin egemenlik alanında zarar meydana getirilmesi ise hukuki sorumluluk gerektirmekle birlikte büyük olasılıkla BM Şartı'nın 2/4 maddesi anlamında meşru müdafaa hakkını doğuracak kuvvet kullanma oluşturmayabilecektir[714]. Kasta dayanmayan siber faaliyetlerden kaynaklanan zarar, savaşma niyeti ve meşru müdafaa konuları ileride daha ayrıntılı olarak incelenecektir.

Asıl olan uyuşmazlıkların barışçıl yöntemlerle çözülmesi ise de bunun her zaman mümkün olduğu söylenemez. Geleneksel anlamda, savaşın diplomatik çözüm yöntemlerinin devamı olduğunun kabul edildiği bir tarihsel anlayışın tamamen değiştirilmesi kolay değildir. Ayrıca yukarıda belirtilen süreç sonunda yaşanan dünya savaşları üzerine gelinen noktada kuvvet kullanmanın kesin olarak yasaklanması sağlanmak istenmiş ise de uluslararası hukukta devletlerin üzerinde yaptırım gücüne sahip bir mekanizma bulunmadığından bazı durumlarda kuvvet kullanımının hukuka uygun kabul edilmesi gerekmiştir. BM nezdinde kurulacak bir ortak askeri güç hedefi yerine getirilemediğinden, Şart'ın VII. kısmı 42. maddesi gereğince Güvenlik Konseyi'nin yetkilendirmesi bu yasağın bir istisnasını oluşturmuştur. Ayrıca Şart'ın 51. maddesi kapsamında silahlı bir saldırıya karşı meşru müdafaa hakkının kullanılması ve hukuka uygunluk sebebi olan devletin rızası[715] yasağın genel manada istisnalarını oluşturmaktadır.

---

[713] Sharp, 1999, s. 87.

[714] Sharp, 1999, s. 102.

[715] Blank, Laurie R. (2013). *International Law and Cyber Threats from Non-State Actors*, Int'l L. Stud., Cilt: 89, s. 411.

BM Şartı'nda yerini bulan bu istisnaları daha açık şekilde sıralamak gerekirse;

> *"a) 51. madde gereği birlikte meşru müdafaa hakkının kullanılması,*
>
> *b) Antlaşmanın VII. Bölümünde düzenlenen Güvenlik Konseyi kararıyla zorlama önlemi olarak güç kullanılması,*
>
> *c) 53. madde uyarınca, bölgesel antlaşmalara göre ya da bir bölgesel örgüt çerçevesinde zorlama önlemi olarak güç kullanılması,*
>
> *d) Genel Kurul ya da Güvenlik Konseyinin kararı ve ilgili devletin rızasıyla barış gücü yerleştirilmesi,*
>
> *e) 106. madde uyarınca daimi beş Güvenlik Konseyi üyesinin ortak eylemi"*[716]

şeklinde ifade etmek mümkündür.

BM tarihinde Güvenlik Konseyince bir saldırı karşısında kuvvet kullanımına Kore savaşı ve Körfez savaşı olmak üzere iki kez yetki verdiği görülmektedir. Ayrıca Konsey, Somali iç savaşında kuvvet kullanılması konusunda da yetki vermiştir[717]. BM 43. maddesine göre bütün BM üyesi devletler barış ve güvenliğin korunması için Güvenlik Konseyi'nin çağrısı üzerine örgüte gerekli silahlı kuvvetleri tedarik etmeyi, yardım ve kolaylıklarda bulunma sorumluluğunu üstlenmiştir[718]. Bu konuda bir diğer örnek olarak Uluslararası Güvenlik Destek Gücü (ISAF) gösterilmektedir. BM Güvenlik Konseyi, terörle mücadele kapsamında Afganistan'daki geçici otoriteye yardım etmek üzere Antlaşma'nın VII. bölümü çerçevesinde 20 Aralık 2001 tarih ve 1386 sayılı kararı ile böyle bir askeri gücün oluşturulmasına hukuksal olanak sağlanmıştır[719].

Şart'ın 2/4. maddesinde düzenlenen kuvvet kullanma ve tehdit etme yasağının Şart'a taraf olmayan devletler yönünden bağlayıcı olup olmadığı konusunda UAD'nın *Nikaragua*

---

[716] Keskin, 1998, s. 134.

[717] Arend ve Beck, 1993, s. 52.

[718] Pazarcı, Hüseyin. (2012). *Uluslararası Hukuk.* Ankara: Turhan Kitabevi, s. 445.

[719] Pazarcı, 2012, s. 447.

Davası'nda verdiği karar dikkate alınmalıdır. Bu kararda da ifade edildiği üzere kuvvet kullanma yasağı, yapılageliş hukukundaki statüleri gereği az sayıdaki üye olmayan devleti de bağlamaktadır[720]. Zira kuvvet kullanma yasağının *jus cogens* kuralı[721] haline gelmesi nedeniyle BM üyesi olsun ya da olmasın tüm devletler açısından bağlayıcı olduğu kabul edilmelidir[722]. Uluslararası Hukuk Komisyonu raporunda sayılan örnekler arasında BM ilkelerine aykırı şekilde kuvvet kullanma yasağı *jus cogens* normlar arasında sayılmıştır[723]. 1969 tarihli Viyana Antlaşmalar Hukuku Sözleşmesi'nin 53. maddesi gereğince antlaşma hükümleriyle *jus cogens* normların çatışması halinde ilgili antlaşma hükümleri geçersiz kabul edilmektedir[724].

Belirtilen yasak tüm devletleri kapsamakta ise de devlet dışı örgütlerin, organize grupların, terör örgütlerinin ya da bireylerin eylemleri bu bağlamda değerlendirilmemekte, bu tür eylemler iç hukuka veya uluslararası hukuka aykırı nitelikte başka eylemler oluşturabilmektedir[725]. Uluslararası antlaşmaların, *jus cogens* nitelikteki kuvvet kullanma yasağına aykırılık oluşturan hükümlerinin siber faaliyetlere uygulanması sürecinde çatışması durumunda bu hükümlerin geçersizliği ileri sürülebilir. Buna paralel olarak soykırım, savaş suçları, insanlığa karşı işlenen suçların yasaklanması ve işkencenin yasaklanması gibi *jus cogens* niteliğindeki buyruk kurallara aykırı olan diğer hükümlerin geçersizliği de söz konusu olacaktır. Bu nedenle mevcut normların siber bağlamda uyarlanması sürecinde, buyruk kurallara aykırılık teşkil edecek uygulama ve yorumlardan kaçınılması bir zorunluluktur.

---

[720] Afroditi, 2010, s. 12.; Pazarcı, 2021, s. 552.

[721] Aksar, 2021, (2. Kitap), s. 127.

[722] *Jus cogens* kuralı halini alan kuvvet kullanma yasağının kişi bakımından uygulanması (ratione personae) sonucunda bütün devletlere bir takım *erga omnes* yükümlülükler yüklenmektedir. Bkz.; Erkiner, 2020, s. 285.

[723] Sur, 2022, s. 56.

[724] Aksar, 2021, (1. Kitap), s. 111.

[725] Schmitt, 2017, *Tallinn Manual 2.0.* s. 330.

Mevcut normların hatalı şekilde yorumlanması suretiyle *jus cogens* kurallarla çatışmasının önüne geçilmesi için Almanya'da uygulanan iç hukuk normları ile uluslararası antlaşmaların çatışması durumunda uygulanan yorum şekli örnek verilebilir. Almanya'da federal kanunların uluslararası antlaşma hükümleri ile çatışması halinde kanun koyucunun antlaşmayı ihlal kastıyla hareket edip bu kanunu çıkardığı yanlışlığa mahal vermeyecek şekilde ispatlanmadıkça, böyle bir niyetin bulunduğunun varsayılamayacağı ve sonraki işlemin antlaşmayla çatışmayacak şekilde yorumlanması gerektiği kabul edilmektedir[726]. Bu nedenle mevcut normların siber faaliyetlere uygun şekilde yorumlanırken aynı zamanda *jus cogens* kurallar ile çatışma sonucunu doğurmayacak biçimde değerlendirme yapılması isabetli olacaktır.

BM Şartı 2/4. madde metnine göre anılan yasak hükmü eylemin bir başka devletin toprak bütünlüğüne veya siyasi bağımsızlığına karşı kuvvet kullanımı veya kuvvet kullanma tehdidi oluşturması veya BM'nin amaçlarına karşı gerçekleştirilmesini kapsamaktadır. Bu kuvvet kullanımı veya tehdidinin BM'nin amaçlarıyla uyumlu olmayacak bir biçimde gerçekleşmesine karşın toprak bütünlüğüne veya siyasi bağımsızlığına karşı gerçekleşmemesi durumunda ise eylemin yasa dışı olduğuna ilişkin bir karine oluşturulmak istenmiştir[727]. Bir başka devletin toprak bütünlüğüne ve siyasi bağımsızlığına karşı gerçekleştirilmeyen ancak sınır ihlali teşkil eden kuvvet kullanımının yasak kapsamına girip girmediği konusunda açık ve kesin bir cevap vermek her zaman olanaklı değildir[728]. Güçlü devletler tarafından madde metninin farklı yorumu sonucunda yasak kapsamında kalıp kalmadığı tartışmaya açık olan çeşitli uygulamalar ile karşılaşılmaktadır. Bazı yazarlar BM Şartı'nın 2/4. maddesinin kuvvet kullanımını mutlak suretle yasaklamadığı, bunun yerine anılan düzenlemenin kolektif güvenlik sistemine ilişkin VII. Bölüm ışığında yorumlanması gerektiğini savunmaktadırlar[729].

[726] Tütüncü ve diğerleri, 2017, s. 279.

[727] Schmitt, 2017, *Tallinn Manual 2.0.* s. 329.

[728] Pazarcı, 2021, s. 552.

[729] Gray, 2008 s. 56.

Sınır ihlali konusunda BM Genel Kurulu'nun 2625 sayılı Dostça İlişkiler Bildirisi[730] devletlere bir başka devletin var olan uluslararası sınırlarını ve hatta antlaşmalarla düzenlenmiş geçici ayrım çizgilerini çiğnemesini yasaklamış görünmektedir[731].

BM Şartı 2/4. maddesinde düzenlenen kuvvet kullanma ve tehdit etme yasağının maddede düzenlenme şekli itibariyle bir devletin toprak bütünlüğü ya da bağımsızlığına karşı veya BM Şartı amaçlarıyla bağdaşmayan herhangi bir biçimde kuvvet kullanmanın yasaklanmış olup olmadığı konusunda sınırlayıcı ve kapsayıcı olmak üzere iki farklı görüş bulunmaktadır[732]. İlk görüşe göre, madde metniyle sınırlı yorum sonucunda bir devletin toprak bütünlüğü veya bağımsızlığına aykırı ya da BM Şartı'nın temel ilkeleriyle bağdaşmayan eylemler dışında kalan kuvvet kullanımları yasak kapsamına girmemektedir. Kuvvet kullanma konusunu dar yorumlayanlara göre silahlı, ekonomik veya politik zorlama, içişlerine karışma ilkesi örneğinde olduğu gibi, uluslararası hukuk kurallarına aykırı olabilir, ancak sadece silahlı kuvvet kullanımı BM Şartı'nın 2/4. maddesinde düzenlenen normu ihlal edebilir[733]. ABD ve müttefikleri arasındaki baskın görüş bu yönde olup BM Şartı'nın 2/4. maddesinde öngörülen kuvvet kullanma yasağı ve tamamlayıcı 51. maddede düzenlenen meşru müdafaanın askeri saldırılar veya silahlı şiddet durumunda uygulanabileceği kabul edilmektedir[734].

İkinci görüş ise kendi içinde, yasağın kapsayıcı ve genel niteliğinin kabul edilmesine rağmen BM Antlaşması'nda öngörülen mekanizmanın kurulamaması nedeniyle bazı savaşa varmayan kuvvet kullanma yollarının hukuka uygun hale geldiğini savunan bir grup ile yapılageliş gereği 51. maddeden daha geniş meşru müdafaa hakkının geçerli

---

[730] BM Genel Kurulu, Declaration on Principles of International Law Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (24 Ekim 1970) Erişim: 12.06.2022 https://www.un.org/ruleoflaw/files/3dda1f104.pdf

[731] Pazarcı, Hüseyin. (2000). *Uluslararası Hukuk Dersleri. 4*. Kitap. Ankara: Turhan Kitabevi, s. 112-113.

[732] Keskin, 1998, s. 39.; Aksar, 2021, (2. Kitap), s. 133.

[733] Benatar, Marco. (2009). *The Use of Cyber Force: Need for Legal Justification?*, Goettingen Journal of International Law I, s. 386.

[734] Waxman, 2011, s. 427.

olduğunu savunan ikinci gruptan oluşur[735]. İkinci görüşe göre hareket eden ve ilk grubu oluşturan kimi devletler, insancıl amaçlı karışma, uyruklarının can ve mal güvenliğinin korunması, bir devletin kendi varlığını koruması ve izleme hakkı[736] ve 2000'li yıllarda ortaya çıkan koruma prensibi gerekçelerine dayanarak yasak kapsamında olup olmadığı tartışmaya açık olan uluslararası hukukta karışma olarak tanımlanan eylemlere başvurmaktadırlar.

Dış müdahalelere karşı oldukları halde uluslararası politik topluma geniş ölçekte dâhil olmak isteyen ikinci gruptaki kimi devletler ise, benzer şekilde iletişim ve bilişim sistemlerini, düşmanca veya zarar verici sayılan veya dış etkilerden veya izinsiz girişlerden yalıtırken, uluslararası bilgi bağlantısından da faydalanmak istemektedir[737]. Bu gruptaki devletler hem uluslararası toplum tarafından kabul edilen müdahalelere karşı durmakta, hem de korunmuş bir sistem içinde olmayı talep etmektedirler. Bunlara göre; Şart'ın 2/4 maddesinin yürürlüğe girmesinden itibaren devletlerin uygulamalarıyla desteklenmiş ve kanıtlanmış uluslararası yapılageliş hukuku, yurtdışındaki vatandaşların korunması için gerekli ve orantılı olan rıza hilafına sınırlı askeri kuvvet kullanımının 2/4 madde anlamında bir kuvvet kullanma olduğuna ve bu kuvvet kullanımının 51. maddeye göre yasal bir meşru müdafaa olduğuna dair güçlü bir delil oluşturur[738]. Bu durumdaki devletler geniş bir meşru müdafaa anlayışıyla kuvvet kullanma oluşturan eylemlere karşı daha geniş bir karşı savunmada bulunmak istemektedirler.

Bu noktada geleneksel anlamda insani kurtarma operasyonundan haberdar olmayan ülke devletinin izinsiz girişi önlemeye yönelik meşru müdafaa hakkını kullanabileceği kabul edilmekle birlikte, devletin sınırlı ve insani kurtarma operasyonundan haberdar olması ve ülke devletine zarar vermek niyetinin bulunmaması durumunda meşru müdafaa

---

[735] Keskin, 1998, s. 79.; Yapılageliş hukuku ile Şart'ın 51. maddesinin birlikte uygulanması gerektiği yönündeki görüş için bkz.: Gill, Terry D. / Ducheine, Paul, A. L. (2013). *Anticipatory Self-Defense in the Cyber Context*, US Naval War College International Law Studies, Cilt:89, s. 442.

[736] Pazarcı, 2000 (4. Kitap) s. 114.

[737] Waxman, 2011, s. 430.

[738] Sharp, 1999, s. 108.

şartlarının kurtarma uçağını düşürme hakkını vermeyeceği [739] savunulmaktadır. Geleneksel kurtarma operasyonu için geçerli olan ve kuvvet kullanma yasağına tabi olsa dahi bazı sınırlandırmaları öngören bu durumun bir devletin toprak bütünlüğüne ya da bağımsızlığına karşı veya BM Şartı amaçlarıyla bağdaşmayan herhangi bir biçimde kuvvet kullanma mahiyetindeki siber müdahalelere uygulanabilirliği tartışmaya değer yeni bir konu oluşturmaktadır.

Bu görüşler bağlamında, bir devletin toprak bütünlüğü veya bağımsızlığına aykırı ya da BM Şartı'nın temel ilkeleriyle bağdaşmayan eylemler dışında kalan siber operasyonların kuvvet kullanma yasağını ihlal etmemekle birlikte uluslararası hukuka aykırı eylem oluşturabileceği söylenebilir. Bu türden siber operasyonların kurtarma operasyonları dâhilinde gerçekleştirilmesi halinde ise kuvvet kullanma oluşturmayacağı ya da kuvvet kullanma oluştursa dahi meşru müdafaa şemsiyesi altında değerlendirileceği sonucu çıkarılabilir. Ayrıca her durumda bir ülkenin toprak bütünlüğünü ve ya da bağımsızlığını hedef almayan bu tür kurtarma operasyonlarına karşı koyacak devletin meşru müdafaa hakkı da sınırlıdır.

Örnek vermek gerekirse, Yunanistan'da rehin tutulan Türk vatandaşlarını kurtarmaya yönelik bir operasyon düzenleyen Türk devletinin, fiziki ve siber operasyonları içeren bir harekâtı gerçekleştirmesi halinde siber operasyonların anılan ülkenin toprak bütünlüğünü ya da bağımsızlığını hedef almadığı tartışmasızdır. Yunanistan'a bilgi verilmeden bu kapsamda gerçekleştirilen siber operasyonların kuvvet kullanma yasağı kapsamında değerlendirilemeyeceği söylenebilir. Bu durumda Yunan devleti, Türk kurtarma uçağını düşüremeyeceği gibi Türk siber birimler tarafından Yunan hava savunmasının devre dışı bırakılmasından dolayı kuvvet kullanma yasağını ihlal iddiası haklı görülemeyecektir. Zira Türk devletinin meşru müdafaa bağlamında gerçekleştirdiği siber operasyon Yunan devletinin toprak bütünlüğünü ya da bağımsızlığını hedef almamaktadır.

[739] Sharp, 1999, s. 109.

BM Genel Kurulu'nda kuvvet kullanımı teriminin kesin anlamı konusundaki görüşmelerde terim genellikle silahlı veya fiziki kuvvet kullanma şeklinde kabul edilmiştir. Bu yorum gerek yapılageliş hukuku ve gerekse de Şart'ın hazırlık çalışmalarında açıkça onaylanmış, zira Brezilya'nın ekonomik saldırının kuvvet kullanma olarak kabulü teklifi San Francisco'da reddedilmiştir[740]. Genel kabul görmeyen, genellikle gelişmekte olan ülkelerce ileri sürülen ve Soğuk Savaş boyunca Sovyet Bloku tarafından desteklenen bir görüşe göre, devletin bağımsızlığını tehdit eden politik ve ekonomik zorlamalar da yasak kapsamına girmektedir [741] . Yerleşik devlet uygulamalarında dostça olmayan eylem türleri, ticaret yapmama kararı, uzay tabanlı izleme, boykot, diplomatik ilişkilerin kesilmesi, iletişimin reddi, casusluk, ekonomik rekabet veya yaptırım, ekonomik ve politik zorlama durumlarında etki ölçeğine bakılmaksızın kuvvet kullanma eşiğine varmadığı kabul edilmektedir[742]. Buna paralel olarak öğretide kuvvet kullanma yasağına aykırı olmayan vazgeçirme yöntemlerinden siyasi ve ekonomik baskı gibi, şiddet içermeyen önlemlerin BM Şartı'nın 2/4'ün getirdiği yasak kapsamı dışında kaldığı genel olarak kabul edilmektedir[743]. Aynı şekilde bir devletin tek taraflı olarak aldığı diğer bir devlet ile ticaret yapmama kararı, bu kararın olası etkilerine bakılmaksızın, kuvvet kullanma olarak değerlendirilmemektedir[744].

Kuvvet kullanma yasağının hangi davranışları kapsadığı konusunda BM Genel Kurulu'nun verdiği kararlar belirleyici olmuştur. BM Şartındaki kuvvet kullanmaya ilişkin hükümler BM'nin kuruşundan itibaren Genel Kurul kararlarına konu olmuş, ilk olarak 1949 Barışın Esasları Kararı, bilahare BM Genel Kurulu'nun 2625 sayılı ve 1970 tarihli Dostça İlişkiler Bildirisi ve 1987 tarihli Kuvvet Kullanımından Kaçınma Bildirisi ortaya çıkmıştır[745]. Zorlayıcı tedbirler yönünden ilk olarak 1970 tarihli ve 1987 tarihli

[740] Ruys, 2010, s. 55-56.

[741] Waxman, 2011, s. 429.

[742] Lin, Herbert S. (2010). *Offensive Cyber Operation and the Use of Force*, Journal of Natiomal Security Law & Policy, Cilt:4, s. 71-72.

[743] Acer, Yücel / Kaya, İbrahim. (2014). *Uluslararası Hukuk.* Ankara: Seçkin, s. 331.

[744] Sharp, 1999, s. 77.

[745] Gray, 2008 s. 9.

Deklarasyonlar üzerinden kuvvet kullanma yasağı kapsamında kalıp kalmadığına dair değerlendirme yapılmış ise de kesin bir cevap bulunamamıştır[746]. Dostça İlişkiler Bildirisi'nde kuvvet kullanma içeren zararla karşılık yöntemlerine başvurmak yasaklanmıştır[747].

Genel Kurul kararları genel olarak bağlayıcı olmasa da UAD'na göre bu hükümler uluslararası yapılageliş hukukunu yansıtmakta olduğu için etkilidir. BM Genel Kurulu'nun 1987 tarihli Uluslararası İlişkilerde Kuvvet Kullanma Tehdidi ya da Kuvvet Kullanmaktan Kaçınma Prensibinin Etkinliğinin Artırılmasına İlişkin Deklarasyonu ile devletlerin bazı gruplara ya da terörist gruplara yaptığı yardımların kuvvet kullanma yükümlülüğüne aykırı bir davranış oluşturacağı kabul edilmiştir[748]. Silahlı kuvvet kullanılması bir devletin düzenli askeri birliklerince doğrudan kuvvet kullanılmasını belirtebileceği gibi, bir devletin destekleyeceği ve yardım edeceği silahlı gruplar ya da gönüllü birlikler gibi düzen dışı kuvvetlerce dolaylı olarak kuvvet kullanılmasını da belirtebilecektir[749]. Dostça İlişkiler Bildirisi ve *Nikaragua Davası*'nda düzen-dışı kuvvetlerce bir başka devlet ülkesinde kuvvet kullanılması da kuvvet kullanma yasağı kapsamında değerlendirilmiştir[750].

BM Şartı 2/4 yalnızca devletlerin uluslararası ilişkilerinde kuvvet kullanmalarını veya kuvvet kullanma tehdidinde bulunmalarını yasaklaması nedeniyle iç çatışmalar, Şart'ın 39. maddesine göre uluslararası barış ve güvenliği tehdit eden ve bu yüzden önlem gerektiren nitelikte görülebilirlerse de kuvvet kullanma yasağına dâhil edilmemektedir[751]. Buna karşın sömürge rejimi altındaki toplumların self determinasyon ilkesi uyarınca bağımsızlıklarını kazanma mücadelesi bir devletin iç güvenliği sorunu biçiminde

[746] Afroditi, 2010, s. 12-13.

[747] Keskin, 1998, s. 92.

[748] Acer ve Kaya, 2014, s. 340.

[749] Pazarcı, 2021, s. 551.

[750] Pazarcı, 2021, s. 553.

[751] Keskin, 1998, s. 25.

değerlendirilmeyip uluslararası ilişkilerde kuvvet kullanılmasının yasaklanması ilkesi kapsamında değerlendirilmektedir[752].

Ayrıca ifade edilmelidir ki uluslararası yapılageliş hukuku gereğince kuvvet kullanımının meşru kabul edildiği durumlarda dahi gereklilik ve orantılılık ilkeleriyle sınırlı şekilde gerçekleştirilmelidir. Orantılılık ilkesi, çatışanlar arasındaki güç kullanımını sınırlandırmak amacını taşımayıp, askeri amaçlı güç kullanımının sadece çevresel zarar doğurduğu ölçüde gereksiz sivil mülkiyetin yıkımı ve sivil can kaybını sınırlandırmaya yöneliktir[753].

Bu noktada ifade edilmesi gereken bir diğer konu siber operasyonların kuvvet kullanma yasağı kapsamında uluslararası hukukta ne şekilde ele alınacağı üzerinedir. Bu husus gerek silahlı çatışmalar hukukunda ve gerekse de kuvvet kullanımına başvuru konusunda ön plana çıkmaktadır. Siber operasyonlar geniş bir kinetik saldırının parçasını oluşturabileceği gibi, tek başına da gerçekleştirilebilirler. İlk durumda kuvvet kullanma eşiği geniş çaplı bir kinetik saldırı bağlamında değerlendirilirken, ikinci halde siber operasyonun sebep olduğu ciddi zarar ya da önemli kayıp değerlendirmeye alınacaktır[754].

Gerek kuvvet kullanmaya başvuru ve gerekse de silahlı çatışmalar hukuku yönünden geçerli olan bu duruma dair iki farklı görüş bulunmaktadır. İlk görüş, mevcut kuralların siber operasyonlara kıyas yöntemiyle uygulanması yönündeyken, ikinci görüş taraftarları ise bu yeni alanla ilgili olarak çok taraflı özel düzenlemelerin yapılması gerektiği yönündedir[755]. Şu ana değin siber savaşa ilişkin çok taraflı bir uluslararası konvansiyonun imzalanmamış olması nedeniyle yazılı ya da yapılageliş kuralı olarak mevcut olan uluslararası hukuk normlarının siber operasyonlara uygulanması gerekmektedir. Silahlı

[752] Pazarcı, 2000, (4. Kitap), s. 112-113.; Pazarcı, 2021, s. 551.

[753] Sharp, 1999, s. 40.

[754] Position Paper, 2021, s. 6.

[755] Güreşçi, Ramazan. (2019). *Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi.* Savunma Bilimleri Dergisi, Cilt:18, Sayı:1, s. 77-78.

çatışmalar hukuku bölüm başlığı altında daha ayrıntılı tartışılacağı üzere siber operasyonlara dair yeni bir antlaşmanın yapılması seçeneğinin ise, bu antlaşmanın uluslararası hukukun tüm alt başlıklarını karşılayamayacağı için yaratacağı yasal boşluklar ve diğer olumsuzluklar kapsamında dikkate alınması gerekir. Bu nedenle *jus ad bellum* kapsamında mevcut normların kıyasen siber operasyonlara uygulanması yöntem olarak bu çalışmada esas alınacaktır.

BM Şartı'nda yasaklanan kuvvet kullanma konusunda, bir eylemin ne zaman kuvvet kullanmaya eşit kabul edileceğine dair herhangi bir ölçüt ortaya konulmamıştır. Melzer'e göre, siber operasyonların BM Şartı 2/4 anlamında kuvvet kullanmaya eşit olması gerekli olmayıp kuvvet kullanmaya eşit tüm siber operasyonların zorunlu olarak hukuka aykırı olması da gerekli değildir[756]. Zira siber operasyonların hukuka aykırılığı, içişlerine karışma yasağı yapılageliş kuralı gibi uluslararası hukukun gerektirdiği bir yükümlülüğün ihlalinden de kaynaklanabilecektir[757].

Kuvvet kullanımına başvurma konusunda, her koşulda kuvvet kullanmanın sınırlarını açıkça belirleyecek beyaz ve siyah, mekanik bir kuralın bulunmadığı gerekçesiyle kuvvet kullanma ve tehdit yasağını oluşturan eylemin ne olduğu sorusunun ilgili hukuk kuralları ve koşullar bağlamında her olayda sübjektif olarak değerlendirilmesi gerekir[758]. Buna göre, bir devletin siber uzaydaki faaliyetleri, diğer herhangi bir yerdeki faaliyetlerinde olduğu gibi kuvvet kullanımına başvurma hukuku kapsamında ve devlet uygulamalarına göre değerlendirilmelidir[759].

Yeni teknolojinin sonuçları, hava bombardımanında olduğu üzere, tanımlanmış olarak kabul edilebilir faaliyetlerin ötesine geçtiğinde savaşın yeni araç ve yöntemleri sadece mevcut yasalarla, gerektiğinde ise antlaşmalar hukuku ve evrilen devlet uygulamalarına

[756] Melzer, 2011, s. 9.

[757] Melzer, 2011, s. 9.

[758] Sharp, 1999, s. 52.

[759] Sharp, 1999, s. 52.

göre düzenlenir[760]. Siber savaşa dair geçmiş örneklerin bulunmaması nedeniyle hükümet yetkililerinin hukuki görüş sunmak, ulusal güvenlik politikalarını deklare etmek, askeri doktrinleri oluşturmak, angajman kurallarını belirlemek gibi diğer devlet uygulamalarını delillendirmek suretiyle uluslararası yapılageliş hukukunun gelişimine olanak sağlaması siber savaş bağlamında eşsiz katkılar sağlamaktadır[761]. Önceki tecrübeler gözetildiğinde, siber saldırıların incelikli ve belirsiz doğası gereği ve BM Güvenlik Konseyi'nin böyle bir saldırıya vaktinde cevap verip vermeyeceğinin belirsizliği nedeniyle devletlerin meşru müdafaa hakkını kullanmayı tercih edecekleri varsayılmaktadır[762].

Diğer konulara geçmeden önce BM Şartı'nın VII. bölümünde öngörülen barışın tehdidi, bozulması ve saldırı eylemi durumunda Güvenlik Konseyi'nce alınacak önlemlerin siber savaşa nasıl aktarılacağı konusu aydınlatılması gereken bir konudur. Güvenlik Konseyi'nce siber kuvvet kullanma yetkisi vermesi konusunda yaşanmış bir örnek bulunmamaktadır. Bu nedenle öğretide bu konuda ileri sürülen farklı görüşler üzerinde değerlendirme yapılmalıdır. Melzer, bu konuda amaçsal bir bakış açısıyla konuya yaklaşmakta ve BM Şartı'nın 42. maddesinin, Güvenlik Konseyi'nin siber uzayda silahlı kuvvet kullanımına yetki vermesi imkânından yoksun olduğu şeklinde yorumlanamayacağını savunmaktadır[763]. Melzer, meşru müdafaa eylemi ve hatta devletlerarası güç niteliği için gerekli eşiğin çok altında kalan siber tehditlere karşı, Güvenlik Konseyi'nin askeri kuvvet kullanımını içeren yerine getirme yetkisi verme gücünü taşıdığını ileri sürmektedir[764]. Buna paralel olarak Roscini, Güvenlik Konseyi'nin siber saldırıdan sorumlu olan devlete karşı saldırının devamının ve tekrarının önlemesi için özellikle BM Şartı'nın 41. maddesi kapsamında bir siber ablukanın uygulayabileceğini savunmaktadır[765].

---

[760] Sharp, 1999, s. 4.

[761] Kanuck, 2010, s. 1585.

[762] Graham, 2010, s. 89.

[763] Melzer, 2011, s. 18.

[764] Melzer, 2011, s. 19.

[765] Roscini, 2010, s. 111.

BM Şartı'nın VII. bölümünde düzenlenen barışın tehdit edildiğini, bozulduğunu veya barışa yönelik saldırı eylemi durumunda alınacak önlemleri belirlemekle yetkili organ Güvenlik Konseyi'dir. BM Şartı'nın 39. maddesi kapsamında belirtilen şekilde bir tehdit veya saldırının varlığını tespit ettiği takdirde Şartı'ın 40. maddesine göre taraflara tavsiyede bulunabileceği gibi, Şartı'ın 41. maddesi uyarınca kuvvet kullanma içermeyen diğer bir önlemi de tercih edebilir. Bu önlemler madde metninde belirtildiği üzere ekonomik ilişkilerin ve demiryolu, deniz, hava, posta, telgraf, radyo ve diğer iletişim ve ulaştırma araçlarının tümüyle ya da bir bölümüyle kesintiye uğratılmasını, diplomatik ilişkilerin kesilmesini içerebilir. Bu kapsamda ağa erişimin önlenmesi ya da kuvvet kullanma seviyesine varmayan diğer bir önlemin Güvenlik Konseyi tarafından alınmasına karar verilmesi Şart'ın 41. maddesine uygun olacaktır.

BM Şartı'nın 42. maddesi uyarınca Güvenlik Konseyi tarafından, Şart'ın 41. maddesinde öngörülen önlemlerin yetersiz kalacağı ya da kaldığı kanısına varılması halinde ise, uluslararası barışın ve güvenliğin korunması ya da yeniden kurulması için, hava, deniz ya da kara kuvvetleri aracılığıyla, gerekli görülecek her türlü girişimde bulunulabilecektir. Madde metninde ifade edildiği üzere bu girişimler gösterileri, ablukayı ve BM üyelerinin hava, deniz ya da kara kuvvetlerince yapılacak başka operasyonları içerebilir. Bu bağlamda madde metnine göre barışın tehdit edilmesi ya da barışa karşı saldırı söz konusu olduğunun tespiti durumunda Güvenlik Konseyi tarafından kuvvet kullanma mahiyetinde bir siber operasyona başvuru konusunda yetkilendirme yapılması olanaklıdır. Ancak Güvenlik Konseyi'nin yapısı gereği uygulamada bu kapsamda bir yetkilendirmenin pek de olası olmadığı söylenebilir.

Buraya kadar yapılan açıklamalar ışığında, hangi siber operasyonun kuvvet kullanma yasağı seviyesine eriştiği konusunda, siber operasyonun sonuçlarının önemli düzeyde zarara, kişilerde yaralanmaya ya da ölüme sebep olup olmadığına göre belirlenebileceği söylenebilir. Buna karşın, ortaya çıkan zararın niteliğinin ve kapsamının belirlenmesi zorluklar taşımaktadır. Zira bir siber operasyonun sebep olduğu veri kaybı, bilgisayar işlev aksamaları, finansal zararlar ya da insanlarda yaratacağı psikolojik etkiler üzerinden

değerlendirme yapılabilmesi için de bazı kıstaslar gerekli olacaktır. Bir sonraki başlıkta açıklanacağı üzere bu konuda Tallinn El Kitabı'nda Uluslararası Uzmanlar Grubu, UAD'nın *Nikaragua* yargılamasını dikkate almışlar ve bu davada kabul edilen ölçek/boyut ve etki (*scale and effects*) kıstasını benimsemişlerdir [766]. Bir siber operasyonun boyutu ve etkisi itibariyle kuvvet kullanımı teşkil edip etmediğinin tespiti için Tallinn El Kitabı 69. Kural'a göre, operasyonun şiddeti (*severity*), yakınlığı (*immediacy*), doğrudanlığı (*directness*), yayılabilirliği (*invasiveness*), etkilerin ölçülebilirliği (*measurability of effects*), askeri karakteri (military charackter) devlet dahiliyeti (*state involvement*) ve hukuka uygunluk karinesi (*presumptive legality*) kıstasları gözetilmelidir[767]. UAD *Nikaragua Davası*'nda BM Şartı hükümleri, devlet uygulamalarının zamanla değişebileceğini gözeterek oldukça dinamik şekilde yorumlandığından [768] bu kararda benimsenen kıstasların siber saldırılara yönelik uygulama olanağı söz konusu olmuştur.

3.2. SİLAHLI SALDIRI

3.2.1. Saldırı Eşiği

Kuvvet kullanma ile silahlı saldırı standartları farklı normatif amaçlara hizmet etmektedir. Kuvvet kullanma standardı, BM Şartı'nın 2/4 maddesinin ve ilgili uluslararası yapılageliş hukukunun yasaklayıcı kuralının ihlal edilip edilmediğini belirlerken silahlı saldırı kavramı, hedef devletin kuvvet kullanma yasağını ihlal etmeksizin kuvvet kullanmak suretiyle karşılık verip veremeyeceğini ortaya koyar[769]. Uluslararası hukukta yasaklanan kuvvet kullanma eylemi silahlı saldırıyı da içine alan daha geniş bir kavramdır. Kuvvet kullanma yasak olmasına karşın bu eyleme maruz kalan bir devletin karşılık olarak kuvvet kullanabilmesi hukuka uygun kabul edilmemektedir. Bunun için ilk olarak, uygulanan

[766] Schmitt, 2017, *Tallinn Manual 2.0.* s. 330.

[767] Gül, 2021, s. 59.

[768] Gray, 2008 s. 8.

[769] Schmitt, 2017, *Tallinn Manual 2.0.* s. 337.

kuvvet kullanma eyleminin belirli bir eşiği aşması ve silahlı saldırı düzeyine erişmesi gerekmektedir.

BM Şartı 51. maddesinde düzenlenen ve ayrıca yapılageliş hukukuna dayanan meşru müdafaa hakkının kullanılabilmesi için kuvvet kullanılması yeterli görülmemekte, eylemin ayrıca silahlı saldırı oluşturması gerekmektedir. Kuvvet kullanmanın en ağır seviyesini oluşturan silahlı saldırı eyleminin[770] sınırlarının çizilmesi, aynı zamanda kuvvet kullanma oluşturan bu eylemin hangi eşiğe varması halinde meşru müdafaa hakkının doğacağına dair objektif kıstasların belirlenmesi gerekir. Buna karşın uluslararası hukuka aykırı kuvvet kullanma veya tehdide eşit olması gereken siber operasyonlara ilişkin kesin bir eşik üzerinde uzlaşma bulunmamaktadır[771].

Bu noktada ayrıca ifade edilmelidir ki silahlı saldırı eşiğine varan bir saldırı eylemine silahlı çatışmalar hukukunun uygulanması söz konusu olmakla birlikte daha sonraki bölümde açıklanacağı üzere silahlı çatışmalar hukukunun uygulanabilmesi için gereken şartların meşru müdafaa şartlarına nazaran daha düşük olduğu gözetilmelidir. Zira kapsam, süre ve yoğunluk itibariyle *de facto* uluslararası silahlı çatışma oluşturan bir silahlı çatışmada *jus in bello* kurallarının uygulanması için gerekli silahlı saldırı eşiği meşru müdafaa için gereken silahlı saldırı eşiğinden farklıdır[772].

Uluslararası silahlı çatışmayı düzenleyen 1949 tarihli Cenevre Konvansiyonları ortak 2. maddesi eşiği, ayrıca çatışma yönetimi paradigması açısından BM Şartı'nın 2/4 ve 51. maddeleri eşiğine varmak için gerekli olan kuvvet kullanma boyutunun seviyesini belirlemeye yardım eder[773]. Belirtilen hükümler birlikte değerlendirildiğinde BM

---

[770] UAD *Nikaragua Davası*'nda, kuvvet kullanımının en ciddi biçimlerinin silahlı saldırı oluşturduğunu belirtmiş ve bunları kuvvet kullanımının daha az ciddi biçimlerinden ayırt etmiştir. bkz.; Gül, 2021, s. 59.

[771] Melzer, 2011, s. 9.

[772] Sharp, 1999, s. 76.

[773] Sharp, 1999, s. 77.

Şartı'ında düzenlenen "kuvvet kullanma" terimi, Cenevre Konvansiyonları'nda belirtilen "silahlı çatışma" terimine, BM Şartı 51. maddesine göre "silahlı saldırı" ise BM Genel Kurulu Saldırının Tanımı kararında benimsenen "saldırı eylemi"ne yakın bir anlam ifade etmektedir[774].

"Saldırı eylemine" ilişkin BM Genel Kurulu 14.12.1974 tarihli, 3314 sayılı Saldırının Tanımı Kararının[775] 1. maddesinde, saldırı (*aggression*) eylemi genel biçimde "bir başka devletin egemenliğine, ülke bütünlüğüne ya da siyasi bağımsızlığına karşı ya da BM Şartı'na aykırı herhangi bir biçimde silahlı kuvvet kullanma" olarak tanımlanmıştır. Saldırının Tanımı Kararı'nın 2. maddesinde ise gerçekleştirilen ilk eylemin "saldırıyı" oluşturacağı ve ayrıca eylemin saldırı olarak kabul edilebilmesi için yeterli bir yoğunlukta gerçekleşmesi gerektiği öngörülmüştür[776]. Kuvvet kullanmanın en ağır şeklini oluşturan silahlı saldırının yeterli yoğunluğa eriştiğinin tespitinde kullanılan ölçüt ise saldırının boyut ve etkileridir[777].

Saldırının Tanımı Kararı'nda saldırı eylemi olarak belirtilen eylemler UAD'nın *Nikaragua Askeri ve Yarı-Askeri Faaliyetler Davası*'nda da teyit edilmiştir. Divana göre de silahlı saldırı eylemi yalnızca yabancı düzenli orduların gerçekleştirdiği sınır-ötesi harekâtı değil, aynı zamanda "eğer bu harekât ölçüleri ve etkileri bakımından düzenli kuvvetlerce yapıldığında yalnızca bir sınır olayı olarak değil, fakat bir saldırı olarak değerlendirilecekse bir devletçe başka bir devletin ülkesine gönderilen silahlı çeteleri de kapsamaktadır[778]. Bu davada da belirtildiği üzere saldırının yoğunluk niteliğini

[774] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s. 517.

[775] BM Genel Kurulu. "Definition of Aggression (A/RES/29/3314)" Erişim: 12.06.2022 A/RES/29/3314 - Definition of Aggression - UN Documents: Gathering a body of global agreements (un-documents.net)

[776] Pazarcı, 2021, s. 555-556.

[777] Gül, 2021, s. 59.

[778] Pazarcı, 2021, s. 555-556.

göstermesi açısından kolay ve klasik bir örnek olarak ifade edilebilecek küçük sınır olayları gibi küçük silahlı çatışmalar saldırı olarak kabul edilmemektedir[779].

Bu konuda tereddüt oluşturan izinsiz şekilde devletin egemenlik alanına girilmesi konusunda, uluslararası hukukta tam bir açıklık bulunmazken, ülke devletinin kuvvet kullanma veya tehdit algılaması ve kendini savunması için başka bir seçenek bulunmaması halinde meşru müdafaa hakkının doğabileceği[780], bir diğer ifade ile eylemin silahlı saldırı olarak kabul edilebileceği savunulmaktadır. Bu bağlamda geleneksel silahlı saldırı eşiği devletlerin meşru müdafaa hakkı kullanabilmesi konusunda kritik bir çizgi oluşturmaktadır. Buna karşın, silahlı saldırı eşiğinin kesin çizgilerle belirlenmesi çok da mümkün olmayıp tereddüt yaratan durumlarda olayın gerçekleştiği şartlara göre değerlendirme yapılması ve meşru müdafaa hakkına ilişkin bölümde tartışılacağı üzere daha dar bir yorum şeklinin benimsenmesi gerekir.

Geleneksel silahlı saldırı kavramı için saldırının boyutu ve etkileri kıstası ortaya konulmakla çalışmanın konusunu oluşturan siber saldırılar yönünden bu kıstasın yeterli olup olmayacağının irdelenmesi gerekmektedir. Neredeyse her zaman geleneksel askeri güç ile diğer zorlama biçimleri arasında gri bir alanda bulunan siber operasyonlar BM Şartı taslağını hazırlayanlar tarafından öngörülememiştir. Ayrıca şu ana kadar ne devlet uygulamalarında ne de bilimsel çalışmalarda BM Şartı 2/4. maddesi kapsamında yasak olarak değerlendirilmesini gerektiren ölüme, yaralanmaya veya yok etmeye sebep olmayan siber operasyonlarda eşik yönünden açık bir kıstas konulamamıştır[781]. Birazdan bahsedileceği üzere Schmitt tarafından ileri sürülen kıstaslara yönelik önemli eleştirilerin getirildiği görülmektedir.

Tallinn El Kitabı 69. Kural'da benimsenen "boyut ve etki" ibaresi hemen yukarıda belirtilen *Nikaragua Davası*'ndan kaynaklanmaktadır. Mahkeme burada silahlı saldırı ile

[779] Pazarcı, 2021, s. 556.

[780] Sharp, 1999, s. 99.

[781] Melzer, 2011, s. 9.

sırf sınır çatışması farkını ortaya koymuştur[782]. Tallinn El Kitabı'nı hazırlayan uzmanlar, siber operasyon olmayan ve kuvvet kullanma olarak değerlendirilen bir eylem ile karşılaştırıldığında bahse konu siber operasyonun boyut ve etkisi itibariyle kuvvet kullanma oluşturabilecek bir eylemin söz konusu olması halinde bu kapsamdan hariç tutulması için bir sebep bulunmadığı konusunda fikir birliği halindedirler[783]. Bir diğer ifadeye göre, Tallinn El Kitabı 11. Kural uyarınca, kuvvet kullanma seviyesine varan bir siber saldırı oluşturmayan saldırıyla karşılaştırıldığında boyut ve etkiye göre bir siber operasyonun kuvvet kullanma oluşturması söz konusu olmaktadır[784].

Ayrıca Tallinn El Kitabı'nda siber saldırının silahlı saldırı niteliğini belirleyen unsurlar olarak boyut ve etki yanında sınır dışı olma boyutu benimsenmiştir[785]. Uluslararası Uzmanlar Grubu, silahlı saldırıya sebep olan sonuçları üreten siber operasyonların belirlenmesinde Tallinn El Kitabı 71. maddesi şerhinde bir silahlı saldırının sınıraşan unsurunun, saldırının diğer bir ülke sınırlarından bu devlet adına devlet dışı aktörler tarafından gerçekleştirilmesi halinde dahi her daim karşılandığı ifade edilmiştir[786]. Ülke içinde bulunan bir bilişim korsanı grubu tarafından yine ülke içinde bulunan özel ya da kamu varlıklarına yönelik olarak gerçekleştirilen tamamen ülke içi karaktere sahip bir siber saldırının ise silahlı saldırı oluşturmayacağı kabul edilmektedir[787].

Tallinn El Kitabı editörü olan Prof. Michael Schmitt'e göre[788], ekonomik ve politik zorlamayı silahlı kuvvet kullanımından ayıran belli başlı ölçütlerin bilgisayar ağı saldırılarında da (siber saldırı) uygulanabileceği yönündedir. Bir siber operasyonun

---

[782] Bu konuda bkz.: Rølsåsen, 2016, s. 23.

[783] Schmitt, 2017, *Tallinn Manual 2.0.* s. 331.

[784] Bu konuda bkz.: Rølsåsen, 2016, s. 23.

[785] Schmitt, 2017, *Tallinn Manual 2.0.* s. 346.

[786] Schmitt, 2017, *Tallinn Manual 2.0.* s. 340.; Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 245.

[787] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 245.

[788] Schmitt, 1999, s. 18-19.

boyutu ve yarattığı etkileri itibariyle silahlı saldırı seviyesine eriştiğinin tespiti konusunda ise Tallinn El Kitabı'nda sınırlı sayıda olmayan sekiz faktör üzerinden gerçekleştirilmektedir. Bunlar sırasıyla; operasyonun şiddeti (*severity*), yakınlığı (*immediacy*), doğrudanlığı (*directness*), yayılabilirliği (*invasiveness*), etkilerin ölçülebilirliği (*measurability of effects*), askeri karakteri (*military character*), devlet katılımı (*state involvement*) ve varsayımsal hukuka uygunluk / hukuka uygunluk karinesi (*presumptive legality*) oluşur[789]. Operasyonun şiddeti, *de minimis* kuralı[790] gereğince kişi veya eşyada fiziki zararla sonuçlanan siber harekâtın kuvvet kullanma olarak nitelendirilmesini sağlar. Sonuçlar ne kadar kritik ulusal çıkarları etkiliyor ise siber operasyon o ölçüde kuvvet kullanma olarak tanımlanmasına katkı sağlayacaktır. Bu açıdan sonuçların kapsamı, süresi ve yoğunluğu önem derecesinin takdirinde büyük bir etki taşır[791].

Schmitt'in önerdiği bu kıstaslar operasyonun nicel ve nitel yönlerini gözeterek olay bazında incelemeye dayanır. Bu yaklaşımın olumsuz tarafının ise, kıstasların objektif ölçülebilir değişkenler olmayıp öznel bir karaktere sahip olduğu ifade edilmektedir[792]. Bu noktada Schmitt'in ölçütleri bazı kusurlar barındırdığı için eleştirilmektedir[793]. Örneğin, zorlamanın meşru, kuvvet kullanmanın ise meşru olmadığı kabul edildiği halde siber saldırının zorlama veya kuvvet kullanma oluşturup oluşturmadığının tespitinde hukuka uygunluk karinesinin bir faktör olarak kabul edilmesi doğru görülmemektedir[794]. Schmitt'in ölçütlerinde eleştiri konusu olan bir başka husus, siber saldırı anında saldırının

---

[789] Schmitt, 2017, *Tallinn Manual 2.0.* s. 334-336.; Terimlerin Türkçe çevirisi için bkz.; Gül, 2021, s. 45.

[790] Latince'de *"de minimis"* kavramı önemsiz şeyler anlamına gelmekte olup "*de minimis non curat lex*" kuralı gereğince önemsiz ve küçük şeyler hukukun konusu değildir. Hukuk sözlüğü için bkz. https://tureng.com/tr/turkce-ingilizce/de%20minimis Erişim: 05.11.2022

[791] Schmitt, 2017, *Tallinn Manual 2.0.* s. 334.

[792] Afroditi, 2010, s. 13-14.

[793] Hoisington, Matthew. (2009). *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, Boston College International and Comparative Law Review, Cilt:32, Sayı:2, Makale:16, s. 452.

[794] Barkham, Jason (2001). *Information Warfare and International Law on the Use of Force*. International Law and Politics, Cilt:34, s. 85.

boyutunun ve müsaade edilen cevabın değerlendirilememesidir. Özellikle de siber saldırının zaman bombası gibi sonuçlarının sonradan ortaya çıkması durumunda olduğu üzere yukarıda ifade edilen kıstasın uygulanması her zaman mümkün olmayacaktır[795].

Yeni bir alan olarak siber saldırılarla ilgili öğretide çoğu konuda farklı görüşlerin bulunması yanında bir siber operasyonun hangi durumda siber saldırı oluşturacağı konusunda siber saldırının doğasının nasıl anlaşıldığına bağlı olarak üç ana yaklaşım bulunmaktadır[796]. Bunlar araç temelli[797], hedef temelli ve sonuç ya da etki temelli yaklaşımlardır. Cenevre Konvansiyonları ortak 2. maddesinde uluslararası silahlı çatışmanın varlığını tespit etme konusunda Jean Pictet tarafından ortaya atılan kıstaslar üzerinde uluslararası uzlaşı oluşmuştur. Bu kıstaslar aynı zamanda belirli bir kuvvet kullanımının silahlı saldırı seviyesine varıp varmadığının değerlendirilmesinde de yararlı bir rehber olmuştur[798]. Pictet'in kuvvet kullanımı ölçütlerinin (kapsam, süre ve yoğunluk) siber saldırıları da içeren geleneksel olmayan güç kullanımına uygulanmasına olanak sağlayacak üç farklı çözümsel yöntem bulunmaktadır. Bunlar sırasıyla, araç temeline dayalı yaklaşım, etki temeline dayalı (ya da sonuç temelli) yaklaşım ve son olarak kusursuz sorumluluk yaklaşımıdır[799].

---

[795] Barkham, 2001, s. 86-87.

[796] Bu konuda bkz.: Rølsåsen, 2016, s. 22. Bir siber saldırının kuvvet kullanma yasağı kapsamında olup olmadığının tespiti konusunda araç ve etki temelli olmak üzere iki yaklaşımın benimsendiğine dair bkz.: Erdem ve Özocak, 2019, s. 135.

[797] Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması'nda kabul edilen yaklaşım araç temelli olup saldırının amacı ya da etkilerinden ziyade gerçekleştirildiği alan olan siber uzay merkeze alınmaktadır. Bunun için bkz.: Hathaway ve diğerleri, 2012, s. 826.; Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması, s.9. Erişim: 17.12.2021

Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO.pdf

[798] Graham, 2010, s. 91.

[799] Graham, 2010, s. 91.

Buradan hareketle öğretide *jus ad bellum*'un siber saldırılara uygulanabilirliği üzerine yapılan tartışmalarda bir siber saldırının ne zaman silahlı meşru müdafaa hakkını tetikleyeceğini belirlemede üç görüş mevcuttur. Bunlar; araç temelli yaklaşım, hedef temelli yaklaşım ve etki temelli yaklaşımdır[800]. Bunlar arasında araç ve hedef temelli yaklaşımın, olayın kolaylıkla nitelendirilebilmesi nedeniyle açık bir avantaj taşıdığı kabul edilmektedir. Buna karşın, siber saldırıların karmaşıklığını karşılamak açısından çok dar olmakla birlikte diğer yandan aşırı kapsayıcı oldukları ifade edilmektedir[801].

Hedef temelli yaklaşımı benimseyen ABD ve bir kısım yazarlara göre, bir siber saldırının hedefi olan bilgisayar ağının işlevini bozmak ve altını oymak amaçlanmaktadır[802]. Hedef temelli yaklaşıma örnek olarak gösterilebilecek kritik altyapı tesislerine yönelen göreceli olarak zararsız siber saldırılara karşı konvansiyonel silahlı saldırı ile cevap verilebileceğinin kabul edilmesi bu yaklaşımın çok geniş ve orantısız misillemeye yol açabileceği için eleştirilmektedir[803].

Saldırının sonuçlarına odaklanan[804] etki temelli teste göre, bir eylem insanlara veya çevresine önemli hasarlara sebep oluyorsa fiziki güç kullanımının gereklilikleri yerine gelmiş kabul edilmektedir[805]. Bu görüşe göre, bir güç merkezinin patlamasına ya da bir uçağın düşmesine sebep olan siber saldırılar silahlı saldırı kabul edilecek iken borsanın düşmesine ya da ulaşım faaliyetlerinin durmasına sebep olan ekonomik ya da sosyal etkileri olan bir siber saldırı silahlı saldırı olarak kabul edilmemektedir[806].

---

[800] Hathaway ve diğerleri, 2012, s. 845.

[801] Bu konuda bkz.: Rølsåsen, 2016, s. 23.

[802] Hathaway ve diğerleri, 2012, s. 826.

[803] Piatkowski, 2017, s. 275.; Hedef temelli yaklaşımı benimseyen Hathaway ve diğerlerine göre. Ayrıntılı bilgi için bkz.; Hathaway ve diğerleri, 2012, s. 826.

[804] Piatkowski, 2017, s. 275.

[805] Benatar, 2009, s. 390.; Waxman, 2011, s. 432.

[806] Waxman, 2013, s. 112.

Siber hukuk alanında çalışan akademisyenlerin çoğunluğu tarafından siber kuvvet kullanmanın geleneksel anlamda kuvvet kullanmaya eşit oluğuna dair etki-temelli yaklaşım benimsenmektedir[807]. Bu yaklaşımın kendi içinde barındırdığı bir kusur olarak, fiziki zarara veya insan kaybına sebep olmayan siber saldırılar konusu gösterilmektedir. Buna örnek olarak, derhal bir insan kaybına sebep olmasa da tüm ülke çapında mevcut iletişimin durmasına sebep olma durumu gösterilebilir[808]. Etki temelli teste yönelik olarak getirilen bir başka bir eleştiri ise, ölüm ya da fiziki zarar üzerinden değerlendirme yapılması ve teknolojiye bağımlı toplum yapısına uygun düşmediği ve ayrıca siber saldırıların etkilerinin ölçülmesi ve doğrudan sonuçlarının değerlendirilmesindeki zorluklar olmuştur[809]. Gerçekten de bir siber saldırı sonucunda bir bilişim sisteminin en kritik verilerinin silinmesi ya da işlevsel aksamalara sebep olunması, saldırının fiziki zarar kapsamında değerlendirilip değerlendirilmeyeceğine dair soru işaretleri doğurmaktadır.

Bu üç yaklaşım yönünden genel bir değerlendirme yapıldığında bu yaklaşımların her olayda beklenen sonuca ulaşmayacağı, zira verilerin yok edilerek bankacılık sektörüne diz çöktürülmesinin hiç bir silahlı kuvvet kullanımı, ekonomik veya politik baskı vasıtasıyla sağlanamayacağı için araçsal yaklaşımın her durumda siber saldırılarda geçerli olmadığı yönündedir[810]. Öğretide bir siber saldırı, siber kuvvet kullanımını içererek BM Şartı madde 2/4'ün kapsamını genişleten silahlı kuvvet kullanımı örneğine benzetilmektedir[811]. Kuvvet kullanımı konusuna geniş anlamda bu bakış açısına sahip olanlara göre araçsal ve etki temelli yaklaşım yöntemleri ile siber operasyonların kuvvet kullanma yasağı kapsamında değerlendirilip değerlendirilemeyeceği belirlenmektedir.

[807] Afroditi, 2010, s. 13.

[808] Afroditi, 2010, s. 13.

[809] Waxman, 2013, s. 112.

[810] Benatar, 2009, s. 391.

[811] Benatar, 2009, s. 387.

Siber operasyonlar bakımından araç temelli yaklaşım, siber saldırının silahlı bir saldırı olarak kabulü için ISP'nin veya internet kablolarının bombalanmasında olduğu gibi geleneksel silahın kullanılmasını ve saldırının belirli bir ağırlığa varmasını gerektirdiğinden haklı olarak siber saldırıların yapısına uygun olmadığından öğretide eleştirilmektedir[812]. Bu konuda uluslararası yargı kararları bağlamında kullanılan silahın tek başına belirleyici unsur olmadığı dikkate alınmalıdır. UAD başta *Nikaragua* olmak üzere *Petrol Platformu Davası* (Oil Platform)[813], *DRC&Uganda* ve *Filistin Duvar Danışma Görüşü*'ne[814] ilişkin kararlarında silahlı saldırı kavramı üzerinde durmuştur[815]. *Nikaragua* Davası'nda UAD silahlı saldırının tanımının yapılmadığını ve antlaşmalar hukukunun bir parçası olmadığını belirtmiş, buna karşın *Nükleer Silahlar Danışma Görüşü*'nde[816] BM Şartı madde 51'in özel bir silaha gönderme yapmadığını, kullanılan silaha bakılmaksızın her kuvvet kullanımına uygulanabileceğini tespit etmiştir[817].

Bir operasyonda bilgisayarın kullanılması, operasyonun kuvvet kullanımına eşit kabul edilip edilmeyeceği konusunda bir etki taşımamaktadır. Bir diğer ifadeyle siber bağlamda, kullanılan enstrüman kuvvet kullanma eşiğinin geçilip geçilmediğini belirlememekte olup, bunun yerine operasyonun sonuçları ve çevreleyen koşullar belirleyici kabul edilir[818]. Buna göre, siber operasyonun kuvvet kullanma eşiğini aşıp aşmadığı her bir olay bazında değerlendirilmelidir[819]. Genel anlamda siber faaliyetlerdeki

---

[812] Hathaway ve diğerleri, 2012, s. 845-846.

[813] UAD, "*Case Concerning Oil Platforms*", 06 Kasım 2003, Erişim: 12.06.2022 https://www.icj-cij.org/public/files/case-related/90/090-20031106-JUD-01-00-EN.pdf

[814] UAD, "*Advisory Oppinion of the International Court of Justice on the Legal Consequences of the Construction of a Wall in The Occupied Palestinian Territory*", 09 Haziran 2004, Erişim: 05.11.2022 https://www.un.org/unispal/document/auto-insert-178825/

[815] Gray, 2008 s. 129.

[816] UAD, "*Legality of the Threat or Use of Nuclear Weapons*", 08 Temmuz 1996, Erişim: 12.06.2022 https://www.un.org/law/icjsum/9623.htm

[817] Roscini, 2010, s. 114.

[818] Schmitt, 2017, *Tallinn Manual 2.0.* s. 328.

[819] Position Paper, 2021, s. 6.

küçük aksamalar ve hedeflenen siber altyapı unsurunun doğası, siber operasyonun kuvvet kullanma olarak nitelendirilmesinde dikkate alınmaz[820]. Zira Tallinn El Kitabı'nın 69. Kural'ı gereğince, siber olmayan bir operasyon ile bir siber operasyon karşılaştırılarak ölçek ve etkisi itibariyle kuvvet kullanma seviyesine erişip erişmediği değerlendirilmektedir. Bu kıstasa göre yapılacak bir değerlendirme esnasında siber altyapı unsurunun doğası ya da yapısı tek başına belirleyici kabul edilmemektedir. Örneğin, kritik altyapı unsuruna yönelen bir siber saldırı, ölçek ve etki kıstası itibariyle gerekli eşiği aşmadığı takdirde tek başına kuvvet kullanma olarak değerlendirilmezken, gerekli eşiği aşan bir siber saldırı, kritik altyapı unsurunu hedef alsa dahi uzmanlar tarafından kuvvet kullanma olarak kabul edilmemektedir.

BM Şartı'nın 41. maddesinde belirtilen iletişim araçlarının silahlı kuvvet kullanma olarak kabul edilmemesi, BM Genel Kurulu'nun silahlı saldırı tanımındaki eylemler listesi ve NATO'nun siber saldırıların NATO Sözleşmesi'nin 5. maddesi kapsamında ortak meşru müdafaa sebebi olarak kabul etmemesi nedeniyle araç temelli yaklaşımın desteklendiği[821] düşünülebilir. Buna karşın siber saldırıların şu ana kadar yarattığı tehdidin boyutunun düşük seviyede olmasının bu tür yaklaşımlara sebep olduğu, gelecekte oluşturabileceği tehditler yönünden öngörülü bir yaklaşımın benimsenmesinin daha uygun olacağı değerlendirilmelidir.

Hedef temelli yaklaşım ise, siber saldırının hedefi olan bilişim sistemlerinin kritik altyapı unsurlarından olması ve ulusal güvenliği hedef alması halinde herhangi bir zarara yol açıp açmadığına bakılmaksızın silahlı meşru müdafaa hakkını doğuracağı gerekçesiyle kolaylıkla sebep olacağı savaş ortamının uluslararası toplumun güvenliğini tehdit edeceği gerekçesiyle eleştirilmektedir[822]. Bu bağlamda kritik altyapı unsurlarına yönelecek herhangi bir siber saldırının silahlı saldırı düzeyine erişmesi için hangi eşiğin kabul edileceği konusu da tartışmaya açık bir konudur.

---

[820] Schmitt, 2017, *Tallinn Manual 2.0.* s. 328.

[821] Hathaway ve diğerleri, 2012, s. 846.

[822] Hathaway ve diğerleri, 2012, s. 847.

En yaygın analiz yöntemi olan[823] etki temelli yaklaşım gerek öğretide daha çok destek bulmakta ve Tallinn El Kitabı'nda da bu yaklaşım tercih edildiğinden uygulamada bu yaklaşımın benimsendiği görülmektedir. Tallinn El Kitabı'nın editörü olan Schmitt'e göre silahlı saldırı eyleminin güç kullanımının en ağır şekli olması nedeniyle en az kuvvet kullanma boyutuna erişmesi, bir diğer ifade ile ortaya çıkan zararın ya da niyetlenen zararın belirli bir ciddiyet eşiğine erişmesi gerekli görülmektedir [824] . Kullanılan konvansiyonel silahın ya da kitlesel imha silahlarının etkileri ile siber saldırının karşılaştırılması suretiyle eylemin silahlı saldırı seviyesine eriştiği kabul edilirken mantıksal çıkarım yapılarak bu tür zararlara ancak kritik altyapı tesislerine karşı gerçekleştiren saldırıların sebep olacağından hareketle siber eylemler nitelendirilebilmektedir[825].

Nükleer güç istasyonunda nükleer erimeye sebep olunması, yoğun bir nüfusun bulunduğu bölgenin yukarısındaki baraj kapaklarının açılması, kötü hava şartlarında yoğun hava trafiğinin işlemez hale getirilmesini amaçlayan siber saldırılar ölüm, yaralanma ve yok etme açısından ağır sonuçlara sahip olduğundan Şart'ın 2/4 maddesi anlamında yasaklanan güç kullanımı örneklerini oluşturur[826]. Belirtilen zararlara sebep olan siber saldırıların etki temelli yaklaşıma göre silahlı saldırı olarak kabulü ve zarar gören devlete meşru müdafaa hakkına başvuru imkânını sunması konusunda herhangi bir tereddüt bulunmamaktadır.

Siber uzayda gerçekleştirilen devlet faaliyetlerini sınırlandırabilecek iki genel durum bulunmaktadır[827]. İlk olarak, yasak olan dolaylı kuvvet kullanma oluşturan ya da bunu

---

[823] Blank, 2013, s. 415.

[824] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 245.

[825] Bkz. Streltsov, 2017, s. 7.

[826] Melzer, 2011, s. 7.

[827] Sharp, 1999, s. 112.

destekleyen siber uzaydaki devlet eylemleri de hukuka aykırılık oluşturur. Buna örnek olarak veri tabanında değişiklik yapılması sonucunda darbeye sebep olmak gösterilmektedir. İkincisi ise, bir devletin bilişim alt yapısını başka bir devlete karşı gerçekleştirilecek saldırı için kullanıma açması gösterilebilir.

Ayrıca kuvvet kullanma seviyesine ulaşmayan her siber saldırı eyleminin uluslararası hukuka uygun hale geldiği sonucu çıkarılamaz. Zira bir siber operasyon, kuvvet kullanma yasağına aykırı olmasa dahi egemenliğin ya da içişlerine karışma yasağının ihlalini oluşturabilir[828]. Kuvvet kullanma eşiğinin altında kalan bu siber operasyonlar, yapılageliş kuralı olarak içişlerine karışmama prensibi kapsamında yasaklanmakla birlikte, başka bir devlet tarafından silahlı saldırı eşiğine erişmeyen uluslararası hukuka aykırı eylemlere karşılık olarak yasal karşı önlemi oluşturabilirler[829].

Nikaragua Davası ışığında değerlendirildiğinde siyasal amaçlı siber saldırı gerçekleştiren bir haktivist grubunun finansal açıdan desteklenmesi kuvvet kullanma yasağına aykırı kabul edilmeyecek [830] ancak bu eylem karışma olarak değerlendirilebilecektir. Yine hükümetin güvenilirliğine zarar veren ve yıkıcı olmayan psikolojik siber operasyon veya diğer bir devlete olumsuz ekonomik sonuçlar doğuran elektronik ticaret yasağının altının oyulması kuvvet kullanma olarak değerlendirilmemektedir[831]. Bir siber operasyonun kuvvet kullanma olarak kabulü için mutlak suretle devletin silahlı güçleri tarafından gerçekleştirilmesi de zorunlu olmayıp istihbarat birimleri ya da devlete atfedilebilmesi kaydıyla sözleşmeli özel bir yüklenici tarafından gerçekleştirilmesi halinde de mümkün kabul edilmektedir[832].

[828] Schmitt, 2017, *Tallinn Manual 2.0.* s. 330.

[829] Melzer, 2011, s. 6.

[830] Schmitt, 2017, *Tallinn Manual 2.0.* s. 331.

[831] Schmitt, 2017, *Tallinn Manual 2.0.* s. 331.

[832] Schmitt, 2017, *Tallinn Manual 2.0.* s. 330.

Gerekli şiddeti içeren bir siber operasyona sığınak ya da güvenli alan sağlayan bir devletin eyleminin kuvvet kullanma olup olmayacağı konusunda Uzmanlar Grubu'nda fikir ayrılığı oluşmuştur[833]. Azınlık, sırf bir güvenli alan sağlamanın kuvvet kullanma oluşturmayacağını savunurken, Uzmanların tamamının söz konusu devlet açısından özen gösterme yükümlülüğünün ihlalinin söz konusu olabileceğini kabul ettiği görülmektedir. Çoğunluk görüşü ise, siber suç için güvenli alan açan devletin bu eyleminin yanında azımsanmayacak bir destek sağlaması veya devlet dışı guruba siber savunma sağlaması gibi hallerde, belirli koşullar altında, eylemin kuvvet kullanma oluşturacağı yönündedir.

Buna göre, diğer bir devlete yönelik siber operasyon gerçekleştirmesi için organize silahlı bir gruba kötü amaçlı yazılım temin etmek ve siber saldırı konusunda gerekli eğitimi vermek kuvvet kullanmaya eşit kabul edilmekte[834] ve buna karşın bu grupların sadece finanse edilmesi kuvvet kullanma olarak kabul edilmemektedir[835].

Burada son olarak ifade edilmelidir ki kuvvet kullanma eşiği seviyesinin belirlenmesi caydırıcılık açısından da önem arz etmektedir. Gerçekleştirilen bir siber saldırıya karşı daha düşük eşikte tanınan meşru müdafaa hakkının saldırganın daha ileri düzeyde saldırma olasılığını azaltacağı gibi, saldırganı daha düşük seviyeli siber saldırılara yeltenmekten de alıkoyabileceği kabul edilmektedir[836]. Buna ilaveten, devletin sorumluluğu kurallarıyla birlikte değerlendirildiğinde devletlere daha geniş ölçekte silahlı meşru müdafaa hakkının tanınması durumunda, devletlerin kendi ülkelerinden kaynaklanan ve diğer devletlere yönelik olan siber saldırılarda çok daha sıkı tedbirler almasına yol açacağı gerekçesiyle silahlı saldırı eşiğinin düşük tutulmasının olumlu sonuçları olacağı açıktır[837].

---

[833] Schmitt, 2017, *Tallinn Manual 2.0.* s. 332.

[834] Schmitt, 2017, *Tallinn Manual 2.0.* s. 332.

[835] Schmitt, 2017, *Tallinn Manual 2.0.* s. 331.

[836] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.228.

[837] Waxman, 2013, s. 117.

3.2.2. Silahlı Saldırı Oluşturan Eylemler

BM Şartı'nın sadece kurumsallaşmaya yönelik bir doküman olmadığı, ayrıca kuvvet kullanımı konusunda devletlerin davranışlarını düzenlemeye yönelik norm yaratan bir yapısı bulunduğu görüşü[838] benimsenirse, yaptırım konusunun devletlerin iradelerine bırakılmadığı kabul edilmelidir. Kelsen'in uluslararası hukukun, bir devletin belli bir davranışını belirten veya izin veren bir normlar sistemi olduğu[839] şeklindeki tespiti bu yaklaşımı desteklemektedir.

BM Şartı'nda devletlerarası kuvvet kullanımına dair üç farklı terim kullanılmıştır. Bunların ilki, madde 2/4'de belirtilen "*kuvvet kullanımının"* veya tehdidin yasaklanması olup, ikincisi, madde 39'da öngörülen barışın tehdidi yahut bozulması ve "*saldırı eylemi"* durumudur. Bir diğer durum ise madde 51'de kullanılan *"silahlı bir saldırı"* terimidir. Bu çelişki silahlı saldırı (*armed attack*) ile saldırı (*aggression*) kavramları arasında soru işaretlerin oluşmasına sebep olmuştur[840]. Ayrıca BM Şartı'nın 51. maddesinde meşru müdafaa hakkının doğması için silahlı bir saldırının vuku bulması bir gereklilik olarak ortaya konulmakla birlikte, Şart kapsamında silahlı saldırının tanımı da yapılmış değildir.

Saldırının tanımı ise 1974 yılında BM Genel Kurulu tarafından yapılmıştır. *Saldırının Tanımı Kararı*'nın 2. maddesinde, bu nitelikli bir eylemin saldırı olarak kabul edilebilmesi için öncelikle eylemin bu yönde ilk hareket eden devlet eylemi olması ve bunun yanında eylemin yeterli yoğunlukta olması gerektiği kabul edilmiştir[841]. Anılan kararın 3. maddesi uyarınca az önce belirtilen koşulların varlığı halinde şu eylemler saldırı niteliği taşımaktadır: bir devletin ülkesinin başka bir devlet silahlı kuvvetlerince saldırıya ya da istilaya uğraması; bombalanması ya da başka silahların kullanılması; bir devletin

[838] Arend ve Beck, 1993, s. 29.

[839] Kelsen, 2012 s. 19.

[840] Ruys, 2010, s. 127.

[841] Pazarcı, 2021, s. 556.

limanlarının ya da kıyılarının bir başka devlet silahlı kuvvetlerince ablukaya alınması; bir devletin karar, deniz ya da hava kuvvetlerine ve sivil uçaklarına ve gemilerine bir başka devletin silahlı kuvvetlerince saldırılması; bir devletin ülkesinde izinli olarak bulunan bir başka devlet silahlı kuvvetlerinin bu izin koşullarına aykırı olarak kuvvet kullanması ya da izin süresinden sonra da zorla burada kalması; bir devletin ülkesinin bir başka devletçe bir üçüncü devlete karşı saldırı eylemi amacıyla kullanılmasına izin verilmesi; bir devletçe ya da onun adına başka bir devlete yukarıda belirtilen saldırı eylemlerinden sayılacak yoğunlukta silahlı kuvvet kullanma eylemlerinde bulunan silahlı çetelerin ya da grupların, düzen-dışı kuvvetlerin ya da paralı askerlerin gönderilmesi ya da böyle bir harekette özlü biçimde yer alınması[842].

Soruna silahlı saldırı temelinde bakıldığında silahlı bir saldırının unsurları genel olarak, silahlı saldırıyı hangi eylemlerin oluşturduğu (*ratione materiae*), silahlı saldırının ne zaman gerçekleştiği (*ratione temporis*) ve silahlı saldırının kimden kaynaklanması gerektiği (*ratione personae*) perspektifi üzerinden çözümlenir[843]. Hangi eylemlerin silahlı saldırı oluşturduğu konusunda belirtilmelidir ki her silahlı saldırı, kuvvet kullanımı oluşturur fakat bazı kuvvet kullanımı eylemleri silahlı saldırı seviyesine erişir[844]. UAD'nın *Nikaragua Davası*'nda yaptığı tespite göre ölçek ve etki açısından küçük sınır uyuşmazlıkları silahlı saldırı kapsamında değerlendirilemez[845]. Buna mukabil bir görüşe göre, küçük çaplı sınır çatışmaları, ölümcül kuvvet kullanımını içermesi halinde, otomatik olarak silahlı saldırı kavramı dışında kalmayacak, bazı hallerde meşru müdafaa hakkını tetikleyebilecektir[846].

Silahlı saldırı eylemi zamansal açıdan değerlendirildiği takdirde, *Nikaragua Davası*'nda da sözü edilen "*ratione temporis"* sınırlama nedeniyle meşru müdafaa hakkının

[842] Pazarcı, 2021, s. 556.

[843] Ruys, 2010, s. 126.

[844] Benatar, 2009, s.392.

[845] Hathaway ve diğerleri, 2012, s. 844.

[846] Ruys, 2010, s. 157.

kullanılabileceği zaman dilimi Güvenlik Konseyi tarafından gerekli önlemlerin uygulanacağı ana kadardır[847]. Bu yönüyle zamansal sınırlama silahlı saldırı eyleminin zamansal çerçevesini belirlemektedir. Belirtilmesi gereken diğer husus ise bir eylemin sonuçları itibariyle silahlı saldırı eşiğine ulaşması halinde dahi saldırıyı gerçekleştiren devletin savaşma niyetini taşımamasının etkili olup olmadığı konusudur ki buna göre silahlı saldırı nitelendirilebilmektedir.

Silahlı saldırı, bir devlete ait silahlı güçlerin diğer bir devlete karşı kullanılması suretiyle doğrudan ya da silahlı grupların, düzensiz veya paralı grupların gönderilmesi suretiyle dolaylı olarak gerçekleştirilebilir. [848]. Düzenli silahlı birliklerin diğer devletin sınırından geçirilmesi ya da aynı amacı gerçekleştirmeye yönelik düzensiz birliklerin veya diğer silahlı grupların gönderilmesi silahlı saldırı oluştururken, isyancı ya da diğer silahlı gruplara silah sağlama ve diğer yardım eylemleri silahlı saldırı eşiğine varan faaliyetler olarak kabul edilmemektedir[849]. Öğretide silahlı bir saldırının muhtemelen ilan edilmiş bir savaş, bir bölgenin işgali, deniz ablukası, bir bölgeye, askeri güçlere ve yurtdışındaki vatandaşlara yönelik silahlı kuvvet kullanımını kapsayabileceği ifade edilmektedir[850]. Bir görüşe göre silahlı saldırı, hedef devletin toprakları dışından kaynaklanan, küçük çaplı, münferit silahlı veya suç konusunu oluşturan faaliyetler seviyesinin üzerinde kalan ve bir devletin ülkesine, uluslararası sularda veya hava ülkesi veya başka bir devlet ülkesinde yasal olarak bulunan askeri gemilerine veya hava araçlarına ya da "tartışmalı olmakla birlikte" belirli durumlarda yurtdışındaki vatandaşlarına karşı gerçekleştirilen kuvvet kullanımıdır[851].

Devletlerin uygulamalarına göre ise, gereklilik ve orantılılık kıstaslarına uygun şekilde, küçük çaplı bombardıman, topçu ateşi, deniz ya da hava saldırıları, malvarlığı hasarı veya

---

[847] Mutlu, 2016, s. 154.

[848] Khan, Kamal Ahmad. (2017). *Use of Force and Human Rights under International Law*, Athens Journal of Law, Cilt:3, Sayı:2. s. 145.

[849] Blank, 2013, s. 413.

[850] Lin, 2010, s. 72.

[851] Gill ve Ducheine, 2013, s. 443.

yaşam kaybı oluşturan veya oluşturma kapasitesine sahip olması halinde, BM Şartı'nın 51. maddesini aktive edebileceği kabul edilmektedir[852]. Güvenlik Konseyi'nin ABD'ye karşı gerçekleştirilen 9/11 saldırısı nedeniyle meşru müdafaa hakkının onaylanmasına ilişkin kararında kaçırılan uçakların silah olarak kabul edilmesi de bu kapsamda değerlendirilebilir[853]. Meşru müdafaa başlığı altında tartışılacak ve bu noktada ifade edilmesi gereken bir diğer husus ise 9/11 saldırısında olduğu üzere devlet dışı aktörler tarafından gerçekleşen silahlı saldırı düzeyindeki bir saldırının da meşru müdafaa hakkının kullanılmasına sebep olabileceği hususudur[854]. Dolayısıyla mevcut uluslararası hukuk kuralları kapsamında oluşan devlet uygulamalarına göre silahlı saldırının mutlak suretle bir devlet tarafından gerçekleştirilmesi de zorunlu değildir.

3.2.3. Silahlı Saldırı Niteliğindeki Siber Saldırılar

Siber saldırılar, geleneksel kinetik, biyolojik, kimyasal ve nükleer silahların erişilebilirliğine bağlı değilken siber uzayı oluşturan gerekli altyapı olmadan gerçekleştirilemezler[855]. Siber saldırıların bu özelliği siber altyapı unsurlarına karşı gerçekleştirilen fiziki saldırılar ile farkını da ortaya koymaktadır. Siber uzayda ya da siber uzay aracılığıyla gerçekleştirilmeyen bir eylemin etkileri ile siber uzayda gerçekleştirilenler ile aynı etkilere sahip olması halinde dahi, eylemin siber saldırı olarak nitelendirilmesini engellemektedir. Bu yönüyle siber uzayda gerçekleşen operasyonların etkileri itibariyle silahlı saldırı düzeyine erişip erişmediğinin tespitinde de kuvvet kullanmanın tespitinde kullanılan boyut ve etki kıstasının kullanıldığı belirtilmelidir.

Bütün devletler meşru müdafaa hakkının söz konusu olabilmesi için silahlı bir saldırının varlığı konusunda görüş birliği içinde iseler de bir önceki konu başlığı altında ortaya konulduğu üzere uluslararası çevrelerde hangi eylemlerin silahlı saldırıyı oluşturduğu

---

[852] Ruys, 2010, s. 155.

[853] Rølsåsen, 2016, s. 33.

[854] Blank, 2013, s. 414.

[855] Melzer, 2011, s. 13.

konusunda uzlaşma bulunmamaktadır[856]. Bu bağlamda hangi siber saldırıların silahlı saldırı düzeyine eriştiğinin tespiti gereklidir. Zira silahlı saldırıya eşit siber saldırıların gerçekleştirilmesi, saldırıya uğrayan devlete meşru müdafaa hakkına başvurma imkânı sağlar[857]. Buna karşın, siber saldırı ya da devam eden bir dizi siber saldırının, meşru müdafaa hakkına başvuracak biçimde kuvvet kullanma hakkını tetikleyecek bir silahlı saldırı oluşturup oluşturmayacağı sorusuna, silahlı saldırı teriminin bir antlaşma veya uluslararası bir antlaşmada tam olarak tanımlanmış olmaması nedeniyle kolay bir cevap bulunamamaktadır[858]. Bu konuda UAD'nin *Petrol Platformu Davası*'nda ortaya koyduğu bir dizi eylemin kümeli etki kıstasının dikkate alınması gerekir[859].

Bu konuda önceleri modern füzeler ve deniz mayınlarında olduğu üzere siber saldırılar konusunda da soru işaretleri ortaya çıkmıştır[860]. Gelinen son aşamada öğretide genel olarak siber saldırıların uluslararası saldırı suçu oluşturabileceği gibi silahlı saldırı kapsamında değerlendirilebileceği ve yasal meşru müdafaa hakkına sebebiyet verebileceği kabul edilmekte ise de[861] bu konuda uluslararası alanda kabul görecek nesnel bir kıstas bulunmamaktadır. Meşru müdafaanın ön şartı olan saldırı türü silahlı saldırı olup diğer anlamda uluslararası saldırı suçu ise BM Güvenlik Konseyi'nin BM Şartı'nın VII. Bölümü'ne göre kuvvet kullanımını gerektiren saldırı şeklidir[862]. Barışa karşı tehdit, barışın bozulması ve saldırı eylemine eşit olan siber saldırılar Güvenlik Konseyi'nin, siber operasyonun Şart'ın 2/4 ve 51. maddesi kapsamında "güç" ya da "silahlı saldırı"

---

[856] Gray, 2008 s. 128.

[857] Melzer, 2011, s. 6.

[858] Graham, 2010, s. 90.

[859] *Petrol Platformu Davası*'na ilişkin bir karar incelemesi için bkz.; Bagheri, Saeed. (2013). *Uluslararası Adalet Divanı'nın Petrol Platformları'na İlişkin Kararının Değerlendirirlmesi,* Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt:17, Sayı:1-2. s. 1171-1172.

[860] Gray, 2008 s. 128.

[861] Afroditi, 2010, s. 18.; Streltsov, 2017, s. 7.

[862] Schmitt, 2017, *Tallinn Manual 2.0.* s. 339.

niteliğine bakılmaksızın, uluslararası barış ve güvenliği onarmak ve sürdürmek için silahlı kuvvet kullanmayı da içeren zorlama tedbirlerine başvurmasına müsaade eder[863].

Önemli bir can kaybına ya da maddi zarara sebep olmamakla birlikte ulusal güvenliği tehdit edecek derecede kritik alt yapı unsurlarını hedef alan saldırılar söz konusu olduğunda ne tür bir yol izleneceği de sorunlu bir alandır. Örneğin, gelecekte bir zamanda verileri silmek üzere kritik bir sisteme zararlı bir yazılım yerleştirmenin silahlı saldırı oluşturup oluşturmadığı konusunda Schmitt'in etki temelli yaklaşımına göre, bu ancak verilerin silinmesiyle sonuçlandığı takdirde mümkündür. Sharp ise, bu konuda yazılımın yerleştirilmesini yeterli görmektedir[864]. Mevcut uluslararası hukuk kurallarını temel alan Schmitt tarafından ve dolayısıyla Tallinn El Kitabı'nda meşru müdafaa hakkının doğabilmesi için siber saldırıların ortaya çıkan sonuçlarına odaklanılırken, daha ileriye dönük yaklaşan Sharp'ın kabulüne göre ise, ülkelerin sürekli artan bir teknolojik duyarlılığı (*vulnerability*) dikkate alınmalıdır[865].

Benzer şekilde finansal sistemi çökerten bir siber saldırının silahlı saldırı düzeyinde kabul edilip edilmeyeceği konusunda tartışmalar devam etmektedir. Örneğin, menkul kıymetler borsasına yapılan bir siber saldırının silahlı saldırı oluşturup oluşturmadığı konusunda Uluslararası Uzmanlar Grubu görüş birliğine varamamıştır[866]. Kimi uzmanlar, sırf finansal kaybın silahlı saldırı olarak kabul edilemeyeceğini savunurken, bazıları ise yıkıcı etkilerin bu eşiğe ulaştırabileceği veya bazıları da yok edici olmasa da ciddi etkileri bulunması halinde devletin kritik alt yapı tesisine yönelik saldırı görüşü üzerinden değerlendirme yapılması gerektiğini savunmuşlardır. İkinci görüşe paralel başka bir görüşe göre ise insan kaybı, önemli düzeyde fiziki zarar, devletin temel işlevlerini yerine getiren kritik altyapı unsurlarına yönelik önemli ve uzun zamanlı maddi hasar veya sosyal

[863] Melzer, 2011, s. 6.

[864] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.225-226.

[865] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.228.

[866] Schmitt, 2017, *Tallinn Manual 2.0.* s. 343.

ve siyasal istikrarı bozacak nitelikteki dolaysız yan etkilere sebep olan siber saldırılar silahlı saldırı eşiğini aşabilecektir[867]. Genel olarak ifade etmek gerekir ki siber vasıtalarla ekonomik zarara sebep olma, siyasi rahatsızlık verme veya zorlama, iletişimin aksatılması ve propaganda eylemleri silahlı saldırı olarak kabul edilmemektedir[868].

Etki temelli yaklaşımla ilgili belirtilen çekincelere karşı önerilen kıstas can kaybı ya da önemli maddi hasara sebep olmasa dahi bunun öngörülebilir olmasının yeterli kabul edilmesi halidir[869]. Schmitt'in bu konudaki son görüşünde niyetlenen zararı esas alması da bu sakıncanın ortadan kaldırılmasına yöneliktir[870]. Bu yöndeki bir başka görüşe göre, siber saldırı sonucunda can kaybı, önemli düzeyde yaralanma veya fiziksel zarar bulunmadığı halde devletin temel işlevlerinde ve istikrarında ağır, uzun dönemli ve makul zaman diliminde onarılamayacak bir işlevsizliğe sebep olacak potansiyel aksama durumlarında silahlı saldırıdan bahsetmek olanaklıdır[871].

Bu bağlamda ifade etmek gerekir ki bir siber saldırının sadece kritik altyapı unsurlarını hedef alması eylemin silahlı saldırı olarak nitelendirilmesinde yeterli görülmemelidir. Silahlı saldırı eşiğine dair objektif kıstasların bulunmadığı bir durumda sadece niyetlenen saldırının sırf kritik altyapı tesislerini hedeflemesinden yola çıkılarak meşru müdafaa hakkının doğduğu kabul edilmemelidir. Bununla birlikte siber saldırının sebep olabileceği potansiyelin gözetilmesi gerekir. Örneğin, faal bir nükleer tesisi hedef alan son derece gelişmiş ve karmaşık bir virüsün sebep olabileceği zarar ve can kayıpları potansiyeli ile bir devletin bankacılık sektöründe aksamalara sebep olabilecek bir siber saldırının sırf kritik altyapı tesislerini hedef aldığı için aynı düzlemde değerlendirilmemesi gerekir.

---

[867] Gill ve Ducheine, 2013, s. 459.

[868] Blank, 2013, s. 415.; Siber saldırı sonucunda ortaya çıkan finansal zararın aynı zamanda fiziksel zararlara sebep olması gerektiği görüşü için bkz.: Erdem ve Özocak, 2019, s. 140.

[869] Hathaway ve diğerleri, 2012, s. 848.

[870] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 245.

[871] Gill ve Ducheine, 2013, s. 445.

Buna karşın, gelinen teknolojik gelişim seviyesi itibariyle devletin ana hizmet işlevlerinin ve finansal altyapısının siber uzaya bağlı şekilde gerçekleştirilmesi karşısında ekonomik baskının kuvvet kullanma oluşturmayacağından yola çıkılarak finansal sistemi veya bankacılık sistemini çökerten bir siber saldırının silahlı saldırı olmadığı sonuca varılması doğru olmayacaktır. Ayrıca kritik altyapı unsurlarına yönelen bir siber saldırıda, mutlak suretle sonuçların ortaya çıkmasını zorunlu kılmak, saldırının kritik altyapı tesislerine karşı gerçekleştirilmesi halinde meşru müdafaa hakkının uygulanamamasına sebep olacağı gibi, önleyici meşru müdafaa kuralarına da uygun düşmemektedir.

Siber saldırının konusunu oluşturan kötücül bir yazılım geleneksel anlamda bir konvansiyonel silahın doğurduğu sonuçlara sebep olduğu ölçüde ya da henüz sonuç gerçekleşmese dahi kritik altyapı unsurlarına yönelik olması ve kritik altyapı unsurlarına yönelen bu tehdidin can kaybı veya önemli fiziki zarara sebep olabilecek nitelikte olduğu halde silahlı saldırı olarak kabul edilmemesi doğru görülemez. Bu durumda gerçekleştirilen siber saldırının politik amaçla ve ulusal güvenliğe karşı gerçekleştirilmesi halinde bir baraj kapaklarının sele sebep olacak biçimde açılması suretiyle can kaybı ya da önemli bir zarar doğurmasının muhtemel olması durumunda siber saldırının silahlı bir saldırı olarak kabulü mümkün olabilecek ve meşru müdafaa hakkına sebebiyet verecektir.

Silahlı kuvvet kullanma eşiğinin daha aşağı düzeyde benimsenmesi sadece hemen yukarıda sözü edilen finansal altyapı hedefleri yönünden belirleyici olması yanında caydırıcılık açısından da daha elverişli sonuçlar doğurabilecektir. Bu kabul özellikle kişilerin, bir bilişim korsanı grubunun ya da terörist odakların gerçekleştirdiği siber saldırıların şiddet seviyesinin düşürülmesine de hizmet edebilecektir. Ancak bu noktada silahlı kuvvet kullanma eşiğinin bu derece alt seviyelere indirilmesi halinde orantılılık ilkesi uyarınca meşru müdafaanın geleneksel yöntemler yerine aktif savunma şeklinde gerçekleştirilmesinin gerekliliği kabul edilmelidir.

Siber istihbarat, siber hırsızlık, esaslı olmayan siber bir hizmetin kısa veya periodik kesintiye uğratılması eylemleri Tallinn El Kitabı'nda silahlı saldırı olarak

değerlendirilmezken birkaç insanın ölümü veya ciddi şekilde yaralanması veya malvarlığının yok edilmesi ya da önemli şekilde zarara uğratılması durumlarında ölçek ve etki kıstasını karşıladığı kabul edilmiştir[872]. Bir devletin ulusal ve ekonomik güvenliğini tehdit eden siber casusluk, siber sabotaj veya siber suç oluşturan eylemler ne kadar ağır olursa olsun meşru müdafaa kapsamında güç kullanımını haklı kılan bir silahlı saldırı olarak kabul edilmezler[873].

Siber güçlerin bir devletin silahlı güçlerin bir parçasını oluşturduğunun kabulü durumunda, siber saldırıların BM Genel Kurulu 1974 saldırı suçu tanımının ilk beş eylemi[874] için yasal kapsamına kolaylıkla girdiği kabul edilmektedir[875]. Siber saldırının kaynağı konusunda Tallinn El Kitabı'nda Uzmanlar Grubu, bir devletin organı tarafından gerçekleştirilmesi halinde inkâr edilemez biçimde silahlı saldırı olarak değerlendirileceği gibi saldırının devlete atfedilebilir devlet dışı aktör tarafından gerçekleştirilmesi halinde de aynı şekilde tartışmasız bir silahlı saldırı olarak nitelendirileceği kabul edilmektedir[876]. 1949 tarihli Cenevre Konvansiyonları 1. Ek Protokolü 43. maddesinde çatışmaya taraf

---

[872] Schmitt, 2017, *Tallinn Manual 2.0.* s. 341.

[873] Gill ve Ducheine, 2013, s. 460.

[874] "Madde 3- Savaş ilan edilmiş olsun olmasın, aşağıdaki fiillerin herhangi birisi 2'nci madde hükümlerine tabi ve ona uygun şekilde bir saldırı fiili niteliği taşır: a- Bir Devletin silahlı kuvvetlerinin diğer bir devleti istila etmesi veya ona hücum etmesi veya ne kadar geçici olursa olsun, böyle bir istiladan veya hücumden ileri gelen herhangi bir askeri işgal veya kuvvet yoluyla başka bir Devletin ülkesinin veya bir bölümünün ilhaki; b- Bir Devletin silahlı kuvvetlerinin, başka bir Devletin ülkesini bombardıman etmesi veya bir Devletin diğer bir Devletin ülkesine karşı herhangi bir şekilde silah kullanması; c- Bir Devletin liman veya kıyılarının diğer bir Devletin silahlı kuvvetleri tarafından abluka altına alınması; d- Bir Devletin silahlı kuvvetleriyle başka bir Devletin kara, deniz veya hava kuvvetlerine veya deniz veya hava filolarına saldırması; e- Bir Devletin başka bir Devlette sonuncusuyla yapılan bir antlaşmaya göre bulunan silahlı kuvvetlerinin o antlaşmada öngörülen hükümlere aykırı şekilde kullanılması veya bu silahlı kuvvetlerinin varlığının bu ülkede antlaşmanın sona ermesinden sonra da sürdürülmesi… Saldırı eylemlerinin tamamı için bkz.; BM Genel Kurulu'nun 3814 sayılı ve 1974 Tarihli Saldırının Tanımı Kararı,

Erişim: 24.08.2022 https://inhak.adalet.gov.tr/Resimler/Dokuman/2312020095336bm_31.pdf

[875] Afroditi, 2010, s. 16.

[876] Schmitt, 2017, *Tallinn Manual 2.0.* s. 344.

silahlı güçler, ilgili tarafa karşı eylemlerinden veya maiyetindekilerin eylemlerinden sorumlu bir komuta altındaki tüm silahlı güçleri, grupları ve birimleri olarak tanımlanır.

Siber saldırıların ortaya çıkmasından önceki dönemlerde gelişen teknoloji ile birlikte ortaya çıkan benzer durumlarda kullanılan silahın niteliğine bakılmaksızın devlet organları tarafından gerçekleştirilen kuvvet kullanımı durumunda benzer bir yaklaşımın benimsendiği görülmektedir. Örneğin, iki devlet arasında başvurulan kuvvet kullanımına eşit olan bir askeri uzay operasyonu söz konusu olduğunda, yoğunluğu, süresi ve kapsamı ne olursa olsun, uluslararası bir silahlı çatışmanın söz konusu olduğu kabul edilmiştir[877].

UAD *Nikaragua Davası*'nda saldırı tanımından yararlanarak, bir devlet tarafından veya onun adına silahlı takım, grup, düzensiz birlikler veya paralı askerler tarafından gerçekleştirilen ve düzenli ordu tarafından veya önemli düzeyde katılımı ile gerçekleştirdiği düzeye eşit ağırlıkta bir başka devlete karşı gerçekleştirilmesini silahlı saldırı olarak değerlendirmiştir[878]. Bunun yanında isyancılara silah veya lojistik ya da diğer tür yardımların silahlı saldırıya eşit olmadığını ancak bunun hukuka aykırı karışma oluşturduğunu da ifade etmiştir[879]. Uluslararası Uzmanlar Grubu buradan hareketle zorlayıcı bir siber operasyonu gerçekleştiren devlet dışı bir örgüte finansal destekte bulunmanın güç kullanımı olarak değerlendirilemeyeceği, ancak kötücül yazılım sağlamanın ve bunun kullanımı konusunda gerekli eğitimi vermenin güç kullanımı oluşturacağı konusunda uzlaşmışlardır[880].

Uluslararası Uzmanlar Grubu'nun Stuxnet saldırısı konusundaki görüşünün eylemin kuvvet kullanma oluşturduğu konusunda fikir birliği içinde olduğu, ancak bir kısmının ön alıcı meşru müdafaa temelinde haklı olmadıkça operasyonun silahlı saldırı eşiğine

---

[877] Mačák, 2018, s. 26.

[878] Gray, 2008 s. 130.

[879] Gray, 2008 s. 130.

[880] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 245.

vardığı görüşünü taşırken, diğer uzmanların ise aksi görüşte olduğu anlaşılmaktadır[881]. Daha öncede ifade edildiği üzere bazılarına göre İran devletinin nükleer enerjiye bağımlı olmaması nedeniyle saldırıya uğrayan nükleer tesislerin kritik altyapı tesisleri oluşturmayacağı gerekçesiyle Stuxnet saldırısının silahlı saldırı düzeyine erişmediği savunulmaktadır[882].

Tek başına silahlı saldırı eşiğine varmayan birden çok sayıda siber eylemin, birlikte bu eşiği aşıp aşmayacağı konusunda Uluslararası Uzmanlar Grubu'nun görüşü, gerekli ölçek ve etki standardını karşılaması durumunda silahlı saldırı oluşturabileceği yönündedir[883]. Etki temelli yaklaşım nazara alınırsa önemli bir kayba neden olan bir saldırının evleviyetle silahlı saldırı eşiğine eriştiğinin kabulü gerekir. Güvenlik Konseyi'nin 11 Eylül saldırıları sonrasında verdiği karar[884] bu düşünceyi desteklemektedir[885].

Silahlı bir siber operasyonun bir devlet tarafından diğer bir devlete karşı gerçekleştirilmesine karşın hedef alınmayan üçüncü bir devletin zarar görmesi halinde Uluslararası Uzmanlar Grubu'nun çoğunluğu, sonuçların silahlı saldırı için ölçek ve etki eşiğine erişmesi halinde meşru müdafaa kapsamında kuvvet kullanma yoluna başvurabileceğini savunmaktadır. Dahası hedef devlet açısından silahlı saldırı niteliğinde olmasa dahi üçüncü devlet yönünden uzamış etkilerin silahlı saldırı kapsamında olması mümkün görülmektedir[886]. Bir devletin ülkesi sınırları dışında vatandaşa veya malvarlığına yönelik gerçekleşen siber operasyonun silahlı saldırı olarak nitelendirilip nitelendirilmeyeceği konusunda yoruma yer bırakmayacak bir hukuk kuralı bulunmamakla birlikte, hasarın boyutu, malvarlığının özel veya devlete ait olma

---

[881] Schmitt, 2017, *Tallinn Manual 2.0.* s. 342.

[882] Gill ve Ducheine, 2013, s. 459.

[883] Schmitt, 2017, *Tallinn Manual 2.0.* s. 342.

[884] Güvenlik Konseyi, 12 Eylül 2001 tarih, 1368 sayılı kararında, bireysel ve toplu meşru müdafaa hakkını tanımış, ABD'nin meşru müdafaa hakkı teyit edilmiştir. Bkz.: Sur, 2022, s. 425.

[885] Roscini, 2010, s. 115.; Buradan yola çıkılarak saldırıda kullanılan aygıt "sanal silah" olarak nitelendirilmektedir. Bkz. Streltsov, 2017, s. 7.

[886] Schmitt, 2017, *Tallinn Manual 2.0.* s. 344.

karakteri, hedef kişinin statüsü, operasyonun politik güdüsü gibi unsurlar belirleyici olabilecektir[887]. Örneğin, bir devlet başkanının yurt dışında öldürülmesi silahlı saldırı olarak kabul edilirken devlete ait bir şirketin CEO'sunun öldürülmesi konusunda fikir birliği bulunmamaktadır.

Uluslararası Uzmanlar Grubu'nun fikir ayrılığına düştüğü bir diğer konu, niyet unsuruna ilişkindir. Örneğin, bir devlete karşı gerçekleştirilen siber casusluk sonucunda ikinci devletin siber alt yapısında beklenmeyen biçimde önemli bir zarar oluşabilecektir. Çoğunluğun görüşü, operasyonun silahlı saldırı niteliğinin tespitinde sadece ölçek ve etki kıstasının önem arz ettiği ve niyetin ilgisinin bulunmadığı yönündedir[888]. Melzer, kritik altyapının işlevsizleştirilmesine kadar varsa dahi, "ölçek ve etki" kıstasının sırf nicel yorumunun tatmin edici olmadığını, zararlı bir yazılımın kazara yayılmasının objektif "ölçek ve etki" kıstasına göre silahlı bir saldırı olarak nitelendirilmesinden kaçınmak için "saldırı"nın olağan anlamı içerisinde, saldırgan niyetin (animus aggressionis) de aranması gerektiğini ileri sürmektedir[889]. Benzer bir görüşe göre de failin niyetinin politik veya ulusal güvenliğe yönelik olmadığı takdirde öngörülmeyen ulusal güvenlikle ilgili sonuçların siber saldırı niteliğinde değerlendirilemeyeceği, bunun yerine siber suçtan bahsedilebileceği savunulmaktadır[890].

Oysa objektif olarak silahlı saldırı niteliğindeki bir siber saldırının gereklilik ve orantılılık ilkesi sınırları dâhilinde hareket eden zarar gören devlet, meşru müdafaa hakkını kullanırken saldırıda bulunan devletin niyetini araştırma yükümlülüğü hakkın özüne aykırı olacaktır. Zira tüm altyapı sistemini çökerten ve ölümlere neden olan ağır düzeyde kuvvet kullanma niteliğindeki bir siber saldırıda saldıran devletin kastı olmadığının tespiti o an için olanaklı olmayıp bu ancak saldıran devletin gerekli tedbirleri alması ve bildirim yapması durumunda söz konusu olabilecektir.

---

[887] Schmitt, 2017, *Tallinn Manual 2.0.* s. 346.

[888] Schmitt, 2017, *Tallinn Manual 2.0.* s. 343.

[889] Melzer, 2011, s. 16.

[890] Hathaway ve diğerleri, 2012, s. 848.

3.2.4. Kritik Altyapı Unsurları

Önceki başlıklarda açıklandığı üzere bir siber saldırının BM Şartı'nın 51. maddesine göre meşru müdafaa hakkını doğuran bir silahlı saldırı oluşturup oluşturmayacağı konusunda uluslararası toplum siber saldırının oluş biçiminden (mekanizmasından) ziyade etkileriyle ilgilenmektedir[891]. Bununla birlikte ölüm, yaralanma veya yok etme ile sonuçlanmasa da bu siber saldırıların başka bir devletin egemenlik alanındaki kritik altyapı unsurlarını işlevsiz hale getirmeyi amaçlaması halinde silahlı bir saldırıya eşit düzeyde olduğu kabul edilmektedir[892]. Bir diğer ifadeyle, kritik altyapı tesislerini hedef alması durumunda siber saldırının silahlı saldırı düzeyine erişip erişmediğine bakılmaksızın saldırıya uğrayan devletin orantılılık ilkesi çerçevesinde meşru müdafaa hakkını kullanması söz konusu olabilecektir[893].

Ancak hangi altyapı sistemlerinin kritik altyapı unsuru olarak kabul edileceği sorusu aydınlanmaya muhtaç olduğu kadar, bu tür sistemlere yönelen siber saldırılara ilişkin bir kıstas gerekip gerekmediği de sorun oluşturmaktadır. Bu sorulardan bağımsız olarak, bu sistemlere yönelen bir siber saldırı halinde meşru müdafaa kapsamında gereklilik unsurunun karşılanması gerekliliği ise meşru müdafaa kapsamında cevap verilebilmesi için gözetilmesi gereken bir başka husustur. Bu nedenle öncelikle kritik altyapı unsurlarını hedef alan siber saldırıların niteliğinin ve uluslararası örgütler ve bazı bölgesel örgütler nezdinde tanımlanan kritik altyapı unsurlarının ortaya konulması gerekir.

---

[891] Department of Defence Office of General Counsel. (1999). *An Assessment of International Legal Issues in Information Operations*, s. 18. Erişim: 18.08.2020. https://fas.org/irp/eprint/io-legal.pdf

[892] Melzer, 2011, s. 16.

[893] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.232-237.

Amerikan başkanı Clinton tarafından çıkarılan 13010 sayılı başkanlık kararnamesinde[894] kritik altyapı unsurları sekiz kategoride detaylandırılmıştır. Bunlar; telekomünikasyon, elektrik güç sistemleri, gaz ve petrol stoku, ulaştırma, bankacılık ve finans, su sağlama sistemleri, sağlık, polis, yangın ve kurtarma dâhil acil durum hizmetleri ve hükümetin devamlılığı olarak belirtilmiştir[895]. ABD Savunma Departmanı tarafından 1999 tarihinde hazırlanan değerlendirme belgesinde ulusal hava trafik kontrol sistemi, bankacılık ve finansal sistem kamu hizmeti tesisleri ve yaygın sivil ölümlerine veya maddi hasara sebep olan sel baskınları için baraj kapaklarının açılması silahlı saldırıya eşit kabul edilmiştir[896].

ABD'de kritik altyapı unsurlarını korumaya yönelik 2001 yılında çıkan yasada[897] ise telekomünikasyon, enerji, finansal hizmetler, su ve ulaşım sektörleri örnek olarak gösterilmiş ve kritik alt yapı unsurları terimi, güvenlik, ulusal ekonomik güvenlik, ulusal halk sağlığı ve güvenliği veya bu konuların karışımı konularında sakatlayıcı, yetersizliği veya yıkımı ABD açısından hayati önem arz eden fiziki veya sanal sistem veya varlıklar şeklinde tanımlanmıştır. Buna göre, kritik altyapı unsurlarının sivil ya da askeri şekilde işletilmesinin önemi bulunmamaktadır. 2003 tarihli Güvenli Siber Uzaya dair ABD Ulusal Strateji Belgesi,[898] kritik altyapı unsurlarını zirai, gıda, su, kamu sağlığı, acil servisler, hükûmet faaliyetleri, savunma endüstri tabanlı, bilgi ve telekomünikasyon, enerji, taşımacılık, bankacılık ve finans, kimyasal ve tehlikeli maddeler, postacılık ve gemicilik alanlarında kamu ve özel kurumlarının fiziki ve siber varlıkları olarak tanımlamaktadır[899].

---

[894] 15.07.1996 tarihli Başkanlık Kararnamesi için bkz.: https://www.hsdl.org/?abstract&did=1613

[895] Sharp, Walter Gary, Sr., 1999, s. 22-23.

[896] Department of Defence Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 1999, s. 18. Erişim: 18.08.2020, https://fas.org/irp/eprint/io-legal.pdf

[897] Critical Insfrustructures Protection Act of 2001, 42 U.S. Code §5195c.

[898] Ayrıntılı bilgi için bkz.: *The National Strategy to Secure Cyberspace*, 2003, s. 16. Erişim: 18.08.2020, https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

[899] Roscini, 2010, s. 117.

BM Genel Kurulu'na göre ise[900], sınırlı sayıda olmamakla birlikte kritik altyapı unsurları; elektrik üretimi, enerji iletimi ve dağıtımı, hava ve deniz ulaşımı, bankacılık ve finansal hizmetler, e-ticaret, su şebekesi, gıda dağıtımı, halk sağlığı ve artan bir şekilde birbirine bağlı ve operasyonları etkileyen kritik veri altyapısı için kullanılanları içerir. Ayrıca her devlet kendi kritik veri altyapı unsurlarını belirleyebilecektir. Şangay İşbirliği Örgütü'ne göre ise kritik altyapı unsurları, saldırılması halinde bireysel, sosyal açıdan ve devlet açısından doğrudan ulusal güvenliği etkileyen sonuçlara sebep olan kamu tesisleri, kurum ve enstitüleri ifade eder[901].

AB Komisyonu'na göre kritik altyapı unsurları, bozulduğunda ya da yok edildiğinde vatandaşların sağlığı, emniyeti ve güvenliği, ekonomik refahı veya hükümet faaliyetleri üzerinde ciddi tesiri olan fiziki kaynak, hizmet ve bilgi teknolojisi hizmet araçları, ağ ve altyapı varlıklarını içerir[902]. Komisyon raporunda kritik bilgi altyapısı sistemleri ayrıca tanımlanmış ve telekomünikasyon, bilgisayar/yazılım, internet ve uydular gibi kritik altyapıların işleyişi için temel olan veya kendileri için kritik altyapı oluşturan unsurlar olarak ifade edilmiştir.

Birleşik Krallık Siber Güvenlik Strateji Belgesinde dokuz sektöre atfen enerji, gıda, su, ulaştırma, iletişim, hükûmet ve kamu hizmetleri, acil servisler, sağlık ve finans alanları kritik altyapı unsurları arasında sayılmıştır[903]. Farklı ülke ve uluslararası kuruluşlar tarafından farklı şekilde tanımlanan kritik altyapı unsurları devletlerin gelişmişlik

---

[900] BM Genel Kurul Kararı, 58/199, 30 Ocak 2004.

[901] Melzer, 2011, s. 15.; Kritik altyapı unsurları Antlaşma'nın Ek 1'de tanımlanmıştır. Bunun için bkz.: Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması, s.10. Erişim: 17.12.2021

Agreement on Cooperation in Ensuring International Information Security between the Member States of the SCO.pdf

[902] Melzer, 2011, s. 15. Karar için bkz.: Commision of the European Communities, *Green Paper on a European Programme for Critical Infrastructure Protection,* COM (2005) 576 final, 17.11.2005, Erişim: 15.05.2020

https://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-576-EN-F1-1.Pdf

[903] Roscini, 2010, s. 117.

seviyesine göre, sosyolojik, kültürel ve coğrafi yapılarına göre farklılık arz edebilir. Bu nedenle her ülkenin ulusal kritik altyapı unsurları zamanla değişme gösterebilecek ve siber güvenlik strateji belgelerinde bu değişimin izleri görülebilecektir.

Genel bir bakış açısına göre kritik altyapı unsurları, karmaşık, bir ulus için mutlak suretle temel olarak görülen bütün geniş ölçekli servisler için önde gelen teslim ve destek sistemini ifade eder. Bu servisler acil müdahale, hukuki yaptırım veri tabanı, gözetimsel kontrol ve veri edinme (SCADA) sistemleri, güç kontrol ağları, askeri destek servisleri, tüketici ağırlama sistemleri, finansal başvuru ve mobil iletişimleri içerir[904]. Kritik altyapı tesislerini hedef alan siber saldırılar elektrik üretim veya nükleer güç gibi tesislerinin yukarıda ifade edilen ve SCADA olarak bilinen izleme ve kontrol sistemlerini ele geçirmek ya da bozmak veyahut bankacılık ve para havale işlemlerini ya da borsayı kapatmak suretiyle gerçekleştirilebilmektedir[905].

Siber saldırıların kritik altyapı unsurları üzerindeki olumsuz etkisinin hangi boyutlara varacağı yakın tarihlerde meydana gelen bazı olaylardan anlaşılabilmektedir. Gürcistan, Estonya, Stuxnet ve bir ölçüde Aramco saldırıları, bir siber saldırının kritik altyapı tesislerine oldukça etkili şekilde hasar verebileceği konusunda önemli örneklerdir. Yine 2007 yılında İsrail'in nükleer tesisleri bombalamasından önce Suriye hava savunma sistemine yönelen siber saldırıları, bu tür saldırıların kritik altyapı unsurlarında ne derecede etkili zararlar yaratabileceğine örnek oluşturmaktadır[906].

Buna karşın, İran nükleer enerjiye bağımlı olmadığı için İran'ın nükleer tesislerinin kritik altyapı unsurları kapsamında değerlendirilmeyeceği kabul edilmektedir[907]. İran'ın Natanz nükleer tesislerinin uranyum zenginleştirme faaliyetinin İran devleti açısından kritik bir

---

[904] Amoroso, Edward G. (2011). *Cyber Attacks Protecting National Insfrustructure.* Burlington: Elsevier, s. 1.

[905] Goldsmith, 2013, s. 132.

[906] Geers, 2009, s.3.

[907] Gill ve Ducheine, 2013, s. 459.

faaliyet olarak kabul edilmesi tek başına yeterli olmayıp uluslararası hukuka göre hangi unsurların bu nitelikte olduğunun tespiti gereklidir. İran devletinin enerji ihtiyacının bu tesisten karşılanmaması dahi yeterli bir gerekçe oluşturmakla birlikte kritik altyapı unsurlarına yönelen her saldırının meşru müdafaa hakkına başvurma imkânı sunmayacağı da belirtilmelidir. Bu saldırı sonucunda uranyum zenginleştirme faaliyetinin süre olarak uzaması dışında ulusal çıkarlara yönelen herhangi bir zarar söz konusu olmamıştır.

Kritik altyapı unsurunun nitelendirilmesinden bağımsız olarak olayda gereklilik unsurunun bulunup bulunmadığı sorusu meşru müdafaa hakkına başvurulabilmesi için cevaplanması gereken bir başka unsurdur. Zira kritik altyapı tesisi olarak kabul edilseydi dahi İran'ın meşru müdafaa hakkına başvurabilmesi için saldırıyı bir devlete atfedecek derecede inandırıcı delil elde etmesi yanında cevabi saldırının gerekli olması gerekir ki meşru müdafaa hakkına başvuru imkânı söz konusu olabilsin.

3.3. SİBER SAVAŞ VE MEŞRU MÜDAFAA

3.3.1. Genel Olarak

Siber savaş hukukunu düzenleyen uluslararası bir antlaşmanın bulunmaması ve mevcut uluslararası hukuk normlarının siber savaşa uygulanmasının gerekliliği karşısında kuvvet kullanma yasağında olduğu şekilde meşru müdafaa konusunda da mevcut normların siber savaşa uyarlanması ve uygulanması bir zorunluluktur. Tallinn El Kitabı 69. Kural'da düzenlenen meşru müdafaanın, kullanılan silaha bakılmaksızın uygulanacağına dair UAD kararı uyarınca siber saldırılara da uygulanabileceği kabul edilmektedir[908]. Buna göre, yukarıda incelenen uluslararası hukukta kuvvet kullanımına başvuru kuralları çerçevesinde yasağın istisnalarından birini oluşturan meşru müdafaa konusunun öncelikle geleneksel yönü ortaya konulmalı ve yeni bir alan olan siber saldırılara karşı meşru müdafaa yoluna başvuru şartları irdelenmelidir.

[908] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 244.

Meşru müdafaa, doğal hak olma yönü bir yana, sözleşme hukuku çerçevesinde de devlet öznesine izne tabi olmaksızın kuvvet kullanımı hakkını veren[909] bir hukuka uygunluk sebebidir. Buna karşın meşru müdafaa hakkının kullanılması sırasında devleti sınırlandıran bazı kurallar söz konusudur. Meşru müdafaa hakkına başvurulabilmesi için gereken koşullardan ayrı olarak meşru müdafaa hakkı kapsamında kuvvet kullanan devletin uluslararası silahlı çatışmalarla ilgili tüm antlaşmalara ve insancıl hukuk kurallarına riayet etme yükümlüğü devam etmektedir[910].

Meşru müdafaa uygulamasının ilk örneği olarak, İngiltere ve ABD arasında uyuşmazlık konusu oluşturan 1837 tarihli *Caroline* olayı gösterilmektedir[911]. Bu tarihten itibaren meşru müdafaanın uluslararası kamuoyunda yapılageliş hukuku karakteri konusunda bir uzlaşı bulunmaktadır [912] . BM Şartı'nın 51. maddesinde bu prensiplerden bahsedilmemesinin sebebi, meşru müdafaa ile ilgili düzenlemenin kapsamlı şekilde kodifiye edilmesi niyetinin bulunmamasından kaynaklanmaktadır. Ayrıca yapılageliş hukukuna özgü bu kıstasların, Şart'ın meşru müdafaaya dair gerekliliklerini tamamlayıcı nitelikte olduğu kabul edilmektedir[913].

Meşru müdafaa konusu, uluslararası hukukçular arasında farklı görüşlerin ortaya çıktığı, devlet uygulamalarında önemli ayrışmaların yaşandığı oldukça sorunlu bir alandır. Sorunun temel kaynağının meşru müdafaa hakkına başvuru şartları üzerinde gelişmiş ülkelerle gelişmekte olan ülkeler arasındaki görüş farkından kaynaklandığı söylenebilir. Kuvvet kullanımı ve kuvvet kullanma tehdidi yasağının devletlerin gücüne bakılmaksızın eşit şekilde tüm devletleri kapsaması karşısında gelişmiş devletlerin bu yasağın çevresini dolanma güdüsüyle hareket ettikleri görülmektedir. İsrail'in Irak'a ait Osirak Nükleer Deneme Tesisleri'ne yönelik saldırısının hukuki dayanağı olan meşru müdafaa hakkının

[909] Mutlu, 2016, s. 126.

[910] Uzun, 2007, s. 51.

[911] Ayrıntılı bilgi için bkz.; Arend ve Beck, 1993, s. 18.

[912] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 244.

[913] Gill ve Ducheine, 2013, s. 448.

hukuka aykırı şekilde genişletilmesinden ibaret olması buna bir örnektir[914]. Yakın tarihe bakıldığında daha pek çok benzer haksız saldırının meşru müdafaa adı altında gerçekleştirildiği görülebilmektedir[915]. ABD veya ABD'nin başını çektiği koalisyon ortaklarının 9/11 sonrası Afganistan'ı ve kitle imha silahı bulundurulduğundan bahisle 2003 yılında Irak'ı işgalinin hukuka uygunluğu konusu tartışmaya açıktır[916].

Meşru müdafaa hakkının kapsamı ve özellikle önleyici meşru müdafaa ve vatandaşı korumanın hukuka uygun olup olmadığı konusunda gerek devlet uygulamalarında ve gerekse de öğretide hala önemli fikir aykırılıkları bulunmaktadır[917]. Meşru müdafaa konusunda verilen BM Genel Kurulu kararlarına rağmen meşru müdafaanın kapsamına dair sorunlar halen çözülmemiş, geniş bakış açısında sahip olan ABD, İsrail ve geçmişte Güney Afrika ile kısmen de İngiltere ve Fransa yurtdışındaki vatandaşlarını koruma hakkı, önleyici meşru müdafaa hakkı ve meşru müdafaanın bir parçası olarak terörizmle mücadele hakkına sahip olduklarını ileri sürmüşlerdir[918].

Bu sorunlar temelinde meşru müdafaanın kapsamı konusunda öğretide iki ana grup bulunmaktadır. Meşru müdafaayı geniş bir hak olarak yorumlayan grup, BM Şartı'nın daha önce var olan uluslararası yapılageliş hukukunu ortadan kaldırmayacağını ve vatandaşı koruma ve önleyici meşru müdafaa haklarının saklı olduğunu savunurken, dar yorumu savunan karşı görüşteki grup ise meşru müdafaa hakkının sadece silahlı saldırı vuku bulduğunda doğacağını savunmaktadır[919]. Buna karşın, her iki görüş dışında Şart'ın uluslararası ilişkilerde kuvvet kullanmaya dair tüm alanları kapsamadığı, uluslararası yapılageliş kurallarının da Şart'ın hükümlerini yorumlamada önemli bir ikinci rol oynadığı, dahası Şart sonrası devlet uygulaması ve *opinio iuris*'in bu hükümlerin

---

[914] Karar için bkz.; BM Güvenlik Konseyi, "Resolution 487 (1981) / Adopted by the Security Council at its 2288th Meeting." 19 Haziran 1981, Erişim: 12.06.2022 Resolution 487 (1981) / (un.org)

[915] Ayrıntılı bilgi için bkz.; Gündüz, Aslan. (2003). *Milletlerarası Hukuk*. İstanbul: Beta, s. 51-54.

[916] Sur, 2022, s. 300.

[917] Gray, 2008 s. 114.

[918] Gray, 2008, s. 10.

[919] Gray, 2008 s. 117-118.

içeriklerinden gittikçe uzaklaşması söz konusu olduğunda güç kullanımına dair hükümlerin tadil edilmesinin muhtemel olduğu savunulmaktadır[920].

Nikaragua Davası'nda UAD yukarıda belirtilen iki görüşü de belli ölçülerde yansıtan, bir anlamda birleştiren bir karar vermiştir. BM Şartı 51. maddede öngörülmeyen gereklilik ve orantılılık koşullarının geçerliliğini kabul etmiş ve UAD, ABD'nin bir uluslararası antlaşmadan doğan sorunları Divan'ın yetkisi dışında bırakmış olması nedeniyle BM Antlaşması'na göre değil yapılagelişe göre karar vermiştir[921]. UAD'nın *Nikaragua Davası*'nda bu konuda takındığı tavır, antlaşma normu ile yapılageliş hukukunun tamamen aynı olması halinde dahi yapılageliş hukukunun tek başına var olduğu ve uygulanabileceği yönündedir[922].

BM Şartı'nın hazırlık çalışmaları sırasında Fransa'nın, meşru müdafaa hakkının Güvenlik Konseyi'nin iznine bağlı tutulması önerisi kabul edilmemiştir. Önerinin kabul edilmeme sebebi, doğal, bir diğer ifade ile kendinde var olan bu hakkın ne zaman kullanılması gerektiğini tek taraflı olarak belirleyecek yasal otoritenin kişisel olarak ilgili devlet olması nedeniyle sınırlamanın makul bulunmamasıdır[923]. Görüşmeler sırasında Türkiye, doğal meşru müdafaa hakkının acil durumlar veya bir devletin saldırıldığı yer ile sınırlandırılması gerektiğini ifade etmiş, Çekoslovakya ise yakın tehdit durumlarında bu hakkın kullanılması yetkisinin Güvenlik Konseyi'ne verilmesini önermiş[924] ise de öneriler kabul görmemiştir.

Meşru müdafaanın yazılı kaynağı ele alındığında, BM Şartı'nın 51. maddesinde meşru müdafaanın şu şekilde düzenlendiği görülmektedir:

---

[920] Ruys, 2010, s. 19.

[921] Keskin, 1998, s. 54.

[922] Rølsåsen, 2016, s. 46.

[923] Alder, Murray Colin. (2013). *The Inherent Right of Self-Defence in International Law.* New York / London: Springer, s. 86-87.

[924] Alder, 2013, s. 87.

> *"Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru müdafaa hakkına halel getirmez. Üyelerin bu meşru müdafaa hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez."*

Uluslararası hukuk çevrelerince bu düzenlemeden dört farklı hukuki sonuç çıkarılmaktadır[925]: Bunlardan ilki, meşru müdafaanın doğal bir hak olarak kuvvet kullanma yasağından muaf tutulmasıdır. İkincisi, Şart'ın işletilmesi suretiyle zayıflatılmasına karşı bu doğal hakkın korunmasıdır. Üçüncüsü, yasal olarak gerçekleştirilecek doğal meşru müdafaa hakkının öncesinde meydana gelen silahlı bir saldırının ön şartlarını ve son olarak, Güvenlik Konseyi'nin devletlere karşı üstünlüğünü ortaya koymasıdır[926].

BM Şartı'nın 51 maddesinin hazırlık çalışmalarına bakıldığında, müzakereci devletler komitesinin "*inherent*" kelimesinin devletin kendisini yasal savunma hakkını ifade ettiği, başka bir hakkın kastedilmediği[927], "*inherent*" kelimesi yapılageliş hukukuna atıf yapsa dahi "silahlı bir saldırı halinde" sözcüklerinin sırf açıklayıcı ve örnekleyici bir anlam ifade edemeyeceği savunulmaktadır. Hatta bunun aksine VAHS'nin 31/1 fıkrasında sıralanan "kelimenin olağan anlamı", "bağlamsal unsurlar" ve "amaç ve niyet" şeklindeki

---

[925] Alder, 2013, s. 84.

[926] Madde metninden meşru müdafaaya ilişkin çıkarılabilecek diğer hususlar hakkında bkz.: Aksar, 2021, (2. Kitap), s. 139.

[927] Alder, 2013, s. 86.

üç yorum unsuru[928] uyarınca, kabul edilebilir meşru müdafaanın kapsamının belirlenmesi olarak yorumlanabileceği[929], ayrılmaz bir parça ve temel bir koşul olduğu[930] ileri sürülmektedir.

Bu bağlamda ifade edilmesi gereken bir husus, VAHS'nin 31 ve 32. maddelerine göre antlaşmanın yorumlanması açısından BM Şartı'nın kuvvet kullanımını düzenleyen hükümlerinin ne şekilde değerlendirileceğinin de sorun oluşturmasıdır. Anılan Sözleşme'nin 31/3-c fıkrasında "taraflar arası ilişkilerde, uygulanabilir ilgili herhangi bir uluslararası hukuk kuralının dikkate alınacağı" hükmü bulunmaktadır. Bu madde uyarınca, yapılageliş kuralları kadar hukukun genel ilkeleri, diğer antlaşmalar hukuku kurallarının da yorum faaliyetinde kullanılacağı söylenebilir[931].

Ayrıca yorum bahsine dördüncü bölümde ve sonuç kısmında daha ayrıntılı olarak değinileceği üzere, özellikle de siber savaş gibi teknolojik gelişimin sonuçlarının doğrudan görüldüğü alanlarda yazılı metnin yorumlanması konusu sadece metnin olağan veya modern anlamı, bağlamı, amaçsal, tarihsel ya da metinsel yöntemler gibi dar bir çerçevede yapılamayacak kadar geniş bir bakış açısını gerektirmekte olup dil felsefesi ve yorum bilim kapsamında değerlendirilmelidir. Siber uzayın karmaşık, dinamik ve öngörülemeyen yapısı nedeniyle siber savaşta kaos teorisinin uygulanmasına yönelik görüşleri de karşılayan dinamik yorum şekli gerekli görünmektedir.

---

[928] Bu yorum şeklinin temellerini Grotius'un Savaş ve Barış Hukuku adlı kitabında bulmak mümkündür. Kısaca belirtilirse, Grotius'a göre uygun yorum; kelimeler veya bağlamlar üzerinden makul işaretler vasıtasıyla tarafların niyetinin tespitine yöneliktir. Bağlamın ana kaynağı ise antlaşmanın konusu, sonuçlar, koşullar ve bağlantılardır. Bağlamın yetersiz olması halinde kelimenin orijinal ve gramatik anlamıyla sıkı şekilde bağlı kalınmamalı, bunun yerine genel kabul gören anlam dikkate alınmalıdır. Bkz.: Grotius, 2001, s. 140-142.

[929] Ruys, 2010, s. 59.

[930] Ruys, 2010, s. 60.

[931] Ruys, 2010, s. 19.

Madde metnine göre silahlı bir saldırıya uğrayan devlet Güvenlik Konseyine durumu hemen bildirilmeli ve meşru müdafaa hakkı Güvenlik Konseyince gerekli önlemlerin alınmasına kadar olan zaman ile sınırlıdır. Bu haliyle öğretide meşru müdafaanın geçici bir hak olduğu ifade edilmektedir[932]. "Güvenlik Konseyi gerekli önlemleri alıncaya dek" ibaresinden anlaşılan ise, doğal meşru müdafaa hakkının kullanılmasının Güvenlik Konseyi'nin iznine tabi olmadığı ve bu hakka başvuracak devletin Güvenlik Konseyi'ne bildirim yükümlülüğünü yerine getirmesiyle meşru müdafaa hakkının sona ermeyeceğidir. Güvenlik Konseyi tarafından meşru müdafaa kapsamında gerçekleştirilen silahlı karşılık eyleminin durdurulmasını açıkça istemedikçe meşru müdafaa hakkını kullanan devletin gerekli cevabı vermesine engel bulunmamaktadır[933].

3.3.2. Meşru Müdafaa Hakkının Koşulları

BM Şartı'nın 51. maddesi hükmünden de anlaşılacağı gibi, meşru müdafaa hakkına başvurulabilmesi için bir silahlı saldırıya hedef olunması ana koşuldur[934]. Uluslararası hukuka uygunluğu sağlamak ve bir hakkı korumak üzere saldırıda bulunulamaz[935]. Silahlı bir saldırının vuku bulmasından bahsedildiğinden saldırıyı gerçekleştiren devletin BM üyesi olması gerekli değildir[936]. Hangi eylemlerin silahlı saldırı oluşturduğu daha önce incelendiğinden bu hususa yeniden değinilmeyecektir.

Meşru müdafaa hakkına sebep olan bir silahlı saldırı eyleminin varlığı halinde bu saldırıya karşı verilecek savunma saldırısının da bazı koşulları taşıması gerekir[937]. Devletlerin gerek doğasından kaynaklı ve gerekse de BM Şartı'nın 51. maddesi uyarınca sahip olduğu meşru müdafaa hakkının hukuka uygun olabilmesi için uygun bir meşru

---

[932] Khan, 2017, s. 147.

[933] Gill ve Ducheine, 2013, s. 447-448.

[934] Pazarcı, 2021, s. 554.

[935] Sur, 2022, s. 299.

[936] Khan, 2017, s. 144.

[937] Meşru müdafaa hakkına başvuru koşulları için bkz.; Sur, 2022, s. 298-299.

müdafaa hakkı olması gerektiği, bir diğer ifade ile "gereklilik (necessity)" , "orantılılık (proportionality)" [938] ve "dolaysızlık/yakınlık (immediacy)" [939] temel prensipleriyle uyumlu olması gerektiği kabul edilmektedir. Bu ilkelerden ilk ikisi konusunda görüş birliği bulunsa da son unsur konusunda fikir ayrılıkları bulunduğu görülmekte ve özellikle de gelecekte olması muhtemel saldırılar üzerinde tartışmalar yoğunlaşmaktadır. Bu tartışmalara geçmeden önce ilk iki unsurdan bahsetmek daha uygun olacaktır.

Meşru müdafaanın ilk unsuru olan gereklilik ilkesi, devam eden ya da olması yakın silahlı bir saldırının varlığı[940] ve erişilebilir alternatif bir gerçekçi telafi aracının bulunmaması halinde başvurulacak son çare olduğu anlamına gelmektedir[941]. Bu ise, kullanılabilir diğer tüm araçların başarısız olması ya da muhtemelen başarısız olacak sayılmasını ifade etmektedir[942]. Ancak bu uygulanabilir tek cevabın "kuvvet kullanma" olması gerektiği anlamına gelmemektedir[943]. Etkili "yasa uygulama" cevabına izin veren veya uygulama kapasitesine sahip ve istekli bir devlet ülkesinde, devlet dışı aktörler tarafından saldırı gerçekleştirildiğinde elverişli ve yeterli cevap oluşturan "yasa uygulama" tedbirlerini içeren meşru müdafaa dışındaki önlemler uygulanabilir[944]. Diğer bir deyişle saldırının kaynaklandığı ülkenin gerekli soruşturma ve önleme tedbirlerini alma konusunda istekli ve etkili olması halinde bu devlete yönelik meşru müdafaa yoluna başvurmak yerine diğer önlemler tercih edilmelidir.

Siber saldırı halinde ise kuvvet kullanımını içeren cevabın gerekli olması, mağdur devletin öncelikle kuvvet kullanmayı içermeyen önlemlerin yetersiz kalacağı sonucuna

---

[938] Graham, 2010, s. 89.

[939] Gill ve Ducheine, 2013, s. 448.

[940] Gill ve Ducheine, 2013, s. 449.

[941] Ruys, 2010, s. 95.

[942] Roscini, 2010, s. 119.

[943] Schmitt, 2017, *Tallinn Manual 2.0.* s. 348.

[944] Gill ve Ducheine, 2013, s. 449.

varmasını gerektirir[945]. Saldırıyı defedecek veya saldırıdan vazgeçirecek kamu diplomasisi ve savunma tedbirleri gibi kuvvet kullanımı içermeyen bir seçeneğin bulunması halinde meşru müdafaa kapsamında kuvvet kullanımı gerekli kabul edilemez[946]. Ayrıca mağdur ülkenin pasif savunma sisteminin etkili şekilde engelleyebildiği bir saldırıya karşı kuvvet kullanımına eşit bir siber ya da konvansiyonel yöntemleri içerecek şekilde meşru müdafaa hakkına başvurulamayacaktır[947].

Bu nesnel gereklilik, nicel bir bakış açısını ihtiva etmekte olup bu ön şart yerine getirildiğinde benimsenen önlemin meşru amacın başarılması için savunma eylemi zamansal olarak, bir diğer ifade ile geçici bir süre için ve nicelik itibariyle gerekli olmalıdır[948]. Yakınlık olarak da ifade edilen zamansal gereklilik, silahlı saldırı eyleminin başlamış veya başlaması yakın ve muhakkak olması anlamına gelir. Tamamlanmış bir silahlı saldırı sonrasında intikam amaçlı bir karşı saldırı meşru müdafaa kapsamında zamansal açıdan gerekli kabul edilemez.

Nicel bakış açısına göre gereklilik ilkesi, meşru müdafaada kullanılan gücün türü ve derecesinin, söz konusu silahlı saldırının püskürtülmesi için fiilen gerekeni aşmamasını ifade eder[949]. Gereklilik ilkesi sadece ilk saldırının önlenmesini içermeyip ayrıca devam eden tehdidin önlenmesini de kapsamaktadır[950]. Gereklilik ilkesinin nicel yönüyle karıştırılan orantılılık ilkesi ise, meşru müdafaa eyleminin hukuken haklı görülebilmesi için yalnızca sebep olunması beklenen zararın boyutunun, önlenmesi amaçlanan zarara oranının makul bir düzeyde kalmasını ifade eder[951]. Buna göre, meşru müdafaa hakkının

---

[945] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 248.

[946] Blank, 2013, s. 418.

[947] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 248-249.

[948] Melzer, 2011, s. 17.

[949] Melzer, 2011, s. 17.

[950] Blank, 2013, s. 418.

[951] Melzer, 2011, s. 17.

kullanılması sırasında verilen cevabi saldırının hukuka aykırı silahlı saldırının önlenmesi için gereken seviyeyi aşması halinde hukuka aykırı hale gelmesi orantılılık ilkesine aykırılıktan [952] kaynaklanmamakta, bunun yerine saldırının önlenmesi için yeter derecenin üstünde bir cevabi saldırının gereklilik unsurunun nicel boyutu itibariyle hukuka aykırı hale gelmektedir.

Gereklilik ilkesi, silahlı bir saldırıyı püskürtmek veya defetmek için nesnel bir şekilde gerekenler açısından hukuki meşru müdafaanın sınırlarını çizerken, orantılılık prensibi, savunma eyleminden kaynaklanan zararın haklılığını sağlamak için hangi boyutta zararın önleneceğini belirler[953]. Ayrıca savunma saldırısının siber saldırı ile aynı neviden olması zorunluluğu bulunmamaktadır. Savunma saldırısı, siber saldırıya karşı kinetik bir cevap ya da tam tersi veya her ikisinin birleşimi olabilmektedir[954]. Bu bağlamda gereklilik unsuru kapsamında gerçekleştirilecek meşru müdafaa eyleminin, saldırıyı defetmeye veya püskürtmeye yetecek derecede olması ile saldırıdan kaynaklanabilecek zararın saldırgan devlete verilecek zarar ile orantılı olması farklı unsurları ifade etmektedir.

Bu açıklamalardan anlaşılacağı üzere meşru müdafaanın unsurları öğretide farklı şekilde kategorize edilmekte, zamansal gereklilik ilkesi yerine "zamansal yakınlık" (imminence) kavramı kullanılarak gereklilik ve orantılılık ilkesi yanında üçüncü bir unsur olarak da ifade edilebilmektedir[955]. Saldırının başlamadan öncesi durumlara ilişkin olarak önleyici meşru müdafaa söz konusu olduğunda zamansal yakınlık unsurunun varlığı bir gereklilik olarak kendini göstermektedir [956] . Bir saldırının gerçekleşmekte olması ya da gerçekleşmek üzere olması anlamına gelen bu unsurun geleneksel saldırılar açısından

---

[952] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 249.

[953] Melzer, 2011, s. 17.

[954] Schmitt, 2017, *Tallinn Manual 2.0.* s. 349.; Gill ve Ducheine, 2013, s. 450.

[955] Melzer, 2011, s. 17.

[956] DeWeese, Geoffrey S. (2015). *Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminance*, 7th International Conference on Cyber Conflict: Architecture in Cyberspace, NATO CCD COE Publications, Tallinn, s. 81.

faydalı olabilmesi mümkün olsa da siber saldırılar açısından aynı şeyi söylemek pek de mümkün değildir. Zira kinetik saldırılarda hedef ülkenin zamansal yakınlık olarak saldırının gerçekleşme ya da gerçekleşmek üzere olmasını tespit edebilmesi, birkaç milisaniyede başlatılabilen siber saldırılarda aynı imkânı sağlamamaktadır[957]. Meşru müdafaa kapsamında gerekli bir cevabın verilmesi failin asgari düzeyde tespitini ve siber saldırının bir kaza olmadığının doğrulanmasını ve bağlamda bilişim korsanının küçük bir müdahale ile önlenememesi gibi meselenin müdahale araçlarıyla çözülememesini gerektirmektedir[958].

Meşru müdafaanın yukarıda belirtilen zamansal yakınlık ve failin kimliğinin akla uygun şekilde belirlenmesinin ise olay gerçekleşmeden önce (*ex ante*)[959] gerçekleştirileceği, yoksa olayın vukuundan sonra (*ex post facto*) [960] değerlendirilemeyeceği kabul edilmektedir[961]. Bir diğer ifadeyle saldırının gerçekleşmek üzere olduğunun ya da başladığının ve doğru faile karşı gerçekleştirilip gerçekleştirilmediğinin, sonradan ortaya çıkan şartlara ve yeni elde edilen verilere göre yapılacak bir değerlendirme ile tespiti yerine, saldırı eyleminin gerçekleştiği şartlara göre belirlenmesi söz konusudur.

Silahlı bir saldırının olmasının yakınlığının bir gereklilik olmasından farklı olarak dolaysızlık (*immediacy*) olarak ifade edilebilecek son unsur ise meşru müdafaanın nihai amacının silahlı saldırının sona erdirilmesi olup saldırganın cezalandırılmamasını ifade eder[962]. Bu ilke meşru müdafaa ile mevcut uluslararası hukukta yasa dışı kabul edilen

---

[957] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 247.

[958] Roscini, 2010, s. 119.

[959] Bir olayın gerçekleşmeden önce değerlendirilmesini ifade eder. Bkz.; https://tureng.com/tr/turkce-ingilizce/ex%20ante

[960] Olayın gerçekleşmesinden sonra yapılan değerlendirme anlamına gelmektedir. Bkz.; https://tureng.com/tr/turkce-ingilizce/ex%20post%20facto

[961] Schmitt, 2017, *Tallinn Manual 2.0.* s. 347.

[962] Roscini, 2010, s. 120.

silahlı zararla karşılık arasındaki fark ile ilgilidir[963]. Buna göre, saldırının sona ermiş olması halinde meşru müdafaa hakkının kullanılması mümkün olmayacaktır[964]. Ayrıca bu ilke uyarınca meşru müdafaa cevabının zorunlu olarak ilk saldırı ile eş zamanlı olmasını gerektirmemektedir[965]. Meşru müdafaanın asıl amacı olan devam eden saldırıyı veya olması yakın saldırıyı püskürtme ve tekrarını önlemeye yönelik gerçekleştirilecek cevabi her saldırı, ilk saldırı ile eş zamanlı olmasa dahi hukuka uygun olacaktır.

Siber faaliyetlerin anlık doğası gereği belirtilen bu son unsur çoğu olayda önem arz etmemektedir[966]. Siber saldırıların gerçekleşme biçimi büyük çoğunlukla klavye tuşuna dokunma süresi kadar bir zaman aralığında başlayıp bitmekte olduğundan anlık gerçekleşen zarar nedeniyle mağdur devletin vereceği cevabın saldırıyı önlemeye yönelik olmadığı açıktır. Buna karşın, bazı siber saldırıları türlerinde henüz harekete geçmemiş bir kötücül yazılıma karşı gerçekleştirilebilecek bir aktif savunma saldırısının, yazılımın aktive olması beklenmeden, kötücül yazılımın yerleştirilmesinden çok sonra gerçekleştirilmesi mümkündür. Bir siber saldırının hedefinin özellikle kritik altyapı unsuru olması halinde saldırı altındaki devletin, önleyici meşru müdafaa hakkını da içeren meşru müdafaa hakkı kapsamında aktif savunma tedbirine başvurabileceği kabul edilmektedir[967].

3.3.3. Ön alıcı / Önleyici Meşru Müdafaa

Meşru müdafaa konusunda tartışmalı alanlardan en önemlisi gelecekte meydana gelmesi muhtemel olan bir saldırıya karşı ön almak ya da önlemek amacıyla gerçekleştirilen savunma saldırılarıdır. UAD'nın muhtemel saldırıya karşı önleyici meşru müdafaanın

[963] Gill ve Ducheine, 2013, s. 451.

[964] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 248.

[965] Gill ve Ducheine, 2013, s. 451.

[966] Blank, 2013, s. 419.

[967] Hoisington, 2009, s. 453.

tespitine yönelik isteksizliği[968] devlet dışı aktörler tarafından gerçekleştirilen siber saldırılar gibi durumlarda devletlere önleyici meşru müdafaa hakkına başvurma konularında alan açmıştır[969]. BM Şartı'nın 51. maddesinde meşru müdafaaya "bir silahlı saldırı halinde" izin vermesine rağmen[970] bazı yazarlar, düzenlemenin daha önce uluslararası yapılageliş hukukunda var olan önleyici meşru müdafaa hakkını kaldırmadığını ileri sürmüşlerdir[971].

Önleyici meşru müdafaanın hukuka uygun olduğunu savunanlara göre, bu savunma şekli yapılageliş hukukundan kaynaklanmakta[972] ve geçmişi C*aroline* olayına kadar gitmektedir. Bu durumda BM Şartı'nın yürürlüğe girmesi sonrasında değişen hukuki durumun önleyici meşru müdafaanın yasallığını etkileyip etkilemeyeceği sorusu gündeme gelmektedir. Şart sonrasında Nuremberg ve Tokyo Mahkemeleri'nin *Caroline* formülüne atıf yapmasının ve Norveç'in işgaline gerekçe olarak gösterilen meşru müdafaa savunmasının Nuremberg Mahkemesi'nce önleyici meşru müdafaa şartlarının bulunmadığından değil de meşru müdafaa dışındaki bir sebepten reddedilmesinin bunu gösterdiği savunulmaktadır[973]. Ayrıca Güvenlik Konseyi, Genel Kurul veya hiçbir uluslararası mahkeme kararlarında önleyici meşru müdafaa hakkının bulunmadığına dair bir kabul yer almadığı gibi saygın kuruluşlar tarafından ve BM Genel Sekreterliği'nce 2004 yılında tavsiye edilen uluslararası panellerde *Caroline* parametreleri dâhilinde önleyici meşru müdafaanın lehine duruş sergilendiği ifade edilmektedir[974]. Buna karşın

---

[968] UAD kararlarında önleyici meşru müdafaa hakkının varlığını ne kabul etmiş ne de reddetmiştir. Bkz.: Pazarcı, 2021, s. 555.

[969] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.221.

[970] Khan, 2017, s. 149.

[971] Ruys, 2010, s. 250.

[972] Karadağ, Ulaş. (2016). *Birleşmiş Milletler Antlaşması'na Göre Meşru Müdafaa Hakkı.* İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt:7, Sayı:2, s. 181.

[973] Gill ve Ducheine, 2013, s. 455-456.

[974] Gill ve Ducheine, 2013, s. 457-458.; Bunlar; *Institut de Droit International* kuruluşu ve "*High Level Panel on Threats, Challenges and Change"* panelidir.

aksi görüşe göre, uluslararası toplum önleyici meşru müdafaayı kabul etmemiş, BM 2004 tarihli Zirve Paneli'nde[975] önleyici meşru müdafaa reddedilmiştir[976]. Ayrıca öğretide, önleyici meşru savunma çok sınırlı şekilde kabul edilse de asıl meselenin gereklilik ve orantılılık koşulunun mevcudiyeti olduğu savunulmaktadır[977].

Tartışmaya klasik uluslararası hukuk perspektifinden bakıldığında, önleyici meşru müdafaa konusunda pozitivist felsefenin, "*birinin silahlı bir saldırıya hedef olması halinde*" ibaresinin orijinal versiyonunda yer alan "occur" kelimesinin zamansal açıdan değerlendirilmesi durumunda Şart'ın 51. maddesinin önleyici meşru müdafaayı etkisiz kıldığını savunduğu görülmektedir[978]. Buna karşın realist felsefe, çağdaş savaş araçlarının güçlü doğası dikkate alındığında bir devletin, yasal olarak yetkilendirildiği kendini savunma hakkını kullanmasından önce silahlı bir saldırının fiziken başlamasının sonuçlarının kabul edilemeyeceğini ileri sürmektedir[979]. Zira "*occur*" kelimesi, silahlı saldırının yakın bir gelecekte gerçekleşmesinin açık olması şeklinde yorumlanmakta, silahlı güçlerin sınırı geçmesi öncesinde meşru müdafaa hakkına başvurulabileceği kabul edilmektedir[980].

Türkçede muhtemel bir saldırıya karşı gerçekleştirilen savunma eylemine yönelik olarak yaygın şekilde kullanılan ön alıcı ve önleyici meşru müdafaa kavramları, saldırı gerçekleştirilmeden önceki bir zamanda meşru müdafaa kapsamında kuvvet kullanılmasına olanak sağlar[981]. Bu kavramlar, saldırının başlamasından geriye doğru farklı zamansal noktaları işaret etmeleri nedeniyle ayrılmaktadırlar. Ön alıcı meşru

[975] Report of the High-level Panel on Threats, Challanges and Changes, UN Doc. A/59/565, para. 189 – 192.

[976] Erdem ve Özocak, 2019, s. 146.

[977] Aksar, 2021, (2. Kitap), s. 147.

[978] Alder, 2013, s. 96.

[979] Alder, 2013, s. 96.

[980] Gill ve Ducheine, 2013, s. 457.

[981] Sharp, 1999, s. 43.

müdafaa şekli, yakın gelecekteki apaçık ve kesin bir saldırı tehdidine cevaben alınan savunma tedbirlerini ifade eder[982]. Önleyici meşru müdafaada ise muhtemel saldırının yakınlığı daha önceki tarihlere gitmektedir.

Bu terimlerin kaynağına bakıldığında, gelecekte gerçekleşme ihtimali üzerine gerçekleştirilen meşru müdafaanın İngilizce olarak "*interceptive*", "*anticipatory*", "*pre-emptive*" ve "*preventive*" olmak üzere dört şekilde gerçekleşebileceği kabul edilmektedir [983] . "*Anticipatory"* terimi ile "*pre-emptive"* terimi eş anlamlı [984] ve uluslararası hukukta birbirine yakın olmakla birlikte zamansal derecelendirme itibariyle farklı anlamlar ifade etmektedir.

"Interceptive" meşru müdafaada, başlamış ancak henüz hedef ülkede sonuçları doğmamış bir saldırıya karşı kullanılan meşru müdafaa olarak ifade etmek mümkündür. Örneğin, komşu devletin ülkesinden bir devlete karşı gerçekleştirilen füze saldırısına karşılık füzenin etkisiz hale getirilmesi meşru müdafaa iken gelecekte gerçekleşecek füze saldırıları için füze atılan tesisin mağdur devlet tarafından vurulması da bu kapsamında değerlendirilmektedir[985]. Bu meşru müdafaa şeklini Türkçeye an alıcı meşru müdafaa olarak çevirmek mümkündür.

Tartışmalı bir konu olan *"preventive"* meşru müdafaa ise, gelecekteki bir saldırı olasılığının önlenmesini amaçlar. Bu durumda savunmaya dair cevap, gelecekteki belirsiz bir noktada, henüz oluşma aşamasında ve potansiyel bir saldırı tehdidine yöneliktir[986]. Belirtilen her iki savunma halinde saldırının yakın bir tehdit oluşturması aranmaz, zira ilkinde saldırının başlamış olması, diğerinde ise geleceğe yönelik olasılık üzerine

[982] Gill ve Ducheine, 2013, s. 452-453.

[983] DeWeese, 2015, s. 84.

[984] Gill ve Ducheine, 2013, s. 453.

[985] Sharp, 1999, s. 46.

[986] Gill ve Ducheine, 2013, s. 453.

savunma söz konusu olduğundan yakınlık unsuru aranmamaktadır[987]. Buna karşın "*pre-emptive*" ve "*anticipatory*" meşru müdafaa hallerinde, var olan tehdidin zamansal bir yakınlık gerektirmesi söz konusudur. Bush doktrini[988] olarak da ifade edilen "*pre-emptive*" meşru müdafaada daha geniş bir zamansal yakınlık benimsenirken "*anticipatory*" meşru müdafaada silahlı saldırı tehdidinin zamansal yakınlığına dair açık emareler söz konusudur.

Bu bahsedilen meşru müdafaa türlerinden çok geniş bir zaman aralığına uzanan tehdit olasılığını içeren "*preventive*" ve "*pre-emptive*" meşru müdafaa türlerinin uluslararası hukuka uygunluğu tartışmaya açık bir konudur[989]. Uygulamada benimsenen diğer meşru müdafaa türleri Türkçede önleyici meşru müdafaa olarak ifade edilmekte olup yakın bir silahlı saldırı tehdidini gerektiren bu savunma şekillerinin konvansiyonel saldırılarda hukuka uygun kabul edilebilmesi mümkündür. Tüm bu savunma şekillerinin siber saldırılar yönünden değerlendirilmesi halinde tehdidin yakınlık unsuru yönünden tamamen farklı bir bakış açısının gerektiği sonucuna varılmaktadır.

Bir klavye tuşu dokunuşuna sığabilecek kısa zamanda saldırının gerçekleşebilmesini olanaklı kılan siber saldırıların ilk hareketi gerçekleşmeden önce yakın tehdit tanımının neye göre yapılacağı başlı başına bir sorundur[990]. Milisaniyeler içinde gerçekleşen siber saldırılarda geleneksel yakınlık unsuru çok bir anlam ifade etmediğinden Michael Schmitt

---

[987] DeWeese, 2015, s. 86.

[988] Bush doktrini temel olarak "ön alıcı vuruş" (pre-emptive strike) ve "önleyici savaş" (preventive war) kavramlarını içermektedir. Bkz.; Karadağ, 2016, s. 184.

[989] Bir görüşe göre, bu meşru savunma türü *Caroline Davası*'ndaki ilkelere uyduğu ölçüde meşru kabul edilmektedir. Bkz.: Ünal, 2005, 317.

[990] Zira siber saldırıların kendine özgü yapısı nedeniyle meşru müdafaa konusunda yasaklayıcı görüşler ortaya çıkabilmektedir. Bir görüşe göre, uluslararası hukukta saldırıların kaynağı açısından önleyici meşru müdafaanın kabul görmemesi karşısında siber saldırılarda meşru müdafaa hakkına başvuru hakkının kabul edilmesi mümkün görülmemektedir. Bkz.: Erdem ve Özocak, 2019, s. 143.

tarafından "son fırsat penceresi" [991] standardı önerilmektedir [992]. Bunun için de üç faktörün birleşmesi gereklidir. Bunlar sırasıyla; saldırıyı gerçekleştirecek olan devletin silahlı saldırı seviyesinde bir siber saldırıyı gerçekleştirebilecek kapasitede olması, saldırganın bu yönde bir niyetinin bulunması ve son olarak mağdur devletin saldırıyı o anda önlememesi halinde kendisini etkili şekilde müdafaa fırsatını kaçıracak olmasıdır (*the last window of opportunity*) [993]. Bu noktada siber kapasitenin geliştirilmesinin ve siber acil durum planlaması yapılmasının tek başına tehdit olarak kabul edilemeyeceği dikkate alınmalıdır[994]. Ayrıca hedef seçimi, silahlı saldırıyı defetmek amaçlı bir askeri hedef olmalıdır ancak siber saldırılar açısından siber uzayın sivil ve askeri şekilde kullanıma yönelik ikili yapısı nedeniyle bu konuda daha esnek değerlendirme yapılmalıdır.

Amerika-İsrail görüşünü yansıtan Michael Walzer'e[995] göre önleyici meşru müdafaanın söz konusu olabilmesi için tehlikenin çok yakın olması ve tehdidin somut olması gereklidir. Önleyici meşru müdafaayı haklı kılan yeterli tehdidin ise üç unsur içermesi gereklidir. Schmitt'in yukarıda bahsedilen önleyici meşru müdafaa görüşü ile benzerlik gösteren bu unsurlar; tarihten gelen veya yakın zamanlı açık bir yaralama niyetinin açığa çıkarılması, olumlu tehlike niyetini, bir diğer ifadeyle somut tehlike algısını oluşturan aktif askeri hazırlık derecesi ve son olarak savaşma dışında bir şeyler yapma veya

---

[991] Bu deyim, arzu edilen sonucun elde edilmesine yönelik adımın atılması gereken zaman dilimini ifade etmekte olup bu zaman diliminde eylemin gerçekleştirilmemesi halinde fırsatın kaçırılması anlamına gelmektedir. Daha ayrıntılı bilgi için bkz.: Wikipedia The Free Encyclopedia. Erişim: 09.11.2022. https://en.wikipedia.org/wiki/Window_of_opportunity

[992] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 247.

[993] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 247.

[994] Goldsmith, 2013, s. 137.

[995] Michael Walzer, "*Just and Unjust Wars*" adlı kitabın yazarı olup, önde gelen bir Amerikalı siyaset teorisyenidir. Walzer'in savaş felsefesi hakkında daha ayrıntılı bilgi için bkz.: Sönmez, Seda. (2019). *Michael Walzer ve Haklı Savaş Problemi*. Yüksek Lisans Tezi, Hacettepe Üniversitesi. Erişim: 16.12.2021 10218355.pdf (hacettepe.edu.tr)

bekleme halinde saldırıya uğrama riskinin büyük oranda artmasıdır[996]. Buna karşın, bu iki farklı görüşe uzlaştırıcı bir yaklaşım geliştiren bazı tarafsız yazarlar, her iki görüşün şartsız bir kabulünden söz edilemeyeceğini ileri sürmektedir[997].

Ayrıca ifade edilmesi gereken bir diğer husus da şudur ki Güvenlik Konseyi kararı uyarınca gerçekleştirilen ortak müdahalenin diğer devletlerin meşru müdafaa haklarını engelleyecek bir biçimde uygulanmaması bir zorunluluktur. Meşru müdafaa dışındaki diğer zorlama önlemleri BM tarafından oluşturulacak bir güç ya da BM izni ile ilgili devletler ya da bölgesel güçler tarafından yerine getirilmektedir. BM Şartı'nın 39. maddesine göre bu önlemlere başvurulabilmesi için BM Şartı'nın 41. maddesinde öngörülen önlemlerin yetersiz kalması üzerine 42. maddesi gereğince gereken müdahalelerde bulunulması söz konusu olmaktadır. Kuvvet kullanımın ne şekilde gerçekleştirileceği ise Güvenlik Konseyi tarafından belirlenecektir.

Ne var ki uygulamada, bazı devletler tarafından meşru müdafaa hakkına başvurulmayıp kuvvet kullanımını içeren zararla karşılık yöntemi ile süresinde gerçekleştirilmeyen meşru tepki hukuka uygun hale getirilmeye çalışılmaktadır. Sonradan gerçekleştirilen bu eylemin, BM Şartı'nda öngörülmemesi nedeniyle hukuki dayanağı bulunmadığından, meşrulaştırma aracı olarak uluslararası hukukun kaynaklarından biri olan yapılageliş kuralı oluşturup oluşturmayacağı konusunda isabetli bir görüşe göre[998]; yapılagelişin oluşması için gerekli olan iki unsurdan ilki olan devletlerin sürekli aynı biçimde bir davranış sergilemesi ve ikinci unsur olarak *opinio juris* unsurunun bir diğer ifade ile bir hukuk kuralı olduğu inancının eksik olduğu gerekçesiyle kuvvet kullanımını içeren zararla karşılık önlemi yapılageliş kuralı olarak değerlendirilemeyecektir.

[996] Orend, 2000. s. 539.

[997] Alder, 2013, s. 108.

[998] Keskin, 1998, s. 100.

3.3.4. Meşru Müdafaanın Diğer Zorlama Yollarından Farkı

Zararla karşılık (*forcible reprisals*) ile meşru müdafaayı ayıran husus, meşru müdafaada devam eden bir saldırıya karşı acil korunma amacıyla verilen bir cevabın söz konusu olmasıdır[999]. Aslında bu tepki eyleminin, hukuka aykırı olsa da uluslararası hukuka aykırı bir eyleme cevap olarak verilmesi nedeniyle meşru olduğu savunulmaktadır. Bir görüşe göre bu eylem normalde uluslararası hukukun ihlali olabilirse de daha önce gerçekleşen bir yasa dışı eyleme cevaben yapılması nedeniyle hukuka aykırı değerlendirilmemektedir[1000].

Zararla-karşılığın tipik örneğini Kelsen, uluslararası sorumluluğu bulunan devletin malvarlığına el konulması veya vatandaşlarının alıkonulması, ya da antlaşma yükümlülüklerinin yerine getirilmemesi olarak göstermektedir[1001]. Savaş zamanı zararla karşılık, savaş araçları bakımından kurallara uymayan taraf yönünden yasağa riayet etmemek şeklinde olabilir. Karşı önlemler başlığı altında ifade edileceği üzere zararla-karşılığın sorumluluk gerektiren eylem ile orantılı olmak zorunda olduğu 1927-1928 tarihli *Naulilaa Davası*'nda[1002] kabul edilmiştir[1003]. Ayrıca kuvvet kullanımını içermeyen bir ihlal durumunda zararla-karşılığın temel kuralı gereği kuvvet kullanılamayacağı kabul edilmektedir[1004].

---

[999] Arend ve Beck, 1993, s. 42.

[1000] Arend ve Beck, 1993, s. 17.

[1001] Kelsen, 2012 s. 24.

[1002] Hakemlik Kararı, "Naulilaa Arbitration", 31 Temmuz 1928, Erişim: 15.07.2022 https://www.scribd.com/document/506919046/Naulilaa-Arbitration-Portugal-vs-Germany-Google-translated

[1003] Arend ve Beck, 1993, s. 17.

[1004] Bu ayrım için bkz.; Keskin, 1998, s. 93.

3.3.5. Siber Savaşta Meşru Müdafaa Hakkı

Meşru müdafaa hakkının genel çerçevesi çizildikten sonra siber saldırı halinde belirtilen kuralların ne şekilde uygulanacağını ortaya koymak adına bu konuda yapılageliş hukukunun oluşup oluşmadığı ve sonrasında BM Şartı'nın 51. maddesi hükmü, hukukun genel ilkeleri, BM kararları ve yargı kararları kapsamında değerlendirme yapmak uygun olacaktır.

Siber saldırıların yeni bir konu olması nedeniyle yapılageliş hukukunun oluşup oluşmayacağı konusunda Roscini, siber saldırıların bilgisayarın icadı kadar eskiye gittiği, yine yapılageliş hukukunun uzay hava sahası ve kıta sahanlığı konularında olduğu üzere çok kısa bir sürede gerçekleşebileceği gerekçesiyle konuya olumlu yaklaşmaktadır[1005]. Buna paralel olarak öğretide bazıları, siber savaşa ilişkin halen çözüme kavuşmamış olan silahlı saldırı eşiği ve meşru müdafaa şartları gibi konularda yeni uluslararası antlaşmaların çözüm olamayacağı, bunun yerine devlet uygulamalarıyla oluşacak yapılageliş hukukunun belirleyici olacağı savunulmaktadır[1006]. Buna karşın siber güvenlik bağlamında küresel düzeyde tartışmasız bir uzlaşı bulunmamaktadır[1007].

Bu konuda Tallinn El Kitabı'nda BM Şartı 51. maddesinin müdafaa hakkının yapılageliş hukukunu yansıttığı ve benimsediği ifade edilmekle bu hak yapılageliş hukuku bağlamında değerlendirilmiştir[1008]. Yapılageliş hukukunun oluşabilmesinde devletlerin yanında önemli bir aktör olan uluslararası örgütler açısından bakıldığında, NATO'nun 2008 tarihli Siber Savunma Politikası Belgesi'ndeki[1009] ve 2010 yıllarında gerçekleşen siber saldırılara yönelik yaklaşımının NATO Kurucu Şartı'nın ortak meşru müdafaayı düzenleyen 5. maddesi yerine danışmayı düzenleyen 4. maddesinin benimsendiği

[1005] Roscini, 2010, s. 123.

[1006] Waxman, 2013, s. 115.

[1007] Weglinski, 2016, s. 81.

[1008] Schmitt, 2017, *Tallinn Manual 2.0*. s. 339.

[1009] NATO Bükreş Zirvesi Bildirisi için bkz.: https://sgp.fas.org/crs/row/RS22847.pdf Erişim: 09.11.2022.

görülmektedir[1010]. Bu bağlamda Gürcistan ve Estonya siber saldırılarına karşı NATO'nun takındığı tavrın bu saldırıların silahlı saldırı düzeyinde kabul edilmediğine işaret etmektedir. Tallinn El Kitabı'nda Uzmanlar Grubu çoğunluğunca silahlı saldırı düzeyine ulaşan siber saldırılara karşı bir devlet adına hareket edilmese dahi devlet dışı aktörlere karşı da meşru müdafaa hakkının kullanılabileceği kabul edilmektedir[1011]. Bu görüşe ulaşırken özellikle 9/11 saldırısı sonrasında devletlerin takındığı tavır üzerinden değerlendirme yapıldığı anlaşılmaktadır. Buna karşın 9/11 saldırıları sonrasında ABD'nin El Kaide ye yönelik saldırısı Afganistan devletinin terör örgütlerine karşı etkisiz kalmasından kaynaklanmış ve yine başka bir devleti hedef almıştır.

Kural olarak devlet dışı örgütlerin bir devlet adına hareket etmesi ya da bir devletin tatmin edici düzeyde dâhil olması halinde mağdur devlet, gereklilik ve orantılılık ilkesi kapsamında meşru müdafaa hakkına başvurabilmektedir[1012]. Devlet dışı örgütün kendi adına hareket etmesi halinde ise zarar gören devletin sıcak takip yapıp yapamayacağı sorusu ortaya çıkmaktadır. Uluslararası deniz hukuku uyarınca geleneksel anlamda sıcak takip yapılabilmesi bir başka devletin karasularına kadar mümkündür[1013]. ABD ve İsrail devletlerinin savundukları karada sıcak takip konusu tartışmalı bir alan olup egemen bir devletin rızası olmadan ülke topraklarında terörle mücadele adı altında silahlı bir müdahalenin hukuka uygun olduğu söylenemez. Deniz hukukuna göre dahi sıcak takip diğer bir devletin egemenlik alanında son bulmakta, her durumda uyarı ve orantılılık şartının da gözetilmesi gerekmektedir. Bu bağlamda Tallinn El Kitabı'nda bu hukuki argüman üzerinden devlet dışı örgütler tarafından gerçekleştirilen siber saldırılara karşı meşru müdafaa hakkının olanaklı görülmesi isabetli bir yaklaşım değildir. Bu konuda geleneksel uygulamalar üzerinden kıyas yapılması uygun olmayacaktır.

[1010] Roscini, 2010, s. 127-128.

[1011] Schmitt, 2017, *Tallinn Manual 2.0.* s. 345.

[1012] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 249.

[1013] Bozkurt ve Erdal ve Poyraz, 2017, s. 150.; Sur, 2022, s. 404-405.; Aksar, 2021, (2. Kitap), s. 95-96.

Siber uzayın fiziki dünyadan farklı yapısı dikkate alındığında devlet dışı bir örgüt tarafından gerçekleştirilen bir siber saldırıya karşı zarar gören devletin yine siber araçlar vasıtasıyla aktif savunma tedbirlerini uygulaması ve suçluların iadesi yoluna başvurması hukuka uygun olacaktır. Aksi durumda tek bir bilişim korsanının eylemi sonucunda siber saldırının kaynağı olan bir başka devlet ülkesine yönelik olarak meşru müdafaa hakkı kapsamında siber ya da konvansiyonel bir silahlı saldırı gerçekleştirilmesi meşru kabul edilemez.

Ancak Uzmanlar Grubunun çoğunluğu, siber saldırının kaynaklandığı ülke devletinin engel olamaması ya da isteksiz davranması ve gereklilik ilkesinin bulunması halinde, ülke topraklarının uluslararası hukuka aykırı şekilde kullandırmama yükümlülüğü bağlamında zarar gören devletin diğer ülke sınırlarından gerçekleştirilen ancak devlete atfedilemeyen bir siber saldırıya karşı meşru müdafaa hakkının kullanılabileceğini savunmaktadırlar[1014]. Ayrıca aksi görüşün kabul edilmesi halinde dahi uluslararası insan hakları hukukuna göre yaşam hakkının korunması ilkesi gibi başka bir sebebe dayanılarak saldırıya cevap verilmek zorunda kalınacağı belirtilmektedir[1015]. Öğretide ilk görüşü destekleyenlere göre ise, BM Şartı'nın meşru müdafaaya ilişkin metninin bu olasılığı hariç tuttuğuna dair bir hüküm taşımadığı gibi yapılageliş hukuku da silahlı bir gruba karşı meşru müdafaa hakkını tanımaktadır[1016]. Oysaki uluslararası metinlerin tüm olasılıkları değerlendirerek yasaklayıcı bir hüküm içermesi beklenemeyeceğinden böyle bir gerekçeye dayanmanın hukuka uygun olduğu söylenemez. Benzer bir uygulama *Lotus&Bozkurt Davası*'nda benimsenmiş iken UDHS ile birlikte bunun aksi bir kural kabul edilmiştir[1017].

[1014] Schmitt, 2017, *Tallinn Manual 2.0.* s. 347. Azınlık görüşünün gerekçesini oluşturan UAD'nın *Duvar Görüşü* ve *Congo ve Uganda Davası*'ndaki muhalif yargıçlara göre devlet dışı örgüt faaliyetlerinin devlete atfedilmedikçe meşru müdafaa hakkı uygulanamayacaktır. Bkz.: Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 249-250.

[1015] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 250.

[1016] Gill ve Ducheine, 2013, s. 446.

[1017] Aksar, 2021, (2. Kitap), s. 50-51-92.

Tallinn El Kitabı'nda 71. Kural başlığı altında doğal meşru müdafaa hakkının silahlı saldırı eşiğine ulaşmış bir siber operasyonun hedefi olan bir devlet tarafından gerçekleştirilebileceği kabul edilerek, bir siber operasyonun silahlı saldırı oluşturup oluşturmayacağının harekâtın boyut ve etkisine bağlı olduğu belirtilmiştir[1018]. Daha önce de ifade edildiği üzere meşru müdafaa hakkının kuvvet kullanma eylemine karşı kullanılıp kullanılamayacağı konusunda uluslararası hukukta açık bir düzenleme bulunmadığından konu, UAD tarafından *Nikaragua Davası*'nda açıklığa kavuşturulmuş ve meşru müdafaanın ancak silahlı saldırı düzeyine ulaşan bir kuvvet kullanma halinde söz konusu olabileceği ortaya konulmuştur.

Siber saldırıların silahlı bir çatışmanın parçasını oluşturmadığı zamanlarda tek başına silahlı bir saldırı oluşturması gerektiği daha önce belirtilmişti. Bu kapsamda barış döneminde hükümete ait bilişim sistemine her sızma halinde önleyici meşru müdafaa hakkı doğmaz ise de devletin hayati ulusal çıkarları yönünden kritik olan hassas sistemlere yönelik olan saldırılarda gerekli ve orantılı olmak kaydıyla uygulanabileceği[1019] daha önce de belirtilmişti. Kritik altyapı tesislerini hedef alan bir siber saldırının önemli bir zarara ya da yaralanmaya ya da ölüme sebep olmadığı halde dahi devletin temel işlevlerinde ve istikrarında ağır, uzun dönemli ve makul zaman diliminde onarılamayacak bir işlevsizliğe sebep olacak potansiyel aksama durumlarında meşru müdafaa hakkının doğduğu kabul edilmelidir.

Bir devletin ülkesinden devlet dışı bir aktör tarafından organize edilen, yönetilen veya yönlendirilen siber saldırı açısından bakıldığında ilgili devletler, uluslararası hukukla uyumlu (insan hakları hukuku ve uluslararası olmayan silahlı çatışmalar için silahlı çatışma hukuku gibi) iç hukuklarına uygun şekilde kuvvet kullanarak cevap verebilir[1020]. Buna paralel olarak öğretide, devlet dışı bir örgüt tarafından gerçekleştirilmesi an meselesi olan bir siber saldırı istihbaratı nedeniyle kaynak devlete yönelik mağdur devlet

[1018] Schmitt, 2017, *Tallinn Manual 2.0.* s. 339.; Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 244.

[1019] Sharp, 1999, s. 129.

[1020] Schmitt, 2017, *Tallinn Manual 2.0.* s. 340.

tarafından ya da kolektif meşru müdafaa kapsamında teknolojik üstünlüğü olan bir başka devlet ile birlikte gerçekleştirilecek orantılı bir önleyici saldırının hukuka uygun olduğu kabul edilmektedir[1021]. Uluslararası hukukun ihlalleri, eğer bu ihlal başka bir devletin ülkesinde kuvvet kullanımını içeriyorsa, silah kullanılmasa dahi madde 2/4 anlamında bir kuvvet kullanma oluşturabilir, ancak meşru müdafaa kapsamında karşılık verilebilmesi için ihlalin doğurduğu tehlike açısından gereklilik ve orantılılık şarttır[1022].

Silahlı saldırı düzeyine ulaşan bir siber saldırıya maruz kalan devletin ne şekilde cevap verebileceği, siber saldırıyı bir siber saldırı ile karşılamak zorunda olup olmadığı konusunda Schmitt, karşılığın konvansiyonel silahlarla verilebileceği gibi bir siber operasyon şeklinde de gerçekleşebileceğini ifade etmektedir[1023]. ABD'nin yaklaşımı da bu yönde olup siber saldırılara karşı her türlü meşru müdafaa araçlarının kullanılabileceği yetkililerce ilan edilmiştir[1024]. Siber saldırıları önleme ya da püskürtme amaçlı bu savunma tedbirleri zamansal bakımdan kritik bir ödeme sahiptir. Zira savunma durumundaki devletin cevabı ne kadar erken olursa saldırının durdurulması ya da püskürtülmesi de o kadar kolay olacaktır[1025]. Buna karşın çoğu siber operasyonun hız, öngörülemezlik ve gizlilik içeren doğası, saldırganın sızmasından aylar sonra ortaya çıkabilecek zararlı etkileri, iyi tasarlanmış ve zamanlanmış devam eden veya olası bir saldırıyı, savunma durumundaki devletin zamanında tespit etme, püskürtme veya önlemeye yönelik tepki verme yeteneğini güçleştirmektedir[1026]. Bu bağlamda siber saldırılara maruz kalan devletin savunma anında zamana karşı yarışı başlarken öngörülemezliğin sebep olduğu sis perdesi içinde saldırıdan sorumlu olanı bulma konusunda da zorluk yaşaması kaçınılmazdır.

[1021] Corn ve Jensen, 2018, s.2.

[1022] Sharp, 1999, s. 100.

[1023] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 244.: Blank, 2013, s. 418.

[1024] Waxman, 2013, s. 113.

[1025] Hruza ve Cerny, 2017, s. 157.

[1026] Melzer, 2011, s. 18.

Gerek zaman baskısı gerekse de siber saldırıların gizli bir yapıya sahip olmasından kaynaklı saldırıda bulunanın açık bir şekilde tespitinin zorluğu karşısında özellikle de aktif savunma önlemlerine başvuru hakkının bulunup bulunmadığı sorusu akla gelmektedir. Saldırganın kimliğine bakılmaksızın aktif savunma hakkının söz konusu olup olamayacağı sorusuna Roscini, devletin uluslararası sorumluluğuyla çelişik olması ve mantığa aykırı olması nedeniyle olumsuz cevap vermekte, ayrıca kritik altyapı unsurlarının tam olarak tanımlanamaması, uluslararası sınırlar arasında aktif savunmaya başvurulamayacağı gerekçeleriyle karşı görüşe itiraz etmektedir[1027]. Daha önce ilgili başlık altında incelendiği üzere kritik altyapı tesisleri konusunda gerek devletler uygulamalarında ve gerekse de öğretide görüş birliği bulunmamaktadır. Zira devlet uygulamalarında genel olarak bu tesislerin fiziki varlıklar olarak tanımlandığı görülmekte ise de öğretide siber savaş durumunda sanal tesisleri de kapsayabileceği savunulmaktadır[1028].

Roscini'nin olumsuz görüşüne karşın ifade edilmelidir ki aktif savunmanın tespit ve izleme yanında en büyük işlevi caydırıcılığa yönelik olup bu da ancak aktif savunma kapsamında bir karşı saldırı ile gerçekleştirilebilir. Karşı saldırının bileşenleri ise, cezalandırıcı karşı saldırı (*retributive counterstriking*) saldırgana zarar vermek suretiyle cezalandırmak ya da saldırının başarıya ulaşmasına engel olmak (*mitigative counterstriking*) şeklinde kendini gösterir[1029]. Pasif savunmanın, sıfırıncı gün açıklığı söz konusu olduğunda etkisiz kalması yanında [1030] saldırganı farklı yöntemlerle tekrar denemeye teşvik etmesi olasılığı ve saldırganın eyleminin ulusal hukuk dâhilinde cezalandırılabilmesi olasılığının da zayıflığı nedeniyle aktif savunma sistemleri kritik alt yapı tesisleri açısından önemli bir yer tutmaktadır.

[1027] Roscini, 2010, s. 119-120.

[1028] Hruza ve Cerny, 2017, s. 157.

[1029] Kesan ve Hayes, (Spring 2012). s. 431.

[1030] Kesan ve Hayes, (Spring 2012). s. 541.

Kendiliğinden ya da sistem yöneticisi tarafından gerçekleştirilecek hasar azaltıcı karşı saldırı halinde, saldırıyla ilgisi olmayan tarafların zarar görmemesi için gerekli saldırı rotasının izlenmesi ve atfedilebilirlik yönünden saldırıyı gerçekleştirenin tespitindeki teknolojik yetersizlik nedeniyle karşı saldırı yönteminin bu şartlarda uygulanması uygun değildir. Zira teknolojik seviyenin hasar azaltıcı karşı saldırı yönteminde istenen başarıyı sağlamaması yanında, düzen koruyucu yasa dışı gönüllülerin hukuka aykırı eylemlerine yol açılacağı endişesi söz konusudur[1031]. Siber saldırılara karşı caydırıcılık yönünden özel hukuk davaları ve pasif savunma tedbirlerine nazaran aktif savunma tedbirleri daha önemli bir yer tutsa da saldırganı doğru şekilde belirleme konusundaki zorluk nedeniyle ulusal sınırlar dâhilinde etkili bir siber suçlar politikasının daha faydalı olduğu tezi yerinde bir tespittir[1032]. Siber saldırılar ile mücadelede failin tespitinin zorluğu, cezai uygulamalara ilişkin uluslararası tutarlı bir sistemin bulunmaması ve yargılama yetkisindeki karmaşıklık nedeniyle ulusal ceza yargılamalarında beklenen sonuç elde edilememektedir. Aynı şekilde, failin tespiti sorunu ve üçüncü kişinin tazminattan sorumlu tutabilmesi olasılığının düşük olması nedeniyle özel hukuk yoluyla tazminat davaları vasıtasıyla da olumlu sonuç alınması mümkün görülmemektedir[1033].

Aktif savunma tedbirleri siber uzayın kendine özgü yapısından dolayı ilave zorluklar barındırmakta olup öğretide kuvvet kullanmayı düzenleyen hukuk kuralları gereğince saldırının atfedilebilmesi, karakterize edilmesi ve tarafsız devlet haklarının çiğnenemezliği olmak üzere üç halde söz konusu olan sınırlandırmayı karşılaması gerektiği kabul edilmektedir[1034]. Buna karşın bu unsurların uygulamada karşılanabilmesi her zaman mümkün olmayabilir. Uluslararası hukuk gereğince kuvvet kullanma yasağı devletleri bağlamakta iken devlet dışı aktörlerin, uluslararası ceza mahkemesi kapsamına

[1031] Kesan ve Hayes, (Spring 2012). s. 484-485.

[1032] Kesan ve Hayes, (Spring 2012). s. 486.

[1033] Kesan ve Hayes, (Spring 2012). s. 541.

[1034] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.231.

giren suçlar dışında, iç hukuka bağlı[1035] olmasından dolayı saldırganın devlet ya da devlet dışı aktör olup olmadığının tespitinin saldırı anında olanaklı olmamasından dolayı atfedilebilirlik kuralının siber uzayın kendine özgü yapısına göre değerlendirilmesi bir gerekliliktir.

Öğretide "oyun teorisi" olarak adlandırılan bir karşı saldırı modelinde, karşı saldırıyı gerçekleştiren devletin üçüncü kişilere verdiği zarardan hukuken sorumluluğu kabul edilmekte ve haklı savaş teorisinden yola çıkılarak bazı şartların gerçekleşmesi gerekli görülmektedir. Bunlar; karşı saldırının gerçekleştirilmemesi halinde ağır bir zarar oluşması tehdidinin varlığı, karşı saldırının önemli bir başarı olasılığını taşıması ve karşı saldırıya alternatif etkili ve uygulanabilir bir tedbir bulunmamasıdır[1036]. Bu model ile savunma saldırısı ancak bazı koşullar altında hukuka uygun kabul edilmekte ve zaruret haline benzer bir durumda aktif savunma yoluna başvurulabileceği kabul edilmektedir.

Aktif savunmanın ağır zarar doğurması tehlikesi özellikle kritik altyapı tesislerinin hedef alınması halinde kendini göstermektedir. Siber saldırının kritik alt yapı tesislerini hedef alması ancak saldırının silahlı saldırı eşiğine varmaması halinde dahi meşru müdafaa hakkının kullanılabileceği kabul edilmektedir[1037]. Eylemin veya saldırganın niyetinin düşmanca bir karaktere sahip olması konusunda ABD uygulaması, ilk merminin ateşlenmesinin beklenmeyeceği; saldırının kritik altyapı unsurlarına yönelik olduğu konusunda yetkililerin makul inancı taşıması halinde aktif savunma tedbirlerinin uygulanacağı yönündedir[1038]. Bununla beraber, siber saldırı halinde aktif savunma tedbirlerine başvuran bir devletin bu tedbirin meşru müdafaa sınırlarını aşmaması, çevresel zararı önlemesi ve gereklilik ve orantılılık ilkesi dâhilinde kalabilmesi için karşı

[1035] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.232-233.

[1036] Kesan ve Hayes, (Spring 2012). s. 487.

[1037] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s. 237.

[1038] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.236.

saldırının zararı azaltıcı (*mitigative*) nitelikte olması ve intikam amaçlı gerçekleştirilmemesi gerektiği kabul edilmektedir[1039].

Bu konuda bazı olasılıklar üzerinden hukuki değerlendirme yapmak mümkündür. İlki, aktif savunma eylemini gerçekleştiren görevlilerin sorumluluğunun sonradan yapılacak yargılamalarda değerlendirilmesine ilişkindir. Siber saldırının gerçekleştiği anda buna muhatap olan devlet birimlerinin kendi iç hukukları gereğince acil önlem alma görevi ve saldırıyı önleme yükümlülükleri gözetildiğinde saldırı anındaki şartlar altında değerlendirme yapılması uluslararası hukuka uygun bir yaklaşım olacaktır.

Bunun yanında, belirtilen devlet görevlilerinin olası bir siber saldırıya karşı gerçekleştirecekleri savunma saldırısının siber güvenlik politikası kapsamında sınırlarının belirlenmesi gerekir. Her devletin siber güvenlik politikasını uluslararası standartlara uygun hale getirmesi ve siber saldırı söz konusu olduğu takdirde uluslararası hukuka uygun bir yönerge dâhilinde hareket edecek uluslararası hukukçu, asker ve siber güvenlik uzmanlarından oluşan birimlerin oluşturulması ikinci bir olasılıktır.

3.4. KARŞI ÖNLEMLER

3.4.1. Genel Olarak

İç hukuktan farklı olarak, hukukun temel unsurlarından olan yaptırım gücü uluslararası hukuk alanında uluslararası barış ve güvenliğin bozulması dışında devletlerin takdirine bırakılmıştır. Uluslararası hukuk kurallarının ihlali suretiyle gerçekleşen bir eylemden zarar gören devletin bu eyleme cevaben gerçekleştirdiği karşı eylem bazı koşullar altında hukuka uygun kabul edilmekte ve devletin uluslararası sorumluluğu doğmamaktadır. Uluslararası hukukta karşı önlem ile zararla karşılık ve silahlı çatışmalar hukukunda söz konusu olan misilleme kavramlarıyla farklı anlamlar taşımaktadır. Devletlerin hukuk ihlali yapan karşı taraf devlete yönelik başvurabileceği kuvvet kullanmayı içermeyen karşı önlem, diğer önlemlerden farklı olarak, ihlal eden taraf devlete yönelik bir yaptırım

[1039] Kesan ve Hayes, (Spring 2012). s. 487.

aracı olarak değerlendirilmemektedir[1040]. Devlet egemenliğinin ihlali anlamına gelen bir siber operasyona karşı alınacak önlemler yönünden bu kavramların açıklanması gerekmektedir.

Uluslararası Hukuk Komisyonu Taslak Çalışması'nın 22. maddesinde düzenlenen karşı önlemler, herhangi bir devletin hukuka aykırı davranışına muhatap olan devletin, karşı önlem yoluyla ona cevap vermesini hukuka uygunluk sebebi kabul etmektedir[1041]. Buna göre, silahlı çatışmalar hukukunda kullanılan misilleme ve uluslararası hukuka aykırı eyleme karşılık yine uluslararası hukuka aykırı bir eylemle cevap verilmesi anlamına gelen ve BM öncesinde kuvvet kullanmayı da içerebilen zararla karşılık kavramları farklıdır. Zararla karşılık ile misilleme arasındaki farkı Pazarcı iki şekilde ifade etmektedir. Bunlardan ilki, misillemenin hukuka aykırı olmayan fakat zarar doğuran bir eyleme karşı olmasına rağmen, zararla karşılıkta zararlı eylemin aynı zamanda hukuka aykırı olması gereğidir. İkinci fark ise, karşı eylem açısından kendisini göstermekte olup buna göre zararlı eylemden dolayı tepki eyleminin uluslararası hukuku aykırı olmasına karşın misillemede tepki eyleminin hukuka uygun olmasıdır[1042].

Dar anlamda misillemenin (*retorsion*) hukuka aykırı olmaması nedeniyle kuvvet kullanmayı içermesi durumunda misilleme olarak nitelendirilemeyeceği ve zararla karşılık (*reprisals*) olarak değerlendirilmesinin gerekeceği, kuvvet kullanma içeren zararla-karşılığın ise BM döneminde hukuka aykırı kabul edildiği ifade edilmelidir. Zararla karşılık konusuna ilişkin olarak 1927-1928 tarihli *Naulilaa Davası*'nda[1043] kabul edilen sorumluluk gerektiren eylem ile orantılı olmak zorunluluğunun misilleme önlemi

[1040] Aksar, 2021, (2. Kitap), s. 309.

[1041] Aksar, 2021, (2. Kitap), s. 308.

[1042] Ayrıntılı bilgi için bkz.; Pazarcı, 2012, s. 439.; Benzer görüşler için ayrıca bkz.: Bozkurt ve Erdal ve Poyraz, 2017, s. 294.; Sur, 2022, s. 294.

[1043] Arend ve Beck, 1993, s. 17.; Karar için bkz.; Hakemlik Kararı, "Naulilaa Arbitration", 31 Temmuz 1928, Erişim: 15.07.2022 https://www.scribd.com/document/506919046/Naulilaa-Arbitration-Portugal-vs-Germany-Google-translated

açısından da geçerli olduğunun kabulü gerekir. Yargı kararlarında kabul edilen orantılılık ilkesinin gerek iç hukukta ve gerekse de uluslararası hukukta geçerli bir genel ilke olması hukuk mantığının da zorunlu bir sonucudur.

Pazarcı misilleme önlemlerinin başlıcaları arasında; "limanların ilgili devlet gemilerine kapatılması; ilgili devletle ticari ilişkilerin kesilmesi; ekonomik ve teknik yardımın antlaşmalara aykırı düşmeyecek biçimde kesilmesi; diplomatların istenmeyen kişi (*persona non grata*) ilan edilmesi; diplomatların ülke içindeki hareketlerinin sınırlanması; boykot (*boycott*) olarak anılan mal ithaline izin verilmemesi; karşı devletin yurttaşlarından vize istenmesi ya da ülkeye girişlerinin yasaklanması" nı saymaktadır[1044].

Zararla karşılık önlemlerinden eskiden beri başvurulan ve BM Şartı'nın kuvvet kullanma yasağına aykırı kabul edilen yöntemleri Pazarcı, barış içinde abluka, barış içinde işgal ve bombardıman olarak belirtmektedir [1045] . Kuvvet kullanılıp kullanılmamasına göre yapılacak bir ayrım halinde ise kuvvet kullanıldığında "abluka, ambargo, kuvvet çıkarma, işgal ve bombardıman" bu kapsamda sayılırken, "bir antlaşma ya da yapılageliş kuralının uygulanmaması ya da yabancıların toplu halde sınır dışı edilmesi" önlemleri güç kullanılmaksızın zararla karşılık yöntemi olarak kabul edilmektedir[1046].

Bu açıklamalara göre zararla-karşılığın hukuka uygun olarak kabul edilebilmesi için ilk olarak, uluslararası hukuka aykırı olan ve daha önce gerçekleşen bir eylemin bulunması ve zararla karşılık eyleminin ihlal oluşturan eyleme cevaben gerçekleştirilmesi gerekmektedir. İkinci olarak zararın tazmini talebinin başarısız kalması ve son olarak zarar ile cevap arasında yaklaşık bir orantılılık bulunması gereklidir[1047]. Bu bağlamda uluslararası hukuku ihlal eden ilk eylemi gerçekleştiren devlete yönelmeyip de üçüncü bir devlete zarar verilmesi eylemi bu kapsamda değerlendirilmeyecek ve uluslararası

[1044] Pazarcı, 2012, s. 439.

[1045] Pazarcı, 2012, s. 442.

[1046] Bu ayrım için bkz.; Keskin, 1998, s. 95.

[1047] Arend ve Beck, 1993, s. 17. Zararla karşılık eyleminin orantılı olması gerektiği konusunda bkz.; Bozkurt ve Erdal ve Poyraz, 2017, s. 296.; Sur, 2022, s. 295.

sorumluluğa sebep olabilecektir[1048]. Kelsen'e göre ise, uluslararası hukuk tarafından yetkilendirilmiş bir devletin misillemede bulunması uluslararası toplumun bir organı olarak hareket ettiği için meşru kabul edilmektedir. Buna karşın hukuka aykırı biçimde kuvvet kullanan devletin eylemi ise uluslararası hukukun ihlalini oluşturmaktadır[1049].

Komisyon çalışması öncesine bakıldığında; BM Genel Kurulu tarafından kabul edilen 1970 tarihli BM Şartı'na Uygun Olarak Devletlerarasında Dostça İlişkilere ve İşbirliğine İlişkin Uluslararası Hukuk Prensipleri Üzerine Deklarasyon, BM Şartı'nın 2/4 maddesi kapsamında kuvvet kullanmayı içeren misillemede bulunmama yükümlülüğü getirdiğinden, bu dönemde kuvvet kullanımını içeren karşı önlemlerin meşru kabul edilmediği görülmektedir[1050]. Bu kavramların farklılığını ortaya koyduktan sonra sonuç olarak; zararla karşılık ve silahlı çatışmalar hukuku kapsamında gerçekleşen misilleme eylemleri ile karşı önlem ya da aynıyla karşılık verme olarak da ifade edilen dar anlamda misillemenin farklı anlamlara geldiği anlaşılmaktadır[1051]. Ayrıca uluslararası hukuka aykırı eylemler nedeniyle zarar gören devletin karşı yükümlülüklerini yerine getirmeyi askıya alması önlemi ile dar anlamda misillemenin yakın anlamlar taşıdığı söylenebilir.

Uluslararası hukukta uygulanan diğer yaptırım ya da önlemlerden farklılığı ortaya konulan karşı önlemlere başvuru olanağı bazı şartlara bağlı tutulmuştur. Uluslararası Hukuk Komisyonu Taslak Çalışması'nın 50. maddesinde karşı önlemlerin sınırları ortaya konulmuştur[1052]. Taslak Çalışma'ya göre, hukuk ihlalinin durması halinde karşı önleme başvurulamayacağı gibi karşı önlemler temel insan haklarının ihlalini, misillemede silahlı çatışmalar hukuku yasaklarının veya uluslararası hukukun emredici hükümlerinin ihlalini

[1048] Uzun, 2007, s. 52.

[1049] Kelsen, 2012 s. 23.

[1050] Acer ve Kaya, 2014, s. 339.;

[1051] Öğretide bu kavramların farklı şekilde gruplandırıldığını görmek mümkün olup, misilleme ve zararla karşılığın karşı önlem başlığı altında tespiti için bkz.; Sur, 2022, s. 294.; Karşı önlemlerin diğer yaptırım araçlarından ayrı tutulması konusunda ise bkz.: Aksar, 2021, (2. Kitap), s. 309.

[1052] International Law Commission, 2001, s. 131.

ve diplomatların dokunulmazlığının ihlalini haklı kılmaz[1053]. Ayrıca yapılageliş hukukundan kaynaklanan orantılılık ilkesi, karşı önlemlere başvurulması halinde dikkate alınması gereken bir başka sınırlandırıcı unsurdur[1054]. Uluslararası sözleşmelerde ihlal halinde öncelikle başvurulabilecek çareler gösterilmiş ise karşı önlemlere başvurmadan önce bu hususun dikkate alınması da bir başka sınırlandırıcı unsur olarak ifade edilmektedir[1055]. Son olarak ifade edilmelidir ki karşı önlemlere başvurmadan önce zorunlu olan ön bildirim gerekliliği[1056] yanında kolektif önlemler ve önleyici önlemler şeklinde gerçekleştirilememesi nedeniyle karşı önlemlerin siber bağlamda meşru müdafaaya nazaran daha sınırlı bir seçenek sunduğu ve siber karşı önlemlerin etkinliğini azalttığı kabul edilmektedir[1057].

3.4.2. Siber Savaşta Karşı Önlemler

Karşı önlemler, yapılageliş hukukundan kaynaklanan ve meşru müdafaayı haklı kılan silahlı bir saldırı seviyesine erişmeyen, üstü kapalı olarak siber saldırıları içeren, uluslararası hukuk ihlallerine karşı devletlerin nasıl karşılık vereceklerini düzenler[1058]. Bu bağlamda, bir siber saldırının mağduru olan devlet, koşulları bulunması halinde, Güvenlik Konseyi ya da uluslararası yargı yolu dışında misilleme ve askeri olmayan karşı önlemlere de başvurabilir[1059]. Silahlı saldırı niteliğinde olmayan kuvvet kullanımına muhatap olan bir devlet ise, istemesi halinde, karşı önlem ya da zaruret ile uyumlu

---

[1053] Hathaway ve diğerleri, 2012, s. 857.

[1054] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 258.

[1055] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 258.

[1056] Siber bağlamda ön bildirim gerekliliği, uygulanabilirlik şartına tabidir. Ön bildirimde bulunmaya elverişli olunması halinde sorumlu devlete önleme imkânı sunulmalıdır. Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 258.

[1057] Corn ve Jensen, 2018, s. 3.

[1058] Hathaway ve diğerleri, 2012, s. 857.

[1059] Roscini, 2010, s. 113.

eylemler gibi tedbirlere başvurabilir[1060]. Meşru müdafaada olduğu üzere, karşı önlemlerin barış döneminde misilleme hukukunun tarihsel süreçte evrimsel sonucu olduğu kabul edilmektedir[1061].

Karşı önleme başvurmaya yol açan en muhtemel ihlal şekli, bir devletin egemenliğinin siber operasyonlarla ihlal edilmesidir[1062]. Uluslararası Uzmanlar Grubu'na göre başka bir devlette fiziki zarara veya yaralanmaya sebep olan siber operasyonlar genellikle devletin egemenliğinin ihlalini oluşturmaktadır[1063]. Uluslararası hukukun bu ihlalleri, zarar gören devlete ihlalden sorumlu devleti hukuka uymaya zorlayacak karşı önlemlere başvurma hakkı sağlar[1064]. Örneğin, bir devletin karasularından zararsız geçiş gerçekleştiren bir savaş gemisinin gerçekleştirdiği siber casusluk eylemine karşı zarar gören devletin karasularını bu devlete kapatmak suretiyle karşı önlem alması gösterilebilir[1065].

Yine Roscini, bir siber saldırının mağduru olan devletin kuvvet kullanımını içeren bir karşı önleme başvuramayacağını, ancak Şart'a veya yapılageliş hukukuna göre siber saldırının meşru müdafaayı tetiklemesi halinde bunun olanaklı olabileceğini ifade etmektedir[1066]. Taslak Çalışma'ya göre, aktif savunma niteliğinde karşı önleme başvuran devletin bunun öncesinde, diğer sınırlamalar yanında, uluslararası hukuka aykırı fiilin

---

[1060] Schmitt, 2017, *Tallinn Manual 2.0*. s. 337.

[1061] Corn ve Jensen, 2018, s. 3.

[1062] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 257.

[1063] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 257.; Siber operasyonların devlet egemenliğini ihlal ettiğini kabul eden Almanya devleti tutum belgesi için bkz.; Position Paper, 2021, s. 3.

[1064] Hathaway ve diğerleri, 2012, s. 857.

[1065] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 256.; Zira kıyı devletinin zararsız olmayan geçişi önlemek için gerekli önlemleri alma yetkisi bulunmaktadır. Bkz.: Toluner, 1996, s. 134.

[1066] Roscini, 2010, s. 113.

zarara sebep olduğunu ve sorumlu devleti belirlemesi zorunludur[1067]. Zira karşı önlemlere başvuru konusunda meşru müdafaadan farklı olarak getirilen bir diğer sınırlama uyarınca bu tedbirlere ancak devletlere yönelik olarak başvurulabilmekte, devlet dışı aktörlere karşı bu tedbirlere başvurulması mümkün görülmemektedir[1068].

Bir siber faaliyete yönelik karşı önlem alınabilmesi için eylemin uluslararası hukuka aykırı olması gereklidir. Örneğin, siber casusluk gibi uluslararası hukuka aykırı olmayan faaliyetlere yönelik karşı önlemlere başvurulamaz[1069]. Siber casusluk tek başına egemenliğin ihlalini oluşturmaz. Buna karşın, siber sistemlere yönelen bir siber operasyonun siber altyapının işlerliğini sürekli şekilde etkilemesi halinde egemenliğin ihlalini oluşturabilir[1070]. Roscini, hedef ülkede iç kargaşa çıkarmaya yönelik siber propagandanın, kuvvet kullanma yasağına ve içişlerine karışma yasağına aykırı olması nedeniyle hukuka aykırı olduğunu ve Devletin Sorumluluğuna İlişkin UHK Çalışması'nın 50, 51 ve 52 maddelerindeki sınırlandırma ve şartlarda mağdur devletin orantılı karşı önlemlere başvurabilme hakkı olduğunu belirtmektedir[1071].

Sınıraşan siber operasyonlara uluslararası hukukun uygulanabilirliği konusunda önemli bir tartışma bulunmamakla birlikte, pek çok uluslararası hukuk ilkesine kesin olarak uygulanabilirliği ve bunları düzenleyen kurallar konusunda uluslararası kamuoyunda uzlaşmaya varılamamıştır[1072]. Örneğin, Rusya'nın ABD seçimlerine müdahale ettiğini iddia eden ABD yönetiminin bu eylemin kabul edilemeyeceğini ve sineye çekilemeyeceğini ileri sürmekle birlikte müdahalenin hukuka aykırı olduğunu belirtmemesi karşısında yönetimin "egemen eşitlik" ilkesinin ihlali gerekçesiyle ABD

[1067] Hathaway ve diğerleri, 2012, s. 858.

[1068] Corn ve Jensen, 2018, s. 7.; Kesan / Hayes, (Spring 2012). s. 529.

[1069] Roscini, 2010, s. 113.

[1070] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 257.

[1071] Roscini, 2010, s. 113.

[1072] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 242.

istihbarat veya askeri birimlerinin aynıyla karşılık verebileceği anlayışı[1073] konusunda soru işaretleri söz konusudur.

Uluslararası haksız bir eyleme maruz kalan bir devletin karşı önlemlere başvurması zorunlu değildir. Zira yukarıda belirtilen Rusya'nın ABD seçimlerine müdahalesi örneğinde olduğu üzere diplomatların sınır dışı edilmesi ve ekonomik yaptırımların uygulanması da mümkündür[1074]. Aynıyla karşılık verme olarak da ifade edilebilecek dar anlamda misilleme söz konusu olduğunda, hukuka aykırı olmayan bir eyleme karşılık olarak fiziki güç kullanılmayıp, ihlal edilen menfaatin benzeri bir tepki göstermek gereklidir. Bir diğer ifadeyle misilleme, herhangi bir uluslararası sözleşme hükümleri ihlal edilmeksizin, herhangi bir zamanda gerçekleştirilebilen dostça olmayan bir eylemi ifade ederken, karşı önlem, öncesinde uluslararası bir yükümlülüğü ihlal eden başka bir devlete cevaben gerçekleştirilen, tek başına değerlendirildiğinde, cevap veren devletin uluslararası yükümlülükleriyle çatışan davranıştır[1075]. Buna göre, misillemeden farklı olarak mağdur olduğunu iddia eden devletin uluslararası bir yükümlülüğü ihlal eden bir davranışın, başka bir devletin hukuka aykırı bir davranışına karşı cevaben gerçekleştirmesi nedeniyle hukuka uygun hale gelmesi söz konusu olmaktadır.

Bunun yanında uluslararası hukukta karşı önlemlere yönelik getirilen yukarıda belirtilen sınırlamalar nedeniyle siber saldırılar yönünden devletlerin saldırıyı silahlı kuvvet kullanma olarak nitelendirerek meşru müdafaa hakkına başvurmaya yöneltmesi de diğer bir tehlikedir. Bu durumda siber saldırılara karşı anında ve etkili bir karşı önleme başvuramayan mağdur devletin silahlı saldırı eşiği konusundaki belirsizlik karşısında meşru müdafaa hakkını da kullanamaması uluslararası barış ve güvenliği tehlikeye

---

[1073] Bu konuda 5 nolu dipnota bakınız; Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 242. Kötücül siber araçlarla seçime müdahalenin içişlerine karışmama prensininin ihlalini oluşturacağına dair devlet tutumu hakkında bkz.; Position Paper, 2021, s. 5.

[1074] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 258.

[1075] Roscini, 2010, s. 113.

atabilecektir. Bununla birlikte, siber bağlamda pasif siber güvenlik yanında caydırıcılık açısından aktif savunma tedbirleri önemli bir rol oynayabilecektir.

Sorumluluğa sebep olabilecek yeterlilikte atfedilebilirlik koşulunun sağlanmasının zorluğu, yaptırım veya kamusal diplomatik protesto gibi misilleme önlemlerinin ötesinde bir tepkiyle cevap verilmesi çabalarını büyük oranda karmaşık bir hale getirmektedir[1076]. Zira siber saldırıların niteliği gereği zararlı eylemin gerçekleştiği anda aynı şekilde siber bir karşı eylem ile yanıt verilebilmesi en başta gelen karşı önlem olarak kendini gösterebilse de siber uzayda atfedilebilirlik koşulunun sağlanabilmesinin yarattığı zorluktan dolayı belirtilen misilleme önlemi dışında geleneksel bir karşı önleme başvurabilmek için ayrıca ilk eylemi gerçekleştiren devlete eylemin yeterli düzeyde atfedilebilir olması gereklidir.

Stuxnet saldırısında olduğu üzere uygulamada karşılan atfedilebilirlik sorunundan dolayı mağdur devletin uluslararası yargı yollarına başvurması etkili bir sonuç doğurmayabilecektir. Bu nedenle siber saldırıya karşı devletlerin alabilecekleri ilk önlem uluslararası mahkemelere başvurmak olabilirse de uluslararası mahkemelerin zorunlu yargı yetkisini haiz olmaması nedeniyle Şart'ın 96. maddesini işletmek suretiyle danışma görüşü talep edebilmeleri de olasılık dâhilinde kabul edilmektedir[1077].

Uluslararası bir antlaşmanın esaslı bir hükmünün ihlali *(material breach)* sonucunu doğuran hukuka aykırı bir fiilin gerçekleştirilmesi durumunda, 1969 tarihli VAHS'nin 60. maddesi [1078] diğer tarafa antlaşmayı sona erdirme veya tamamen veya kısmen yürürlüğünü askıya alma hakkı vermektedir. Uluslararası antlaşmanın sona erdirilmesi kural olarak iki tarafın iradesinin bu konuda birleşmesine bağlı olmakla birlikte bir tarafın antlaşmanın temel hükümlerine aykırı fiili söz konusu olduğundan tek taraflı fesih mümkün olabilmektedir. Anılan hükme göre antlaşmanın esaslı bir hükmünün ihlali iki

[1076] Jensen ve Watts, 2017, s. 1564.

[1077] Roscini, 2010, s. 111.

[1078] Antlaşma metni için bkz.; http://www.unicankara.org.tr/doc_pdf/Viyana_69.pdf Erişim: 15.04.2018

şekilde gerçekleşebilmekte olup bunlardan ilki, bu sözleşmenin onaylamadığı şekilde antlaşmanın inkâr edilmesi ve ikincisi ise antlaşmanın konu ve amacının gerçekleştirilmesi için elzem olan bir hükmün ihlal edilmesi halleridir.

Sözleşmenin hükümsüz kılınmasının aracı olarak uygulanan uluslararası hukuk, ayrıca, uluslararası hukukun öngördüğü antlaşmaların geçerlilik koşullarına aykırı olarak yapılan antlaşmaların geçersiz olacağını öngörmekte olduğu gerekçesiyle hukuka aykırı bir antlaşmanın batıl kılınması yoluyla hukuksal bir yaptırım uygulanmasının gerçekleştirilmekte olduğu ileri sürülmektedir[1079]. Kanaatimizce, VAHS'nin 65-68 maddelerine göre yapılacak bir geçersizlik iddiasının hukuka aykırı bir taraf fiilinden çok, irade sakatlığı gibi antlaşmanın oluşturulması veya yorumuyla ilgili bir konudan kaynaklanması nedeniyle sözleşmenin hükümsüz kılınması karşı önlem ya da yaptırım kapsamında değerlendirilmemelidir.

[1079] Pazarcı, 2012, s. 436.

4. BÖLÜM: SİBER SİLAHLI ÇATIŞMALAR HUKUKU JUS IN BELLO PARADİGMASINDA SİBER SAVAŞ

4.1. SİLAHLI ÇATIŞMALAR HUKUKUNUN TARİHSEL GELİŞİMİ VE KAPSAMI

Uluslararası hukukta silahlı çatışmaları düzenleyen kurallar, bu çatışmaların savaşan devletler ve üçüncü devletlerarasındaki hukuksal etkileri ile birlikte ele alınarak geleneksel anlamda savaş hukuku olarak adlandırılmaktadır[1080]. Savaş hukuku yerine sonraları insancıl hukuk ya da silahlı çatışmalar hukuku (*jus in bello*) kavramları kullanılmıştır[1081]. Bu çalışmanın adı ile uyumlu olacağı düşüncesiyle burada "siber" silahlı çatışmalar hukuku terimi tercih edilmiştir.

Silahlı çatışmalar hukuku kuralları ayrım yapılmaksızın genel olarak üç temel ilkeye dayanmaktadır. Söz konusu ilkeler; orantılılık, askeri gereklilik ve gereksiz acı ve ıstırabın önlenmesidir[1082]. Bunlar her silahlı çatışmada öncelikle gözetilmesi beklenen ve vazgeçilmez ilkelerdir. Bu ilkeler yanında silahlı çatışmalarda zorunlu olarak sivil kişi ve nesnelerin askeri hedeften ayrılması ve hedef alınmaması da bir yükümlülük olarak ortaya çıkmaktadır. Silahlı çatışmalar hukukunun geliştiği süreç içerisinde bazı silahların kullanılmasının yasaklanması söz konusu olmuştur. Bu yasak silahlar yanında hainlik olarak ifade edilen bazı yöntemlere başvurmak da hukuka aykırıdır. Ayrıca korunan kişiler sadece sivillerden ibaret olmayıp silahlı çatışma dışı kalan kişiler, esirler, sağlık ve din görevlileri gibi diğer kişilerin de koruma altında olması nedeniyle ayrıca incelenmesi gerekmektedir.

[1080] Pazarcı, 2021, s. 566.

[1081] Aksar, 2021, (2. Kitap), s. 175.

[1082] Mutlu, 2016, s.109.

Konunun daha iyi anlaşılabilmesi için silahlı çatışmalar hukukunun tarihsel süreç içerisinde nasıl şekillendiğine bakmak ve kapsamını tespit etmek gereklidir. Bu nedenle öncelikle tarihsel gelişim ve kapsam ortaya konulacak, sonrasında silahlı çatışmalar hukukunun siber savaşa uygulanabilir olup olmadığı tartışılıp, devamında siber silahlı çatışmalar yönünden ayrım, orantılılık, askeri gereklilik, gereksiz acı ve ıstırap verilmemesi ilkeleri ve diğer ilkeler ile silahlı çatışmalar hukukunda amirin emri ve tarafsızlık konuları incelenecektir.

4.1.1 Silahlı Çatışmalar Hukukunun Tarihsel Gelişimi

İsviçreli bir tüccar olan Henry Dunant, bizzat şahit olduğu Fransa ve Avusturya arasında bir Kuzey İtalya şehri olan Salferino'nun yakınında gerçekleşen savaşta binlerce İtalyan, Fransız ve Avusturya askerinin hayatını kaybetmiş olduğunu ve savaş alanında terkedilmiş vaziyette yatan büyük sayıdaki yaralı askerleri görmüş ve yaralı askerlere yardım etmek istemiştir. Bu amaçla, yakın köylerde kendi güvenliği için saatler öncesinden savaştan kaçan, hazırlıksız köylülerden bir yardım ekibi oluşturmuştur. Savaştan üç yıl sonra Dunant'ın, bu anılarını Solferino Hatırası ismiyle kitaplaştırması ve bu kitabın toplumda yarattığı şok etkisi sonucunda 1863 yılında Kızıl Haç kurulmuştur[1083]. Bunun ardından 1864 yılında imzalanan Cenevre Sözleşmesi ise silahlı çatışmalar hukukunun temellerinin atılması konusunda ilk adım olmuştur[1084].

Bu sözleşme ile başlayıp gelişen silahlı çatışmalar hukuku, uluslararası antlaşmalara ya da yapılagelişe dayanmaktadır[1085]. Antlaşma ve yapılageliş kurallarının yetersiz kalması

[1083] Ayrıntılı bilgi için bkz.: Burkle, Frederick M. (Aralık 2019). *Revisiting the Battle of Solferino: The Worsening Plight of Civillian Casualties in War and Conflict*, Disaster Medicine and Public Health Preparedness Journal, Cilt:13, Sayı: 5-6, s. 1-2. Erişim: 28.12.2021 https://www.researchgate.net/publication/335088896_Revisiting_the_Battle_of_Solferino_The_Worsening_Plight_of_Civilian_Casualties_in_War_and_Conflict

[1084] Gül, 2021, s. 7.

[1085] Silahlı çatışmalar hukuku, insan hakları hukukundan daha eski olup, yapılageliş hukuku kaynaklıdır. Aksar, 2021, (2. Kitap), s. 178.

halinde ise ortaya çıkabilecek boşlukların doldurulmasında uygulanabilecek kaynak genel hukuk ilkeleridir. Bu ilkeler arasında özellikle silahlı çatışmalar hukuku yönünden öne çıkan *Martens kaydı* önemli bir yer tutmaktadır[1086]. Belirtilen çok taraflı antlaşmalar arasında merkezi bir yer tutanları 1907 Lahey Konvansiyonları ve 1977 tarihli iki Ek Protokol dâhil 1949 tarihli Cenevre Konvansiyonları'dır. Bu konuda uygulanabilir yapılageliş kuralları derlemesi ise Kızıl Haç tarafından 2005 yayımlanmıştır[1087]. Ayrıca 2005 yılında ilave ayırıcı amblemlerin benimsenmesine ilişkin 3. Ek Protokol yayınlanmıştır[1088]. Bu konuda yapılageliş hukukunun önemi ortya çıkmaktadır. Zira silahlı çatışmalar hukukuna ilişkin bir antlaşmanın tarafı olmayan bir devlet yapılageliş hukuku niteliğini almış kurallarla bağlıdır[1089].

Silahlı çatışmalar hukukunun temelini oluşturan bu konvansiyonlar sınırlandırıcı çatışma kurallarını belirlemektedir. İlk olarak Lahey Konvansiyonları, çatışma eylemlerinin uygulamada askeri yönleriyle ilgili olup belirli silahların ve askeri taktiklerin yasaklanmasına yöneliktir[1090]. Bir diğer ifade ile bu Konvansiyonlar çatışma sırasında tarafların kullanacakları yöntemlerin nasıl sınırlanacağını ve güç kullanımında hangi oranda şiddet kullanılabileceğinin çerçevesini çizmekte ve bunu kurallara bağlamaktadır[1091].

Cenevre hukuku ise, 1864, 1906, 1929 tarihli önceki Konvansiyonları tamamlayıcı nitelikteki dört adet 1949 Konvansiyonlarını kapsamakta, sivillerin, savaş tutsaklarının, denizde ve karada yaralı ve hastaların korunmasına odaklanmaktadır[1092]. Bu haliyle devletlerin birey ve insan topluluklarına yönelik eylemlerini düzenlemeyi amaçlamakta

[1086] Aksar, 2021, (2. Kitap), s. 179.

[1087] Mačák, 2018, s. 9.

[1088] Afroditi, 2010, s. 22.

[1089] Aksar, 2021, (2. Kitap), s. 179.

[1090] Afroditi, 2010, s. 22.

[1091] Hoş, 2013, s. 92.

[1092] Afroditi, 2010, s. 22.

olan Cenevre Konvansiyonları Lahey Hukuku'ndaki gibi karşılıklılık esasına göre değil, devletlerin mutlak olarak uymaları gereken kurallardan oluşmaktadır[1093].

4.1.2. Silahlı Çatışmalar Hukukunun Kapsamı

Silahlı çatışmalar hukuku silahlı çatışma süresince kullanılan savaş araç ve yöntemlerine bakılmaksızın, herhangi bir kimseyi ya da nesneyi hedef alma durumlarına uygulanır[1094]. Zira silahlı çatışmalar hukukunun temelinde yatan amaç sivilleri korumaktır[1095]. Sivil kişi veya nesnelere yönelen saldırılarda yöntem ve araçlara bakılmaması, silahlı çatışmaların hiçbir kurala tabi olmadığı anlamına gelmemektedir. Sivil kişi ve nesnelerin her koşulda korunması yanında silahlı çatışmaların yöntem ve araçları belirli kurallara bağlanmıştır. Bu konuda kabul edilen 1907 Lahey IV Sayılı Kara Savaşının Kanunları ve Adetleri Hakkında Konvansiyon'a Ek Yönetmelik'in 22. maddesinde[1096] ve 1977 I. Protokolü'nün 35/1. maddesinde kabul edilen "tarafların düşmana zarar verme araçlarının seçiminde sınırsız bir hakka sahip olunmadığı" ilkesi çatışmanın taraflarını sınırlandırmaktadır[1097]. Sınırlama ilkesi olarak adlandırılan bu ilke silahlı çatışmalar hukukunun esas dayanak noktası ve en temel ilkesini oluşturmaktadır[1098]. Silahlı çatışmalar hukukunun ortaya çıkış nedeninin çatışmanın taraflarının silah seçiminde ve sebep olduğu zararın sınırlandırılması gereği olduğu dikkate alınırsa sınırlama ilkesinin önemi anlaşılabilir.

[1093] Hoş, 2013, s. 93.

[1094] Schmitt, 2017, *Tallinn Manual 2.0*. s. 414.; Schmitt, 2013, *Classification of Cyber Conflict*. s. 239-240.

[1095] Pascucci, CDR Peter. (2017). *Distiction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, Minnesota Journal of Int'l Law, Cilt:26:2, s. 452.

[1096] 1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022 http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

[1097] Pazarcı, 2021, s. 623.

[1098] Güneysu, Gökhan. (2011). *Çevrenin Silahlı Çatışmalar Esnasında Korunması*. Doktora Tezi, Eskişehir, Anadolu Üniversitesi, s. 163.

Silahlı çatışmalar hukukunun uygulanmasında bazı hususlar öne çıkmaktadır. Bunlar; çatışmanın vuku bulduğu bölge, silahlı karşılaşmada kullanılan yöntem ve silahlar, silahlı çatışmanın taraflarının uluslararası hukuki statüsü, bir silahlı çatışma boyunca kişi ve nesnelerin yasal olarak korunması, silahlı çatışmalar hukukunun ihlalinden sorumluk hususlarıdır[1099]. Buna göre silahlı çatışmalar hukuku, çatışan taraflar ve çatışma kuralları yanında korunan kişi ve nesneler ile kuralların ihlali halinde doğacak sorumluluğu da düzenlemektedir.

Bu noktada belirtmek gerekir ki çatışmanın taraflarının hukuki statüsünün ve devlet ile bağlantısının tespiti sorumluluk açısından önem arz etmektedir. Son yıllarda yaşanan silahlı çatışmaların çoğunlukla düzenli askeri birlikler arasında gerçekleşmediği, çatışmaların vekâlet savaşları şeklinde vuku bulduğu gözetilirse bu kuralların önemi ortaya çıkmaktadır. Bu konuya bakıldığında silahlı çatışmalar hukukunun uygulanabilirliği sadece devletin silahlı güç unsurlarıyla sınırlandırılmamakta, ayrıca savaşan taraflar adına *de jure* ya da *de facto* şekilde bir devlet ajanı olarak hareket eden diğer kişilerin eylemlerini kapsayacak biçimde genişletilmektedir[1100].

Silahlı çatışmalar hukukunun uygulanabilirliğinin ön şartı, silahlı bir çatışmanın varlığıdır[1101]. Çatışmayı oluşturan saldırı (*attack*) ise, Ek Protokol'ün 49. maddesinde düşmana karşı gerçekleştirilen saldırı ya da savunma şeklinde şiddet eylemi olarak tanımlanmıştır. Buna karşın uluslararası hukukta en yüksek düzenleme oranına sahip hukuk dallarından biri olarak kabul edilen[1102] uluslararası silahlı çatışmalar hukukunda, *jus in bello* ile ilgili sözleşmelerde silahlı çatışmanın tam olarak bir tanımı yapılmamıştır[1103]. Silahlı çatışmanın söz konusu olmaması halinde ise, uluslararası insan

[1099] Streltsov, 2017, s. 5.

[1100] Melzer, 2011, s. 24.

[1101] Schmitt, 2017, *Tallinn Manual 2.0*. s. 375.

[1102] Güneysu, 2012, s. 95.

[1103] Piatkowski, 2017, s. 273.; Aksar, 2021, (2. Kitap), s. 181-182.

hakları hukuku da dâhil diğer yasal rejimler öncelikle gündeme gelmekte olup bu halde barış zamanını düzenleyen uluslararası hukuk kuralları uygulanmaktadır[1104].

1949 tarihli Cenevre Konvansiyonları'nın ortak 2. maddesi, silahlı çatışma hukukunun uygulanacağı zamanı belirleyen, barış zamanı ile silahlı çatışma arasındaki geçiş noktasıdır[1105]. Bu maddede öngörülen silahlı çatışma hukukunun ne zaman başlayacağını belirleyen eşik, BM Şartı'nın 51. maddesi kapsamında silahlı saldırı eşiğine karşılık gelir[1106]. Sonuç olarak, 1949 tarihli Cenevre Konvansiyonları ortak 2. maddesindeki eşik anlayışı, çatışma yönetimi hukukuna göre kuvvet kullanımı ve silahlı bir saldırının ne olduğunu tanımlamaya yarar [1107] . Buna karşın, silahlı çatışmalar hukukunun uygulanabilmesi *jus ad bellum* kurallarına bağlı değildir[1108]. İnsancıl hukuk, silahlı çatışmaların *jus ad bellum* perspektifinde haklı ya da haksız olarak nitelendirilmesinden bağımsız olarak uygulanmaktadır[1109]. Buna paralel olarak saldırı kavramı konusunda olduğu kadar, özellikle orantılılık ve gereklilik ilkeleri yönünden her iki alanda farklılıklar kendini göstermektedir.

Daha önce de belirtildiği üzere; Uluslararası Kızıl Haç Komitesi (UKHK) tarafından yayımlanan 1949 tarihli IV. Cenevre Konvansiyonu Şerhi ortak 2. maddesi uyarınca, *de facto* silahlı çatışma için taraflardan birinin savaş durumunu inkâr etmesi, çatışmanın

[1104] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 261.; Silahlı çatışma söz konusu olmadığında, uluslararası hukuk uyarınca insan haklarının korunması konusunda bkz.: Bozkurt, Enver. (2003). *İnsan Haklarının Korunmasında Uluslararası Hukukun Rolü*. Ankara: Nobel Basımevi.

[1105] Sharp, 1999, s. 57-58.

[1106] Sharp, 1999, s. 58.

[1107] Sharp, 1999, s. 58.

[1108] Schmitt, 2017, *Tallinn Manual 2.0*. s. 377.

[1109] Position Paper, 2021, s. 7.

süresi, ne kadar kıyım yapıldığı, sonuca etki etmemektedir[1110]. Bu ibareden anlaşılması gereken ise, *de facto* silahlı çatışmanın varlığını belirleyici esas faktörler, iki devletin silahlı güçleri arasındaki kuvvet kullanımının kapsam, süre ve yoğunluk (*scope, duration and intensity*) durumlarıdır[1111]. Silahı çatışmanın varlığı konusunda asıl belirleyici faktör kuvvet kullanımının boyutudur.

Bu başlık altında son olarak ifade edilmelidir ki silahlı çatışmalar hukukunun çatışmaların sebep olduğu zararların sınırlandırılmasına yönelik geldiği nokta itibariyle yaşadığımız dönemde meydana gelen sivil can kayıplarını ve korunan tabiat ve doğal varlıkların zarar görmesini önleyemediği de bir gerçektir. Bu nedenle silahlı çatışma ve savaş durumlarında bazı eylemleri hukuka aykırı kabul eden bu hukuk dalının aynı zamanda savaşın meşrulaştırılmasına sebep olduğu yönünde eleştiriler söz konusu olmaktadır[1112]. Buna karşın kuvvet kullanmaya başvuru kurallarını *jus ad bellum*'un düzenlemesi ve silahlı çatışmalar hukukunun ancak kuvvet kullanımına başvurulduktan sonrasını düzenlemesi nedeniyle çatışmalarda yaşanan vahşetin dizginlenmesine hizmet etmesi nedeniyle silahlı çatışmalar hukuku kuralları vazgeçilmez kabul edilmektedir[1113].

4.1.3. Silahlı Çatışmalar Hukukunun Siber Savaşa Uygulanabilirlik Sorunu

Siber saldırının uluslararası hukuk açısından incelenmesi, barış hukuku yerine savaş hukuku içinde başlayıp gelişme göstermiş, 1990'ların sonunda silahlı çatışmalar hukuku

---

[1110] Pictet, Jean S. (Ed.) (1958). International Commitee of the Red Cross, *Commentary on the Geneva Conventions Relative to the Protection of Civilian Persons in Time of War,* s. 20. (bundan sonra 1949 tarihli IV. Cenevre Konvansiyonu Şerhi)

[1111] Sharp, 1999, s. 60.

[1112] Kolasi, Klevis. (2017). *Savaşın Değişen Niteliği ve Jus ad bellum ve Jus in bello'ya Etkisi.* İnsan Hakları Yıllığı, Cilt:35, s. 23.

[1113] Güneysu, Gökhan. (2012). *Askeri Gereklilik İlkesi ve Uluslararası İnsancıl Hukuk*. Ankara Barosu Dergisi, Sayı:4, s. 98-99.

dâhilinde yapılan akademik çalışmalar ile devam etmiştir[1114]. Buna paralel şekilde uluslararası silahlı çatışmalar hukukunun yeni alanlara uygulanabilirliği konusu hukuk insanlarının ve askeri çevrelerin tartıştığı bir konu olmuştur. Teknolojik gelişimin sebep olduğu yeni durumlar mevcut hukuk kurallarının yeni şartlara uygulanabilmesinde önemli zorlukları da beraberinde getirmektedir. Büyük önerme olarak hukuk normlarının, hayatın değişen şartlarına ve gerçekliğine göre değişen küçük önermeye, bir diğer ifade ile somut olaya uygulanması sürecinin ötesinde daha geniş ölçekte, hukuk sosyolojisi kapsamında teknolojik gelişimin yarattığı toplumsal yapıdaki değişimlerin de gözetilmesi gereklidir.

Bu gereklilik özellikle insanlık tarihinin sosyolojik yapısını değiştiren dönüm noktalarında kendini göstermektedir. Bunun, tarım toplumundan sanayi toplumuna geçiş sürecinde olduğu kadar, sanayi toplumundan bilgi toplumuna geçiş sürecinde de yaşanması kaçınılmazdır. 10 bin yıllık tarıma dayalı toplum yapısı, birkaç yüz yıl süren sanayi çağı ile değişirken son birkaç on yıllık dönemde bu değişim katlanarak devam etmiş ve yeni bir çağa girilmiştir.

Bilgi çağı olarak adlandırılan bu dönemde 20. yüzyıldan kalma hukuk kurallarının uygulanabilmesinde yaşanan zorluklar anlaşılabilir bir durumdur. Bu yeniçağda toplumların yapısı sadece kendi içinde değişmemiş, küresel düzeyde tüm toplumları hep birlikte değişime zorlarken bireysel olarak da insanların yaşamında kökten değişimler yaşanmıştır. Çağın en önemli icadı olan internetin toplumsal etkisi, siber uzayın sosyal katmanını yaratmış ve bu katman bireylerden başlayarak, küresel düzeyde toplumları ve devletleri de içine alarak büyümüştür. Böylece, ortaya çıkan bu yeni sanal dünyada gerçekleştirilen birey ya da devlet eylemlerine ve bu eylemlerin fiziki dünyadaki sonuçlarına hukuk kurallarının uygulanması zorunluluğu ile karşılaşılmıştır. Bunun bir

[1114] Mačák, Kubo. (2017). *From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law*, s. 4. Erişim: 20.04.2020 https://ccdcoe.org/uploads/2018/10/Art-09-The-Impact-of-the-Development-of-the-Cyber-Law-of-War-on-General-International-Law.pdf

adım ötesinde yeni bir konu olarak yapay zekâ eylemlerinden sorumluluk konusu bir kenarda durmaktadır[1115].

Gerek Cenevre Konvansiyonları ve gerekse 1977 tarihli bunlara Ek Protokollerin kabul edilmesinin ardından teknolojinin hızla gelişmesiyle bu sözleşmelerde açıkça düzenlenmeyen yeni silah türleri ortaya çıkmıştır[1116]. Siber uzay ise, çatışmaların gerçekleştiği diğer bir alan olarak kabul edilmiştir[1117]. Bu noktada internetin gelişiminden önce hayat bulan silahlı çatışmalar hukuku kurallarının siber uzayda gerçekleşen çatışmalara uygulanıp uygulanamayacağı sorusunun cevabı da öğretide görüş ayrılıklarına sebep olmuştur. Siber saldırılara silahlı çatışmalar hukukunun uygulanması konusunda yaşanan zorlukların, bir taraftan siber uzayın yeni bir alan olmasından, diğer taraftan silahlı saldırının aracı olarak siber uzayda gerçekleşen saldırılar konusunda uluslararası antlaşmaların yetersizliğinden kaynaklandığı savunulmuştur[1118]. Kimine göre ise bu eksiklik, siber savaşın kendine özgü yapısının yarattığı kusurdan kaynaklanmamakta, bunun yerine silahlı çatışmalar hukuku ilkelerinin belirsizliğinden ve geleneksel savaştan kaynaklanan etkilerine tarihi şekilde odaklanmaktan kaynaklanmaktadır[1119].

Bu bağlamda bir görüşe göre, silahlı çatışmalar hukuku düzenlemelerinin siber savaşın yeni paradigmasına uymadığı gerekçesiyle yeni antlaşmalar gerekli görülürken, Amerikan Hükümeti'nin de içinde bulunduğu bazı devletlere ve öğretide karşıt bir görüşe göre ise, yeni antlaşmalara gerek bulunmamakta, mevcut düzenlemelerin kıyas yoluyla

---

[1115] Bir karar verme süreci sonunda, insan müdahalesi olmadan, hedefi belirleyen, tanımlayan ve etkisiz hale getiren silah sistemlerinin eylemlerinden kaynaklı devletlerin uluslararası sorumluluğu konusunda daha ayrıntılı bilgi için bkz.: Pino, Beatriz. (2020). *International Responsibility of States and Artificial Intelligence*. Master Thesis, Barcelona Üniversity. Erişim: 30.12.2021. http://diposit.ub.edu/dspace/bitstream/2445/170430/1/TFM_Beatriz_Pino.pdf

[1116] Gül, 2021, s. 11.

[1117] Hruza ve Cerny, 2017, s. 156.

[1118] Streltsov, 2017. s. 1.

[1119] Pascucci, 2017. s. 452-453.

silahlı çatışmalar hukukuna uygulanması gerekli ve yeterlidir[1120]. Bu çözüm seçenekleri yeni antlaşma veya ek protokoller suretiyle olabileceği gibi mevcut antlaşmaların yapılageliş oluşturmaya yönelik devlet uygulamalarıyla düzeltilmek suretiyle de gerçekleştirilebilecektir[1121].

İlk görüşte olanlar, uluslararası silahlı çatışmalar hukukunun siber savaşa uygulanması halinde mevcut yasal boşlukların doldurulamamasından dolayı silahlı çatışmalar hukukuna ilişkin antlaşmaların yeniden düzenlenmesinin gerektiğini savunmaktadır[1122]. Bu görüşe göre, askeri ve sivil ağların birbirine bağımlı yapısı nedeniyle silahlı çatışmalar hukukunun temel ilkelerinin siber savaş durumunda yeterince etkili biçimde uygulanması söz konusu olmamakta ve bu durum sivil nüfusun ve sivil altyapı sistemlerinin gerektiği gibi korunamamasıyla sonuçlanmaktadır[1123]. Bu konuda balondan atılan patlayıcılar, kör edici lazer silahları ve genişleyen mermilerle ilgili olarak daha önce yeni silahların yasaklanmasına ilişkin pek çok antlaşmada düzenlemeler yapılması örnek olarak gösterilebilir[1124].

Diğer durumda ise, siber uzay gibi tamamen sonradan ortaya çıkmış ve fakat dış dünyada insan yaşamında son derece etkili sonuçlar doğuran yeni sanal çevreye silahlı çatışmalar hukukunun uygulanabilirliğine dair benzer alanlardaki örnekler üzerinden çıkarımlar yapılmalıdır. Örneğin, *Jus in Bello* kurallarının uzay boşluğunda uygulanmasına dair bir açık düzenleme bulunmamasının -devlet egemenliğini sınırlayıcı kural bulunmadığı gerekçesine dayanan *Lotus&Bozkurt Davası*'nda kabul edildiğinin aksine [1125] - uluslararası hukuk kurallarının uygulanamayacağı anlamına gelmediği, 1949 tarihli Cenevre Konvansiyonları'nın ortak 1. maddesinde belirtilen "taraf devletlerin bu

[1120] Bkz.: Kelsey, Jeffrey T.G. (Mayıs 2008). *Hacking into International Humaniterian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.* Michigan Law Review, Cilt:106, s. 1430.

[1121] Pascucci, 2017. s. 452.

[1122] Afroditi, 2010, s. 29.

[1123] Afroditi, 2010, s. 38.

[1124] Gül, 2021, s. 13.

[1125] Mačák, 2018, s. 12.

Konvansiyon'a her koşulda saygı göstermesi ve gösterilmesini sağlama yükümlülüğü "ne dair "her koşulda" ibaresinin yapılagelişi yansıtan bir düzenleme olduğu ve uzay boşluğundaki şartları da kapsadığı ileri sürülmüştür[1126].

Buna paralel olarak siber uzay gibi teknolojik gelişim sonucunda ortaya çıkan yeni bir alanda uygulama yeri bulan uluslararası hukuk kurallarının yine teknoloji sayesinde ulaşılabilen fiziki uzay boşluğu gibi yeni alanlarda da aynı şekilde uygulanabilmelidir[1127]. ABD'ye ait 2011 tarihli Siber Uzay için Uluslararası Strateji Belgesi'nde ifade edildiği üzere "siber uzaydaki devlet faaliyetleri için normların gelişimi, yapılageliş hukukunun yeniden keşfini gerektirmediği gibi mevcut uluslararası hukukun tamamen geçersiz kılınmasını da gerektirmez"[1128]. Buna paralel olarak 2004 yılında ABD ve İngiltere, bilgi teknolojisinin askeri olarak kullanılmasını sınırlayan antlaşmalara karşı olduklarını, mevcut silahlı çatışmalar hukuku düzenlemelerinin bu tür teknolojinin kullanımını yeterli şekilde yöneteceğini resmi olarak belirtmişlerdir[1129].

Bu konuda dikkate alınması gereken bir diğer husus da yeni teknolojilerin açıkça düzenlenmemiş olmasının, bunlara silahlı çatışmalar hukukunun uygulanmasını engellememesidir. Bu görüşe göre[1130], zamanla bir teamül kuralı haline gelen *Martens kaydına* ve 1977 tarihli Ek Protokol'ün 1-2. maddesine göre, mevcut düzenlemelerde öngörülmeyen hususlar da koruma altındadır.

Genel olarak bakıldığında, silahlı çatışma anında uygulanabilecek uluslararası hukuk kuralı olarak *jus in bello* tarafından belirlenen savaş kısıtlamalarının karasal sınırların ötesine eriştiği kabul edilir[1131]. Aynı görüşte olan Melzer, uluslararası silahlı çatışmalar

[1126] Bkz.; Mačák, 2018, s. 15.

[1127] Bkz.; Mačák, 2018, s. 14.

[1128] Jensen, 2015, s. 280.

[1129] Kanuck, 2010, s. 1588.

[1130] Gül, 2021, s. 11.

[1131] Mačák, 2018, s. 37.

hukukunun çoğu çağdaş enstrümanlarının benimsenmesi ve hazırlanması anında siber operasyonların var olmamasının, kuralların bu operasyonlara uygulanabilirliğini önlemeyeceğini ifade etmektedir [1132] . Örneğin, astronotlar insanlığın elçisi kabul edilmekle [1133] birlikte silahlı çatışmalar hukukuna göre savaşçı olarak kabul edilip edilmeyeceği konusunda; astronotlar çatışan tarafların silahlı gücüne resmi olarak ait olsalar dahi, savaşçı kabul edilmezler ancak bunlara *jus in bello*'nun kişisel uygulanabilirliği mümkün kabul edilmektedir[1134]. Bu bağlamda mevcut normların yeni alanlara uygulanabilirliğini savunan Melzer'e göre, başka bir devlete karşı gerçekleştirilen devlet destekli ve kuvvet kullanma niteliğindeki bir siber saldırı sadece 2/4 yasağına girmekle kalmaz, ayrıca doğal olarak uluslararası silahlı bir çatışmayı da tetikler[1135]. Örneğin, Almanya devleti resmi görüşünü yansıtan tutum belgesinde, kısmen ya da tamamen siber araçların kullanılması suretiyle gerçekleştirilen husumet halinde silahlı çatışmalar hukukunun uygulanabilirliği kabul edilmiştir[1136].

Bu noktada ifade edilmelidir ki mevcut normların siber savaş gibi yeni gelişen alanlara uygulanmasında konvansiyonel silahlı çatışmaların tarihsel etkilerine ağırlık verilmesi yanıltıcı olabilecektir. Ayrıca siber operasyonlara ya da çatışmalara mevcut normların uygulanmasında fiziki ortamda ortaya çıkan sonuçlar üzerinden değerlendirme yapılması yöntemi de siber faaliyetlerin doğasına her zaman uygun düşmemektedir. Bu durumda yüksek düzeyde siber kapasiteye sahip devletler mevcut normların bu yeni alana uygun düşmeyecek biçimde yorumlanması sonucunda siber teknolojinin sunduğu, örneğin siber casusluk gibi olanaklardan yoksun kalmayı istemeyeceklerdir. Bu nedenle antlaşma metinlerinin yaşanan çağın şartlarına göre ve erişilen yeni paradigmalar üzerinden yorumlanması halinde yazılı metnin anlamının tespitinin sağlanabileceği ve daha elverişli yorumların elde edilebileceği gözden uzak tutulmamalıdır. Bu bağlamda, dinamik bir

[1132] Melzer, 2011, s. 22.

[1133] BM Genel Kurulu'nun 1963 tarihli Uzaydaki Faaliyetlerin Tabi Olduğu Hukuk İlkeleri Bildirisi gereğince astronotlar bütün insanlığın elçisi kabul edilmiştir. Bkz.: Ünal, 2005, 168.

[1134] Mačák, 2018, s. 31.

[1135] Melzer, 2011, s. 6.

[1136] Position Paper, 2021, s. 7.

yorum şekli ile uluslararası hukuk kurallarının siber savaşa uygulanması suretiyle yeni bir siber savaş hukuku antlaşmalarına gerek olmadığı kabul edilebilir ise de diğer taraftan özel olarak silahlı çatışmalar hukuku açısından soruna bakılması da bir gereklilik olarak kendini göstermektedir[1137]. Soyut ve muğlak silahlı çatışmalar hukuku ilkelerinin her bir somut olayda uygulanmasının yarattığı uygulamadaki sorunlar gözetildiğinde siber savaş bağlamında sınırlandırıcı yeni normların kabul edilmesi de mümkün görülmelidir.

Zira yeni bir siber savaş hukuku antlaşmasının gerekmediğinin kabulü ve hemen yukarıda belirtildiği şekilde dar bir yorum şeklinin benimsenmesi halinde mevcut silahlı çatışmalar hukukunun siber saldırı ve savaş durumlarına ne şekilde uygulanacağı sorunu ortaya çıkacaktır. Devlet uygulaması ve yapılageliş hukukunun bu boşluğu nasıl dolduracağı da yeni bir zorluk olarak kendini gösterebilecektir. En gelişmiş devletlerin bu konudaki çalışmalarına bakıldığında dahi uygulama sorununu ortadan kaldıracak düzeyde yeterli olduğundan söz edilememektedir. Örneğin, ABD Savunma Bürosunun 2015 yılında yayınladığı Savaş Hukuku Hakkında El Kitapçığı'nın bir bölümü siber savaşa ayrılmış ve bunun da sadece altı sayfası *jus in bello'*nun siber savaşa uygulanmasına ilişkin olduğu görülmüştür[1138].

Geleneksel silahlı çatışmalar hukukunun siber saldırılara uygulanabilirliği konusunda öncelikle tespiti gereken en önemli husus silahlı bir çatışmanın var kabul edilip edilmeyeceği konusudur. Yoğunluk, vahamet ve niyet unsurlarının, mevcut silahlı çatışma tanımının uluslararası silahlı çatışmalar hukukunun düşük yoğunluktaki uluslararası silahlı çatışmaların yarattığı gri hukuksal alanda ve siber saldırılarda uygulanabilirliğini sağlayacağı savunulmaktadır[1139]. Silahlı çatışmalar hukukunda süre, yoğunluk ve kapsam yanında saldırıda bulunanın düşmanca niyetini gösterilmesi de

[1137] Ayrım gözetme ilkesinin siber savaşçılara nasıl uygulanması gerektiği konusunda yeni düzenleme yapılmasına ilişkin görüş ve yeni bir antlaşmanın imzalanmasındaki zorluklar hakkında bkz.; Padmanabhan, 2013, s. 307.

[1138] Pascucci, 2017. s. 427.

[1139] Piatkowski, 2017, s. 278.

saldırının silahlı saldırı olarak kabul edilmesine sebep olabilmektedir[1140]. Bu bağlamda uluslararası bir siber silahlı çatışmadan bahsedebilmek için geleneksel silahlı çatışmalarda ortaya çıkan sonuç ile eşit bir zarara sebep olması yanında bazıları tarafından yeterli derecede vahamet, kapsam, yoğunluk ve savaşma niyeti unsurlarının da gerektiği ileri sürülmüştür[1141].

Siber operasyonların, geleneksel düşmanlık ile paralel şekilde ortaya çıkmaması halinde silahlı bir çatışmaya sebebiyet verip veremeyeceği, bir diğer ifade ile uluslararası silahlı çatışmalar hukukunun uygulanabilirliğini tetikleyebilir olup olmadığı sorusuna Melzer, Kızılhaç'ın silahlı çatışmalara ilişkin 2008 tarihli görüşünden yola çıkarak olumlu cevap vermektedir[1142]. Buna göre uluslararası veya uluslararası olmayan bir silahlı çatışmanın tüm gerekli kurucu unsurlarını meydana getirebildiği ölçüde silahlı çatışmalar hukukunun uygulanması mümkün kabul edilmektedir.

Tallinn El Kitabı'nda uzmanlar arasında görüş ayrılığına sebep olan bu hususta bir görüşe göre, 1949 tarihli Cenevre Konvansiyonları hükümleri uyarınca iki silahlı güç arasındaki çatışmanın süre, yoğunluk ve kapsamına bakılmamasından yola çıkılarak küçük bir askeri tesiste yangına sebep olan bir siber saldırı, silahlı bir çatışmayı tetikleyebilecektir. Karşı görüşe sahip olan uzmanlar ise, sınırlı hudut çatışmaları veya deniz kazaları örneklerine kıyasen basit siber eylemlerin silahlı çatışmayı tetiklemeyeceğini ifade etmektedir[1143]. Baskın görüşe göre, ara sıra meydana gelen, münferit ve kısa süreli olayların silahlı saldırı eşiğine erişmediği kabul edilmektedir[1144].

[1140] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.224.

[1141] Piatkowski, 2017, s. 277.

[1142] Melzer, 2011, s. 23.

[1143] Schmitt, 2017, *Tallinn Manual 2.0.* s. 383.

[1144] Piatkowski, 2017, s. 276.

Yakın bir geçmişte gerçekleşen bazı olaylar üzerinden bakıldığında benzer düzeyde gerçekleşen bazı siber saldırılar konusunda farklı sonuçlara varıldığı görülmektedir. Tallinn El Kitabı'nda 2008 Gürcistan-Rusya çatışmaları dâhilinde gerçekleştirilen siber saldırıların silahlı çatışmalar hukuku kapsamında değerlendirilmesine karşın, 2007 yılında gerçekleşen Estonya saldırısının silahlı çatışma seviyesine erişmediği gerekçesiyle olayda silahlı çatışmalar hukukunun uygulanamayacağı kabul edilmiştir[1145]. Bahsedilen olaylardan ilkinde geleneksel bir silahlı çatışma içerisinde gerçekleşen bir siber saldırı söz konusu iken, ikincisinin sırf siber saldırı şeklinde gerçekleştiği ve silahlı çatışmalar hukukunu tetikleyebilecek unsurların bulunmadığı kabul edilmiştir.

Siber operasyonlara silahlı çatışmalar hukukunun sınırlandırıcı kurallarının uygulanıp uygulanmayacağı konusunda Melzer, belirleyici olanın "saldırı" teriminin karşılanıp karşılanmaması konusu olmayıp bunun yerine siber operasyonların silahlı çatışmalar hukuku anlamında çatışmanın bir parçasını oluşturup oluşturmaması olduğunu savunmaktadır[1146]. Silahlı çatışma sırasında gerçekleşebilecek siber saldırılar ile çatışma arasında bağ bulunması konusunda Uzmanlar Grubunda fikir birliği bulunsa da bahse konu irtibatın niteliği konusunda uzmanlar ayrı düşmektedir. Silahlı bir çatışma esnasında gerçekleşen her türlü siber faaliyetin bu kapsamda değerlendirilmesinin gerektiğini savunan görüş ile askeri çabaya katkı sağlayacak, husumetin devamı mahiyetindeki siber faaliyetlerin bu kapsamda değerlendirilmesi gerektiğine dair görüş ayrılığı söz konusudur. Bu görüş ayrılığının sonuca etkisi ise, silahlı çatışma halinde gerçekleşebilecek, ticari sırlara yönelik bir siber faaliyet noktasında kendisini gösterebilmektedir[1147].

Bu halde askeri hedefe yönelik olmayan siber casusluk gibi faaliyetlerin silahlı çatışmalar hukukuna dâhil edilmemesi gerekir. Zira çatışmaya taraf devletlerin askeri olmayan eylemleri ile silahlı çatışmayla ilgili olmayan özel kişi ve varlıkların eylemleri silahlı çatışmalar hukukun alanı dışında kalmaktadır. Sırf suç ile ilgili olan veya diğer bir şekilde

[1145] Schmitt, 2017, *Tallinn Manual 2.0.* s. 376.

[1146] Melzer, 2011, s. 27.

[1147] Bkz.: Schmitt, 2017, *Tallinn Manual 2.0.* s. 376.

silahlı çatışmayla ilgisiz, genel istihbarat toplamak amacıyla gerçekleştirilen eylemler gibi ölüm, yaralanma veya askeri zarara sebep olmayan siber operasyonlara silahlı çatışmalar hukuku hükümleri uygulanmaz ve doğrudan saldırıya karşı korunmaya sebep olmaz[1148]. Hemen yukarıda belirlenen gerekli kıstaslar dikkate alındığında silahlı çatışma esnasında muharip taraflarca karşı taraf ticari sırlarının siber faaliyetler vasıtasıyla elde edilmesi nedeniyle silahlı çatışma hukukunun uygulanması söz konusu olmayacaktır. Ayrıca silahlı çatışmalar hukuku tarafından zorunlu olarak yönetilmeyen siber suçluluk ve siber terörizm gibi olgular siber saldırıdan ayrı tutulmalıdır[1149].

Daha önce siber saldırı başlığı altında açıklandığı üzere Tallinn El Kitabı'nda; kişilerde ölüm veya yaralanmaya, nesnelerde zarar veya yıkıma sebep olması makul şekilde beklenen saldırı ya da savunma şeklinde gerçekleşebilecek siber operasyonlar siber saldırı olarak tanımlanmıştır[1150]. Ancak her türlü zarar veya yıkımın, eylemin siber saldırı olarak kabulüne imkân tanınmamakta ve bunun için nesnede yıkım veya zararın önemsizden (*de minimis*) daha fazla olması gerekli görülmektedir[1151]. Örneğin bir askerin kendi ülke sınırından rakip devlet sınırına doğru bir kaya parçası atma eylemi, silahlı çatışma düzeyinde kabul edilemeyeceği gibi siber faaliyet sonucu tek bir bilgisayarın devre dışı bırakılması halinde de benzer bir durum söz konusu olabilecektir[1152].

Bu açıklamalar ışığında silahlı çatışmalar hukuku anlamında çatışmanın parçasını oluşturabilmesi için söz konusu siber operasyonların gerekli zarar eşiğine doğrudan (*direct causation*) erişmesi yanında savaşan taraflardan birinin lehine ve diğerinin zararına (*belligerent nexus*) olacak şekilde bir operasyonun tasarlanmış olması gerekli görülmektedir[1153]. Diğer tarafa zarar vermek üzere tasarlanması ise doğrudan ölüm,

[1148] Melzer, 2011, s. 28.

[1149] Melzer, 2011, s. 3-4.

[1150] Siber saldırı tanımı Kural 92'de yapılmış olup ayrıntılı bilgi için bkz.: Schmitt, 2017, *Tallinn Manual 2.0*. s. 415.

[1151] Pascucci, 2017. s. 443.

[1152] Schmitt, 2013, *Classification of Cyber Conflict*. s. 241.

[1153] Melzer, 2011, s. 27-28.

yaralanma veya yok etmeye sebep olma şeklinde olabileceği gibi, askeri operasyonlarını veya askeri kapasitesini kötü yönde etkilemek şeklinde de olabilecektir[1154].

Bir siber operasyonun çatışmanın parçasını oluşturması açısından gerekli zarar eşiğine ulaşması ya da bir çatışmaya dâhil olmamakla birlikte silahlı saldırı düzeyine erişen bir siber saldırı için gereken zarar hususunda farklı görüşler söz konusudur. Bu konuda somut bir zararın varlığını gerekli görenler yanında nesnenin işlevsiz kılınmasının da zarar şartını karşıladığını ileri sürenler bulunmaktadır[1155]. Zira ikinci görüşe göre, fiziki zarara sebep olma kavramı, yeniden yüklenebilen bir programın silinmesi gibi kolayca telafi edilebilme dışında kalan ve bir siber tesis için gerekli olan bir nesnenin işlevsiz kılınmasını da kapsamaktadır[1156]. Bu çalışmanın üçüncü bölümünde silahlı saldırı düzeyine erişen siber saldırılar başlığı altında daha ayrıntılı olarak tartışıldığı üzere kritik bir siber altyapı tesisini hedef alan siber saldırıların da tek başına zarar şartını karşıladığı kabul edilmektedir. Bu durumun, tek başına silahlı çatışmaları tetikleyebileceği kabul edildiğine göre bu halde silahlı çatışmalar hukukunun uygulanması söz konusu olabilecektir.

Sonuç olarak, siber operasyonlara hangi durumda silahlı çatışmalar hukukunun uygulanabileceği konusu iki ihtimalde değerlendirilebilir. İlk olarak, yukarıda ifade edilen ve sınırları ortaya konulan bir konvansiyonel silahlı çatışmanın söz konusu olması halinde bu silahlı çatışma dâhilinde gerçekleştirilebilecek siber operasyonlara silahlı çatışmalar hukukunun uygulanması mümkündür. Bu durumda siber operasyon ile devam eden konvansiyonel çatışma arasında gerekli bağ bulunmalıdır[1157]. İkincisi ise, herhangi bir şekilde konvansiyonel silahlı çatışmanın söz konusu olmamasına rağmen gerçekleştirilen siber operasyonun silahlı saldırı seviyesine erişmesidir ki bu durumda

[1154] Melzer, 2011, s. 28.

[1155] Gül, 2021, s. 34.

[1156] Schmitt, 2013, *Classification of Cyber Conflict*. s. 241.

[1157] Position Paper, 2021, s. 7.

silahlı saldırı eşiğine varan siber operasyonlar tek başına silahlı çatışmalar hukukunu tetikleyebilmektedir.

4.1.4. Silahlı Çatışmalar Hukukunun Siber Savaşa Uygulanmasında Karşılaşılan Zorluklar

Siber savaşta uluslararası silahlı çatışmalar hukuku kurallarının uygulanıp uygulanamayacağı tartışmaları bir yana bırakılırsa, bu uygulama kapsamında yaşanacak sorunların sebebini siber uzayın kendine özgü yapısı oluşturmaktadır. Geleneksel silahlı çatışmaların gerçekleşme şekli ile siber operasyonların gerçekleştirilme şekli çok farklıdır. Her şeyden önce siber operasyonların başlatıldığı yer ile zararın meydana geldiği yer arasında mesafe ölçüsü farklıdır. Ayrıca zamansal olarak saldırının çok önceki bir tarihte programlanmış olması da mümkün olup eylem ile sonuç arasında zamansal ve mekânsal bağın azalması da söz konusu olabilmektedir. Eylem ile zarar arasındaki fiziki bağın zayıflaması nedeniyle silahlı çatışmalar hukuku kurallarının uygulanabilirliği de zorlaşmaktadır.

Siber sistemlerin iç içe girmiş sivil-askeri yapısı ve kademeli şekilde[1158] ortaya çıkabilecek dolaylı zararların öngörülememesi nedeniyle gerçekleştirilecek bir siber saldırıda bulunan devlet dâhil üçüncü devletlerde ekonomik ya da fiziki zararlara sebep olabilmesi mümkündür. Siber saldırıların farklı yapısı geleneksel silahlı çatışmalar hukuku kurallarının siber savaşa uygulanmasında bazı durumlarda beklenen sonuca ulaşılamayacaktır. Özellikle savaşçı statüsünün tanınması için gerekli silah ve amblem taşıma kuralının uygulanmasının neredeyse olanaksızlığı buna örnek olarak gösterilebilir.

Uluslararası hukuk normlarının yeni şartlara uygulanmasında yaşanan zorluklar daha önceleri farklı şekillerde kendini göstermiştir. Örneğin, uluslararası toplumun hava bombardımanına yönelik ilk tepkisi doğrudan yasaklamak olmuşsa da Birinci ve İkinci Lahey Barış Konferansları'nın neticesi mevcut uluslararası hukukun yeni teknolojiye

[1158] Goldsmith, 2013, s. 134.

uygulanmasından ibaret[1159] olduğu kabul edilmiştir. Benzer şekilde, uzay hukukunun ortaya çıkması, uzayın uluslararası hukukun kapsamına girmesi ile *jus in bello*'nun astronotlar için kişisel uygulanabilirliği mümkün hale gelmiştir. Böylece uzay hukukunun ortaya çıkmasından önce düzenlenen silahlı çatışmalar hukuku kuralları, sonradan ortaya çıkan bu yeni alana uygulanabilmektedir.

Siber savaşta istenilen sonucun alınamamasının belli başlı sebepleri olarak öğretide, kavramsal tanımlama sorunu ve etkilerin değerlendirilmesindeki muğlaklık gösterilmektedir. Bunlar: siber savaşta askeri nesnelere nazaran sivil nesnenin tanımının kapsamı ve uygulanmasının açık olmaması; saldırı tanımının kinetik olmayan etkileri yeterince açıklamaktaki başarısızlığı; siber savaştaki zarar tanımı ve zararın hesaplanmasındaki yöntemin muğlaklığı ve son olarak orantılılık analizinde dikkate alınması gereken dolaylı etkilerin boyutunu değerlendirmedeki yönlendirme eksikliği ifade edilmektedir[1160].

Belirtilen zorluklar sadece tanımlama ve değerlendirmeden ibaret olmayıp, insancıl hukukun siber uzaydaki ihlallerinin soruşturulmasında da benzer sorunlar yaşanmaktadır. İnsancıl hukuk ihlaline dair işaretin tespiti; ihlalden sorumlu faillerin belirlenmesi; eylemlerin elektronik izlerinin analizi, belgelendirilmesi ve keşfi; siber uzayda gerçekleştirilen düşmanca eylemlerden sorumlu kişilerin devletlerin silahlı güçlerine ya da diğer örgütlü silahlı gruplara ait olup olmadığının belirlenmesi ve silahlı çatışmalar hukuku ihlallerinin sınıflandırılması ve faillerin gerektiği gibi soruşturulması[1161] konuları da sorunlu alanlardır. Genel olarak bir soruşturmanın asıl amacının fiil ile fail arasındaki bağın tespitine yönelik olması nedeniyle siber operasyona ilişkin elektronik izlerin tespiti ve kaynağına ulaşılması hedeflenir. Operasyonun kaynağı ile sonuçları arasındaki teknik bağın kurulması geleneksel çatışmalara oranla içinde önemli zorlukları barındırmaktadır. Bu zorluk sadece teknik yetersizlikten kaynaklanmamakta, bunun yanında failin

[1159] Sharp, 1999, s. 3.

[1160] Pascucci, 2017. s. 419-420.

[1161] Streltsov, 2017. s. 9.

yanıltmaya yönelik sahte veya dolaylı elektronik izler yaratmasından da kaynaklanabilmektedir.

Bunlardan başka, siber uzayın özgün yapısı *jus in bello*'nun gereklilik, orantılılık, ayrım ve tarafsızlık prensiplerinin uygulanmasında da birtakım zorluklar yaratmaktadır[1162]. Ulusal bilgi altyapısının nesneleri ile topluluk altyapısının nesneleri arasında eşlenmiş bir bağlantının olmaması silahlı çatışmalar hukukunun askeri personel ile siviller arasında ayrım gözetme, çatışmada yer almayanlara saldırma yasağı, gereksiz acıya sebep olmanın yasaklanması, orantılılık, gereklilik ve insancıllık prensiplerinin savaşan taraflarca dikkate alınmasını oldukça zor bir hale getirmektedir[1163].

Ayrım ve orantılılık ilkesi özelinde silahlı çatışmalar hukukunun siber saldırıya uygulanması konusunda ortaya çıkan temel yetersizlikler yukarıda belirtilen tanımlama ve zararın tespiti konusundan kaynaklanmaktadır. Daha açık şekilde ifade etmek gerekirse bunları; askeri olanlara nazaran sivil nesnelerin tanımı ve neyin sivil nesneleri oluşturduğu, siber savaşta zararın nasıl hesaplanacağı ve neyin zararı oluşturduğunu belirleme, dolaylı ve yansıma zararların boyutu ve kapsamanın belirlenmesi konuları oluşturmaktadır[1164]. Bu konular kendi başlıkları altında incelenirken silahlı çatışmalar hukukunun siber saldırılara uygulanmasında karşılaşılan sorunlar daha ayrıntılı şekilde ortaya konulacaktır.

4.1.5. Uluslararası ve Uluslararası Olmayan Silahlı Çatışmalar ve Siber Savaş

1949 tarihli Cenevre Konvansiyonları'nda ve uluslararası yargı kararlarında sınırları çizilen bir silahlı çatışmanın parçasını oluşturan ya da geleneksel anlamda silahlı bir çatışma bulunmamasına rağmen silahlı çatışma şartlarını taşıyan bir siber saldırının

[1162] Hathaway ve diğerleri, 2012, s. 850.

[1163] Streltsov, 2017, s. 5.

[1164] Pascucci, 2017. s. 451.

varlığı halinde silahlı çatışmalar hukukunun uygulanabileceği yukarıda açıklanmıştı. Silahlı çatışmalar hukukunun ortaya koyduğu sınırlamalara aykırı eylemlerin gerçekleşmesi halinde eylemi gerçekleştiren kişilerin cezai sorumluluğu yanında ilgili taraf devletin de uluslararası hukuki sorumluluğu doğmaktadır.

Uluslararası silahlı çatışmalar nedeniyle devletlerin, diğer devletlere ya da yabancı uyruklu kişilere karşı işlediği hukuka aykırı fiillere bağlı olarak, uluslararası sorumluluğun dayanağını öncelikle uluslararası hukukun genel nitelikli yapılageliş kuralları oluşturmaktadır[1165]. Bunun yanında uluslararası silahlı çatışmalar hukukunun temel kaynaklarını 1899-1907 tarihli Lahey Konvansiyonları, 1949 tarihli Cenevre Konvansiyonları ve bunlara Ek Protokol-I oluşturmaktadır[1166]. Belirtilen sözleşmeler dizisinden 1907 Lahey IV Sayılı Kara Savaşının Kanunları ve Adetleri Hakkında Konvansiyon'a Ek Yönetmelik'in 3. maddesinde, 1977 I. Protokolü'nün 91. maddesinde, 1949 tarihli Cenevre Savaş Esirleri Konvansiyonu 12. maddesinde, 1949 tarihli Cenevre Sivillerin Korunmasına İlişkin Konvansiyonu'nun 29. maddesinde kişilerin cezai sorumluğu ortadan kaldırmadan devletlerin sorumluluğu öngörülmüştür[1167].

UKHK tarafından yayımlanan 1949 tarihli IV. Cenevre Konvansiyonu Şerhi ortak 2. maddesi uyarınca, *de facto* silahlı çatışma için taraflardan birinin savaş durumunu inkâr etmesi, çatışmanın süresi, ne kadar can kaybına sebep olunduğu silahlı çatışma hukukunun uygulanmasına engel değildir. Ayrıca savaş niyetinin, "*animus belligerent"* unsurunun gerekmemesi gözetildiğinde silahlı çatışmalar hukukunun uygulama alanının geniş bir şekilde değerlendirilmesi gerekir.

Tadić Davası'nda *ad hoc* ceza mahkemesince yapılan tanımın bu konuda kesin ifadeler içermemesi nedeniyle Kelsen'in "*animus belligerent"* unsuru, bir diğer ifadeyle savaş niyetinin aranması hususu, çatışmanın yoğunluğuna ilişkin ortaya çıkan belirsizlik ve

[1165] Pazarcı, 2021, s. 687.

[1166] Gül, 2021, s. 45.

[1167] Pazarcı, 2021, s. 688.

silahlı çatışmalar hukukunda gerilemeye sebep olacağı gerekçesiyle öğretide kabul görmemiştir[1168]. Konunun uzmanlarının çoğunluk görüşü ise, ara sıra gerçekleşen, izole ve kısa süreli olaylar söz konusu olduğunda silahlı çatışma eşiğine varılmadığı yönünde olup Etiyopya-Eritre Araştırma Komisyonu Raporu'nda bu hususun altı çizilmiştir[1169].

Uluslararası hukukta devletlerarasında vuku bulan silahlı çatışmalardan yola çıkılarak silahlı çatışmalar hukuku kurallarının silahlı çatışmalara uygulanmasından anlaşılan uluslararası silahlı çatışma hukukudur. Cenevre Konvansiyonları'nda açık bir tanımı yapılmasa da *Tadić Davası*'nda ortaya konulduğu üzere uluslararası silahlı bir çatışmadan söz edilebilmesi için devletlerarasında ya da devlete atfedilebilir şekilde bir organize silahlı bir grup ile devlet arasında gerçekleşen bir çatışmanın bulunması gerekir[1170]. Uluslararası olmayan silahlı çatışmalar hukukunun kaynağını ise, 1949 tarihli Cenevre Konvansiyonları ortak 3. maddesine ve 1977 Ek II. Protokolü'ne dayandırmak mümkündür[1171].

Bahsedilen normlar uyarınca silahlı çatışmaların dört şekilde düzenlendiği kabul edilmektedir. Bunlar: devletlerarasında gerçekleşen uluslararası silahlı çatışmalar; ulusal kurtuluş hareketlerini içeren uluslararası silahlı çatışmalar; bir devlet ile organize silahlı bir grup veya iki organize silahlı grup arasında gerçekleşen uluslararası olmayan silahlı çatışmalar ve son olarak II. Ek Protokol'ün öngördüğü seviyede bulunan uluslararası olmayan silahlı çatışmalardır [1172].

[1168] Piatkowski, Mateusz. (2017). *The Definition of the Armed Conflict in the Condition of Cyber Warfare*, Polish Political Science Yearbook, Cilt:46 (1). s. 276.

[1169] Piatkowski, 2017, s. 276.; Geiss, Robin. (2013). *Cyber Warfare: Implications for Non-international Armed Conflicts*, Int'l L. Stud., Cilt:89, s. 633.

[1170] Gül, 2021, s. 42.

[1171] Pazarcı, 2021, s. 673.

[1172] Schmitt, 2013, *Classification of Cyber Conflict.* s. 238-239.

Silahlı çatışmalar hukuku önceleri sadece uluslararası silahlı çatışmaları konu almakta iken, daha sonra yapılan düzenlemelerle uluslararası olmayan silahlı çatışmalar da kapsama dâhil edilmiştir. Uluslararası hukukta silahlı çatışmalarda uygulanacak kurallara yönelik Lahey Konvansiyonları'nda silahlı çatışmaların devletlerarasında gerçekleşmesi, bir diğer ifade ile uluslararası silahlı çatışma niteliğinde olması halinde uygulanabileceği öngörülmüştür. Buna göre, bir devlet ülkesi içinde yaşanan isyan veya diğer tür silahlı çatışmaların devletin iç meselesi olarak kabul edilmesi söz konusu olmaktadır. Buna karşın, 1949 tarihine gelindiğinde Cenevre Konvansiyonları'nın ortak 3. maddesi ile uluslararası olmayan silahlı çatışmalar da silahlı çatışmalarda uygulanması gereken kurallara tabi tutulmuştur. Cenevre Konvansiyonları'na Ek 1977 tarihli II. Protokol ile uluslararası olmayan silahlı çatışmalara gerilla faaliyetleri de dâhil edilerek çerçeve genişletilmiştir[1173].

Ayrıca bazı uluslararası yargı kararlarında ve Roma Statüsü'nde hükümet güçleri ile organize silahlı grupları arasındaki ve bir devlet içindeki organize silahlı gruplar arasındaki silahlı çatışmalar, uluslararası olmayan silahlı çatışmalar olarak kabul edilmiştir[1174]. EYUCM, *Tadić Davası*'nda silahlı çatışmanın varlığını devletlerarasında silahlı güç kullanımına başvurma ya da devlet ile organize silahlı gruplar arasındaki veyahut devlet içindeki iki silahlı organize grup arasında gerçekleşen uzatmalı silahlı şiddet (*protracted armed violence*) durumlarına bağlamıştır[1175]. Uzatmalı silahlı şiddet eylemlerinin değerlendirilmesinde ise, mahkeme saldırının ağırlığı ve tekerrürü, mağdur sayısı, şiddetin zamansal ve bölgesel genişliği gibi bir takım belirtici kıstasları gözetmiştir[1176].

[1173] Pazarcı, 2021, s. 619.

[1174] Örneğin; *Tadić Davası*, *Akayesu Davası*, *Rutaganda Davası*, *Fofana Davası*, *Bemba Gombo Davası* ve Uluslarası Ceza Mahkemesi Roma Statüsü m. 8(2)f. Bkz.: Schmitt, 2013, *Classification of Cyber Conflict*. Dipnot 41, s. 245.

[1175] Blank, 2013, s. 422.

[1176] Geiss, 2013, s. 632-633.

Tallinn El Kitabı'nın 82. Kural'ı uluslararası çatışmalarda söz konusu olan siber saldırıları düzenlerken 83. Kural uluslararası olmayan siber saldırıların varlığı halinde silahlı çatışmalar hukukunun ne şekilde uygulanabileceğini incelemektedir. Kural 83'ün metninde iki cümlede ifade edilen ve yapılageliş hukukunu yansıtan 1949 tarihli Cenevre Konvansiyonları ortak 3. maddesine dayanan, uluslararası olmayan bir çatışmandan söz edilebilmesi için ilk unsur çatışmanın bir devlet ile organize bir silahlı grup arasında veya iki grup arasında gerçekleşmesi gereğidir. İkinci cümlede ifade olunan diğer unsur ise, çatışmanın belirli bir yoğunluk seviyesine ulaşması ve grubun örgütlenme seviyesidir[1177].

Daha açık olarak ifade etmek gerekirse, uluslararası olmayan bir silahlı çatışmanın varlığından söz edilebilmesi için ilk olarak; çatışmanın devlet olmayan tarafının askeri biçimde organize olmuş, sorumlu komutanı içerir bir işareti haiz, askeri disipline ve *jus in bello*'ya saygı kapasitesine sahip olması gerekir. İkinci olarak, husumetin belli bir yoğunluk seviyesine ulaşmasıdır[1178]. Bu noktada öncelikle ifade etmek gerekir ki tek başına hareket eden bir birey ya da organize olmayan bir silahlı grup belirtilen şartı karşılamamaktadır [1179] . Bu şarta ilişkin olarak belirtilmesi gereken *Lubanga Davası*'nda [1180] Uluslararası Ceza Mahkemesi (UCM) Ön inceleme Dairesi, askeri operasyonu planlama ve yürütme yeteneğine sahip örgütün belli bir organizasyon derecesine sahip olması gerektiğini belirtmiştir[1181]. İkinci olarak dikkati çeken bir husus, uluslararası silahlı çatışmalardan farklı olarak uluslararası olmayan silahlı çatışmaların belli bir yoğunluk derecesini haiz olması gereğidir [1182] . Zira belirli bir yoğunluk derecesine varmayan herhangi bir iç huzursuzluğun uluslararası olmayan silahlı çatışma olarak kabulü mümkün değildir.

[1177] Bkz.: Schmitt, 2017, *Tallinn Manual 2.0.* s. 385.

[1178] Mačák, 2018, s. 27.

[1179] Schmitt, 2013, *Classification of Cyber Conflict*. s. 246.

[1180] Bkz.; Posecutor vs Thomas Lubanga Dyilore, Decision on the confirmation of charges, 29 Jan. 2007, Trial Chamber I, No: ICC-01/04-01/06.

Erişim: 06.02.2022 https://www.icc-cpi.int/CourtRecords/CR2007_02360.PDF

[1181] Geiss, 2013, s. 634.

[1182] Schmitt, 2013, *Classification of Cyber Conflict*. s. 248.

Ayrıca silahlı çatışmalar hukukunun, askeri operasyonun türüne, savaş araç ve yöntemlerine bağlı olmadığı gerekçesiyle Tallinn El Kitabı'nda, konvansiyonel çatışmanın bulunmadığı sırf siber çatışma halinde uluslararası bir silahlı çatışmanın söz konusu olabileceği kabul edilmektedir[1183]. Bununla birlikte, konvansiyonel bir çatışma ile birleşmeyen sırf siber silahlı bir çatışma söz konusu olduğunda, II. Ek Protokol'ün uygulanabilmesi için belirli bir bölgeyi kontrol eden organize bir silahlı örgütün varlığı gereklidir. Bu nedenle, fiziki varlık göstermeyen örgütün bir bölgeyi kontrol etmesi mümkün olamayacağından, sırf siber çatışmalar yönünden silahlı çatışma kurallarının pratikte bir sonuç doğurmayacağı gözden kaçırılmamalıdır[1184].

Bir siber çatışma uluslararası olmayan bir silahlı çatışmayı oluşturabilir ise de Tallinn El Kitabı Kural 83'ün 2. cümlesinde belirtilen örgütsel gereklilik ve ayırt edici işaretlerin bulunması gibi unsurlar, siber çatışmalarda uygulanamayacaktır. Örneğin, savaşanlarca silahların görülebilir şekilde taşınması kuralının siber savaşta uygulanabilirliği bulunmamaktadır[1185]. Aynı şekilde, örgütlenme kapasitesi yönünden bakıldığında da küçük bilişim korsanı gruplarının ve bireysel siber faaliyetlerin yeterli olmadığı kabul edilmektedir[1186]. Estonya saldırısı örneğinde olduğu üzere hacktivist grupların gerekli organizasyon eksikliği nedeniyle bu tür bir saldırı uluslararası olmayan bir silahlı çatışmaya eşit kabul edilmemektedir[1187]. Örgütsel yeterlilik yönünden öğretide Taliban ve Kolombiya Devrimci Silahlı Güçleri'nin gerekli şartı karşıladığı kabul edilmektedir[1188].

[1183] Schmitt, 2017, *Tallinn Manual 2.0.* s. 385.

[1184] Schmitt, 2013, *Classification of Cyber Conflict.* s. 250.

[1185] Streltsov, 2017. s. 8.

[1186] Schmitt, 2017, *Tallinn Manual 2.0.* s. 389.

[1187] Schmitt, 2013, *Classification of Cyber Conflict.* s. 246.

[1188] Geiss, 2013, s. 635.

Uluslararası olmayan silahlı çatışmalar için genel olarak kabul gören devletin ülkesiyle sınırlı olması gerekliliğinin son on yıllık süreçte, Afganistan'da gerçekleşen çatışmada olduğu üzere, önemli olanın coğrafi sınırlar yerine aktörlerin olduğu gerekçesiyle tartışmalı bir hal aldığı görülmektedir[1189]. Silahlı çatışmaların ülke sınırlarının dışına da taşabileceği görüşünün siber çatışmaların varlığı halinde daha fazla taraftar toplayacağı tahmin edilebilir. Bu halde uluslararası olmayan silahlı çatışmaların vuku bulduğu devletin ülke sınırlarıyla bağlı kalınamayacağı, aynı hedefe hizmet eden ülke içinde olan ya da olmayan gerekli kapasiteye sahip örgütlü bir bilişim korsanı grubu faaliyetlerinin silahlı çatışma hukukuna tabi olduğu söylenebilir.

Belirtilen ülke sınırları dışına uzanan örgütlü bir bilişim korsanı grubunun eylemlerinin uluslararası bir silahlı çatışma olarak nitelendirileceğine ilişkin görüşün karşısında konumlanan Uzmanlar Grubu çoğunluk görüşüne göre, uluslararası olmayan bir silahlı çatışma dâhilinde gerçekleşen ve ülke sınırları dışına uzanan siber saldırı tek başına çatışmayı uluslararası seviyeye taşımayacaktır[1190]. Bu bağlamda II. Ek protokol 1(2) maddesinde ortaya konulan standarda göre fiziki zarara ve yaralanmaya sebep olsa da zaman zaman gerçekleşen siber faaliyetler (*sporadic cyber incidents*) veya iç huzursuzluk, terörizm ve isyan gibi (örn.; 2007 Estonya siber saldırısı) olaylara sebep olan siber faaliyetler uluslararası silahlı çatışma oluşturmamaktadır[1191]. Silahlı çatışmanın varlığı için gereken yoğunluk, çatışmanın ciddiyetinin ayaklanma ya da rastgele gerçekleşen şiddet eylemlerinin ötesine geçmesini, düzenli askeri faaliyetlere daha yakın şekilde gerçekleşmesini gerektirmektedir[1192]. Aynı şekilde sırf ağa sızma, siber sömürü operasyonu, veri hırsızlığı ve manipülasyonu veya devlet dışı aktör tarafından gerçekleştirilen rastgele DoS saldırısı gibi eylemler, ulusal hukukta suç oluşursa ya da silahlı bir çatışmanın içerisinde gerçekleştirilmesi halinde Ek Protokol 49. maddesi

[1189] Schmitt, 2017, *Tallinn Manual 2.0*. s. 379.

[1190] Schmitt, 2017, *Tallinn Manual 2.0*. s. 386.

[1191] Schmitt, 2017, *Tallinn Manual 2.0*. s. 387.

[1192] Blank, 2013, s. 422.

kapsamında tartışmalı şekilde saldırı olarak kabul edilebilirse de gerekli yoğunluk eşiğine erişmediği için uluslararası bir silahlı çatışmayı tetiklemeyecektir[1193].

Geleneksel savaşta askeri araç ve yöntemleriyle elde edilen sonuçlara nazaran devlet dışı silahlı örgütlerin kullanılarak silahlı çatışmalar hukukunun gri alanlarından yararlanılması daha avantajlı olduğundan "*lawfare*" olarak adlandırılan yeni bir stratejik doktrinin siber savaşa uygulanmasının daha uygun olduğu ileri sürülmüştür. Zira siber uzayın sivil ve askeri altyapısı itibariyle iç içe girmiş, iki taraflı yapısının ve saldırının arkasındaki devletin kendisini daha kolay gizleyebilmesinin siber savaşta bu doktrinin kolay bir uzantısını sunmaktadır[1194]. Nükleer silahların caydırıcı etkisinden dolayı soğuk savaş döneminde dahi çatışmaların yoğunlaşması ihtimali daha düşük iken siber uzayın sunduğu avantajlar nedeniyle siber saldırıların daha yoğun şekilde yaşanması daha olası kabul edilmektedir[1195]. Yaşanılan dönemde sıkça karşılaşılan vekâlet savaşlarının siber saldırıları içerecek biçimde hibrit savaşlarda ya da tek başına siber savaşta devletler tarafından uygulanmasının hukuki mazeretine zemin hazırlayan bu görüş, silahlı çatışmalar hukukunun siber savaş söz konusu olduğunda özellikle korunması ve geliştirilmesinin önemini ortaya koymaktadır.

Bunun yanında, Uluslararası Uzmanlar Grubu, silahlı bir organize örgüt ile diğer bir devlet arasında gerçekleşen çatışmanın bir uluslararası silahlı çatışma olarak kabulü için *Tadić Davası*'na atfen bu örgütün bir devletin desteğinin ötesinde genel (*overall*) kontrolü altında olması gerektiği görüşündedir[1196]. Buradan hareketle örgütlü bir bilişim korsanı grubunun bir devletin genel kontrolü altında olduğu halde başka bir devlete karşı siber eylemi gerçekleştirmesi halinde eylemin silahlı saldırı eşiğine varması halinde

---

[1193] Geiss, 2013, s. 633.

[1194] Bkz.; Piatkowski, 2017, s. 276.; Tüm NATO askeri faaliyetleri artan bir şekilde sivil kritik bilişim altyapı tesislerine bağımlı hale gelmektedir. Bkz.; Hruza ve Cerny, 2017, s. 156.

[1195] Pernik, Piret (Ed.). (2022). *Cyberspace Strategic Outlook 2030 Horizon Scanning and Analysis.* Tallinn: CCDCOE Publication, s. 13. Erişim: 24.01.2023. https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_v2_170x240_220513.pdf

[1196] Schmitt, 2017, *Tallinn Manual 2.0*. s. 380.

uluslararası silahlı çatışmadan bahsetmek olanaklıdır. Devlet dışı bir aktörün üzerindeki denetimin genel kontrol seviyesine varmaması halinde ise içişlerine hukuka aykırı şekilde müdahale söz konusu olabilmektedir[1197].

Siber operasyonu icra edenler savaşan devletin silahlı güçleri üyesi olduğu takdirde statüleri, hakları ve yükümlülükleri I. Cenevre Konvansiyonu'nun 43. maddesinde düzenlenen geleneksel savaşanlardan farklı değildir[1198]. Bir silahlı çatışmanın oluşması için devletin silahlı kuvvetlerinin çatışmaya müdahil olmasının gerektiği yönündeki yorumun günümüzde daha esnek değerlendirilmesi gerektiği savunulmaktadır.

1949 tarihli Cenevre Konvansiyonları'nda ve Ek Protokolleri'nde sivillerin silahlı çatışmalara doğrudan katılmaları halinde doğrudan saldırıdan korunma haklarının askıya alınacağı öngörülmüştür. Bu hükümden yola çıkılarak sivil uzmanların veya bireysel bilişim korsanlarının çatışmaya doğrudan katılma mahiyetindeki siber operasyonlarından dolayı bu kişilerin silahlı çatışmalar hukuku kurallarıyla bağlı oldukları kabul edilmekle birlikte, sanki savaşan gibi meşru askeri hedef oluşturacakları da kabul edilmektedir[1199]. Dahası bu kişilerin çevresel zararın en aza indirilmesi ve kaçınılması için önlem alınırken dikkate alınmaması söz konusudur.

4.2. SİLAHLI ÇATIŞMALAR HUKUKUNA HÂKİM OLAN TEMEL İLKELER VE SİBER SAVAŞ

4.2.1. Ayrım Gözetme İlkesi

Öncesinde sivil ve savaşçı ayrımı yapılmaksızın savaşların yaşanmasına karşın sivil-savaşçı ayrımının ilk kez Jean Jacques Rousseau'nun Toplum Sözleşmesi adlı eserinde

[1197] Schmitt, 2017, *Tallinn Manual 2.0*. s. 381.

[1198] Melzer, 2011, s. 33.

[1199] Melzer, 2011, s. 27.

ifade edildiği ve 1863 tarihli Lieber Klavuzu'nda kodifiye edildiği görülmektedir[1200]. Ayrıca bu ilkenin uygulanabilmesinde etkili olan 1968 tarihli St Petersburg Deklarasyonuna göre, savaş süresince devletin başarmaya çabaladığı meşru hedef sadece düşmanın askeri gücünü zayıflatmaya yönelik olması gereklidir [1201] . Böylece savaşmaktaki amaç ve başarıya ulaşmak amacıyla hedef alınan unsurlar itibariyle bir paradigma değişimi ortaya çıkmıştır.

Jus in bello'nun merkezinde yer alan ayrım prensibi, meşru askeri hedef ile saldırıya karşı korunan kişi ve nesneler arasında ayrım yapılmasını ifade eder[1202]. Bu ilkeye göre savaşçılar ile savaş dışı kalan kişiler silahlı çatışmalar sırasında saldırının hedefi olma bakımından kesin olarak ayrılmak zorundadır[1203]. Ayrım prensibinin asıl amacı çatışma dışı kişileri korumaktır[1204]. Siber saldırılar yönünden bakıldığında siber uzayın ikili yapısı nedeniyle hedeflerin doğru tayin edilerek sivil-asker ayrımının uygulamada gözetilmesi ise birazdan açıklanacağı üzere hiç de kolay değildir[1205].

Ayrım gözetme yükümlülüğü, *Tadić Davası*'nda ortaya konulduğu üzere, hem uluslararası hem de uluslararası olmayan silahlı çatışmalarda gözetilmesi gereken bir ilkedir[1206]. 1949 tarihli I. Cenevre Konvansiyonu m. 48'de ve 1977 tarihli 1. Ek Protokol'ün 51. maddesinin 4. fıkrasında düzenlenen ayrım gözetme prensibi, sivil nüfusun ve sivil nesnelerin askeri hedeflerden ayrı tutulmasını gerektirmektedir. Konvansiyon'un 52/2. maddesi de saldırıları sıkı şekilde askeri hedefle sınırlamaktadır. Bu bağlamda bu ilkenin uygulanmasında gerekli olan dört kuralın bulunduğu ifade

---

[1200] Gül, 2021, s. 88.

[1201] Schmitt, 2017, *Tallinn Manual 2.0.* s. 420.; Bu görüş Sun Tzu'ndan itibaren gelen savaş yönteminin temelini oluşturmaktadır. Bkz.; İlhan, Hasan (Çev.). (2010). *Savaş Sanatı Sun Tzu*. Ankara: Tutku Yayınevi, s.7.

[1202] Melzer, 2011, s. 29.

[1203] Pazarcı, 2021, s. 624.

[1204] Thürer, Daniel (2011). *International Humanitarian Law: Theory, Practice, Context.* Zurich: Brill, s. 87.

[1205] Gül, 2021, s. 91.

[1206] Blank, 2013, s. 427.

edilmelidir. Bunlar; saldırıların sadece askeri hedeflere yöneltilme zorunluluğu, ayrım gözetmeyen saldırıların yasaklanması, çevresel sivil hasarın en aza indirilmesi ve saldırılacak askeri hedefin değeriyle orantısız zararlardan kaçınma gerekliliği ve son olarak bu üç kuralın gereğinin yerine getirilmesini sağlama gerekliliğidir[1207].

I. Ek Protokolün 85. maddesinde bu yükümlülüğe aykırı davranışlar Protokol'ün ağır ihlali olarak kabul edilmiş ve Roma Statüsü'nde de benzer şekilde sivillerin hedef alınması ve ayrım gözetilmeden yapılan saldırılar cezai yaptırıma tabi tutulmuştur[1208]. Silahlı çatışmalar hukukunun bu ilkesinin ihlalini oluşturabilecek saldırıların silah teknolojisinin gelişmesiyle birlikte daha önemli bir hal aldığı görülmektedir. Savaşta asıl amacın hasmın savaşma iradesinin yok edilmesi olarak kabulü halinde savaşan tarafların Hiroşima ve Nagazaki saldırılarında olduğu üzere kolaylıkla ayrım ilkesinin ihlaline yönelebileceği bir gerçektir. Aynı şekilde askeri gereklilik ilkesinin bahane edilmesi yoluyla ayrım ilkesinin uygulanmasını olanaksız kılan kitle imha silahlarının kullanılmasına kadar giden hukuka aykırı saldırıların yaşanması olasıdır.

Tallinn El Kitabı 105. Kural gereğince Ek Protokol'ün 51/4-b ve c fıkralarına atfen gerek uluslararası ve gerekse de uluslararası olmayan silahlı çatışmalarda ayrım gözetmeyen araç ve yöntemlerin kullanılmasının yasaklandığı belirtilmiştir[1209]. Bu kurala göre belirli bir meşru hedefe yönelmeyen araç ya da yöntem[1210] yasak olup kontrol edilme imkânı bulunmayan ve sivil ve korunan diğer bir siber altyapı unsuruna gereken düzeyde zarar verebilen siber silahlar yasak kapsamına girmektedir. Yalnızca askeri hedef teşkil eden ve sivillerin herhangi bir şekilde etkilenmesinin mümkün olmadığı bölgelerde bu araç ve yöntemlerin uygulanması ise yasaklanmamıştır[1211]. Buna göre meşru hedef dışında bir

[1207] Schreier, 2015, s. 74.

[1208] Blank, 2013, s. 427.

[1209] Schmitt, 2017, *Tallinn Manual 2.0*. s. 456.

[1210] Harward El Kitabı'nda savaş yöntemleri saldırıların ve diğer düşmanca eylemlerin nasıl yürütüldüğünü ifade ederken savaş araçları ise doğrudan bu saldırıları yürütmekte kullanılan araçları belirtmektedir. Bkz.: Gül, 2021, s. 145.

[1211] Gül, 2021, s. 148.

kişi ya da nesneye zarar veren ve bunu önleme olanağının saldırıyı gerçekleştirenin kontrolünde olmayan bir kötücül yazılımın kullanılması ayrım gözetmeyen bir araç ya da yöntem kapsamında yasak kabul edilmektedir. Bu noktada Tallinn El Kitabı'nda sivil ağlara yayılsa da sadece belirli bir askeri hedef üzerinde etki gösteren Stuxnet türü bir yazılımın kuralı ihlal etmediği kabul edilmiştir [1212]. Sivil ağa bulaşma olanağı bulunmadığı bir durumda ayrım gözetmeyen bir kötücül yazılımın kural ihlalinden söz edilemeyeceği söylenebilir. Dış etkenler nedeniyle kontrol dışı şekilde oluşabilecek bir zarar meydana geldiğinde ise saldırının gerçekleştiği zamanki şartlara göre değerlendirme yapılmalı ve gerekli önlemlerin alınmasına rağmen niyetlenmeyen bir sonuçtan dolayı kuralın ihlal edilmediği sonucuna varılması gereklidir.

Ayrıca ifade edilmelidir ki savaşanlarla savaş dışı kişilerin ayrılması konusunda uygulanan uluslararası hukuk, birtakım kural dışılıklar getirmektedir. Genellikle askeri gerekliliğin bulunması halinde sivil hedeflere ve sivillerin bulunduğu bölgelere saldırıda bulunulabileceği kabul edilmekte, ancak yapılacak operasyonda beklenilen askeri sonuç ile yapılan eylem arasında bir orantılılık aranmaktadır[1213]. Orantılılık testini de içeren ve "*collateral damage*" doktrini olarak da adlandırılan [1214] bu kural dışılık gereğince operasyonun yapılmasının askeri bir gereklilik oluşturması ve sonuçta askeri bir avantaj sağlanması halinde hedefin sivil unsurları da içermesi mazur görülebilmektedir. Ancak bunun için operasyonların sıkı şekilde askeri hedeflerle sınırlı biçimde gerçekleştirilmesi yanında bunun askeri faaliyete etkin biçimde katkı sağlayacak nesnelere karşı gerçekleştirilmesi ve kesin bir askeri avantaj sağlaması gereklidir [1215]. Bu haliyle, öncelikle hedeflerin doğası, konumu, amacı ve kullanımı itibariyle askeri faaliyete etkili bir katkı sağlaması halinde kısmen veya tamamen yıkımı, ele geçirilmesi veya etkisizleştirilmesi, o anki şartlar altında, kesin bir askeri avantaj sağlamasına bağlı tutulmuştur.

[1212] Benzer bir devlet uygulaması için bkz.; Position Paper, 2021, s. 9.

[1213] Pazarcı, 2021, s. 625.

[1214] Aksar, 2021, (2. Kitap), s. 212.

[1215] Kelsey, (2008). s. 1437.

Ayrım ilkesi silahlı çatışmada kuvvet kullanımına ön şart olarak meşru hedefin belirlenmesini gerektirmektedir[1216]. Bu noktada akla gelebilecek soru hem askeri hem de sivil olarak iki taraflı fayda sağlayan bir nesneye karşı etkin bir katkı sağlaması nedeniyle gerçekleştirilen bir saldırının sivil hedefi meşru hedefe dönüştürüp dönüştürmeyeceği konusudur ki bu konu tartışmalıdır[1217]. Anılan ilkenin siber uzayda gerçekleşen saldırılar yönünden sivilleri ve sivil nesneleri yeterli şekilde koruyamamasının sebebi olarak siber uzayın özgün yapısı ve her yerde olma özelliği ile sivil siber altyapı sistemlerinin askeri birimlerce kullanılması ve bu sistemlere bel bağlanması gösterilmektedir[1218].

Bu ilkenin siber saldırı eylemlerinde uygulanmasındaki engellerden biri de silahlı çatışmalar hukuku açısından saldırının tanımındaki yeterince açık olmama halidir[1219]. Ayrım prensibi kapsamında çatışan taraflara yüklenen diğer ödevler arasında; çatışmalar sırasında doğal çevrenin korunması, barajlar ve nükleer güç tesisleri gibi tehlikeli yapıları koruma ve sivil nüfus üzerinde terör oluşturmama yükümlülükleri sayılabilir[1220].

UAD, gereksiz acıya sebep olmama ilkesi ve ayrım gözetme ilkesini de[1221] ihlal edilemez bir prensip olarak görmüştür[1222]. Bu ilkenin ihlal edilip edilmediğinin belirlenmesi ile saldırıya herhangi bir haklı sebep veya mantıksal gerekçeye silahlı çatışmalar hukukunca izin verilmemesinin bir ilgisi bulunmamaktadır. Örneğin sivil can kaybının önlenmesi

---

[1216] Blank, 2013, s. 427.

[1217] Kelsey, (2008). s. 1437.

[1218] Pascucci, 2017. s. 420.

[1219] Pascucci, 2017. s. 420.

[1220] Kelsey, (2008). s. 1437.

[1221] Schmitt, 2017, *Tallinn Manual 2.0.* s. 420.

[1222] *Nükleer Silah Kullanımı ve Tehdidinin Yasallığına dair 1996 tarihli Danışma Görüşü*; Bkz.: Pascucci, 2017. s. 430.

için saldırının kısa tutulması halinde dahi o ana kadar gerçekleştirilen sivil bir hedefe saldırı eylemi, hukuka aykırı kabul edilecektir[1223].

Ayrım ilkesi ayrıca gerçekleştirilen silahlı çatışmalarda sivillerin yaşam kaybının ve sivil hedeflerin uğrayacağı zararın minimize edilmesi konusunda çatışan taraflara sürekli bir özen gösterilmesi ödevini de yükler[1224]. "Sivil"in tanımı 1. Ek Protokol'ün 50. maddesinde savaşan veya savaş tutsağı kategorisine dâhil olmayan tüm insanlar olarak ifade edilir[1225]. Meşru askeri hedef, savaşanlar, organize silahlı grup üyeleri ve çatışmaya doğrudan katılan sivillerden oluşur. Ancak, siviller, tıbbi ve dini personel, yaralandığı, hastalandığı, tutsak edildiği, teslim olduğu veya diğer bir sebepten dolayı savaş dışı kalan savaşanlar ayrılmalı ve korunmalıdır[1226].

Ek Protokol'ün 43. maddesi ise, çatışmaya katılma hakkı olan silahlı güçleri tanımlamaktadır. Savaşan devletler, geleneksel olarak askeri personel tarafından gerçekleştirilen çeşitli faaliyet alanlarında özel yüklenici veya sivil çalışanlar istihdam etmektedir. Günümüzde silahlı güçler, siber operasyonların gerçekleştirilmesini, hazırlanmasını ve desteklenmesini de kapsar. Bu tür personel doğrudan çatışmaya katılmaya eşit faaliyetler üstlenmedikçe sivil kabul edilirler[1227]. Kötücül yazılımın oluşturulması ve işletilmesi, bir DDoS saldırının gerçekleştirilmesi, kötücül yazılımın veya diğer siber saldırı aracının çatışmanın tarafına sağlanması ise çatışmaya doğrudan katılma olarak değerlendirilmekte[1228] ve meşru hedef oluşturabilmektedir.

İyi yönetilmiş bir siber saldırının, İran nükleer zenginleştirme programının geciktirilmesinde olduğu üzere, hava saldırısının büyük olasılıkla sebep olacağı can

[1223] Schmitt, 2017, *Tallinn Manual 2.0.* s. 422.

[1224] Kelsey, 2008. s. 1437.

[1225] Afroditi, 2010, s. 26.

[1226] Melzer, 2011, s. 29.

[1227] Melzer, 2011, s. 34.

[1228] Blank, 2013, s. 430.

kaybına veya yaralanmaya nazaran önemli bir avantaj sağlayacağı bir gerçektir[1229]. Siber saldırıların yarattığı bu imkânlar geleneksel anlamda kuvvet kullanma ile ekonomik zorlama gibi eylemler arasında bulunan boşluğun doğurduğu olumsuzluklar için bir fırsat oluşturabilecektir[1230]. Bu açıdan bakıldığında siber saldırıların can kaybına ve sivil nesnelere zarar vermeden gerçekleştirilmesi daha olası görülebilir ise de siber saldırıların sonuçları konvansiyonel saldırılara göre daha geniş ölçekli ve öngörülemez olduğundan dolayı ayrım prensibinin her zaman sağlanabileceği anlamı çıkarılamaz.

NATO'nun gerçekleştirdiği ve Kosova'da 16 kayıpla neticelenen Sırp Medya İstasyonu RTS'nin bombalanması olayı yerine, operasyonun siber araçlarla gerçekleştirilmesi halinde can kaybına sebep olmadan kolaylıkla amaca ulaşılabileceği kabul edilmektedir[1231]. Zira konvansiyonel bir saldırı düşmanın askeri-endüstriyel tesislerine odaklanırken siber saldırılarda fiziki zarar minimize edilmek suretiyle konvansiyonel hedeflere ulaşılabilir[1232]. Bununla birlikte Tallinn El Kitabı'nda olduğu üzere[1233] siber saldırı halinde ayrım prensibine uygun bir örnek olarak Stuxnet saldırısı gösterilebilir ise de bunun gelecekteki tüm siber saldırılarda ayrım ilkesinin gözetileceği anlamına da gelmemektedir[1234]. Zira siber uzayın hem sivil hem de askeri birimlerce kullanılan ikili yapısı ayrım prensibi gerekliliklerinin siber saldırılar açısından karşılanmasını geleneksel yapıya nazaran güçleştirmektedir[1235].

Siber saldırıların hangi durumda silahlı çatışmalar hukukunu ihlal etmeyeceği konusunda öğretide verilen örneklerden dikkat çekeni; genel bir kampanya dâhilinde hava savunma

[1229] Farwell ve Rohozinski, 2011, s. 34.

[1230] Barkham, 2001, s. 58.

[1231] Afroditi, 2010, s. 25.

[1232] Barkham, 2001, s. 58.

[1233] Bunun için bkz.: Schmitt, 2017, *Tallinn Manual 2.0.* s. 457.

[1234] Rølsåsen, 2016, s. 18.

[1235] Hathaway ve diğerleri, 2012, s. 852-853.

sisteminin etkisiz hale getirilmesidir[1236]. Bu bağlamda düşman devletin tabiiyetindeki sivil halka yönelik siber propagandanın geleneksel yöntemlerde olduğu üzere ayrım prensibine aykırı olmadığı kabul edilmektedir[1237].

4.2.2. İnsancıllık ve Askeri Gereklilik İlkesi

İnsancıllık ilkesi gereksiz acıya ve mazur görülemez yaralanmaya sebep olunmamasını gerekli kılar[1238]. Gereksiz acıya sebep olunmaması savaşan askerlerle ilgili olup bir silahın doğrudan sivillere karşı kullanılması, bu silah gereksiz acıya yol açsın ya da açmasın, yasaktır[1239]. Gereksiz acıya sebep olunmaması ilkesi 1907 Lahey Yönetmeliği, m. 23/e ve 1977 I. Protokolü madde 35/2'de düzenlenmiştir[1240]. Tallinn El Kitabı'na göre gereksiz acı verme ifadesi, "bir silahın veya bir silahın belli şekilde kullanımının, saldırana daha fazla askeri avantaj sağlamadığı halde çekilen acının ağırlaşması durumu"na işaret etmektedir [1241] . Nihayetinde silahlı bir çatışmanın taraflarının gerçekleştirdiği saldırıların amacı düşmana acı çektirmek değildir. Askeri harekâtın asıl amacı hasmın askeri gücünü zayıflatmak suretiyle istenilen koşulları kabul etmeye zorlamak olduğundan bu hedefe ulaşmaya yönelik olmayan acı verici eylemler gerekli görülemez. Düşman askeri zayiatının hasmın savaşma iradesini kırma konusunda etkili olacağı açık olmakla birlikte siber operasyonlar gibi daha az acıya sebep olan ve aynı hedefe ulaşmayı sağlayan savaş yöntemlerine başvuru olanağının bulunması halinde de sebep olunacak ölüm ya da yaralanma ile sonuçlanan eylemler gereksiz olacaktır.

Askeri gereklilik ilkesi ise, sınırlama ilkesi olarak da adlandırılan savaşan tarafların savaş araç ve yöntemlerinin seçiminde sınırsız bir hakka sahip olmayacağı kuralının

---

[1236] Kelsey, (2008). s. 1438.

[1237] Schmitt, 2017, *Tallinn Manual 2.0.* s. 422.

[1238] Afroditi, 2010, s. 27.

[1239] Gül, 2021, s. 14.

[1240] Pazarcı, 2021, s. 624.

[1241] Gül, 2021, s. 15-16.

somutlaşmış hali olarak kabul edilmektedir [1242] . 1949 tarihli IV. Cenevre Konvansiyonu'nun 53. maddesinde askeri gereklilik şartı yer almaktadır[1243]. Kullanılan silahın yasallığı tek başına yeterli olmayıp bu silahların yasal şekilde de kullanılması gereklidir[1244]. Bu nedenle kullanılan yöntemlere ve saldırılan hedeflere ilişkin sınırlar konulmakta ve ilaveten bu kurallar sivillere ve sivillere ait nesnelere verilen zararın en aza indirilmesi için gerekli önlemlerin alınmasını gerektirmekte, yine beklenen askeri avantajı aşırı aşan düzeyde zarara sebep olacak saldırıları yasaklamaktadır[1245].

Bu ilkelere göre yüksek seviyede sivil ölümüne ve gereksiz acıya sebep olan ve açıkça askeri avantaj sağlamayan bir saldırıdan kaçınılmalıdır[1246]. Zira askeri gereklilik ilkesi uyarınca amaçsız şiddet uluslararası silahlı çatışmalar hukuku tarafından yasaklanmıştır[1247]. İnsancıllık ilkesinin uygulanmasına yönelen tanımlamaların soyut olması ve kesin bir kıstas içermemesi nedeniyle ileri sürülen eleştiriler[1248] siber silahlarda daha olasıdır. Siber silahların konvansiyonel silahlara nazaran çok daha az fiziki zarara ve ölüme sebep olacak şekilde kullanılabilmesi seçeneklerini taşıması nedeniyle bu ilkenin ihlali daha düşük bir ihtimaldir. Buna karşın siber silahların daha az acıya sebep olabilmesine yönelik teknolojik seçenekler mümkün olduğu halde askeri avantaj sağlamayacak biçimde bu seçeneklerin kullanılmaması ilkenin ihlaline sebep olabilecektir.

Daha önceki başlıkta incelenen ayrım prensibi ağırlıklı olarak hedefin meşru olabilmesi için askeri başarıya katkı sağlayacak ve korunan kişi veya nesnelerden ayrı tutulmuş bir

---

[1242] Güneysu, 2012, s. 99.

[1243] Güneysu, 2011, s. 167.

[1244] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 261.

[1245] Schmitt, 2017, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law.* s. 261.

[1246] Kelsey, (2008). s. 1438.

[1247] Thürer, 2011. s. 68.

[1248] Bu konudaki eleştirilere yönelik ayrıntılı bilgi için bkz.; Gül, 2021, s. 16-17.

hedef tespitini öngörür. Ayrım prensibinin konu ettiği meşru hedefin belirlenmesi aşamasından sonraki saldırının icrası sırasında gözetilecek insancıllık ve askeri gereklilik ilkesi, meşru askeri hedefe yönelen saldırının dahi sınırlandırılmasını gerektirir. Örneğin, uzaktan kumanda edilen askeri silahlı hava aracını düşürme imkânını kullanmak yerine, hava aracının kumanda edildiği birimin bulunduğu yapının bombalanmasının askeri gereklilik ilkesine uygun düşmeyeceği söylenebilir. Bununla birlikte belirtilen birim personelin görev dışı bırakılması için gerçekleştirilmesi gerekli bir siber saldırıda personelin daha ağır yaralanmalarını önlemek ve kaçabilmelerine olanak vermek yerine, tüm çıkışların bilhassa uzaktan kilitlenmesi sonrasında yangın çıkarılması suretiyle gerçekleştirilmesi halinde gereksiz acıya sebep olmama ilkesinin ihlali söz konusu olabilecektir.

Bu örnekler gözetildiğinde gereksiz acıya sebep olmamaya esas olan gereklilik düzeyinin tespitinin zorluğu gündeme gelmektedir. Bir siber silahın hangi düzeyde ölüme ya da yaralanmaya sebep olduğu ya da tedavisi bulunmayan etkilere sebep olması kıstaslarının[1249] da her olaya uygulanabilir olmadığı söylenebilir. Zira siber silah örneği üzerinden gidilirse, en az ölüm ve yaralanmaya sebep olacağı düşünülen bir siber silah kullanılmasına rağmen sonradan ortaya çıkan etkilerden kaynaklı öngörülemeyen bir zarar vukuunda silahın gerekli ya da gereksiz olduğunun tespiti sağlıklı bir değerlendirme olarak kabul edilemez.

Örneğin, stuxnet saldırısında kullanılan siber silahın üretildiği ve ağa bırakıldığı an itibariyle sadece nükleer reaktörleri devre dışı bırakacağı varsayılırken, saldırının gerçekleşmesinden belki iki yıl sonra hedefine ulaşan siber saldırının, diğer etkenlerin katkısıyla meydana gelebilecek bir patlamada tüm personelin ölmesi halinde olduğu üzere, ölüm oranına göre değerlendirilmesi doğru kabul edilemez. Bu açıdan gereksiz acıya sebep olma değerlendirmesinin siber saldırıların programlandığı zamandaki

[1249] Coupland, Robin M. / Herby, Peter. (1999). Review of the legality of weapons: a new approach The SIrUS Project, International Committee of the Red Cross. Erişim: 01.01.2022 https://www.icrc.org/en/doc/resources/documents/article/other/57jq36.htm

şartlara, teknolojik imkânlara, silah seçimine ve gereksiz acının hafifletilmesi için sonradan müdahale imkânının bulunup bulunmadığına göre yapılması gerekir.

Askeri gereklilik ilkesinin yazılı bir metin olarak ilk kez tanımlanması Lieber Yasası'nın 14. maddesinde yapılmıştır[1250]. Buna göre, askeri gereklilik ilkesi savaş amaçlarına ulaşılması için vazgeçilmez olan tedbirlerin aynı zamanda hukuka uygun olmasını gerektirmektedir. Bu ilkenin bir mazeret olarak kullanılması ve hukuka aykırı saldırıların meşrulaştırılmasına hizmet etmesi olasıdır. Örneğin, askeri gereklilik ilkesini öne sürerek silahlı çatışmalar hukukunun diğer tüm ilkelerinin ihlali ve doğrudan sivil hedeflere saldırılması hukuka uygun kabul edilemez.

Bu ilkenin uzun dönemdeki olumlu etkilerine işaret eden Kantçı yaklaşıma göre savaş ve çatışma zamanlarında dahi minimum bir düzenin korunması gelecekteki barışın kurulabilmesi için vazgeçilmezdir[1251]. Savaşan tarafların amacı hasmını teslim olmaya zorlamak olup düşmanın topyekûn yok edilmesi hukuka uygun bir amaç olarak kabul edilemez. Bu yönüyle silahlı çatışmalarda hasma yönelik gerçekleşecek bir saldırının hedeflenen amacın askeri yönden gerektirdiği kadarıyla sınırlı tutulması lüzumu ve her durumda askeri gereklilik bahanesiyle insancıllık ilkesinin ihlal edilmemesi gerektiği kabul edilmelidir. Aksi takdirde tüm silahlı çatışmalar hukuku ilkelerini ihlal eden bir saldırının askeri gereklilik ilkesine sığınılarak hukuka uygun kabul edilmesi sonucunu doğuracak biçimde yorumlanması silahlı çatışmalar hukukunun içinin boşaltılmasına sebep olacaktır.

[1250] Güneysu, 2012, s. 100.; Lieber Yasası'nın 14. maddesi orijinal metni için bkz.: *"Art. 14. Military necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war."* Erişim: 12.11.2022 https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=8FC14110FCE40830C12563CD00514A6E

[1251] Güneysu, 2012, s. 95.

4.2.3. Orantılılık İlkesi

Orantılılık ilkesi özellikle 20. yüzyılda silah teknolojisinde meydana gelen gelişmeler nedeniyle silahlı çatışmalarda ölen sivil sayısının aşırı derece artması sonucu büyük önem kazanmış bir ilkedir[1252]. Bu ilkenin kaynağını Ek I. Protokol'ün 51/5-b ve 57/2-b fıkralarında bulmak mümkündür. Anılan hükmün dışında orantılılık ilkesi Roma Statüsü m. 8/2-b-4 hükmünde, Lieber Yasası'nın 15. maddesinde ve Hava Savaşlarına İlişkin 1923 tarihli Lahey Kuralları'nın 24/4. maddesinde düzenlenmiştir[1253].

Ek Protokol'ün siviller ve sivil halk başlığı altında 51/5-b hükmüne bakıldığında; *"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"*ın yasaklandığı görülmektedir. Bu düzenlemeye göre; bir saldırının bulunması, bu saldırıdan kaynaklı bir zararın doğması, zararın belirli bir seviyeye ulaşması ve zararın beklenen somut ve doğrudan askeri avantaja kıyasla aşırı olması gerekli görülmektedir[1254].

Ek Protokol'ün saldırıda alınacak önlemler başlıklı 57. maddesinin 2-b fıkrasında;*"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."* hükmü düzenlenmiştir. Bu düzenlemeye göre bir saldırı sonucunda ortaya çıkabilecek zararın elde edilmesi beklenen askeri avantaja oranla

---

[1252] Gül, 2021, s. 153.

[1253] Güneysu, Gökhan. (2013). *Orantılılık İlkesi ve Uluslararası İnsancıl Hukuk*. TAAD, Sayı:14, s. 456-457.

[1254] Gül, 2021, s. 158.

aşırı olduğunun anlaşılması halinde saldırının tedbiren durdurulması ya da askıya alınması gerekmektedir.

Belirtilen düzenlemelerin merkezinde yer alan ilke orantılılık ilkesidir. Zira bu düzenlemeler ile kurulması gereken denge beklenen askeri avantaj ile ortaya çıkacak zararın aşırı bir oranda siviller aleyhine bozulmamasını sağlamaya dönüktür. Zira pek çok kez ifade edildiği üzere insancıl hukuka göre savaşan taraflar savaş yöntemlerini diledikleri ölçüde ve şiddette belirleyemezler[1255]. Silahlı çatışmalarda meşru kabul edilen hedeflere yönelik saldırı gerçekleştirildiğinde dahi kaçınılmaz olarak bazı çevresel zararların doğması ve sivil can kayıplarının yaşanması mümkündür. Bu bağlamda silahlı çatışmalarda orantılılık ilkesi, sivil can kaybının öngörülen askeri avantaj ile mukayese edilmesi temeline dayanır[1256].

Bu ilke, meşru hedeflere yönelik gerçekleştirilen bir saldırıda sivillerin can ve mallarına verilecek zarar ile beklenen askeri avantajın orantılı olmasını ve burada sivillere verilmesi öngörülen zararın, gerçekleştirilen saldırının sonucunda elde edilmesi beklenen askeri avantaja oranla aşırı olmamasını şart koşmaktadır[1257]. Orantılılık ilkesinin koruma altına aldığı sivil yaşamı ve sivil nesneler yanında UAD *Nükleer Silahlar Danışma Görüşü*'nde benimsenen devletlerin kullanacakları silahların seçiminde sınırsız bir seçeneğe sahip olmadığı tespitinden yola çıkılarak askeri operasyon nedeniyle ortaya çıkacak çevresel zararların orantılılık ilkesini karşılaması gerekmektedir[1258].

Orantılılık ilkesi sivil hedeflere saldırma yasağından farklılık arz etmekte olup askeri meşru bir hedefe saldırılması halinde dahi bazı sivil can kayıpları, yaralanma durumu veya sivil nesnelerde zarar doğması beklenebilir. Doğrudan hedef alınmasa dahi zarar görmesi beklenen sivil nüfus ya da nesnelerin uğrayabileceği zararın somut ve doğrudan

[1255] Hoş, 2013, s. 131.

[1256] Afroditi, 2010, s. 28.

[1257] Gül, 2021, s. 155.

[1258] Güneysu, 2013. s. 455.

elde edilmesi beklenen askeri avantaj ile mukayese edildiğinde aşırı (*excessive*) olmaması gereklidir. Aksi durumda operasyonun orantılılık ilkesini ihlal ettiğinden bahsedilecektir.

Orantılılık ilkesi gerek uluslararası ve gerekse de uluslararası olmayan silahlı çatışmalar kapsamında gerçekleştirilen siber saldırılara da uygulanacaktır[1259]. Geleneksel silahlı çatışmalarda kabul edilen bağlam-bağımlı tespit durumunun[1260] siber saldırılarda da uygulanabileceğinin kabul edilmesi gerekmektedir. Bunun anlamı, gerçekleşen zararın aşırı olup olmadığının, zarar ile beklenen askeri avantaj arasında orantı bulunup bulunmadığının olay bazında değerlendirme yapılarak tespit edilecek olmasıdır. Örneğin, gerek fiziki ve gerekse de hibrit bir çatışmada bir devletin siber operasyon birimi tarafından başlatılan siber saldırıya karşılık olarak siber operasyon birimini devre dışı bırakmak amacıyla yakınlardaki bir nükleer tesisin ya da barajın siber saldırıyla patlatılması ve binlerce insanın ölümüne sebep olunması halinde normal şartlarda orantılılık ilkesinin ihlal edildiği söylenebilir. Buna karşın siber operasyon biriminin yarattığı tehlikenin boyutu gözetildiğinde operasyon birim binasının bulunduğu yoğun yerleşim yerinde, birim binasında yangın çıkarmaya yönelik bir siber saldırı ya da akıllı füze kullanılarak gerçekleştirilen bir silahlı insansız hava aracı saldırısı sonucunda meydana gelebilecek sivil kaybının orantılı kabul edilebilmesi çatışmanın mevcut şartları itibariyle mümkündür.

Değinilmesi gereken bir diğer husus, siber saldırıların doğası gereği orantılılık ilkesinin uygulanmasında bazı avantaj ve dezavantajları içinde barındırmasıdır[1261]. Siber saldırılar gerçekleştirilirken teknolojik gelişimin hedef seçiminde kolaylık sağladığı bir gerçektir. Böylece sivil hedeflerin en alt düzeyde etkilenmesini sağlamak geleneksel saldırılara göre daha kolaydır. Buna karşın siber altyapı unsurlarının iki taraflı kullanımından dolayı bu ilkenin uygulanmasında zorluklar yaşanması kaçınılmazdır. Böyle durumlarda sivil hedeflere saldırma yasağı söz konusu edilemeyeceğinden orantılılık ilkesine göre

[1259] Gül, 2021, s. 161.

[1260] Güneysu, 2013, s. 453.

[1261] Gül, 2021, s. 161.

değerlendirme yapılmalıdır. Sivil siber altyapı sisteminin askeri amaçlı kullanımı ya da askeri siber sistemin aynı zamanda sivil nüfusa hizmet vermesi halinde bu sistemlere karşı ya da bu sistemler vasıtasıyla siber saldırı gerçekleştirilmesi sonucunda sivil nüfusun olumsuz etkilenmesi ya da sivil siber altyapı sistemlerinin zarar görmesi durumunda orantılık ilkesi uyarınca beklenen somut askeri avantaj ile ortaya çıkan sivil zararın orantılı olması gereklidir.

Gerçekleştirilecek saldırının hedefinin belirlenmesi sırasında sivillerin ve sivil nesnelerin askeri hedeflerden ayrı tutulmasını sağlamak yönünden ayrım ilkesi tek başına yeterli değildir. Bu nedenle askeri bir hedefe karşı gerçekleştirilecek bir saldırının sonuçlarının da somut ve doğrudan beklenen askeri fayda ile orantılı olması gereklidir. Bu bağlamda askeri avantajın, askeri nitelikte olması, çatışmanın yürütülmesiyle doğrudan bağlantılı olması[1262] ve ayrıca somut, gerçekçi ve elle tutulabilir olması gerektiği gözetilmelidir. Çatışma sırasında elde edilmesi beklenen avantajın ekonomik, finansal, sosyal ya da psikolojik nitelikte olması halinde askeri bir avantajdan bahsedilemeyecektir[1263]. Aynı şekilde elde edilmesi olasılığı çok düşük ya da gerçeklikten kopuk bir askeri avantajın somut, elle tutulabilir bir avantaj olarak değerlendirilmesi olası değildir.

Bu ilkeye göre askeri bir hedefe yönelik gerçekleştirilecek saldırıdan kaynaklanacak ikincil zararın belirtilen askeri fayda ile orantılı olması aynı zamanda sivillerin ve sivil nesnelerin de korunmasını sağlamaktadır. İkincil zararlar doğrudan olabileceği gibi dolaylı şekilde de gerçekleşebilmektedir. Doğrudan gerçekleşen zarar, başka bir olay ya da mekanizmanın etkisi karışmaksızın birincil olarak meydana gelen zarar iken; dolaylı zarar, başka etkenler sonucu sonradan vuku bulan zararlardır[1264]. Siber savaşta orantılılık ilkesinin nasıl uygulanacağı konusunda işlev kaybı, aşırı zarar, siber saldırının yaratacağı dolaylı ve yansıma zararları (*knock-on effects*) kıstaslarına göre değerlendirme

[1262] Gül, 2021, s. 162.

[1263] Gül, 2021, s. 162.

[1264] Schmitt, 2017, *Tallinn Manual 2.0*. s. 472.

yapılmaktadır[1265]. Siber saldırıların ikincil etkisinin sivil can kaybı veya yaralanması ya da sivil nesnelere zarar verme düzeyine ulaşmamakla birlikte korku, stres veya rahatsızlık yaratması halinde yansıma zarar düzeyine ulaştığı kabul edilmemektedir[1266].

İkincil zararın belirsizliği konusunda Uzmanlar Grubu'nda fikir ayrılığı bulunmakta olup azınlık görüşüne göre çevresel zarar olasılığı ne kadar az ise orantılılık kuralı vasıtasıyla operasyonun haklı kabul edilmesinde askeri avantaja bir o kadar az ihtiyaç duyulacaktır. Bunu kabul etmeyen çoğunluk görüşü ise, çevresel zarar bir kez bekleniyor ise olası çevresel zarar yönünden belirlilik derecesine bakmak uygun değildir[1267].

Siber saldırıların tipik doğrudan etkilerinin ölümcül olmaması, geçici olması buna karşın şiddetli olması nedeniyle sivil can kaybı, sivil yaralanması ve sivil nesnelere hasar verme konusunda orantılı olup olmadığını değerlendirmek kolay değildir[1268]. Zira geleneksel askeri saldırıların olası etkilerini tahmin etmek ve istenildiğinde saldırıyı sonra erdirmek mümkün olabilirken siber saldırıların yapısı gereği sebep olabileceği olumsuz sonuçları öngörmek ve sona erdirmek mümkün olamayabilecektir. Örneğin Stuxnet saldırısı soncunda Hindistan'a ait bir uydu olumsuz etkilenmiş olduğu gözetilirse bu saldırının plan dışı zararlarının yaratabileceği risk açısından saldırıyı gerçekleştiren devletin tespit edilebilmesi halinde ne kadar ciddi politik sorunlar yaratabileceği tahmin edilebilir[1269].

Siber saldırıların interneti ya da çatışma ile ilgisi olmayan ancak asker ailelerince kullanılan bir ağı hedef almasının askeri avantaj oluşturup oluşturmayacağı konusunda öğretide görüş ayrılıkları bulunmaktadır[1270]. Bu konuda ağların ya da sosyal medya sitelerinin askeri operasyona yaptığı katkı gözetilerek askeri bir avantajın var olduğu

[1265] Pascucci, 2017. s. 448-451.

[1266] Schmitt, 2017, *Tallinn Manual 2.0.* s. 472.

[1267] Schmitt, 2017, *Tallinn Manual 2.0.* s. 475.

[1268] Hathaway, 2012, s. 851.

[1269] Farwell ve Rohozinski, 2011, s. 34.

[1270] Ayrıntılı bilgi için bkz.: Gül, 2021, s. 167-168.

düşünülebilir ise de internetin sivil kullanım yönünün askeri boyutunun çok ötesine geçtiği göz ardı edilememelidir. Gelinen noktada insanlığın ortak malı olarak kabul edilen internet altyapısının meşru bir hedef olarak kabul edilmemesi gerektiği gibi, sırf moral üstünlüğü elde etmeye yönelik olarak yok edilmesi de orantılılık ilkesine uygun olarak kabul edilemez. Teknolojik gelişimin sunduğu olanakların kullanılması ve yeni savaş alanının kurallarının buna uygun bir yaklaşımla benimsenmesi gerekir. Bir diğer ifade ile bu yeni siber alanında savaşın kuralları değişmiş olup internete ya da sosyal medya sitelerine bu yeni siber savaş kuralları düzleminde ancak sınırlı bir müdahalenin gerekli ve orantılı kabul edilmesi mümkün olmalıdır.

Bu bahiste belirtilmesi gereken son husus olarak saldırının sebep olduğu zararın fiziki zarar oluşturmayıp psikolojik yıkım oluşturması halinde elde edilmesi beklenen askeri avantaj ile ortaya çıkan psikolojik yıkımın orantılılık ilkesinin ihlaline sebep olup olmayacağı konusudur. Bu konuda EYUCM tarafından verilen *Prlic Davası*'nda Müslüman halk için çok önemli bir yer tutan Mostar köprüsünün imhasının köprünün meşru hedef teşkil etse dahi yarattığı psikolojik etkinin orantılılık ilkesinin ihlali anlamına geldiği yönündeki tespiti[1271] oldukça yerinde bir karardır. Askeri avantaj kavramının değerlendirilmesinde çatışma koşullarının dikkate alınması gerekmekte olduğu kadar meşru hedef oluşturabilecek bir nesnenin dar bir askeri bakış açısının ötesinde değerlendirilmesi de zorunludur. Bir önceki paragrafta belirtildiği üzere askeri avantaj bulunduğundan bahisle bir ülkenin tüm internet altyapısının ya da sıradan bir köprüden çok farklı olarak Mostar köprüsü gibi bir simgenin yok edilmesi orantılı bir saldırı olarak değerlendirilmemelidir.

4.2.4. Sivillere ve Sivil Hedeflere Saldırma Yasağı

Temeli ayrım gözetme prensibine dayanan[1272] bu kural uluslararası silahlı çatışmalar bakımından Cenevre Konvansiyonu'na Ek I. Protokol'ün 51 ve 52. maddelerinde

[1271] Gül, 2021, s. 177.

[1272] Schmitt, 2017, *Tallinn Manual 2.0*. s. 422.

düzenlenmiştir. Ek Protokol'ün 51/2. maddesi gereğince sivil nüfusa saldırmak ve esas amacı sivil nüfus üzerinde terör yaymak olan şiddet hareketleri ya da tehdidi oluşturmak yasaktır. Sivil nüfus ya da sivil halk kavramı kapsamı içine giren sivillerin korunmasına ilişkin temel ilke, 1949 tarihli Cenevre Savaş Esirleri Konvansiyonu madde 27 ve 1977 I. Protokolü madde 75'de ifade edilen uluslararası silahlı çatışmalar sırasında sivillerin insanca muamele görme ilkesidir[1273].

Aynı Protokolün 52/1 maddesinde ise sivil nesnelerin saldırı veya misillemenin hedefi olamayacağı ifade edilmiştir. Bu ilke genel biçimde 1907 Lahey Yönetmeliği'nin 23/g maddesinde, savaş gereksinimlerinin kaçınılmaz kıldığı durumlar hariç, düşman mallarını yok etmeyi ya da bunlara el konulmasını yasaklamaktadır[1274]. Protokol'ün 52/2. fıkrasına göre ise, saldırının katı şekilde askeri maksatlarla sınırlı olduğu belirtilerek bu nesnelerin, doğaları, konumları, askeri eyleme etkili bir katkı sağlama amacı ve kullanımı ve bunların tamamen veya kısmen yok edilmeleri, alıkonulmaları veya etkisizleştirilmeleri kesin bir askeri avantaj sunmalarıyla sınırlı tutulmuştur. Bu maddede askeri hedeflerin işlevine göre tanımlandığı gözetildiğinde herhangi bir malın ya da binanın askeri kuvvetlere ya da sivil kişi ya da kurumlara aidiyetine bakmadan, askeri hedef oluşturması onun yok edilmesine olanak vermektedir[1275].

1977 tarihli 1. Ek Protokol'ün 57. maddesinin 2. bendi ile 52. maddesinin 2. bendi birlikte düşünüldüğünde dikkat edilmesi gereken yükümlülüklerin; hedefin askeri hedef olduğundan emin olma, sivil halka verilebilecek zararı en aza indirme ve zararın aşırı olma olasılığı söz konusu olduğunda saldırıdan vazgeçme olduğu kabul edilmektedir[1276]. Cenevre Konvansiyonları'na Ek 2. Protokol'ün 13. maddesinde uluslararası olmayan silahlı çatışmalarda sivil halkın ve sivil kişilerin korunması amaçlanmış, bu kişilerin

[1273] Pazarcı, 2021, s. 644.

[1274] Pazarcı, 2021, s. 647.

[1275] Pazarcı, 2021, s. 648.

[1276] Hoş, 2013, s. 129.

düşmanlığa doğrudan katılmaları durumu dışında bu korumadan yararlanacakları kabul edilmiştir.

Belirtilen kurallara paralel olarak Tallinn El Kitabı'nda Kural 92, 94 ve 99 gereği sivillere ve sivil hedeflere yönelik siber saldırı gerçekleştirmek yasaklanmıştır. Sivil hedefe yapılacak bir siber saldırının bu yasak kapsamında değerlendirilebilmesi için sivil nüfusun, sivil kişilerin veya sivil nesnelerin saldırının doğrudan hedefini oluşturması gerekir. Tallinn El Kitabı'nda bu konuya verilen örnekte; bir uçağın siber saldırı sonucu düşürülmesi neticesinde uçağın düştüğü yerdeki sivil can kaybı saldırının hedefini oluşturmadığı için yasak kapsamına girmediği ancak bu noktada orantılılık ilkesinin uygulanmasının gündeme geleceği belirtilmektedir[1277].

Bu noktada ortaya çıkan sorunlu bir alan olarak dijital verinin yok edilmesi ya da değiştirilmesinin yukarıda belirtilen sivil nesneye saldırı yasağında kalıp kalmadığının tespiti yönünden "veri" teriminin nesne olarak kabul edilmeyeceği ve meşru askeri hedef oluşturup oluşturmadığı konusu üzerinde durulmalıdır. Tallinn El Kitabı'na göre fiziki bileşeninin değişikliğine sebep olmadıkça sırf verilerin yok edilmesi silahlı çatışmalar hukuku kurallarının işletilmesini gerektirmemektedir[1278]. Tallinn El Kitabı'nda, dijital verinin nesne olarak kabul edilememesi nedeniyle bir bilişim sisteminin işleyişine zarar vermeyen sırf veriye zarar verme eyleminin silahlı çatışmalar hukukunun koruması altında olmadığı sonucu çıkarılmaktadır[1279]. Doğrudan fiziki sonuçları bulunmayan dijital verinin yok edilmesinin daha çok psikolojik operasyonlara yakın olduğu ve verinin nesne olarak kabulü halinde devletlerin operasyon yeteneklerini çok sınırlandıracak bu sınırlandırmadan kaçmak isteyeceğine dair itirazlar söz konusudur[1280].

[1277] Schmitt, 2017, *Tallinn Manual 2.0.* s. 423.

[1278] Mačák, 2015, s. 77.

[1279] Pascucci, 2017. s. 420.

[1280] Mačák, 2015, s. 73.

Dijital veriye yönelen siber saldırı sonucunda hastane kayıtları yok edilebilir, değiştirilebilir ya da yeni bilgiler eklenebilir. Bu saldırılar, sivillerin hayatını kaybetmesine, yaralanmasına veya sivil nesnelerin zarar görmesine sebep olduğu takdirde hiç şüphesiz ki sonuç odaklı yaklaşım gereğince silahlı çatışmalar hukuku sınırlandırmalarına tabi olacaktır. Buna karşın sırf verinin yok edilmesi halinde dijital verinin nesne olarak kabul edilip edilmeyeceğine göre meşru askeri hedef ya da sivil nesnelere saldırı oluşturup oluşturmayacağı konusunda farklı görüşler ortaya çıkmıştır. Bu bağlamda silahlı çatışmalar hukukunun siber savaşa uygulanmasında VAHS'nin 31 ve 32. maddelerine göre ne şekilde yorumlanacağı önem kazanmaktadır. Zira Tallinn El Kitabı'nda verinin nesne olarak kabul edilmemesine gerekçe olarak verinin Ek Protokol'ün 1987 tarihli Uluslararası Kızıl Haç Komitesi Şerhi kapsamında "görülebilir" ve "dokunulabilir" şeylerden olmaması gösterilmektedir[1281]. Bu yorum şekline ise katılmak mümkün değildir.

Öğretide, Tallinn El Kitabı'nda kabul edilen görüşün karşısında yer alan bir görüşe göre; yukarıda belirtildiği üzere VAHS'nin 31. maddesi gereğince yapılacak yorum şekli uyarınca verinin nesne olarak değerlendirilmesi gerektiği kabul edilmektedir[1282]. Buna göre "nesne" teriminin olağan anlamı Protokol'deki terimin bağlamı ve antlaşmanın niyet ve amacı kapsamında günün koşullarına göre tespit edilmelidir. Bu yorum faaliyeti ise, teknolojik gelişimin getirdiği, devlet uygulamaları ya da *opinio juris*'den bağımsız olarak ortaya çıkan yeni kavram ve kategorilere ilişkin olarak devlet uygulamalarının yerine geçen bir uygulama şeklinde kabul edilmemelidir[1283].

Sosyolojide pozitivizmin temsilcilerinden olan yorumcu okula göre, pozitif hukukun en üstün kaynağı, yasa koyucunun niyetidir[1284]. Bu görüşe göre, uygulayıcının görevi yasa koyucunun görüşünü bulup çıkarmak olduğundan teknolojik gelişimin sebep olduğu yeni

---

[1281] Schmitt, 2017, *Tallinn Manual 2.0.* s. 437.

[1282] Mačák, Kubo. (2015). *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humaniterian Law*, Israel Law Review, Cilt:48, s. 56.

[1283] Mačák, 2015, s. 63.

[1284] Can, Cahit. (1996). *Hukuk Sosyolojisinin Gelişim Yönü.* Ankara: AÜHF Yayınları, s. 113-114.

şartlara uygun bir yorum şekli kabul edilmemektedir. Buna karşın, siber uzayın henüz olmadığı bir dönemde oluşan uluslararası hukuk normlarının yorumlanması sırasında yasa koyucunun niyetini tespit etmek olanaksızdır.

Yorumun tarafların niyetinin araştırılmasına yönelmesi gerektiği yönünden bakıldığında ise, niyet ve amaca göre antlaşmanın yorumlanması konusunda farklı görüşler söz konusudur. Bunlar, antlaşma metninde ifade edilen niyet ya da metnin dışında kalan niyettir. Bir diğer görüşe göre ise, yorumda antlaşmanın konu ve amacı esas alınmalıdır. Bu son görüşte tarafların antlaşma metninde veya antlaşmanın akdi sırasında ifadesini bulan niyetinden ayrılabilen bir şekilde yorumlanması mümkündür[1285].

Kısaca özetlemek gerekirse, terimin metinsel bağlamı içerisinde yorumlanması sırasında metnin farklı dillerdeki sürümlerine[1286] bakılmalı, günün koşullarına göre ortaya çıkan yeniliklere uygun modern anlam gözetilmeli, sadece mevcut hukuka göre değil gelecekteki hukuka uygun bir yorum şekli benimsenmelidir. Birden çok dilde hazırlanan antlaşmalarda uyuşmazlık halinde sadece bir dilin esas alınacağına dair hüküm bulunması da mümkündür[1287]. Bu durumda antlaşmada işaret edilen dilin esas alınarak yroum faaliyetinin gerçekleştirilmesi gerekir.

Bununla birlikte, terimin olağan anlamının tespitine yönelen bir yorum faaliyetinde karşılaşılacak birtakım sorunlar ise kaçınılmazdır. Daha öncede belirtildiği üzere internet teknolojisinin gelişiminden çok önceleri hazırlanan uluslararası metinlerin geleneksel şekilde olağan anlamını tespit etmek çok da mümkün olmayacaktır. “Dijital veri” kavramının bilinmediği bir dönemde yazılı metinlerde ifadesini bulan “nesne” kavramına dâhil olup olmadığı konusunda metnin farklı dillerdeki anlamları üzerinden yapılacak bir

[1285] Ayrıntılı bilgi için bkz.: Tütüncü ve diğerleri, 2017, s. 230.

[1286] Ayrı dilde yazılmış ve tevsik edilmiş olan antlaşma metinlerinden hangisinin muteber metin olduğu antlaşmada belirtilememişse, tevsik edilmiş olan bütün metinler muteber ve eşittir. Antlaşma hükümlerinin tevsik edilmiş olan bu metinlerin hepsinde aynı anlamı taşıdığı farz edilir. Bkz.: Tütüncü ve diğerleri, 2017, s. 234.

[1287] Aksar, 2021, (1. Kitap), s. 167.

yorum şekli de her olayda uygulanabilir değildir. Örneğin "nesne" teriminin bahse konu metnin Fransızca ve İspanyolca versiyonlarında dokunulabilir olanlar yanında fiziki varlığı bulunmayan şeyleri de kapsadığı gerekçesiyle günün şartlarına uygun şekilde metnin modern anlamın tespitine yönelen bu yorum şekli[1288] siber alanda ortaya çıkması kaçınılmaz yeni kavramlarda her zaman amaca hizmet etmeyecektir.

Olaya ulusal hukuk yönünden bakıldığında, yorum yapılırken gösterge bilim ve dil felsefesi gözden uzak tutulduğunda yorum faaliyeti, elektrik enerjisinin mal olarak kabul edilmemesi[1289] ya da somut örnekte olduğu üzere verinin nesne olarak kabul edilmemesi ile sonuçlanmaktadır. Bu örnek ulusal hukuktan uluslararası hukuka kural aktarımı olarak değerlendirilmemelidir. Ulusal hukuklarda tarihsel, amaçsal ya da bağlamsal yöntemlerin uygulanması kabul edilmişken; uluslararası hukukta VAHS daha geniş bir yorum yöntemi belirlemiştir. Buna karşın VAHS'ın bu yorum yöntemi dahi olağan üstü teknolojik değişime ayak uyduramamakta ve birtakım zorlayıcı yeni yöntemlerin denenmesi gündeme gelebilmektedir. Dolayısıyla bu sadece ulusal hukuklarda yaşanan bir sorun olmayıp tüm sosyal bilim dallarında söz konusu olan bir durumdur. Bir diğer ifade ile hermönitik, yorum faaliyetini gerçekleştiren[1290] her asker, hukukçu ya da teknik uzmanın yazılı metni anlamasının ön şartı olarak gerek ulusal hukukta gerekse de uluslararası hukukta kendini göstermektedir.

Anayasal hükümler açısından bakıldığında görüşümüzü destekler biçimde, bir normun objektif bir anlatım taşımadığı, her hükmün birçok anlatımı kapsadığı, her metnin birden çok anlatımın taşıyıcısı olduğu gerekçesiyle yorum faaliyetinin metne yaşam vermek

---

[1288] Mačák, 2015, s. 72.

[1289] 765 sayılı mülga TCK'nun 491/1-2. fıkrasına getirilen "Ekonomik bir değer taşıyan her türlü enerji de taşınabilir mal sayılır" hükmü öncesinde elektrik enerjisi hırsızlığının suç oluşturmadığı kabul edildiğinden, belirtilen yasal düzenlemenin yapılması gerekmiştir.

[1290] Uluslararası hukukta yorum faaliyetini diplomatik, ulusal ve milletlerarası organlar gerçekleştirmektedir. Siber savaş açısından yapılacak yorum faaliyetlerini de bu organlarda görev yapan diploma, asker, hukukçu ve teknik personel gibi uygulamacı ya da karar vericiler oluşturmaktadır. Bkz.; Bozkurt ve Erdal ve Poyraz, 2017, s. 81.

anlamına geldiği kabul edilmektedir[1291]. Buradan hareketle soyut metnin yansıtmaya çalıştığı gerçekliğin[1292] uygulayıcılar tarafından her somut olaya özgü şekilde yapılacak yorum faaliyetiyle tespit edilebileceği belirtilmelidir.

Bu açıklamalar ışığında yazılı metinlerin yorumunda VAHS'ne göre yapılabilecek yorumda dahi kelimenin olağan anlamının sadece metnin hazırlandığı tarihteki anlamına göre yapılmaması gerektiği gibi aşırı yorumdan kaçınılarak metnin doğal sürecinde zamanla gelişen ve olgunlaşan yeni anlamları da dâhil edilmelidir. Aksi takdirde metnin anlamsal gelişimine olanak sağlamayan yorum biçimiyle varılacak yer her daim yeni antlaşma gereksinimi olacaktır.

Yazılı hukuk metinlerinin, değişen şartlara göre farklı bir paradigmadan yeni neslin anlam dünyasına göre bakılarak anlamlandırılması kaçınılmaz bir durumdur. Sosyal bilim felsefesi teorisinde yerini alan, bilimin yanlışlama ile değil de yeni paradigmaların oluşmasıyla ilerleyebileceğine dair kabul bağlamında değerlendirme yapıldığında[1293], yukarıda belirtilen şekilde yorumlama biçimi uluslararası hukuku da içeren sosyal bilimlerin her alanında kabul edilmesi gereken bir yöntemdir. Yazılı bir metinin tek bir alıcı yerine okurlar topluluğu için üretilmesi halinde, yorumlamanın sadece yazarın niyetine göre değil, o dilin ürettiği kültürel gelenekleri, okurun okumakta olduğu ve daha

---

[1291] Kaboğlu, İbrahim Ö. (1994). *Anayasa Yargısı*. İstanbul: İmge Kitabevi Yayınları, s. 153-155.

[1292] Wittgenstein'in "Paris'te bir mahkemede, bir otomobil kazasının kuklalarla temsil edilmesinde olduğu gibi, bir cümle içinde de bir dünya eğreti olarak bir araya getirilebilir" sözü anlatılmak istenen gerçeklik ile yazıya dökülen gerçekliğin bir kukla ile gerçeği arasındaki benzerlik kadardır. Bkz.; Arnheim, Rudolf. (2015). *Görsel Düşünme* (Çev. Rahmi Öğdül). İstanbul: Metis Yayıncılık, s. 268.

[1293] Karl Popper ve Thomas Kuhn arasında fikir ayrılığı söz konusu olup, ilkine göre bilim yanışlanabilir olmalı ve yanlışlanabildikçe gelişebilmekte iken, Kuhn'a göre bilimin gelişmesi ancak yeni neslin getirdiği yeni paradigmalar sayesinde olabilmektedir. Paradigma değişimi konusunda bkz.; Bernstein, Richard J. (2009). *Objektivizmin ve Rölativizmin Ötesi Bilimi Hermenoytik ve Praxis* (Çev. Feridun Yılmaz). İstanbul: Paradigma, s. 119-120.

önceden okuyup yorumlamalarını da kapsar şekilde ve değişen paradigmaya göre okurun niyetini de kapsayacak şekilde gerçekleştirilmesi gerekir[1294].

Bu tartışmanın vardığı nokta itibariyle devlet uygulamalarının kaçınılmaz olarak verinin nesne olarak kabul edilmesi yönünde olduğu, örneğin Fransa tarafından yayınlanan Uluslararası Hukukun Siber Uzaya Uygulanmasına dair Belge'de ve Türkiye 2020-23 Ulusal Siber Güvenlik Strateji Belgesi'nde benzer şekilde ifadelerin bulunduğu görülmektedir[1295]. Yukarıda açıklanan yorum yöntemi bir yana, uluslararası hukukun siber operasyonlara uygulanmasında, uygulamada ve öğretide yaygın biçimde benimsenen yaklaşımın etki temelli olmasına ve verinin hedef alınması halinde ortaya çıkacak ağır zararlara karşın eylemin silahlı saldırı düzeyine erişmediğinin kabulü çelişkili bir durum oluşturacaktır. Bu bağlamda veriye yönelen siber saldırı halinde verinin nesne olarak kabul edilip edilmeyeceğine dair lafzi yorum yönteminin yeterli olmadığı söylenebilir. Yazılı metinlerin, teknolojik gelişimin doğurduğu değişen şartlara uygun biçimde yorumlanması sürecinde, kelimenin sırf geçmişine yönelen etimolojik araştırma suretiyle anlamını tespiti yerine, kelime veya terimin geleceğe uzanan değişiminin tespitine yönelik bir değerlendirme gereklidir. Bahse konu olayda olduğu üzere, nesne teriminin anlamı ve kapsamı zamanla değişmekte, genişlemekte ve değişen koşullara paralel olarak dili ve kavramları da evrime tabi tutmaktadır. Bu nedenle uygulayıcıların, bu evrimin bilincinde olmaları ve uluslararası hukuk metinlerinin buna uygun şekilde yorumlamaları gerekmektedir.

4.2.5. Kişi veya Hedefin Statüsünde Şüphe

I. Cenevre Konvansiyonu 50/1 maddesi gereğince şüphe halinde herhangi bir kişinin doğrudan saldırıya karşı korunması gereken sivil olarak varsayılması gerekir[1296]. Tallinn El Kitabı'nda 95. Kural gereğince, hangi düzeyde şüphe söz konusu olduğunda hedefin

[1294] Eco, Umberto. (2013). *Yorum ve Aşırı Yorum* (Çev. Kemal Atakay). İstanbul: Can, s. 87-88.

[1295] Gül, 2021, s. 142-143.

[1296] Melzer, 2011, s. 30.

sivil bir hedef olarak kabul edileceği konusunda iki ihtimal söz konusudur. Bazı devlet uygulamalarına göre tatmin edici ya da önemli düzeyde bir şüphe (*substantial doubt*) halinde hedefin sivil olarak kabulü gerekirken; diğer ihtimalde, uluslararası ceza hukukuna göre sorumluluğu belirlemekte, benimsenen makul şüphe (*reasonable doubt*) hali gerekli görülmektedir[1297]. Örneğin, Alman devletinin bu konudaki duruşu, özenli bir değerlendirmenin yapılmasına karşın hala önemli düzeyde şüphenin bulunması halinde sivil nesne olarak kabulün gerekliliği yönündedir[1298].

Buna göre sivil hedefe saldırı yasağının ihlali yönünden gerekli şüphe düzeyi her durumda belirli bir seviyeye erişmiş olmalıdır. Bu şüphe kavramlarının siber saldırılar açısından nasıl uygulanabileceği konusunda siber altyapı tesislerinin ikili kullanımdan gelen kendine özgü bir zorluğun söz konusu olduğu söylenebilir. Silahlı çatışmanın tarafı olan bir devletin hazırladığı siber silahın kullanılması hedeflenen siber alt yapı tesisinin, örneğin sivil havacılık sistemi olma ihtimaline dair önemi şüphelerin söz konusu olması durumunda sivil bir hedef olarak kabulü gerekir. Askeri hedef mahiyetindeki bir siber tesise gerçekleştirilen bir siber saldırının dolaylı olarak sivil sistemleri etkilemesi ise yukarıda belirtildiği üzere sonuçların orantılılık ilkesine göre değerlendirilmesini gerektirecektir.

4.2.6. Savaş Hilesi ve Hainlik

Silahlı çatışmalar hukuku, çatışmalar sırasında başvurulacak araçların yanında birtakım yöntemlerin de yasaklanmasını ya da belirli koşullarla sınırlandırılmasını öngörmektedir. Bu yasaklama ya da sınırlandırmanın bir kısmı güven suiistimalinin yasaklanması ilkesinden kaynaklanmaktadır[1299]. Cenevre Konvansiyonu'na Ek (I.) Protokolün 37/1. maddesinde silahlı çatışmada yasaklanan ve hainlik (*perfidy*) olarak nitelendirilen eylemler ortaya konulmuştur. Madde metninde hasmını öldürmek, yaralamak veya tutsak

[1297] Schmitt, 2017, *Tallinn Manual 2.0*. s. 424.

[1298] Position Paper, 2021, s. 8-9.

[1299] Pazarcı, 2021, s. 633.; Sur, 2022, s. 309.

etmek amacıyla hainlik veya kalleşlik olarak dilimize çevrilebilecek yollara başvurulmasını yasaklamakta ve örneklendirilmektedir.

Bunlar:

- Ateşkes veya teslimiyet bayrağı altında görüşme niyetindeymiş gibi davranmak;
- Yaralanma veya hastalıktan dolayı acizmiş gibi davranmak;
- Savaşan değilmiş veya sivilmiş gibi davranmak;
- Çatışmanın tarafı olmayan diğer devletlerin, tarafsız devletlerin veya BM'nin işareti, amblemi veya üniforması tarafından korunuyormuş gibi davranmak olarak sayılmıştır.

Anılan maddenin 2. fıkrasında ise hainlik olarak değerlendirilemeyecek savaş hilelerinin yasaklanmadığı açıklanmış, kamuflaj kullanımı, tuzağa düşürme, sahte operasyon ve yanlış bilgilendirme buna örnek olarak sayılmıştır. Silahlı çatışmalar sırasında düşmanı aldatmaya yönelik bu son sayılan yöntemler ile kalleşlik arasında bir ayrıma gidilmektedir[1300].

Bu düzenlemeye uygun şekilde Tallinn El Kitabı'nda 123. Kural'da "*ruses*" olarak ifade edilen siber eylemlerin yasak olmadığı kabul edilmiştir. Örneğin siber silahın düşürülmüş bir harici bellek şeklinde askeri personeli cezbedecek bir yere konulması, Stuxnet saldırısında olduğu üzere nükleer santrifüjlerin düzgün şekilde çalışıyormuş gibi ekrana yansıtılmasına benzer hileler yasak kapsamında değerlendirilemez. Buna karşın Uzmanlar Grubu çoğunluğuna göre, sivil nüfusu veya nesneleri riske atacak şekilde ayrım gözetme prensibini zayıflatan siber kamuflajın yasak kapsamında kalması gerekmektedir[1301].

[1300] Pazarcı, 2021, s. 634.

[1301] Schmitt, 2017, *Tallinn Manual 2.0*. s. 496.

Kurallara sadakatsizlik oluşturdukları kabul edilen 1907 Lahey Yönetmeliği'ndeki[1302] başlıca durumlar ise şunlardır[1303]:

- Düşman ulusa ya da orduya mensup kişilerin ihanet yoluyla öldürülmesi ya da yaralanması;
- Görüşmeci bayrağı kullanılarak eylem yapılması;
- Düşman sancağı, askeri işaretleri ya da üniforması kullanılarak eylem yapılması;
- 1906 tarihli Yaralı ve Hastaların Durumunun İyileştirilmesi Cenevre Konvansiyonu'nda öngörülen sağlık ve din personeli işaretleri kullanılarak eylem yapılması halleridir.

Anılan düzenlemelerin yanında özünde aynı eylemleri yasaklayan 1977 I. Protokolü'ne göre ise, yasak kapsamına sokulan eylemler özetle şunlardır: görüşmeci bayrağı ya da teslim olma kisvesi altında eylem yapmak; yaralı ya da hasta kisvesi altında eylem yapmak; sivil ya da savaşçı olmayan kişi kisvesi altında eylem yapmak; BM ya da tarafsız devletlerin işaret ya da üniformaları altında eylem yapmak[1304].

Yukarıda adı geçen uluslararası hukuk kurallarında farklı şekilde ifade olunan bu yasakların, Tallinn El Kitabı'nda dört unsurunun bulunduğu kabul edilmektedir. Bunlar; hasmın özellikle güvenini sağlayacak bir eylem, güvene ihanet niyeti, uluslararası hukuk tarafından sağlanan özel bir koruma ve hasmın ölmesi ya da yaralanmasıdır[1305]. Ortaya çıkan yaralanma veya ölümün meydana gelmesine sebep olan eylem ile arasında yakın

[1302] 1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022 http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

[1303] Pazarcı, 2021, s. 634.

[1304] Pazarcı, 2021, s. 635.; Sur, 2022, s. 125.

[1305] Schmitt, 2017, *Tallinn Manual 2.0*. s. 492.

sebep ilişkisi (*proximate cause*) gerekli görülmektedir[1306]. Gerçekleştirilen yanıltıcı bir siber eylemin beklenmeyen şekilde sonuçlanması halinde gerekli olan sebep sonuç ilişkisi arasında uygun bir illiyet bulunduğundan bahsedilemez.

Tallinn El Kitabı'nda 122. Kural olarak düzenlenen yasak davranışların siber operasyonların söz konusu olduğu çatışmalarda güvene ihanet eylemlerinin yasaklandığı kabul edilmiştir. Lahey Konvansiyonu'nun 23 (b) maddesinde düzenlenen silahlı çatışmalarda hainlik yasak olarak ifade edilmiş olup yasağın uluslararası olan ya da olmayan silahlı çatışmalarda geçerli olduğu kabul edilmektedir[1307].

Yasak kapsamındaki eylem sonucunda neticenin gerçekleşmemesi halinde veya bilgisayar üzerinden tıbbi veriler üzerinde gerçekleştirilen ancak insanların algılamalarında bir güvenin suiistimali mahiyetinde olmayan ve sadece bilgisayar verilerine olan güven ile ilişkili olan yanıltıcı müdahalelerin bu kapsamda değerlendirilip değerlendirilmeyeceği konularında Uzmanlar Grubunda görüş ayrılığı çıkmıştır.

Benzer şekilde korunan amblem, sembol veya işaretlerin uygunsuz kullanımlarının Kızılhaç veya Kızılay gibi kurumların alan adlarının siber operasyonlarda taklit edilmesini kapsayıp kapsamadığı konusunda da görüş ayrılıkları bulunmaktadır[1308]. Bu halde antlaşmaların dar şekilde yorumlanmaması gerektiği, önemli olanın BM amblemi de dahil korunan amblem, sembol veya işaretlerin ve hatta tarafsız bir devlete ya da düşmana ait bayrak, amblem, kamuflaj veya işaretlerin kötüye kullanımının geleneksel çatışmalarda yaptığı etkiyi sağlaması halinde, değişen duruma göre alan adlarının veya bu türden kayıtların kullanılmasının da aynı yasağa tabi olduğu kabul edilmelidir.

Uzmanlar Grubu'nun çoğunluğuna göre, siber saldırılarda kullanılan araçların düşmana ait olduğunu gösteren kayıtların silinmedikçe ve yeniden işaretlenmedikçe

[1306] Schmitt, 2017, *Tallinn Manual 2.0*. s. 492.

[1307] Schmitt, 2017, *Tallinn Manual 2.0*. s. 492.

[1308] Schmitt, 2017, *Tallinn Manual 2.0*. s. 498.

kullanılamayacağı kabul edilmekte iken azınlık görüşüne göre yerden havaya atılan füze sistemine müdahalede olduğu üzere düşman işaretlerinin yeniden adlandırılmasına elverişli olmaması hali gibi duruma özgü değerlendirme yapılmalıdır[1309]. Bunu daha da ileri götüren örnekler ise, düşmana ait insansız hava araçları veya diğer savaş araçlarının kontrolünün ele geçirilmesi sonrasında yere indirilerek ambleminin sökülmesi gerekip gerekmediği konusudur ki bu konuda da fikir ayrılıkları bulunmaktadır.

4.3. SİLAHLI ÇATIŞMALAR HUKUKUNDA MEŞRU AKTÖRLER VE HEDEFLER İLE KORUNAN KİŞİ VE NESNELER

4.3.1. Saldırıyı Gerçekleştirebilecek ve Saldırının Yasal Hedefi Olan Kişiler ve Nesneler

Silahlı çatışmalara katılabilecek ve savaşın gerektirdiği şiddet eylemlerini gerçekleştirebilecek kişilerin bazı ayrıcalıklara sahip olmaları ve çatışmada meşru hedef oluşturmaları nedeniyle bu konunun incelenmesi gerekir. Bu kişilerin başında savaşçılar gelmektedir. Uygulanan uluslararası hukuka göre savaşçı, silahlı çatışma eylemlerine doğrudan katılma hakkı olan kişi anlamına gelmektedir. Savaşçının tanımı ilk kez 1977 tarihli I. Protokol'ün 43/2. maddesinde dolaylı şekilde yapılmıştır. Bu tanıma göre tıbbi ve dini birim görevlileri dışındaki çatışmalara katılan bir tarafın silahlı kuvvetler mensupları bu kapsamda değerlendirilmiştir[1310]. Bu kuralın siber savaşçılara uygulanması sonucunda bir siber savaşçının devletin iç mevzuatına göre resmi şekilde silahlı kuvvetlere entegre olması halinde hukuken savaşçı kabul edilmesi söz konusu olmaktadır[1311]. Buna göre silahlı bir çatışmada bir devlete yönelik sempati beslenmesi ya da devletle ilişkili olunması, siber faaliyette bulunan bir kişinin hukuken savaşan olarak kabul edilmesi için tek başına yeterli görülmemektedir[1312]. Buna uygun örneği 2008 tarihli Gürcistan siber saldırısı oluşturmakta olup Gürcistan Hükümeti web sitelerini ve

[1309] Schmitt, 2017, *Tallinn Manual 2.0.* s. 502.

[1310] Pazarcı, 2021, s. 616-617.

[1311] Padmanabhan, 2013, s. 292.

[1312] Padmanabhan, 2013, s. 296.

kritik altyapı tesislerini hedef alan DDoS saldırısını gerçekleştiren çok sayıdaki siber saldırganın Rusya devletine olan sempatisi bu kişilerin savaşan olarak kabulü için yeterli değildir.

Bu konuda diğer bir hukuki dayanak olan 1949 tarihli III nolu Cenevre Konvansiyonu'nun 4. maddesinde ise savaşçıların kimlerden ibaret olduğu açıklanmış, ihtilafa dâhil olan tarafların silahlı kuvvetleri mensupları yanında[1313] uluslararası silahlı çatışmalarda savaşçı statüsü tanınan ikinci grubun ise bazı koşulları yerine getirmek şartıyla, bir devletin ordusunda yer alan milis kuvvetleri ve gönüllü birlikler mensupları olduğu ifade edilmiştir[1314]. Milislerin ve gönüllü birliklerin hangi şartları yerine getirmeleri halinde savaşçı statüsünde olacakları ise anılan Konvansiyon'un 4. maddesi yanında 1907 IV sayılı Lahey Konvansiyonuna'na Ek Yönetmeliğin[1315] 1. maddesinde düzenlenmiştir. Bu hükümlere göre bu birliklerin başlarında astlarından sorumlu bir kişinin bulunması, sabit ve uzaktan seçilebilir bir işaretin bulunması, açıkça silah taşımaları ve çatışma kurallarına riayet etmeleri gereklidir[1316]. Siber operasyonları gerçekleştiren yarı bağımsız gruplar kadar siber silahların tasarlanmasında ve faaliyete geçirilmesine dâhil olan siber savaşçıların belirtilen gereklilikleri karşılaması ihtimal dâhilinde kabul edilmektedir[1317].

Hukuken savaşan statüsüne sahip olmanın şiddet kullanma ve düşman öldürme yetkisi tanınması ve bu eylemlerden dolayı cezai sorumluluğa maruz kalmama hakkı gibi bazı ayrıcalıkları sağlaması yanında bu kişilerin düşman birlikleri tarafından hedef alınmasına da sebep olduğu kabul edilmektedir. Savaşçı statüsüne sahip kişilerin çatışmalar hukukunu ihlal eden eylemleri dışında cezai sorumlulukları bulunmazken bu kişiler karşı

[1313] Gül, 2021, s. 93.

[1314] Pazarcı, 2021, s. 617.

[1315] 1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022 http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

[1316] Pazarcı, 2021, s. 617.; Gül, 2021, s. 93.

[1317] Padmanabhan, 2013, s. 294.

tarafın eline düştükleri zaman savaş tutsağı muamelesine bağlı tutulmaktadırlar[1318]. Savaşan tarafların askeri kuvvetleri mensubu olmakla birlikte tıbbi ve dini birim görevlileri ise savaşçı statüsünü haiz olmadığı gibi meşru hedef de oluşturmazlar.

Silahlı çatışmalar hukukuna göre çatışmaya katılma hakkı bulunan kişilerin aynı zamanda meşru hedef oluşturduğu yukarıda belirtilmişti. Buna göre sadece üç kategoride sayılan kişiler meşru hedef olabililecektir: savaşanlar, çatışmaya doğrudan katılan siviller ve çatışmada doğrudan katılıma eşit kabul edilecek operasyon veya eylemi hazırlama, uygulama veya komuta etme eylemlerini düzenli şekilde gerçekleştiren siviller[1319]. Hemen yukarıda belirtildiği üzere siber faaliyette bulunan kişilerin savaşan olarak kabul edilebilmesi için silahlı kuvvetler mensubu olması gerekmekte olup sadece devletle ilişkili olmak ya da sempati duymak bu konuda yeterli kabul edilmediğinden bu kişiler meşru hedef de oluşturmamaktadırlar. Silahlı kuvvetler mensubu olmamakla birlikte siber savaşçılar, çatışmaya doğrudan katıldıkları takdirde meşru hedef oluşturacaktırlar. Siber savaşçılar açısından doğrudan katılım standartlarının belirlenmesi kolay olmayıp doğrudan katılıma eşit düzeyde bazı eylemlerin gerçekleştirilmesi durumunda meşru hedef olabilmeleri mümkündür. Bu konu daha önce incelendiği için tekrar edilmeyecek ancak siber savaşçıların doğrudan katılım süresinin sonucun ortaya çıktığı zamana değin uzandığı ve doğrudan katılımda aranan doğrudan sebep olma (*direct causation*), zarar eşiği (*threshold of harm*) ve bir tarafın lehine diğer tarafın aleyhine hareket etme (*belligerent nexus*) kıstasları karşılanmalıdır. Buna göre, bilimsel araştırmalar veya siber silah tasarımı ile zarar arasında sebep sonuç ilişkisi, bir diğer ifade uygun illiyet bağının bulunmaması nedeniyle silahlı çatışmaya doğrudan katılma kapsamında değerlendirilememekte, yine düşmanın ekonomik refahını zarar uğratma niyetiyle gerçekleştirilen sivil sistemlere yönelik istismar eylemleri zarar eşiğini karşılamaması nedeniyle bu kapsamda değerlendirilmemektedir[1320].

[1318] Pazarcı, 2021, s. 623.

[1319] Hathaway ve diğerleri, 2012, s. 853.

[1320] Padmanabhan, 2013, s. 298.

Öğretide ve Tallinn El Kitabı'nda bu üç gruba ilaveten uluslararası bir silahlı çatışma durumunda halkın işgalci güçlere karşı direniş göstermesi anlamına gelen *levée en masse* katılımcılarının da meşru hedef olabileceği kabul edilmektedir[1321]. Bir devletin ordusunda yer alan milis kuvvetleri ve gönüllü birlik mensuplarının savaşan statüsüne dâhil olması için koşul olan dört şartı taşıması gerekli olmayan ayaklanan sivillerin, savaşan olarak kabul edilebilmelerinin tek yolu kitle ayaklanması suretiyle işgale karşı direnen durumunda olmalarıdır [1322] . Bu statüdeki kişilerin işgal edilmemiş bir bölgede kendiliğinden gerçekleşen bu ayaklanmaya katılanların astlarından sorumlu bir komutana bağlı olma ve uzaktan ayırt edilebilir bir işaret taşıma kıstaslarını yerine getirmeleri gerekliliği bulunmasa da geleneksel çatışmalarda silah taşıma ve silahlı çatışmalar hukuku kurallarına uyma yükümlülüğü bu kitle için de geçerlidir.

Siber kitle ayaklanması durumunda geleneksel çatışma kurallarının ne şekilde uygulanacağı konusunda önemli sorular ortaya çıkmaktadır. Öğretide bazıları bu duruma örnek olarak kritik altyapı unsurlarını yöneten sivillerin siber operasyonlara yanıt olarak aktif savunma sistemlerini kullanmaları halinde siber *levée en masse* katılımcıları olarak kategorize edilebilecekleri ve bu suretle meşru savaşçı statüsünü kazanacaklarını belirttikleri görülmektedir[1323]. Buna karşın siber *levée en masse* halinde bir bölgesel işgalin önemini kaybetmesi ve açıktan silah taşıma olanağının bulunmaması nedeniyle bu gibi durumlarda ayırt edici başka bir araç kullanılması ve milis kuvvetleri, gönüllü birlikler mensupları veya organize direniş hareketleri tanımının değiştirilerek siber kitlesel ayaklanma katılımcılarının sivillerden ayrımının sağlanabileceği de savunulmaktadır[1324].

Bundan başka, savaşçı statüsünden yararlanan kişilerin birtakım koşullarda bu niteliklerini kaybettikleri kabul edilmektedir. Savaşçı tanımı kapsamına kural dışılık

---

[1321] Bkz.: Kural 96, Schmitt, 2017, *Tallinn Manual 2.0.* s. 425.; Pazarcı, 2021, s. 617.

[1322] Gül, 2021, s. 104.

[1323] Padmanabhan, 2013, s. 294.

[1324] Wallace, David / Reeves, Shane R. (2013). *The Law of Armed Conflict's "Wicked Problem: Levée en Masse in Cyber Warfare*, Int'l L. Stud., Cilt:89, s. 664-665.

oluşturan bu kişi gruplarından bazıları casuslar ve paralı askerlerdir[1325]. Savaşanlar, düzenli silahlı güçlerin üyeleri olabileceği gibi organize silahlı grup üyeleri de savaşan statüsünü haiz oldukları için meşru askeri hedef oluşturmaktadırlar. Organize silahlı grup üyelerinin çatışmaya katılmadıkları süre içinde meşru hedef olup olmayacakları konusunda Uzmanlar Grubu'nun ikiye ayrıldığı görülmektedir[1326]. Uzmanlar Grubu'na göre organize silahlı grupların sadece askeri kanadı bu kapsamda değerlendirilmekte askeri kanat dışında kalan sosyal ya da politik kanadının ise meşru hedef oluşturan organize silahlı grup kapsamında değerlendirilmemektedir.

Sivillerin ise ancak silahı çatışmalara doğrudan katılımı halinde yasal hedef olarak kabul edildiği[1327] dikkate alındığında siber savaş halindeki sivillerin durumunun geleneksel çatışmalara nazaran farklılık arz etmesi anlaşılabilir bir durumdur. Zira siber saldırıyı gerçekleştirebilecek kişilere silahlı çatışmalar hukuku kuralları uygulanacak olmasına rağmen devletlerin gerekli teknik uzmanlığa sahip olmaması nedeniyle ve yapılacak operasyonu gizlemek amacıyla siviller istihdam edilmektedir[1328]. Bu amaçla istihdam edilen özel askeri ortaklıklar (şirketler) görevlilerinin anonim şirket haline gelmiş paralı askerler olarak değerlendirip değerlendirilmeyeceği ya da paralı askerlikten farklılık arz edip etmediği konusunda uzlaşı bulunmamaktadır[1329].

Siber savaşa katılan sivillerin yukarıda bahsedilen dört şartı yerine getirmesinin gerekli olup olmadığı tartışmalı bir konu olsa da[1330] uzakta bir yerde bilgisayar başında ayırt edici bir işaret taşıma yükümlülüğünün siber savaşta geçerli olmadığı, yine açıktan silah taşıma

---

[1325] Paralı askerler konusunda öğretide farklı görüşler bulunmakla birlikte 1977 I. Protokol'ün 47. maddesi bir paralı asker tanımı yaparak bu tanım kapsamına giren paralı askerlerin savaşçı statüsünden yararlanamayacağını açıkça öngörmektedir. Bkz.; Pazarcı, 2021, s. 621-622.; Aksar, 2021, (2. Kitap), s. 197-198.

[1326] Schmitt, 2017, *Tallinn Manual 2.0.* s. 426.

[1327] Padmanabhan, 2013, s. 290.

[1328] Hathaway ve diğerleri, 2012, s. 854.

[1329] Pazarcı, 2021, s. 623.

[1330] Öğretideki bu konuya ilişkin farklı görüşler için bkz.; Gül, 2021, s. 100.

gereğinin siber savaşta sağlanmasının olanaksızlığı ortadadır. Buna karşın siber operasyonlarda askeri IP adresin kullanılması halinde savaşçı statüsünden yararlanabilme imkânının sağlanacağı ve şeffaflığın yanlış IP kullanımını azaltacağı gibi saldırıya dâhil olmayan üçüncü bir devlet ya da sivil altyapı tesislerine misilleme riskini düşüreceği savunulmaktadır[1331]. Bu yönüyle siber savaşçıların ayırt edici işaret ya da açıktan silah taşıma koşullarını yerine getirmesi beklenilemez ise de operasyonun niteliğinin gerektirdiği askeri IP adresi kullanma gerekliliği makul bir öneridir. Astlarından sorumlu bir komutanın bulunması ve çatışma kurallarına uyulması şartlarının karşılanması geleneksel çatışmalardan pek de farklı değildir.

Organize silahlı örgüt üyelerinin çatışmalarda meşru hedef oluşturup oluşturmadığı konusunda Uzmanlar Grubu'nda görüş ayrılıkları bulunmaktadır. Bir kısım uzmanlar tüm örgüt üyelerinin meşru hedef olabileceğini savunurken çoğunluğun sürekli çatışma işlevini (*continuous combat function*) taşıyanların bu kapsamda değerlendirebileceğini benimsediği görülmektedir. Sözleşme gereğince çalışan sivil kişilerin meşru hedef olup olmadığı konusunda Uzmanlar Grubu'nun yalnızca çatışmaya doğrudan katılmaları durumuna dair hemfikir oldukları, uluslararası silahlı çatışmanın tarafı ile sözleşme yapan şirketlerin ise çoğunluk görüşüne göre organize silahlı grup olarak nitelendirilecekleri kabul edilmektedir[1332]. Bu şirketlerin uluslararası silahlı çatışmanın tarafa ait olmasının gerekip gerekmediği konusunda görüş ayrılığı bulunmakta olup çoğunluk ait olmayı yeterli görürken azınlık görüşünde çatışmaya doğrudan katılmalarının gerekli olduğu kabul edilmektedir[1333]. Bu durumda düşman ordusunun temizlik görevlisi de dâhil üyeleri meşru hedef kabul edilirken, silah ve askeri donanımları üretip yol, köprü, havaalanı ve diğer altyapıların yapımında dolaylı katkıda bulunan şirket üyelerinin çatışmaya doğrudan katılmadıkları gerekçesiyle korunan kişiler kapsamında değerlendirilmeleri eleştirilmektedir[1334].

[1331] Padmanabhan, 2013, s. 295-296.

[1332] Schmitt, 2017, *Tallinn Manual 2.0*. s. 427.

[1333] Schmitt, 2017, *Tallinn Manual 2.0*. s. 427.

[1334] Gül, 2021, s. 112.

Bu başlık altında bahsedilmesi gereken bir diğer husus olan ve meşru hedef teşkil eden nesneler konusu, Ek Protokol'ün 52/2. maddesinde düzenlenmiştir. Bu hükme göre ilk olarak hedefin "askeri eylemlere etkin bir katkıda" bulunması ve ikinci olarak bu nesnenin "tamamen ya da kısmen yok edilmesi, ele geçirilmesi ya da etkisiz hale getirilmesi durumunda, mevcut koşullar altında kesin bir askeri avantaj" sağlaması gereklidir[1335]. Siber saldırılarda bu şartları taşıyan nesnelerin hedef alınması konusunda geleneksel saldırılardan farklı bir uygulama söz konusu değil ise de siber altyapı tesislerinin çift taraflı yapısı gözetilerek sağlayacağı askeri avantaj ve orantılılık ilkesi kapsamında askeri kullanım yönünün hedef alınmasının teknik olarak mümkün olması hali dışında meşru hedef olarak kabul edilmemesi gerekir. Alman Tutum Belgesi'nde ise bilgisayar, bilgisayar ağı ve depolanan veri, sivil ve askeri şekilde ikili kullanım ya da sadece askeri amaçlı kullanım halinde saldırının hedefi olabileceği ifade edilmektedir[1336].

4.3.2. Korunan Kişiler ve Nesneler

Cenevre Konvansiyonları ve I. ve II. Ek Protokoller'de çatışmada görev alan bazı personelin korunması ve bunlara saygı gösterilmesi yükümlülüğü öngörülmüştür. Bunlar tıbbi ve dini birim personelleri ile tıbbi amaçlı ulaşım hizmet personelleridir. Bu personellerin bir saldırının hedefi olarak seçilmemesi bir yükümlülüktür. Bu bağlamda siber saldırılar yönünden El Kitabı'nda 132. Kural altında tıbbi amaçlı kullanılan ağ, veri ve bilgisayarlara yönelik siber saldırı gerçekleştirilmesi yasaklanmıştır. Bununla birlikte korunan bu kişi ve nesnelerin amacı dışında ve düşmana zarar verecek biçimde kullanılması halinde Kural 133 gereğince korumanın kalkacağı ancak öncelikle gerekli uyarının yapılarak zaman tanınması gerekliliği kabul edilmektedir.

Savaş esirleri, enterne edilmiş korunanlar ve diğer alıkonulan kişilerin siber operasyonların olumsuz etkilerinden korunması Kural 135'de belirtilmiş olup Kural

[1335] Gül, 2021, s. 125.

[1336] Position Paper, 2021, s. 8.

gereğince belirtilen kişilerin sadece fiziki varlığının değil siber operasyonlar aracılığıyla iftiraya uğratan ve tahkir edici, onur kırıcı bilgilerin yayılması yasaklanmıştır[1337]. Ayrıca 136. Kural gereğince bu kişilerin ailelerini durumdan haberdar etmelerine izin verilmesi yanında siber takibe alınmaması gerekmektedir. 137. Kural uyarınca bu kişilerin kendi ülkeleri aleyhine siber operasyonlarda kullanılmaya zorlanmaması da geleneksel çatışma kurallarının siber uzayda yansıması olarak ifade edilebilir.

Geleneksel çatışma kurallarının siber uzayda uygulanan diğer bazı kurallarına göre 15 yaş altı çocukların siber operasyonlarda kullanılması Kural 138 gereğince yasak kapsamında bulunmaktadır. Kural 139' da siber saldırılardan korunması gereken bir diğer meslek gurubu gazetecilerdir. Doğrudan çatışmalara katılmadıkça bu meslek mensuplarına saygı gösterilmesi ve bu meslek mensuplarının korunması esastır.

4.3.3. Tehlikeli Kuvvet İçeren Tesisler, Sivil Nüfus için Hayati Nesneler, Kültür ve Tabiat Varlıklarının Korunması

Silahlı çatışmalar hukukunda çevrenin korunmasına ilişkin düzenlemeler 1970'li yılların ortasında hayata geçmeye başlamış olup daha öncesinde var olan antlaşmalar sivillerin ya da mülkiyetin korunmasına yönelikti[1338]. 1899-1907 Lahey Konvansiyonları ve 1949 tarihli Cenevre Konvansiyonları'nın bahse konu alanlardaki eksikliklerini gidermek amacıyla ilk olarak 1954 tarihli Silahlı Bir Çatışma Halinde Kültür Mallarının Korunmasına Dair Lahey Sözleşmesi ile kültür varlıklarının korunması amaçlanmış, bu sözleşmenin koruma alanı 1999 tarihli Ek Protokol ile genişletilmeye çalışılmıştır[1339]. Uluslararası hukukta silahlı çatışmalar sırasında çevreye verilecek zararın önlenmesine yönelik 1977 I. Protokolü'nde öngörülen düzenlemeler yanında 18.05.1977 tarihli Askeri Amaçlarla ya da Daha Başka Düşmanca Amaçlarla Çevrenin Değiştirilmesi Tekniklerinin

[1337] Schmitt, 2017, *Tallinn Manual 2.0*. s. 521.

[1338] Güneysu, 2011, s. 116-117.

[1339] Ayrıntılı bilgi için bkz.; Güneysu, 2011, s. 120-124.

Kullanılmasına İlişkin Sözleşme söz konusudur[1340]. Gerçekleştirilecek saldırılardan sivil halkın ve kültür ve tabiat varlıklarının zarar görmemesi amacıyla çatışmanın taraflarına belirtilen düzenlemeler ile saldırıdan kaçınma ve gerekli özeni gösterme yükümlülüğü getirilmiştir. Bu sözleşmelerden önce 1907 Lahey IV. Konvansiyonuna Ek Yönetmeliğin[1341] 23 (g) ve 55. maddelerinde ve 1949 tarihli IV. Cenevre Konvansiyonu 53. maddesinde askeri gereklilik ya da işgal sırasında mülkiyetin korunmasına yönelik kısıtlamalar içermekteyse de doğal çevrenin bu koruma alanına dâhil olmadığı kabul edilmekteydi[1342].

Tallinn El Kitabı'na bakıldığında 143. Kural'da doğal çevre sivil nesne olarak kabul edilerek ayrımcılık ilkesi temelinde incelenmiş, doğal çevrenin korunması Uzmanların çoğunluğunca gerek uluslararası ve gerekse de uluslararası olmayan silahlı çatışmalar bu Kural kapsamında değerlendirilmiştir. El Kitabı'nın 140. Kuralı'nda tehlikeli kuvvet içeren tesislere ve bu tesislerin yakın çevresine yönelik siber saldırılardan kaçınılması ve özel bir dikkat gösterilmesi zorunluluğu ifade edilmiştir. Kuralda bu tesisler barajlar, su setleri ve nükleer elektrik üreten tesisler olarak sınırlandırılmış[1343], kimyasal tesisler ve petrol rafinerileri Kural 99-101'de düzenlenen sivil nesnelerin korunması hükümlerine tabi tutularak Kural 113-120 arasındaki önlem alma yükümlülüğüne tabi olduğu belirtilmiştir[1344]. Uzmanların çoğunluğu özel bir dikkat gerekliliğini, tesisin yarattığı özel tehlikenin uygulamada elverdiğince dikkate alınması olarak yorumlarken; azınlık görüşü, sivillerin çevresel zarardan korunması için elverişli tüm tedbirlerin alınması gerekliliği Kural 114-120'de zaten düzenlendiği gerekçesiyle bu özel önlem hükmüne bu kuralda yer verilmemesi gerektiği yönündedir.

[1340] Pazarcı, 2021, s. 649.

[1341] 1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022 http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

[1342] Güneysu, 2011, s. 117.

[1343] Sözleşme metnine göre geleneksel saldırılar için yapılan yorum da bu yöndedir. Bkz.; Güneysu, 2011, s. 117.

[1344] Schmitt, 2017, *Tallinn Manual 2.0*. s. 530-531.

El Kitabı'nda 141. maddede sivil nüfus için hayati nesnelerin siber saldırılara karşı korunması amaçlanmış ve siber operasyonlar ile bu nesnelere saldırmak, bu nesneleri yok etmek, bertaraf etmek ya da etkisiz kılmak yasaklanmıştır. Bu kural kaynağını 1. Ek Protokol'ün 54. maddesinden almakta olup bu hüküm ile sivil halkın yaşaması için vazgeçilmez nitelikteki bazı mekân ve malların saldırılara karşı korunması suretiyle sivil halkın aç bırakılması ve taşınması önlenmek istenmiştir[1345]. Ek Protokol I ve II hükümlerine göre, gıda maddeleri ve bu maddeler ile ürün, canlı hayvan varlığı üretiminin yapıldığı zirai bölgeler, içme suyu tesisatı, levazım ve sulama işleri bu mekân ve mallar kapsamında değerlendirilmekte, bunların yanında gıda ve tıbbi malzemeler genellikle sivil nüfusun hayatta kalmasına temel maddeler olarak kabul edilmektedir[1346]. Ayrıca uzman çoğunluğuna göre bu hüküm uluslararası olmayan silahlı çatışmalarda da uygulama yeri bulurken azınlık görüşüne göre kaynak maddenin uluslararası silahlı çatışmalara ilişkin olması ve yapılageliş hukuku gereği sadece sivil halkın aç bırakılmasına yönelik belirli eylemler söz konusu olduğunda uluslararası olmayan silahlı çatışmalarda bu kural uygulanabilecektir[1347].

Tallinn El Kitabı 142. Kural'da kültür varlıklarının siber saldırılar karşısında korunmasına dair düzenlemeye yer verilmiş, çatışmanın taraflarına bu varlıklara yönelik saygı duyma ve koruma yükümlülüğü getirilmiştir. Bu kural kaynağını 1954 tarihli Lahey Sözleşmesi ve buna ek 1999 tarihli Ek II. Protokol ile I. Ek Protokol'ün 53. maddesi ve II. Ek Protokolün 16. maddesinden almaktadır. Uzmanlar Grubu'nca bu kuralın uluslararası ve uluslararası olmayan silahlı çatışmalarda da uygulama yeri bulduğu kabul edilmiştir[1348].

[1345] Güneysu, 2011, s. 129.

[1346] Schmitt, 2017, *Tallinn Manual 2.0*. s. 533.

[1347] Schmitt, 2017, *Tallinn Manual 2.0*. s. 532.

[1348] Schmitt, 2017, *Tallinn Manual 2.0*. s. 534.

4.3.4. Siber Operasyonların İcrası Sırasında Alınması Gerekli Önlemler

Siber operasyonların gerçekleştirilmesinden sorumlu birimlerin mümkün olan önlemleri alması yükümlülüğü 1907 Lahey IV Sayılı Kara Savaşının Kanunları ve Adetleri Hakkında Konvansiyon ve Hava Savaşlarına İlişkin 1923 tarihli Lahey Kuralları'nda zımni şekilde düzenlenmiştir. En detaylı kurallar ise, 1956 tarihli Savaş Zamanı Sivil Nüfusun Maruz Kaldığı Tehlikelerin Sınırlandırılmasına Dair Taslak Kurallar'ın saldırıların planlanması ve yürütülmesi aşamalarında alınacak aktif önlemleri düzenleyen 8. ve 9. maddeleri ile saldırıların etkilerine karşı alınacak pasif önlemleri düzenleyen 11. maddesinde yer almıştır[1349]. Bunların yanında silahlı çatışmalarda hem saldıran hem de savunan tarafın sivil halkı ve nesneleri korumak için önlem alması gerekliliği Ek Protokol-1 ile getirilmiştir[1350]. Buna göre, siber operasyon icra eden devlet tarafından, sivil can kaybına, yaralanmaya neden olmaktan ve sivil nesnelere zarar vermekten kaçınma ve zararı en aza indirmeye yönelik araç ve yöntem seçiminde elverişli tüm önlemler alınmalıdır[1351].

Siber operasyonu gerçekleştiren tarafın alması gereken bu önlemler Tallinn El Kitabı'nda madde 114-120'de yer alır. Buna göre, sivilleri korumaya yönelik olarak yöntem ve araçların seçimi ve sürekli özen yükümlülüğü gibi önlemlerin alınması beklenmektedir. Bunun yanında seçilecek hedefin sivil yaşamına veya sivil nesnelere en az zarar verecek şekilde belirlenmesi ve hedefin askeri olmadığının ya da özel korumaya tabi bir hedef olduğunun yahut yapılacak karşılaştırmada sivil kayıplarına nazaran aşırı düzeyde gerçekleşebileceğinin belirgin hale gelmesi durumunda saldırıdan vazgeçilmesi veya askıya alınması gereklidir.

[1349] Gül, 2021, s. 199.

[1350] Gül, 2021, s. 199-200.

[1351] Position Paper, 2021, s. 9-10.

Doğrudan sivilleri uyarma yükümlülüğü El Kitabı'nda Kural 120'de düzenlenmiştir. Bu kurala göre, silahlı saldırı düzeyine erişen siber saldırı durumunda sivil nüfusun uğrayacağı zararı en aza indirebilmek için şartlar aksini gerektirmedikçe sivillerin uyarılması gerekir. Çatışmanın diğer tarafını ve karşı tarafın sivilleri kalkan olarak kullanması halinde olduğu gibi durumlarda sivilleri doğrudan uyarma önlemi etkisizdir. Ayrıca savaş hilesi olarak yapılan gerçek dışı siber saldırı uyarısı, normal şartlarda yasak kapsamına girmemekle birlikte sivil nüfusun gelecekteki uyarıları dikkate almaması durumuna sebep olacak ise meşru kabul edilmeyecektir[1352].

El Kitabı'nda 121. Kural'da ise, saldırıya uğrayan tarafça alınması gerekli pasif önlemler belirtilmiştir. Gerçekleşebilecek bir siber saldırı halinde sivil nüfusun ya da sivil nesnelerin görebileceği zararı en aza indirecek önlemler bu kapsamda değerlendirilebilir. Özellikle iki taraflı hizmet veren siber altyapı tesislerine veya bu tesisler aracılığıyla gerçekleşecek bir siber saldırı halinde sivil nüfusu korumaya yönelik bir tedbir olarak bu tesislerin askeri kullanımından kaçınılması örnek olarak ifade edilebilir. Silahlı çatışmalarda savaşan tarafların belirtilen önlemleri almaması halinde bir sonraki başlıkta inceleneceği üzere Roma Statüsü hükümleri uyarınca kişilerin cezai sorumlulukları söz konusu olabilecektir.

4.4. SİBER SAVAŞTA AMİRİN SORUMLULUĞU

Amirin cezai sorumluluğu konusu ele alınırken amirin emrinin hukuka uygunluk sebebi oluşturabilecek olan amire bağlı kişiler ayrı tutulmaksızın konunun aynı başlık altında incelenmesi daha uygun görülmüştür. Uluslararası olan veya olmayan bir silahlı çatışma durumunda çatışmanın tarafı olan devletlerin silahlı güçlerini oluşturan kişilerin, silahlı çatışmalar hukukuna aykırı olan veya bireylerin uluslararası cezai sorumluluğunu düzenleyen Roma Statüsü kapsamında yer alan birtakım suçlardan sorumluluğunun siber saldırılar yönünden de tespiti gerekmektedir.

[1352] Schmitt, 2017, *Tallinn Manual 2.0*. s. 487.

Silahlı çatışmalarda Cenevre Konvansiyonları'na aykırı şekilde gerçekleşen ya da sonradan uluslararası antlaşmalarla cezai sorumluluk getirilen soykırım gibi suçlardan bu eylemlerin siber faaliyetlerle gerçekleştirilmesinde sorumluluğu bulunan asker ya da sivil veya amir ya da emir altındaki kişilerin cezalandırılması internetin gelişimiyle gündeme gelmiştir. Cenevre Konvansiyonları'nın devletlere yüklediği bu görevlerin gerektiği gibi yerine getirilmemesi ve sorumluların etkin şekilde cezalandırılmaması durumunda Roma Statüsü'nün kapsamına giren suçlar yönünden 18 yaş üstü faillerin Uluslararası Ceza Mahkemesi'nin önüne çıkarılması söz konusu olabilecektir.

Tallinn El Kitabı Kural 85'e göre, I. Cenevre Konvansiyonu'nun 49. ve II. Konvansiyon'un 50., III. Konvansiyon'un 129., IV. Konvansiyon'un 146., Ek Protokol'ün 86-87., Kültürel Varlıklar Konvansiyonu'nun 28., 2. Kültürel Varlıklar Protokolü'nün 15/2. ve Roma Statüsü'nün 25/3-b, 28. maddeleri ile içtihat hukuku gereğince uluslararası olan veya olmayan silahlı çatışmalarda savaş suçuna eşit bir siber operasyon emrini veren, sivil üstler de dahil amirin, eylemi kendisinin gerçekleştirmediği bahanesine sığınarak sorumluluktan kaçamayacağı kabul edilmektedir [1353] . Burada bahsedilen savaş suçları ise genel anlamdadır. Bir diğer ifade ile bu kavram insanlığa karşı suçlar, dar anlamda savaş suçları, saldırı suçu ve soykırım suçunu da kapsamaktadır. El Kitabı'nda her suç türü için ayrı bir değerlendirme yapılmamış savaş suçları yönünden genel bir değerlendirmede bulunulmuştur.

Cenevre Konvansiyonları'nın belirtilen hükümleri uyarınca çatışmanın tarafı olan devletin savaş suçlarından sorumlu olan kişilere etkin bir cezai yaptırım uygulanabilmesine yönelik gerekli iç hukuk düzenlemelerini yasalaştırma ve savaş suçu iddialarının soruşturulmasını ve sorumluların yargı önüne götürülmesini sağlama ya da bunun için diğer bir tarafa teslim etme yükümlülükleri bulunmaktadır[1354]. Çatışmanın tarafı olan ilgili devletin bu yükümlülüklerini hiç ya da gerektiği gibi yerine getirmemesi

[1353] Schmitt, 2017, *Tallinn Manual 2.0*. s. 397.

[1354] Schmitt, 2017, *Tallinn Manual 2.0*. s. 397.

halinde bahse konu uluslararası suçların yargılanması için daimi şekilde kurulan Uluslararası Ceza Mahkemesi'nin tamamlayıcı yargı yetkisi gündeme gelmektedir[1355].

Kural 85/2'ye göre amir, ayrıca savaş suçuna eşit bir siber saldırının önlenmesi için gerekli önlemleri almak ve gerçekleştiğini öğrenmesi halinde uygun şartlar altında soruşturulması için gerekli adımların atılmasını sağlamak ve gerekli soruşturma ve adli mercilere bildirmekle yükümlüdür. Roma Statüsü'nün 28. maddesine karşılık gelen bu kural gereğince amirin etkin yetki ve kontrolü altında olan kişilerin eylemlerini bilmesi veya bilmesinin gerekmesi halinde ya da hemen yukarıda belirtilen gerekli önleyici tedbir ya da sonrasında soruşturulmasına yönelik adımların atılmaması halinde cezai sorumluluktan bahsedilebilecektir[1356].

Siber suçlar yönünden bakıldığında savaş suçlarına eşit düzeyde sonuçlar doğuran siber saldırı emrini vermek veya emrindeki personel üzerinde yeterli kontrol sağlayamama eylemleri, amir açısından suçun maddi unsurunu (*actus reus*) oluşturmaktadır. Amirin emrinin yazılı veya sözlü olması sonuca etkili olmayıp emrindekilerin eylemi gerçekleştirmesi veya teşebbüs aşamasında kalması halinde ortaya çıkan neticeden veya buna teşebbüsten dolayı amirin doğrudan sorumluluğu söz konusudur.

Amirin savaş suçlarından sorumluluğunun söz konusu olabilmesi için suçun maddi unsuru yanında manevi unsurunun (*mens rea*) da bulunması gerekir. Bunun anlamı savaş suçlarına eşit düzeyde sonuçlar doğuran bir siber saldırının emrini veren amirin suç işleme kastını taşıması gerektiğidir. Amirin suç kastı doğrudan olabileceği gibi dolaylı ya da sonradan gerçekleşen nihai bir kast şeklinde de gerçekleşebilir. Örneğin, amirin emri üzerine gerçekleşen bir siber saldırının hedeflenen sonucu aşıp askeri gereklilik bulunmadığı halde sivil halka da zarar verecek boyuta ulaşmasına rağmen bu sonucu

[1355] Esas sorumluluk ve yetki devletlere aittir. Ulusal mahkemeler tarafından görülmekte olan bir davayı uluslararası mahkeme ele alamaz. Ayrıca ulusal mahkeme tarafından yapılan yargılamanın bağımsız ve tarafsız şekilde yapılmaması ve kişiyi UCM'nin yetkisinden kaçırmak amacıyla yapılması halinde *non bis in idem* kuralı uygulanmayacaktır. Bkz.: Sur, 2022, s. 324.

[1356] Schmitt, 2017, *Tallinn Manual 2.0*. s. 399.

önlemeyen amirin sonradan ortaya çıkan kastı, cezai sorumluluğuna sebep olacaktır. Benzer şekilde teknik sonuçlarından emin olunamayan ancak korunması gereken kişiler ya da nesnelere sirayet etmek olasılığı bulunduğu halde bu riski alarak emri veren amirin olası kast nedeniyle sorumluluğu söz konusu olabilecektir.

Roma Statüsünde düzenlenen ve amirin sorumlu olabileceği suçlardan biri olan soykırım suçunun ancak özel kastla (*dolus specialis*) işlenebileceği [1357] gözetildiğinde amirin ulusal, etnik, ırki ve dini bir grubu kısmen veya tamamen ortadan kaldırmak niyetiyle hareket ettiğinin ispatlanması gereklidir. Diğer suçlar yönünden amirin sorumluluğu için genel kastın yeterli olması nedeniyle suçun manevi unsuru için bilmek ve istemek yeterlidir. Örneğin, amirin savaş suçlarına eşit olacak bir siber saldırı emrini bilerek ve isteyerek vermesi halinde sorumluluğu söz konusudur.

Amirin sorumluluğunda özel bir durum olan altındaki personelin savaş suçlarına eşit bir siber saldırı eyleminin gerçekleştiğini bilmesi ya da bilmesinin gerekmesi halinde bilmenin ötesinde etkin kontrolü sağlamada ihmal halinde de sorumluluktan bahsedilebilecektir. Bu durumda amirin teknik bir konu olan siber saldırı emrini vermesi durumunda bu saldırının olası sonuçlarını ve etkilerini uygun vasıtalarla tespit ettirmesi ve kontrol etmesi gerekirken; amir, sonuçların öngörülemediği bahanesine sığınamayacaktır.

Eylemi gerçekleştiren personel yönünden amirin emrinin hukuka uygunluk sebebi oluşturup oluşturmadığı konusuna bakıldığında, bireyin uluslararası cezai sorumluluğuna ilişkin Roma Statüsü'nün 33. maddesinde düzenlenen amirin emri konusunda 2. fıkrada soykırım ve insanlığa karşı suçlar yönünden açık bir düzenleme öngörülerek 1. maddede belirtilen hukuka uygunluk durumunun uygulanma imkânının ortadan kaldırıldığı görülmektedir[1358]. Madde metninde bu suç dışında mahkemenin yetkisine giren diğer suçlar açısından ise amirin emrine uymanın yasal bir zorunluluk olması ve eylemi

[1357] Özarslan, 2014, s. 200.

[1358] Sur, 2022, s. 324.

gerçekleştirenin emrin kanunsuz olduğunu bilmemesi veya emrin açıkça kanunsuz olmaması halinde hukuka uygunluk sebebinin mevcut olduğu anlaşılmaktadır.

Bunla birlikte, saldırı suçu bir ülkenin askeri ve siyasi eylemlerini aktif şekilde kontrol ve yönlendirebilme pozisyonundaki kişiler tarafından da işlenebilmektedir. Bu suç açısından amir konumunda olan kişiler için amirin emrinin bir hukuka uygunluk sebebi veya mazeret olarak kabul edilemeyeceği[1359] kabul edilmektedir. Bu nedenle amirin emrinin yalnızca dar anlamda savaş suçları açısından hukuka uygun sebebi olarak kabul edilebileceği sonucuna varılmaktadır.

Bir siber saldırının silahlı saldırı düzeyine erişmesi ya da silahlı çatışma dâhilinde gerçekleştirilmesi ve soykırım veya insanlığa karşı suç oluşturması halinde amirin emrinin hukuka uygunluk sebebi olarak uygulanamayacağı açıktır. Benzer şekilde ülkenin askeri ve siyasi eylemlerini aktif şekilde kontrol ve yönlendirme durumundaki kişiler yönünden gerçekleşebilecek saldırı suçu açısından da amirin emri bir hukuka uygunluk sebebi oluşturamayacaktır.

Tallinn El Kitabı'nda 84. Kural başlığı altında bireyin savaş suçlarından cezai sorumluluğu konusu düzenlenmiştir. Roma Statüsü'nde genel manada savaş suçları, dört başlık altında düzenlenmiş olup Tallinn El Kitabı'nda ayrım yapılmaksızın genel anlamda savaş suçlarına eşit olan siber operasyonlara ilişkin değerlendirme yapılmıştır.

Roma Statüsü 25/3-f gereğince savaş suçu sayılabilecek siber saldırı eyleminin gerçekleştirilmesine rağmen failin elinde olmayan nedenlerden dolayı neticenin ortaya çıkmaması halinde teşebbüs hükümlerinden dolayı sorumluluktan bahsetmek olanaklıdır. Örneğin, baraj kapaklarının açılması sonucu sivil halkın zarar görmesine sebep olacak kapasiteye sahip bir siber silahın kullanılmasına karşın, karşı önlemler sayesinde zararın

[1359] Güneysu, Gökhan. (2015). *Uluslararası Hukukta Amirin Emri.* İstanbul: On İki Levha Yayıncılık, s. 160.

önlenmesi halinde faillerin, teşebbüs aşamasında kalan bu siber saldırıdan sorumlulukları söz konusu olabilecektir.

Eylemin gerçekleştirilmesi sırasında tamamlanmasını önleyen failin ise teşebbüsten cezalandırılamayacağı öngörülmüştür. Madde metnine bakıldığında suçun eksik teşebbüs aşamasında kalması ve neticenin gerçekleşmemesi gereklidir. Aksi takdirde eylemin gerçekleştirilmesi sonucunda zarar doğduktan sonra vazgeçen failin eylemi tam teşebbüs niteliğinde ve faal nedamet olarak vasıflandırılacağından cezasızlık söz konusu olmayacaktır. Siber saldırı yönünden örneklendirmek gerekirse, bir ülkenin sivil havacılık sistemini bozacak ve sivillerin hayatını kaybetmesine sebep olabilecek bir siber silahın SCADA sistemine yüklenmesi sonrasında vazgeçen bir failin, ilgili devleti zarar doğmadan önce uyarmasından dolayı neticenin önlenmesi halinde vazgeçen açısından bir cezasızlık söz konusu iken, diğer faillerin teşebbüsten cezalandırılması olasıdır.

Aynı şekilde siber silah kullanılarak savaş suçu işlenmesi eylemine mevcut iştirak hükümlerinin de uygulanması mümkün olup, daha önce oluşturulan *ad hoc* ceza mahkemeleri ve UCM'nin iştirak ile ilgili sorumluluk konusunda kendi standartları bulunmaktadır[1360]. Roma Statüsünün 25/3-b bendinde teşvik ve ikna etme, (c) bendinde yardım ve araç temini, (d) bendinde ortak hareket eden bir gruba bilerek katkı sağlama ve (e) bendinde soykırım suçu açısından doğrudan ya da dolaylı kışkırtma eylemleri suça iştirak kapsamında kabul edilmiştir.

Buna göre, eylemi doğrudan gerçekleştirenler yanında siber silahın kullanılmasına teknik destek verilmesi ve bilerek katkı sağlanması halinde siber silahı geliştirenlerin de

[1360] Hathaway, Oona A. / Francis, Alexandra / Haviland, Aaron / Kethireddy, Srinath Reddy / Yamamoto, Alyssa T.. (2019). *Aiding and Abeting in International Criminal Law*. Cornell Law Review, Cilt:104, s. 114. Erişim: 20.12.2020

https://poseidon01.ssrn.com/delivery.php?ID=653004094099107076079024000006072095049017031083090035064100084096008125125091027121022102098031119063013103096080008000097072000020066087035098003101022064025073047043021000082028081019113118092114112081123091120981230860250190800220891101161190 65&EXT=pdf&INDEX=TRUE

sorumluluğundan bahsetmek mümkündür. Buna karşın, siber silahın geliştirilmesi tek başına sorumluluk doğurmak için yeterli bir unsur değildir. Zira silahın geliştirilmesi yardım olarak değerlendirilse de bunun yanında manevi unsurun (*mens rea*) da bulunması gereklidir. Siber silahın meşru sınırlar dâhilinde kuvvet kullanımına elverişli olmadığını bilerek üretmek durumunda sorumluluktan bahsedilebilir. Örneğin, bir hastanede yoğun bakım ünitesini etkisiz kılmaya yönelik geliştiren bir siber silahın üretimi, kullanılması ve teknik veya istihbari destek verilmesi dar anlamda savaş suçu oluşturacaktır.

Uluslararası ceza mahkemeleri statülerinde ise, iştirak halinde suçun manevi unsuruyla ilgili olarak üç farklı standart kabul edilmiştir[1361]. Bunlar; bilme, amaç ve niyet olarak ifade edilebilir. "Bilme" standardı, suçun maddi unsurunu oluşturan yardım, suçun işlenmesini kolaylaştırma veya teşvik etme eylemini bilerek gerçekleştirme olarak açıklanabilir. "Bilme" hali gerçek bilme veya farz edilen bilme şekilde olabilir[1362]. "Bilme" standardına göre asıl failin niyetini bilmek gerekli görülmediğinden daha geniş bir alanı kapsamaktadır. Roma Statüsü'nde kabul edilen standart ise "amaç" olup, "bilme" den daha yüksek eşik öngörmektedir. Bu halde suçun işlenişine yardım, işlenişini kolaylaştırma veya teşvik etmek amacıyla hareket edilmesi gerekli görülmektedir.

4.5. SİBER SAVAŞTA TARAFSIZLIK

Tarafsızlık hukuku, devletlerin savaşçıları aracılığıyla çatışmalara katılmadan ilişkilerini sürdürerek, savaş ve barışın birlikte var olmasını düzenlemektedir[1363]. Bir savaş sırasında belirli bir devletin tarafsızlığı, bu devlet ile savaşan devletler ya da öteki tarafsız devletlerarasında olağan olarak barış zamanı uluslararası hukuk kurallarının uygulanacak olmasını ifade etmektedir[1364]. Sürekli tarafsızlık, savaşa girme hakkından vazgeçme

[1361] Hathaway ve Francis ve diğerleri s. 120.

[1362] Hathaway ve Francis ve diğerleri s. 121.

[1363] Şeyda, 2013, s. 1212.

[1364] Pazarcı, 2021, s. 592.

anlamını taşımakta, egemenlik yetkilerinin birini kaybeden devlet sadece maşru madafaa hakkını muhafaza etmektedir[1365].

Tarafsızlığı düzenleyen kuralların temel kaynağını oluşturan 1907 tarihli Lahey Konvansiyonları, çatışan tarafların ve tarafsız devletlerin hak ve yükümlülüklerini belirlemektedir[1366]. Tarafsızlık hukuku, Lahey Konvansiyonları ile yapılageliş hukukuna dayanır ve tarafsız devlet, çatışmanın tarafı olmayan devleti ifade eder[1367]. Önceleri tarafsızlık hukukunun aslında sadece uluslararası silahlı çatışmalarda uygulandığı kabul edilmekte ise de[1368], sonraları tartışmaya açık bir şekilde, temel ilkenin faydacı mantığı gereği tarafsızlık hukuku, uluslararası olmayan çatışmalarda da uygulama yeri bulmuştur[1369].

UAD tarafından *Nükleer Silahların Kullanımı ve Tehdidi Danışma Görüşü*'nde kabul edildiği üzere tarafsızlık uluslararası hukukun temel ilkelerinden biri olup bu ilke her ne tip silah kullanılırsa kullanılsın uygulanacaktır[1370]. Bu ilke uyarınca tarafsızlığını ilan eden bir devlet, çatışmanın tarafı olan devletler tarafından saldırıya uğrama ya da tarafsız bölgenin ihlal edilmesine karşı koruma altındadır[1371]. Kural bu olmakla birlikte, internetin yapısı gereği çatışmanın tarafı olan devletlerin birbirlerine karşı gerçekleştirdiği siber saldırıların tarafsız devletlerin ülkelerinde bulunan internet altyapılarını kullanarak gerçekleştirilmesi halinde siber saldırıya uğrayan devletin saldırıyı bertaraf etmesi için tarafsız devletin ülkesindeki siber altyapılara müdahalede bulunması söz konusu olabilecektir. Siber saldırıyı gerçekleştiren aktörlerin dijital izlerini gizlemek amacıyla da

---

[1365] Sur, 2022, s. 296.

[1366] Kelsey, (2008). s. 1442.

[1367] Schmitt, 2017, *Tallinn Manual 2.0*. s. 553.

[1368] Tallinn El Kitabı'ndaki bu yönde kabul için bkz.; Schmitt, 2017, *Tallinn Manual 2.0*. s. 553.

[1369] Melzer, 2011, s. 21.

[1370] Melzer, 2011, s. 20.; Karar için bkz.; UAD, "*Legality of the Threat or Use of Nuclear Weapons*", 08 Temmuz 1996, paragraf 89, Erişim: 13.11.2022 https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf

[1371] Schreier, 2015, s. 75.

tarafsız devlete ait siber unsurları kullanması mümkündür. Böyle bir durumda tarafsızlık hukukunun ihlalinin söz konusu olup olmayacağının tespiti gerekecektir.

1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu'nun[1372] 5. maddesine göre, tarafsız devletin kendi ülke sınırlarına yönelik ihlalleri mutlak suretle önleme yükümlülüğü bulunmaktadır[1373]. 1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu 5. maddesine göre uluslararası silahlı çatışma durumunda tarafsız devletlerin ülkelerinin muharip taraf devletlerce kullanılmasını önlemekle yükümlü olmasının siber uzayı da kapsayacak şekilde yorumlanacağı savunulmaktadır[1374]. Buna karşın, siber uzayda bilgi akışı karasal ülkeden farklılık arz etmekte olup aynı anda dünyanın her köşesini dolanarak hedefine giden bir veri akışının tarafsız ülkelerce kontrol edilmesinin zorluğu bir yana, hukuken böyle bir yükümlülüğün de bulunduğu iddiası tartışmaya açıktır. Tarafsız devletin böylesi bir yükümlülüğün altına sokulması uygulamada pek mümkün görülmese de mağdur devletin tarafsız devlete ait siber altyapılara müdahale etmesine olanak tanımak bazı durumlarda gerekli görünmektedir. Zira ağ tarafsızlığı ilkesi gereği tarafsız bir devletin çatışmanın tarafı olan devletlere karşı bazı yükümlülükleri bulunmaktadır. Bu kapsamda saldırıyı tespit ve önlemeye yönelik araçları kullanıma sunması gereklidir[1375].

Bu noktada ağ tarafsızlığından bahsetmek gerekir. Ağ tarafsızlığı olarak anılan ve ağdaki her veri paketinin kaynağına, hedefine, içeriğine ve niyete bakılmaksızın eşit öncelikle iletilmesini gerektiren ilke, internetin devletlerin çıkarlarına bakılmaksızın yönetilmesi

---

[1372] 1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu. Erişim: 13.11.2022 https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/200-220002?OpenDocument

[1373] Kelsey, (2008). s. 1444.

[1374] Melzer, 2011, s. 20.

[1375] Deeks, Ashley. (2013). *The Geography of Cyber Conflict: Through a Glass Darky*, Int'l L. Stud., Cilt:89, s. 3.

anlamına gelmektedir[1376]. Buna göre devletlerden egemenlik alanında bulunan ağların yönetimini tarafsız şekilde gerçekleştirilmesi beklenir. Bir çatışmaya taraf olmayan devletin egemenliği alanında bulunan siber altyapıların kullanılmasında da bu husus geçerlidir. Buna karşın kötü niyetli aktörler farklı saldırı yöntemlerini kullanarak hâkimiyet kurmak amacıyla ağ tarafsızlığını kötüye kullanabilirler[1377]. Bu durumda tarafsız devletin ağ yönetimini ne şekilde gerçekleştireceği de tartışmaya açıktır.

Bu konuda tarafsız devletin ülke sınırlarını içeren siber faaliyetlerin denetiminde ya da siber savaşın yönetiminde kullanılabilecek bir test olarak "*means at a neutral's disposal*" testi önerilmektedir. Deniz savaşlarında uygulanan bu test "tarafsız devletin kullanımındaki araçlar" testi olarak ifade edilebilir ki bu testin, internetin yapısı gereği tarafsız devletin müdahaleyi tespit ve önleme şansının çok düşük olması nedeniyle uygulanamayacağı savunulmaktadır[1378]. Bunun yanında, bir araç takibinde suçluların kırmızı ışıkta durmaması ve trafiği kilitlemesine karşın polislerin hız limitlerine ve trafik kurallarına uymasının beklenmesi [1379] örneğinin ağ tarafsızlığında uygulanamayacağından bahisle ağ tarafsızlığı ilkesine karşıt bir görüş oluşmuştur. Ağ tarafsızlığının sağlanması kullanıcılar yönünden bir özgürlük alanı sağlarken, devletlerin temel çıkarları ya da vatandaşlarının güvenliği dikkate alınırsa kötücül olarak değerlendirilen veri akışının kısılması ya da veri içeriğine müdahalede dengenin sağlanması internetin yönetimi açısından bir zorunluluktur.

Tallinn El Kitabı'na bakıldığında Uzmanlar Grubu'nun oybirliğiyle tarafsızlık hukukunun siber operasyonlara uygulanabileceğini kabul ettikleri görülmektedir[1380]. Bununla birlikte tarafsızlık hukukunun siber savaşın taraflarınca gözetilmesinin gerekliliği yanında tarafsızlık hukukunun genel olarak siber operasyonlarda ne düzeyde

[1376] Hartmann, Kim / Giles, Keir. (2018). *Net Neutrality in the Context of Cyber Warfare*, 10th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, s. 150.

[1377] Hartmann ve Giles, 2018, s. 150.

[1378] Kelsey, (2008). s. 1445.

[1379] Hartmann ve Giles, 2018, s. 142.

[1380] Schmitt, 2017, *Tallinn Manual 2.0*. s. 553.

uygulanabileceği konusu açıklığa kavuşturulmalıdır. Tarafsız bir devlet ülkesinde bulunan internet altyapısının çatışan taraflarca kullanılması konusunda Konvansiyon'un tarafsız devlet ülkesine ve telekomünikasyon sistemlerine ilişkin mevcut hükümleri dikkate alınmalıdır.

1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu'nun 1. maddesine göre tarafsız devletin hava ve kara bölgesini kapsayan ülke alanları ihlal edilemez, aksi halde tarafsız devletin bunu önlemesi gereklidir. Deniz alanına ilişkin olarak ise geçiş serbestisi söz konusudur[1381]. Anılan Konvansiyon tarafsız devlete telefon ve telgraf sistemlerini tüm çatışan taraflara ayrımcılık yapmadan kullandırma yükümlülüğü getirilmiştir. Çatışan tarafların eşit şekilde yararlanabilecekleri haberleşme olanağı askeri istihbarat ile ilgili olmamak koşuluna bağlı tutulmuştur [1382] . ABD'ye göre bu hüküm uydu sistemlerini de kapsamaktadır [1383] . Nisan 2014 tarihinde AB Parlamentosu tarafından onaylanan telekomünikasyon tekel pazarını düzenleyen düzenlemede ağ tarafsızlığı ilkesi bulunmakta iken bir yıl sonra yapılan değişiklik ile bu terim çıkarılarak internette bütün paketlere eşit davranma yükümlülüğü benimsenmiştir. Düzenlemenin devlet yargı erkleri tarafından farklı şekilde yorumlanması sonucunda bazı AB ülkelerince ileri işlemleme, kovuşturma ve izleme ile sonuçlanabilen DPI (*deep packet inspection*) uygulamaları mümkün bulunmaktadır[1384].

Bu bağlamda, tarafsızlığını sürdürebilmesi için iç sular da dâhil olmak üzere; kara ülkesi ile karasuları ve bazı hallerde bitişik bölgelerde geçiş serbestisi bulunmak kaydıyla, bunların üzerindeki hava sahasını muharip taraflara kullandırmama yükümlülüğü bulunan tarafsız bir devletin siber altyapı unsurları yönünden de benzer şekilde yükümlü olduğu söylenemeyecektir. Zira telekomünikasyon sistemlerini çatışmanın taraflarına

[1381] Kelsey, (2008). s. 1442.

[1382] Pazarcı, 2021, s. 594.

[1383] Kelsey, (2008). s. 1442.

[1384] Hartmann ve Giles, 2018, s. 145-146.

ayrımcılık yapmadan kullandırmakla ya da kullandırmamakla yükümlü olan tarafsız devletin siber sistemleri yönünden bunun aksini kabul etmek doğru görülemez.

Tallinn El Kitabı'nda da Uzmanlar Grubu'nun siber altyapı unsurları açısından tarafsızlık hukukuna yönelik bakış açısı karasal sınırlardaki tarafsızlık yaklaşımından farklıdır. Buna göre, tarafsız bir devletin siber altyapı tesisleri de dâhil tüm dünyayı dolaşan bu geçiş üzerinde tarafsız devletin denetleme yükümlülüğü söz konusu değildir[1385]. Uzmanlar Grubu'nun çoğunluk görüşüne göre yapılageliş hukuku kuralını yansıtan 1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu'nun 8. maddesi düzenlemesi siber iletişim sistemlerine de uygulanabilir[1386]. Uzmanlar Grubu'nun hemfikir olduğu görüşe göre, tarafsız devletin siber altyapı tesislerini muharip devletlere kısmen veya tamamen kapatabilmesi, ayrımcılık yapmamak kaydıyla, olanaklıdır[1387].

Siber saldırıya maruz kalan bir devletin, atfedilebilirlik unsuru açısından saldırganın kimliğini tespite yönelik girişimi sonucunda saldırının tarafsız bir devletin topraklarında ya da uluslararası alanda bulunan bir siber tesisin kullanılarak gerçekleştirildiğini belirlemesi olasıdır. Bu durumda mağdur devletin bu tesislere yönelik meşru müdafaa hakkına başvurup başvuramayacağı sorunu gündeme gelmektedir. Böyle bir durumda, siber saldırıya uğrayan bir devletin meşru müdafaa hakkına başvurması ve tarafsız bir devletin egemenliğini ihlal etmesi üzerine tarafsız devletin de meşru müdafaa hakkı kapsamında karşılık vermesi halinde çatışmanın daha da büyümesi muhtemeldir[1388]. Zira tarafsızlık hukuku genel kuralları gereğince öncelikle tarafsız devleti bilgilendirerek devletin rızası alınarak gerekli müdahalede bulunması konvansiyonel saldırılar yönünden geçerli kabul edilebilir ise de siber saldırıların çok kısa zaman dilimlerinde gerçekleşmekte olması nedeniyle bu olanaktan bahsetmek her zaman mümkün

[1385] Schmitt, 2017, *Tallinn Manual 2.0*. s. 554.

[1386] Schmitt, 2017, *Tallinn Manual 2.0*. s. 557.

[1387] Schmitt, 2017, *Tallinn Manual 2.0*. s. 557.

[1388] Kelsey, (2008). s. 1445.

olmayabilecektir. Ayrıca ülkesi kullanılan devletin saldırıda bulunana göz yumması ya da bilgi sızdıracağına dair kanaatin bulunması halinde ülke devletine bilgi verme yükümlülüğünün bulunmaması gerektiği ileri sürülmektedir[1389].

Devleti bilgilendirme ve rızasının alınması olanağının bulunmadığı durumlarda ise, saldırıya uğrayan devletin müdahalede bulunabilmesi bazı koşullar altında mümkün kabul edilmektedir. Bir devletin ülkesinden kaynaklanan ve devlete atfedilebilir olmamakla birlikte, devlet dışı bir aktör tarafından gerçekleştirilen bir saldırıya ilişkin uluslararası hukukun uygulanmasında "*unwilling or unable*" testi gündeme gelmektedir[1390]. Bu teste göre, çatışmanın tarafı olmayan bir devlet ülkesinden kaynaklı bir saldırı söz konusu olduğunda, ülkesi kullanılan devletin bunu önlemeye isteksiz davranması ya da önleme olanağının bulunmaması halinde saldırıya uğrayan devletin müdahalesi uluslararası hukukun ihlali olarak değerlendirilmemektedir.

Belirtilen bu testin, siber saldırılar söz konusu olduğunda ne şekilde uygulanacağı ise ayrıca ele alınması gereken bir husustur. Zira küresel bir ağ niteliğindeki bir ortamda aynı anda taraflı tarafsız birçok devlete ait sunucu kullanılarak gerçekleştirilen bir siber saldırıya karşı koymak için bu testin sınırsızca kullanılması bazı sakıncalar doğurmaktadır. 11 Eylül saldırıları sonrasında ABD'nin sonradan ortaya çıkacak devletlerin rızasına dayanarak ya da bahse konu teste göre terörle mücadele edileceği yönündeki beyanında belirtilen "terörle küresel savaş" konsepti[1391] gibi bir yaklaşımın siber uzayda kabul edilmesi tarafsızlık hukukunun ihlaline sebep olacaktır.

Tarihsel süreç içerisinde uygulamada ortaya çıkan ve bu testin uygulanmasına yardımcı olabilecek beş unsur bulunduğu kabul edilmektedir[1392]. Bunlar; tek taraflı kuvvet kullanımı yerine işbirliğini önceleme ya da ülke devletinin rızasını alma, ülke devletine

[1389] Deeks, 2013, s. 12.

[1390] Deeks, 2013, s. 1.

[1391] Deeks, 2013, s. 4.

[1392] Deeks, 2013, s. 9-10.

tehdidi ele alması ve gereken cevabı vermesi için yeterli süreyi verme, ülke devletinin ilgili bölgedeki kontrol ve kapasitesini makul şekilde değerlendirme, ülke devletinin tehdidi bertaraf etmek için önerdiği araçları makul biçimde değerlendirme ve son olarak ülke devleti ile önceki etkileşimleri değerlendirmedir.

Tallinn El Kitabı'nda tarafsız devlet ülkesinde bulunan siber unsurların muharip taraflarca kullanılması halinde, mağdur devletin *self-help* doktrini kapsamında gerekli önleme amaçlı müdahalesini iki unsurun gerçekleşmesi halinde gerçekleştirebileceği kabul edilmektedir[1393]. Bunlardan ilki tarafsız devlet ülkesine yönelik ihlalin ciddi, bir diğer ifadeyle ağır bir ihlal olması gereğidir. Bu ise soyut şekilde değerlendirilmeyip olayın hal ve şartlarına göre ihlal eden muharip tarafın diğer tarafa karşı önemli bir askeri avantaj sağlamakta olması anlamına gelir. İkinci unsur ise ihlalin çatışmanın tarafı olan mağdur devlete yakın bir tehdit oluşturması yanında, tarafsız devletin ihlali önlemeye yönelik elverişli ve zamanlı alternatif bir imkânının bulunmamasıdır. Böylesi bir durumda temel çıkarları yakın bir tehlikeye maruz kalan tarafsız devletin gerçekleştireceği fiilin hukuka uygunluk sebeplerinden zaruret haline dayandırılması da mümkündür.

Ağır bir siber saldırı altında bulunan devletin yukarıda açıklanan *self-help* doktrini kapsamında müdahalede bulunabilmesi için öncelikle tarafsız devletin bilgilendirilmesi ve ihlali önleme imkânının tanınması da beklenir. Buna karşın, yukarıda da değinildiği üzere siber uzayın kendine özgü yapısı gereği tarafsız devletin müdahalesi ve gerekli tedbiri alması gerek teknik yetersizlikten ve gerekse de zaman sorunu nedeniyle mümkün olamamaktadır. Tarafsız devlete ait siber altyapı unsurları kullanılarak gerçekleştirilen siber saldırının mağduru olan devletin tarafsız devlete başvurmasından sonuç alınamayacağının açık olması halinde mağdur devletin doğrudan aktif savunma gerçekleştirmesi olanaklıdır[1394]. Bu nedenle saldırıya cevaben önceden programlanmış aktif savunma tedbirlerine başvurulması, önleyici meşru müdafaaya uygulanan orantılılık

[1393] Schmitt, 2017, *Tallinn Manual 2.0.* s. 560-561.

[1394] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.239.

ilkesine uygun olmak kaydıyla, tarafsız devlet haklarının ihlali olarak değerlendirilmemektedir[1395].

Tarafsız devletlerin siber altyapı unsurlarının siber araçlarla gerçekleştirilen düşmanca eylemlerden (*hostile act veya belligerent rights*) korunması konusu Tallinn El Kitabı 150. Kural'da düzenlenmiştir. Tarafsız bölgelerde çatışan taraflarca gerçekleştirilecek hasmane eylemlerin yasaklanmasının bir uzantısı olarak siber altyapı unsurları da koruma altına alınmaktadır. Tallinn El Kitabı'nda "tarafsız siber altyapı tesisleri" çatışmanın tarafı olan bir devlete ya da bu devlet vatandaşlarına ait olanlar ve tarafsız devlet vatandaşlarının çatışma bölgesi dışında sahip oldukları da dâhil tarafsız devlet bölgesinde yer alan özel veya kamusal siber altyapı tesisleri olarak kabul edilmiştir[1396]. Buna göre, tarafsız bir devletin sadece ülkesi üzerinde bulunan unsurları tarafsızlık koruması altında bulunmayıp tarafsız devlete ya da vatandaşlarına ait olup da çatışma bölgesi dışında bulunan tüm tesislerin çatışan taraflarca hedef seçilmemesi gerekmektedir. Tarafsız devlete yönelik olarak gerçekleştirilen uluslararası hukukta tek başına yasak olmayan siber casusluk faaliyetlerinin yasak kapsamında bulunmadığı kabul edilmektedir[1397].

Çatışma bölgesinde gerçekleştirilmiş olup da tarafsız bölgeye taşan ve olumsuz etkileri görünen bir durumda Uzmanlar Grubu, bu olumsuz etkilerin öngörülememesi durumunda tarafsızlık hukukuna bir aykırılık oluşmayacağı konusunda hemfikirdir. Öngörülebilir sonuçlar yönünden ise, olay bazında konuya yaklaşmak gerektiği ve çatışan taraf hakları ile tarafsız devletin yarışan haklarının dengede tutularak tarafsız bölge içinde veya denizaltı kablolarında olduğu üzere dışında olup olmamasına göre bir değerlendirme yapılmalıdır[1398].

[1395] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.239.

[1396] Schmitt, 2017, *Tallinn Manual 2.0*. s. 553.

[1397] Schmitt, 2017, *Tallinn Manual 2.0*. s. 555.

[1398] Schmitt, 2017, *Tallinn Manual 2.0*. s. 555-556.

Tallinn El Kitabı'nın yukarıda açıklanan 150. Kural'ı tarafsız devlete ait siber altyapı unsurlarını koruma amacını taşımakta iken; 151. Kural'ın muharip devletlerin tarafsız bölgedeki altyapı unsurlarını kullanmasını yasakladığı görülmektedir. Ayrıca, tarafsız bölgedeki siber altyapı unsurlarının kullanılarak siber operasyon gerçekleştirilmesi yasağı, bu unsurların uzaktan kontrolünün ele geçirilerek gerçekleştirilmesini de kapsamaktadır[1399]. Yine, tarafsız bölgede bulunan siber altyapı tesisleri, bu devlete ait olan ve egemen bağışıklığını haiz, ticari olmayan bir gemi veya hava aracını da kapsamaktadır[1400].

1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu'nun 2. maddesine göre, savaşan devletler tarafsız devlet ülkesinden savaş mühimmatı ya da malzemesi geçirememektedir[1401]. Siber silahların tarafsız bölgeden fiziken nakledilmesi konusunda Tallinn El Kitabı'nda kabul edilen görüş, konunun 1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu'nun 2. maddesinin öngördüğü genel yasak kapsamında değerlendirilmesi yönündedir[1402]. Buna karşın, siber silahların muharip devletlerce kullanımı serbest olan kamuya açık internet vasıtasıyla nakledilmesi halinde Uzmanlar Grubu fikir ayrılığına düşmektedir. El Kitabı'nın 152. maddesinde öngörülen tarafsız devletin yükümlülükleri başlığı altında, tarafsız bölgede veya tarafsız devletin münhasır kontrolü altındaki bir yerde siber silahın tarafsız devletin bilgisi dâhilinde nakledilemeyeceği kabul edilmektedir. Maddede belirtilen tarafsız devletin münhasıran kontrolü altında olan yer ibaresinden ticari olmayan veya hükümetin doğrudan kontrolü altında bulunan devlet gemileri veya araçlarında bulunanlar gibi siber altyapı tesisleri anlaşılmaktadır. Yine maddede belirtilen bilme durumunun devlet organlarının durumu tespit etmeleri halinde olduğu şekilde gerçek bilme mi yoksa farz edilen bilme mi olup olmayacağına dair de fikir ayrılıkları bulunmaktadır[1403].

[1399] Schmitt, 2017, *Tallinn Manual 2.0*. s. 556.

[1400] Schmitt, 2017, *Tallinn Manual 2.0*. s. 556.

[1401] Pazarcı, 2021, s. 594.

[1402] Schmitt, 2017, *Tallinn Manual 2.0*. s. 557.

[1403] Schmitt, 2017, *Tallinn Manual 2.0*. s. 559.

Sonuç olarak tarafsızlık hukuku, siber saldırılar yönünden gerek uluslararası ve gerekse de uluslararası olmayan silahlı çatışmalarda uygulama yeri bulmaktadır. Bununla birlikte konvansiyonel saldırılardan farklı olarak tarafsız devletin egemenlik alanında bulunan siber altyapı tesislerinin kullanımını muharip devletlere ayrımcılık yapmaksızın sağlaması halinde tarafsızlık hukukunun ihlal edilmeyeceği söylenebilir. Ağ tarafsızlığı olarak da ifade edilen tarafsız bir devletin bu müdahalesizliğinin de bazı sınırları bulunmaktadır. Zira hiçbir devlet, ülkesini diğer devletlere zarar verecek şekilde ve terörist faaliyetlerde fırlatma rampası olarak kullandırmamak yükümlülüğü altındadır. Ağ tarafsızlığı ile özen gösterme yükümlülüğü arasındaki dengenin nasıl kurulacağı ise uygulamada sorun yaratmaya elverişli bir konudur. Bu açıdan uluslararası işbirliğinin geliştirilmesi ve devletlerin siber güvenlik politikalarında ağ tarafsızlığına ve önleme yükümlülüklerine yer vermeleri uygun olacaktır. Her alanı kapsayan yeni bir siber savaş antlaşmasının imzalanması yerine tarafsızlık hukuku ya da insancıl hukukla ilgili bazı alanlarda uluslararası antlaşmaların yapılması gereklidir.

Genel olarak ifade etmek gerekir ki ağ tarafsızlığı ilkesi gereği tarafsız devletin ülkesinden geçen tüm veri akışını kontrol etmesi beklenemez ise de egemenliği altındaki siber altyapı tesislerinin savaşan devletler tarafından kullanılmasını ya da ele geçirilmesini önlemesi gereklidir. Ayrıca her devlet kendi ülkesini diğer devletleri hedef alan bir fırlatma rampası olarak kullandırmamak için gerekli özeni gösterme yükümlülüğünü taşımaktadır. Yine uluslararası terörizmle mücadele kapsamında uluslararası hukuka uygun şekilde siber gözetim ve denetim yapılması da mümkündür. Aksi takdirde temel çıkarları ağır ve yakın bir zarar tehdidi altında bulunan bir devletin, bu kez *self-help* doktrini ya da meşru müdafaa kapsamında tarafsız devletin ülkesinde bulunan siber tesislerine müdahalede bulunması ve çatışma alanlarının daha da genişlemesi söz konusu olabilecektir.

SONUÇ

İnternet teknolojisinin insan hayatına girmesi, sadece bireylerin yaşam biçimlerini değiştirmekle kalmamış; bu değişim gerek ulusal gerekse de uluslararası düzeyde oldukça önemli sonuçları olmuştur. Bu çalışma kapsamında öncelikle belirtilmesi gereken temel sonuç, siber savaş hukukunun uluslararası hukukun neredeyse bütün alt başlıklarında uygulama alanı bulmasıdır. Bunun etkilerini, Westfalya Barışı'nın getirdiği klasik devlet egemenliği anlayışından başlamak suretiyle kuvvet kullanımı, meşru müdafaa, deniz hukuku, hava hukuku, uzay hukuku, insancıl hukuk ve bunun gibi diğer tüm alanlarında görmek olanaklıdır. Bu kapsamda, uygulanmakta olan uluslararası hukukun mevcut normlarının gerek barış döneminde, gerek kuvvet kullanımına başvuru durumunda ve gerekse de silahlı çatışmalar süresince siber uzay zemininde gerçekleşen faaliyetler için yeniden yorumlanarak uygulanması söz konusudur. Geleneksel uluslararası hukuk normlarının yeni şartlara uygulanması konusunda ise, doğal olarak farklı yaklaşımlar ortaya çıkmaktadır.

Siber savaş konusunda benimsenen farklı yaklaşımların ilki terimlere ilişkindir. Siber uzaydaki devlet egemenliğinin sınırları konusundaki gelişmiş devletler ile gelişmekte olan devletlerarasındaki görüş farkı ise bir diğeridir. Buna paralel olarak internetin yönetilmesi de internette faaliyet gösteren bireylerin temel insan haklarının korunması ile devletlerin temel çıkarlarının çatıştığı bir ortamda sorunlu alanlardan biri olmuştur. Yine uluslararası hukukta benimsenmiş *jus cogens* kurallar, yapılageliş kuralları ya da uluslararası hukukun diğer prensipleri bağlamında siber faaliyetlerin ne şekilde tanım ve tasnif edileceği de görüş farklılıklarının bir diğer sebebi olmuştur. Ayrıca mevcut normların yanında yeni bir uluslararası siber savaş hukuku antlaşmasının gerekli olup olmadığı da tartışılan en önemli konular arasında gelmektedir. Bu çalışmada, tüm bu sorular dikkate alınarak uluslararası hukukta siber saldırı kavramı tüm yönleriyle incelenmeye çalışılmış, yeni bir uluslararası siber savaş hukukunun çerçevesinin çizilmesi amaçlanmıştır.

Gelinen noktada devletlerin kamu hizmetlerini ağa bağlı olarak gerçekleştirmesinin sağladığı kolaylık, devletleri ağa bağımlı hale getirmiştir. Uluslararası hukukun temel aktörü olan devletlerin ağa bağlı kamu hizmetleri yürütmesinin yaygınlaşmasıyla birlikte siber uzayın kapsama alanı daha da genişlemiştir. İnternetten daha geniş bir alanı ifade eden siber uzay, zamanla bireylerin yanında e-devletlerin de süjesi olduğu bir ortam olmuş, devletlerarası ilişkiler ve hatta çatışmaların da gerçekleştiği yeni bir alan halini almıştır. Bu durum ise öncelikle, bir devletin ülkesi üzerinde sahip olduğu egemenlik hakkını siber altyapı tesisleri ve ülke sınırlarından geçen veriler üzerinde nasıl kullanabileceği sorununu gündeme getirmiştir. Zira internetin küresel kamu mallarından olduğu görüşü uyarınca, devletlerin internet üzerindeki egemenlik hakları sınırlı kabul edilirken, aksi bakış açısı devletin ülke egemenliğinin interneti de kapsayacağı yönündedir.

Egemenlik konusunun ötesinde siber uzayın uluslararası hukuk alanında yarattığı sonuçlardan belki de en önemlisi siber faaliyetlerin kuvvet kullanma seviyesine erişmesi ve hatta silahlı saldırı düzeyine erişen kuvvet kullanımlarının olanaklı hale gelmesidir. Böylece kuvvet kullanma ve hatta silahlı saldırı düzeyine erişen siber faaliyetlerin, kuvvet kullanma yoluna başvurma hakkını düzenleyen, bir diğer ifade ile çatışma yönetimi olarak da anılan *jus ad bellum* kapsamında uygulanabilirliği gündeme gelmiştir. Uluslararası hukuk kişilerinin siber uzayda gerçekleştirdikleri faaliyetlerin hangi eşiğe varması halinde kuvvet kullanma ya da silahlı saldırı oluşturacağı, meşru müdafaa hakkına imkân tanıyacağı gibi soruların ortaya çıkması nedeniyle siber operasyon, siber saldırı ve silahlı saldırı gibi kavramların nitelendirilmesi gerekmiştir.

Bu bağlamda, siber operasyon, siber saldırı, siber savaş, siber casusluk, siber terörizm, siber sabotaj, siber suç ve hacktivizm kavramlarını içeren geniş anlamdaki siber faaliyetler kavramı bu çalışmada tanımlanmış, uluslararası hukuk yönünden önemli görülen bazı kavramların diğerlerinden farkı ortaya konulmuştur. Genel olarak siber faaliyetler olarak adlandırabileceğimiz bu kavramlardan bazılarına ilişkin olarak gerek uygulamada ve gerekse öğretide farklı nitelendirmelerin yapıldığı, terimler üzerinde fikir birliği bulunmadığı görülmüştür. Bu nedenle, siber faaliyetlerin bir kısmını oluşturan siber operasyonların hangi seviyede siber saldırıyı ve siber saldırıların hangi seviyede

silahlı saldırı oluşturacağı ve böylece meşru müdafaa hakkına başvuru olanağı sağlayacağı hususları tespit edilmiştir. Yine "siber savaş" kavramından bahsedilebilmesi için söz konusu siber saldırının kritik altyapı tesislere yönelik gerçekleştirilmesi ya da silahlı çatışmalar hukuku dâhilinde vuku bulması gerekliliği ifade edilmiştir.

En geniş ölçekte ele alınabilecek siber faaliyetlerin siber casusluk ya da kriminal faaliyetleri de içine alan bir kavram olduğu ifade edilmelidir. Siber operasyonlar ise, kanaatimizce uluslararası hukuk kişilerince, politik dürtü dâhilinde gerçekleştirilen siber faaliyetlerdir. Siber operasyonların kişilerde yaralanmaya ya da eşyalarda hasara sebep olabilecek daha ağır türlerini ise siber saldırılar oluşturmaktadır. Bu noktada bir önceki paragrafta belirtildiği üzere devletlerin hayati çıkarlarına yönelen veya silahlı çatışmalar dâhilinde gerçekleştirilen siber saldırıların söz konusu olduğu durumda ise siber savaştan bahsetmek mümkündür. Zira son zamanlarda kinetik silahlarla gerçekleştirilen geleneksel anlamda savaşların da vasıf değiştirerek hibrit savaşlara evrildiği görülmektedir. Bu nedenle meşru müdafaaya sebep olma eşiğine varan, bir diğer ifade ile silahlı saldırı düzeyine erişen siber saldırılar ile konvansiyonel savaş kapsamında gerçekleştirilen ve silahlı çatışmalar hukukuna dâhil olan siber saldırıların siber savaş olarak nitelendirilmesi daha uygun bir yaklaşım olacaktır.

Bu noktada, kuvvet kullanma yoluna başvuru yanında, uluslararası silahlı çatışmalar hukukunun siber faaliyetlere uygulanabilirliği konusu bir diğer önemli meseledir. Bu konuda konvansiyonel çatışmaların doğasına uygun olacak biçimde hazırlanmış uluslararası normların siber operasyonlara uygulanması, çözümü daha zor bir sorundur. Silahlı çatışmalar hukukuna hâkim olan ayrım gözetme ve orantılılık ilkeleri ile meşru hedefin belirlenmesi gibi kuralların siber operasyonlara uygulanmasında karşılaşılan güçlüklerin bu çalışmada çözüme kavuşması amaçlanmıştır. Zira BM ambleminin veya Kızılhaç veya Kızılay amblem sembol veya işaretlerinin kötüye kullanılması yasağının siber operasyonlarda bu kurumların alan adlarının kötüye kullanılmasını kapsayıp kapsamadığı konusunda Cenevre Konvansiyonları'nda değişiklik yapılmasının gerekip gerekmediği konusu tartışılmıştır. Bu konuda varılan sonuç itibariyle, mevcut uluslararası normların siber uzaya uygun şekilde yorumlanmasının önemi ortaya konulurken

tarafsızlık hukuku gibi bazı durumlarda yeni düzenlemelerin ya da uluslararası işbirliği içerisinde siber güvenlik politikalarının oluşturulmasının gerekliliği ifade edilmiştir.

Mevcut uluslararası hukuk normlarının siber alana uygulanması konusunda özel durum arz eden bir diğer konu, geleneksel anlamda karşı önlemlere başvurma imkânının siber alanda da aynı şekilde kısıtlanmasıdır. Bu önlemlerin sadece devlete karşı, ön bildirim yükümlülüğü yerine getirilmek suretiyle ve önlemlerin önleyici şekilde uygulanmaksızın gerçekleştirilmesi siber alana uygun düşmemektedir. Siber saldırılar yönünden aktif savunma tedbirlerine başvurulması olanağının sağlanması gerek caydırıcılık açısından ve gerekse de uluslararası barış ve güvenliğin sürdürülebilmesi için önemli bir etken oluşturabileceği değerlendirilmektedir. Bu noktada hatırlanması gereken bir konu da uluslararası hukuk sisteminde yaptırım gücünün BM organları tarafından gerektiği gibi yerine getirilememesidir. Bundan dolayı devletlerin siber güvenlik politikalarını kendi egemenlik alanını korumaya yönelik olarak oluşturması gerekmektedir. Bunun yanında, caydırıcılık konusuna ve aktif savunma tedbirlerine ağırlık verilmesi çatışmaları önlemede faydalı olacaktır.

Siber saldırılara karşı aktif savunma tedbirlerinin sınırı ve özel sektörün aktif savunma tedbirlerine başvurabilmesi yanında, zarara uğrayan üçüncü kişilere karşı devletin sorumluluğu sorunu çözüme kavuşturulması gereken bir diğer husustur. Başka bir devlet ülkesinde bulunan internet kullanıcılarının zararlı siber faaliyetlerinden zarar gören devletlerin evrensel yargı yetkisi kullanabilmesinin zorluğu ortadadır. Bu nedenle Uluslararası Denizcilik Organizasyonu benzeri bir örgütün siber saldırganlık suçlarında evrensel yargı yetkisi kullanabilmesi ve siber güvenliğin sağlanabilmesinde uluslararası işbirliğinin sağlanabilmesi için BM nezdinde kurulması ve daha da ötesinde uluslararası bir siber suçlar mahkemesinin kurulması önerisi[1404] kabule şayandır.

Bir siber faaliyeti tespit eden siber önlem birimi görevlileri tarafından eylemin ne şekilde değerlendirileceği konusu ayrıca üzerinde durulması gereken bir durumdur. Siber

[1404] Stahl, 2011, s. 270-272.

faaliyetin devlet ya da devlet dışı bir organize örgüt tarafından gerçekleştirilmesi olasılığı yanında tamamen güç denemesi peşinde genç bir bilişim korsanı tarafından da gerçekleştirilmesi mümkündür. Eylemin kaynağını ve devlet ile bağlantısını tespit etmek siber saldırı anında kolay deildir. Siber acil önlem birimi görevlilerinin böylesi bir durumda faaliyetin niteliğini tespit etmek yanında kaynağını ve devlet bağlantısını tespit etmesini beklemek her koşulda doğru olmayabilir. Bu yönüyle siber faaliyeti gerçekleştirenin niyetini hatalı değerlendirme veya siber birimlerin yanıltılarak eylemle ilgisi olmayan başka bir devlete yönelik karşı saldırı gerçekleştirmeleri riski de bulunmaktadır.

Eylemin veya saldırıyı gerçekleştirenin niyetinin düşmanca bir karaktere sahip olması konusunda ABD uygulaması ilk merminin ateşlenmesinin beklenmeyeceği yönünde olup, bu doğrultuda saldırının kritik altyapı unsurlarına yönelik olduğu konusunda yetkililerin makul inancı taşıması halinde aktif savunma tedbirlerinin uygulanacağı kabul edilmektedir [1405] . Bu konuda yapılacak bir hukuki değerlendirme sonucunda bazı olasılıklar dikkate alınabilir. Bunların ilki, aktif savunma eylemini gerçekleştiren görevlilerin sorumluluğunun sonradan yapılacak yargılamalarda değerlendirilmesine ilişkin olabilecektir. Siber saldırının gerçekleştiği anda buna muhatap olan devlet birimlerinin, kendi iç hukukları gereğince acil önlem alma gerekliliği ve saldırıyı önleme yükümlülükleri gözetildiğinde, saldırı anındaki şartlar altında değerlendirme yapılması uluslararası hukuka uygun bir yaklaşım olacaktır.

Bunun yanında, belirtilen devlet görevlilerinin olası bir siber saldırıya karşı verecekleri savunma saldırısının siber güvenlik politikası kapsamında sınırlarının belirlenmesi gerekmektedir. Her devletin siber güvenlik politikasını uluslararası standartlara uygun hale getirmesi ve siber saldırı söz konusu olduğu takdirde uluslararası hukuka uygun bir yönerge dâhilinde hareket edecek uzman uluslararası hukukçu ve siber güvenlik uzmanlarından oluşan birimlerin oluşturulması ikinci bir olasılıktır.

[1405] Jensen, 2002. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense, s.236.

Buraya kadar belirtilen tüm konular kapsamında gerek acil önlem birimlerinin ve gerekse de siber güvenlik politikası metinlerinde siber faaliyetlerin, uygulanan uluslararası hukuk normlarına göre doğru şekilde yorumlanması ön koşuldur. Hâlihazırda siber savaş hukukuna ilişkin uluslararası düzeyde hazırlanmış ve norm yaratan antlaşmaların bulunmaması ve de her alanı kapsayacak antlaşmaların gerekli olmamasından dolayı yorum faaliyeti son derece önemlidir. Bu çalışmanın en temel çıkarımlarından birini oluşturan konu da yorum şekline ilişkindir. Zira uygulanan uluslararası hukuk normlarının tamamının siber savaş hukukuna göre yeniden düzenlenmesi olanaksızdır. Bu bağlamda, teknolojik gelişim ile başlayan yeni silahların savaşlarda kullanılması sürecine benzer bir biçimde siber uzayda gerçekleşen saldırılara ilişkin olarak mevcut normların yorumlanması esastır. Geleneksel yorum metotlarının ötesinde, daha önce hiç tecrübe edilmeyen bir ortamda gerçekleşen yeni savaş yöntemlerinin bu yeni dünyanın yapısına uygun şekilde yeni bir bakış açısıyla yorumlanması gereklidir.

Bu noktada ifade edilmesi gerekir ki mevcut normların siber faaliyetlere ilişkin olarak yeniden yorumlanması faaliyeti buyruk kurallara aykırı olmamalıdır. Aksi takdirde kuvvet kullanma yasağı, soykırım, savaş suçları, insanlığa karşı işlenen suçların yasaklanması ve işkencenin yasaklanması gibi *jus cogens* niteliğindeki buyruk kurallara aykırılık oluşturacak yorumlar nedeniyle ilgili hükümlerin geçersizliği ya da buyruk kurallara aykırılık oluşturan siber faaliyetlerden dolayı devletlerin ulusararası sorumluluğu gündeme gelebilecektir. Bu nedenle mevcut normların siber bağlama uyarlanması sürecinde, buyruk kurallara aykırılık teşkil edecek uygulama ve yorumlardan kaçınılması bir zorunluluktur.

Mevcut normların lafzıyla sınırlı şekilde veya norm oluşturanların amacını araştırmaya dönük olarak yapılan yorum yöntemlerinin ya da tarihsel yorum yönteminin siber saldırılar yönünden doğru netice vermeyeceği aşikârdır. VAHS'nin 31/1. fıkrasında sıralanan "kelimenin olağan anlamı", "bağlamsal unsurlar" ve "amaç ve niyet" şeklindeki üç yorum unsurunun da hermönitik ve gösterge bilim ışığında gerçekleştirilmesi isabetli olacaktır. Bunun için de kelimenin olağan anlamının yaşanılan çağa göre tespiti yanında

bağlamsal unsurların da bu tez çalışmasında açığa çıkarılmaya çalışılan siber savaş hukuku bağlamında gerçekleştirilmesi gerekir. Amaç ve niyet unsurunun, uygulanmakta olan uluslararası hukuk normlarının bilgi çağının öncesinde hazırlandığı gözetilerek teknolojik gelişime uygun şekilde ve sanal dünyayı anlayabilecek bir paradigma ile gerçekleştirilmesi gerekliliktir.

Savaş hukuku kurallarının tam olarak düzenlenmemiş olması nedeniyle savaş kurallarının komutanın keyfine bırakılmaması adına savaşı, uluslararası hukuk prensipleriyle sınırlandırmayı amaçlayan *Martens kaydı* [1406] yönünden bakıldığında, gelişen teknolojinin sebep olduğu yeni durumlara, uluslararası hukuk prensipleri çerçevesinde silahlı çatışmalar hukukunun uygulanması mümkündür. *Martens kaydının* varlığını sürdürüp sürdürmediği sorusu bir yana bırakılırsa, savaş esnasında insanlık dışı faaliyetten kaçınmayı amaçlayan bu kaydın siber savaş ya da hibrit savaşlarda da geçerli olduğu söylenebilir.

Martens kaydı kapsamında ve bu çalışmada savunulan şekilde bir yorum yapılması halinde yasal boşluktan bahsedilmesi mümkün değilse de uygulamada yaşanacak sorunlardan dolayı bu gibi durumlar için antlaşmalarda gerekli düzenlemelerin yapılması gerekli olabilir. Bu doğrultuda uluslararası veya ulusal siber altyapı tesislerine yapılacak bir saldırının etkilerine göre insanlığa karşı suç oluşturma koşullarının çerçevesi çizilmeli ve UCM'nin alanının bu kapsamda genişletilmesi mümkün kılınmalıdır. Siber saldırıların UCM'nin yetkisi dâhilinde dördüncü uluslararası suç olarak değerlendirilip değerlendirilemeyeceği konusunda 1974 tarihli ve 3314 sayılı BM Genel Kurulu'nda tanımlanan saldırı suçu öncelikle irdelenmelidir.

Siber savaş konusunda zorunlu olarak düzenlenmesi gereken bir diğer konu internetin yönetimidir. Devletlerin bireysel çıkarlarının ötesinde, bağımsız uluslararası örgütler nezdinde internetin yönetimi sağlanırken, internetin kişi ve devletlere sağladığı özgürlük

[1406] Ayrıntılı bilgi için bkz.; Erdem, Mete. (2015). *İnsancıl Hukukta Martens Kaydı*. İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt:6, Sayı:2, s. 223.

ve tarafsızlık da korunmalıdır. Bu çalışmanın hazırlanması sırasında yaşanan Ukrayna-Rusya çatışmalarında tecrübe edildiği üzere çok sayıda siber saldırının büyük ölçüde etkisiz hale getirilmesine olanak sağlayan küresel siber güvenlik mekanizması oluşturulmalıdır.

Uygulanan uluslararası hukukun en önemli eksikliklerinden birini oluşturan ve yaygın eleştirilerin merkezinde bulunan BM'nin sorunlu yapısında yapılacak değişiklikler ve yeni yapılanmalar sürecinde; internetin yönetimi, siber saldırı ve siber güvenlik konuları uluslararası çok taraflı konvansiyonlar düzeyinde ele alınmalıdır. Bu süreçte güney-kuzey yarım küre, gelişmiş-gelişmekte olan ya da doğu-batı mücadelesi kapsamında dengelerin gözetilmesi gereklidir. Bu konularda küresel düzeyde yapılacak düzenlemeler yanında, tüm üye devletlerin siber güvenliği teminat altına almalı ve nükleer silahların siber saldırılar aracılıyla kullanılmasını önlemeye yönelik ulusal tedbirlerin alınmasına yönelik yükümlülükler getirilmeli ve mevcut örgütlerin siber uzaya yönelik olarak yapılandırılması sağlanmalıdır.

Netice olarak, uygulanan uluslararası hukuk normlarının bilgi çağına uygun olmadığı ve bu normların tamamen yeniden oluşturulmasının da mümkün olmaması nedeniyle, siber savaşa uygun düşmeyen konularda yeni antlaşmaların varlığı gerekli görülmekte iken diğer tüm alanlarda bilgi çağının gerektirdiği şekilde bir yorum yöntemi ile mevcut normların hayata geçirilmesi sağlanmalıdır. Bu amaçla tüm devletlerin siber güvenlik politikalarını evrensel standartlara uygun hale getirebilmesi için uluslararası işbirliğinin geliştirilmesine yönelik çalışmalar yapılmalıdır. Bu noktada Birleşmiş Milletlere ve diğer uluslararası örgütlere önemli görevler düşmektedir.

KAYNAKÇA

KİTAPLAR

Acer, Yücel ve Kaya, İbrahim. (2014). Uluslararası Hukuk. Ankara: Seçkin.

Akgül, Fatih, (Ed.: Yıldız, Gültekin ve Ateş, Barış). (2022). *Hibrit Tehditleri Anlamak.* Ankara: Milli Savunma Üniversitesi Yayınları.

Aksar, Yusuf. (2021). *Teoride ve Uygulamada Uluslararası Hukuk I.* Ankara: Seçkin.

Aksar, Yusuf. (2021). *Teoride ve Uygulamada Uluslararası Hukuk II.* Ankara: Seçkin.

Alder, Murray Colin. (2013). *The Inherent Right of Self-Defence in International Law.* New York / London: Springer.

Amoroso, Edward G. (2011). *Cyber Attacks Protecting National Insfrustructure.* Burlington: Elsevier.

Arend, Antony Clark ve Beck, Robert J. (1993). International Law and the use of Force. London and New York: Routledge.

Aust, Stefan ve Ammann, Thomas. (2018). *Dijital Diktatörlük Kitlesel Gözetim Verilerin Kötüye Kullanımı Siber Savaş* (Çev. Erdinç Yücel, Hasan Yılmaz). Ankara: Hece Yayınları.

Arnheim, Rudolf. (2015). *Görsel Düşünme* (Çev. Rahmi Öğdül). İstanbul: Metis Yayıncılık.

Bernstein, Richard J. (2009). *Objektivizmin ve Rölativizmin Ötesi Bilimi Hermenoytik ve Praxis* (Çev. Feridun Yılmaz). İstanbul: Paradigma.

Betz, David J. ve Stevens, Tim. (2011). *Cyberspace and the State.* London New York: Routledge.

Bozkurt, Enver. (2003). *İnsan Haklarının Korunmasında Uluslararası Hukukun Rolü*. Ankara: Nobel Basımevi.

Bozkurt, Enver ve Erdal, Selcen ve Poyraz, Yasin. (2017). *Devletler Hukuku.* Ankara: Yetkin.

Can, Cahit. (1996). *Hukuk Sosyolojisinin Gelişim Yönü.* Ankara: AÜHF Yayınları.

Çifci, Hasan. (2013). *Her Yönüyle Siber Savaş*. Ankara: Tübitak.

Clarke, Richard A. ve Knake, Robert K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threath*. New York: Penguin Press.

Convertino, Sebastian M. ve DeMattei, Lou Anne ve Knierim, Tammy M. (2007). *Flying and Fighting in Cyberspace.* Alabama: Air University Press.

Devetak, Richard ve Burke, Anthony ve George, Jim. (2012). *An Introduction to International Relations.* Cambridge: Cambridge University Press.

Doğan, İlyas. (2016). *Devletler Hukuku*. Ankara: Astana Yayınları.

Dülger, Murat Volkan. (2004). *Bilişim Suçları.* Ankara: Seçkin Yayıncılık.

Eco, Umberto. (2013). *Yorum ve Aşırı Yorum* (Çev. Kemal Atakay). İstanbul: Can.

Even, Shmuel ve Siman-Tov, David. (2012). *Cyber Warfare: Concepts and Strategic Trends*. Tel Aviv: Institute for National Security Studies.

Gray, Christine. (2008). *International Law and the Use of Force.* Oxford New York: Oxford University Press.

Grotius, Hugo. (2001). *On the Law of War and Peace* (Çev. A.C. Campbell). Kitchener: Batoche Books.

Gül, Yunus Emre. (2021). *Savaş Hukuku 2.0 Siber Saldırılar ve Hukuk*. İstanbul: Hukuk Akademisi.

Gündüz, Aslan. (2003). *Milletlerarası Hukuk.* İstanbul: Beta.

Güneysu, Gökhan. (2015). *Uluslararası Hukukta Amirin Emri.* İstanbul: On İki Levha Yayıncılık.

Hoş, H. Serdar. (2013). *Haklı Savaş ve İnsancıl Hukuk.* İstanbul: On İki Levha Yayıncılık.

İlhan, Hasan (Çev.). (2010). *Savaş Sanatı Sun Tzu*. Ankara: Tutku Yayınevi.

Jessop, Bob. (2008). *Devlet Teorisi* (Çev. Ahmet Özcan). Ankara: Epos Yayınları.

Lawson, Stephanie. (2012). International Relation. Cambridge / Malden: Polity Press.

Kaboğlu, İbrahim Ö. (1994). *Anayasa Yargısı.* İstanbul: İmge Kitabevi Yayınları.

Kapani, Münci. (1992). *Politika Bilimine Giriş*. Ankara: Bilgi Yayınevi.

Keskin, Funda. (1998). *Uluslararası Hukukta Kuvvet Kullanma: SAVAŞ, KARIŞMA ve BM*. Ankara: Mülkiyeliler Birliği Vakfı Yayınları.

Mutlu, Erdem İlker. (2016). *Savaşın ve Barışın Hukuku*. Ankara: Turhan Kitabevi.

Pazarcı, Hüseyin. (2012). *Uluslararası Hukuk.* Ankara: Turhan Kitabevi.

Pazarcı, Hüseyin. (2003). *Uluslararası Hukuk Dersleri,* 2. Kitap (7. bs.). Ankara: Turhan Kitabevi.

Pazarcı, Hüseyin. (2000). *Uluslararası Hukuk Dersleri.* 4. Kitap. Ankara: Turhan Kitabevi.

Pazarcı, Hüseyin. (2021). *Uluslararası Hukuk.* Ankara: Turhan Kitabevi.

Pictet, Jean S. (Ed.). (1958). International Commitee of the Red Cross, *Commentary on the Geneva Conventions Relative to the Protection of Civilian Persons in Time of War.*

Rousseau, Jean Jaques. (2008). *Toplum Sözleşmesi* (Çev. Ali Alper). İstanbul: Oda Yayınları.

Ruys, Tom. (2010). *Armed Attack' and Article 51 of the UN Charter.* Cambridge: Cambridge University Press.

Ryngaert, Cedric. (2008). *Jurisdiction in International Law.* Oxford: Oxford University Press.

Sağıroğlu, Şeref ve Alkan, Mustafa. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları.

Schmitt, Michael N. (1999). *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* US Force Academy.

Schmitt, Michael N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge New York: Cambridge University Press.

Sharp, Walter Gary, Sr. (1999). *Cyberspace and the Use of Force.* Virginia: Aegis Research Corporation.

Sur, Melda. (2022). *Uluslararası Hukukun Esasları.* İstanbul: Beta.

Tarcan, Ahmet. (2005). *İnternet ve Toplum.* Ankara: Anı Yayıncılık.

Thürer, Daniel. (2011). *International Humanitarian Law: Theory, Practice, Context.* Zurich: Brill.

Toluner, Sevin. (1996). *Milletlerararası Hukuk Dersleri Devletin Yetkisi*. İstanbul: Beta.

Tütüncü, Ayşe Nur ve Arıkoğlu, Enver ve Akün, Verda Neslihan ve Başkaracaoğlu, Elif. (2017). *Milletlerarası Hukuk.* İstanbul: Beta.

Ünal, Şeref. (2005). *Uluslararası Hukuk*. Ankara: Yetkin.

MAKALELER

Adkins, Bonnie N., Major USAF. (2001). *The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?*, AU/ACSC/003/2001-4.

Akkutay, Ali İbrahim. (Ekim 2017). *Sivil Havacılığa Yönelik Gerçekleştirilen Siber Saldırılar: Uygulanacak Uluslararası Hukuk Kuralları, Yetki ve Sorumluluk*, Yıl: 8, Sayı: 32, s. 151-196.

Ayalew, Yohannes Eneyew. (2015). *Cyber Warfare: A New Hulloballoo under International Law.* Beijing Law Review, Cilt:6, s. 209-223.
Erişim: 21.01.2023 https://www.scirp.org/pdf/blr_2015101514533777.pdf

Aybudak, Utku. (2017). *Modern Devlet Bağlamında Ortaya Çıkan Egemenlik Kavramı ve Egemenliğin Dönüşümü.* Uluslararası Sosyal Araştırmalar Dergisi, Cilt:10, Sayı:54, s. 226-237.

Bagheri, Saeed. (2013). *Uluslararası Adalet Divanı'nın Petrol Platformları'na İlişkin Kararının Değerlendirirlmesi,* Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt:17, Sayı:1-2. s. 1155-1180.

Bakshi, Bipin. (2018). *Information Warfare: Concepts and Components*, International Journal of Research and Analytical Reviews, Cilt:5, Sayı:4, 178-185.

Barkham, Jason (2001). *Information Warfare and International Law on the Use of Force*. International Law and Politics, Cilt:34, s. 57-113.

Benatar, Marco. (2009). *The Use of Cyber Force: Need for Legal Justification?*. Goettingen Journal of International Law I, s.375-396.

Blank, Laurie R. (2013). *International Law and Cyber Threats from Non-State Actors*, Int'l L. Stud., Cilt:89, s. 406-437.

Burkle, Frederick M. (Aralık 2019). *Revisiting the Battle of Solferino: The Worsening Plight of Civillian Casualties in War and Conflict*, Disaster Medicine and Public Health Preparedness Journal, Cilt:13, Sayı:5-6, s. 1-5. Erişim: 28.12.2021. https://www.researchgate.net/publication/335088896_Revisiting_the_Battle_of_Solferino_The_Worsening_Plight_of_Civilian_Casualties_in_War_and_Conflict

Canbek Gürol, Sağıroğlu, Şeref. (2007). *Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme.* Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Cilt:23, Sayı:1-2, s. 1-12.

Coco, Antonio ve Dias, Talita de Souza. (2021). '*Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*, EJIL, Cilt:32, Sayı:3. S. 771-805.

Craig, Anthony ve Valeriano, Brandon. (2016). *Conceptualising Cyber Arms Races*, 8th International Conference on Computational Intelligence, s. 141-158.

Çelebi, Hakan ve Özdemir, Ali Murat. (Bahar 2010). *"Uluslararası Hukukta Eleştirel Yaklaşımlar"*, Uluslararası İlişkiler, Cilt:7, Sayı: 25. s. 69-90.

Çelik, Şener. (2013). *Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme*. DEÜ Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, s. 137-175.

Deeks, Ashley. (2013). *The Geography of Cyber Conflict: Through a Glass Darky*, Int'l L. Stud., Cilt:89, s. 1-20.

Değer, Ozan. (Yaz 2009). *Soykırım Suçu ve Devletin Uluslararası Sorumluluğu: Uluslararası Adalet Divanı'nın Bosna-Hersek v. Sırbistan-Karadağ Kararı*, Uluslararası İlişkiler, Cilt:6, Sayı:22, s. 61-95.

Erdem, Merve ve Özocak, Gürkan. (2019). *Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü.* Ankara Üniversitesi Dergisi, Sayı:68, s. 127-212.

Erdem, Mete. (2015). *İnsancıl Hukukta Martens Kaydı*. İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt:6, Sayı:2, s. 211-285.

Farwell, James P. ve Rohozinski, Rafal. (2011). *Stuxnet and the Future of Cyberwar*, Survival, Cilt:53:1, s. 23-40.

Garrie, Daniel ve Simonova, Masha. (2020). *A Keystroke Causes a Tornade: Applying Chaos Theory to International Cyber Warfare Law*, Broklyn Journal of Int'l Law, Cilt:45:2, s. 497-535.

Geers, Kenneth, (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory, Information Security Journal: A Global Perspective, Cilt:18, Sayı:1, s.1-7.

Geiss, Robin. (2013). *Cyber Warfare: Implications for Non-international Armed Conflicts*, Int'l L. Stud., Cilt:89, s. 627-645.

Gill, Terry D. ve Ducheine, Paul, A. L. (2013). *Anticipatory Self-Defense in the Cyber Context*, US Naval War Collage International Law Studies, Cilt:89, s. 438-471.

Goldsmith, Jack. (2013). *How Cyber Changes the Laws of War*, The European Journal of International Law, Cilt:24, Sayı:1, s. 129-138.

Gomez, Miguel Alberto N. (Spring 2016). *Arming Cyberspace: The Militarization of a Virtual Domain*, Global Security and Intelligence Studies, Cilt: 1, Sayı: 2, Makale:5, s. 42-65.

Göker, Zeliha. (Temmuz-Aralık 2008). *Kamusal Mallar Tanımında Farklı Tanımlar*, Maliye Dergisi, Sayı:155.

Graham, David E. (2010). *Cyber Threats and the Law of War*, Journal of National Security Law and Policy, Cilt:4:87. Erişim: 23.04.2020. https://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf

Gül, Yunus Emre. (2019). *Devletler Düzeyinde Siber Zorlama Faaliyeti*, Düşünce Dergisi, Sayı:11, s. 41-51.

Güleç, Özge ve Kişman, Zülfükar Aykaç. (2021). *Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri*. Akademik Açı Dergisi, Cilt:1, Sayı:1, s. 127-154.

Güneş Ceylan, Seldağ. (2004). *Roma Hukukunun Günümüz Hukuk Düzenlerine Etkisi*. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, Cilt:8, Sayı:2.

Güneysu, Gökhan. (2012). *Askeri Gereklilik İlkesi ve Uluslararası İnsancıl Hukuk*. Ankara Barosu Dergisi, Sayı:4, s. 91-108.

Güneysu, Gökhan. (2013). *Orantılılık İlkesi ve Uluslararası İnsancıl Hukuk*. TAAD, Sayı:14, s. 451-465.

Güreşçi, Ramazan. (2019). *Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi.* Savunma Bilimleri Dergisi, Cilt:18, Sayı:1, s. 75-99.

Hardin, Garrett. (1968). *Trajedy of the Commons*, Science, New Series, Cilt:162, s. 1243-1248.

Hathaway, Oona A. ve Crootof, Rebecca ve Levitz, Philip ve Nix, Haley ve Aileen, Nowlan ve Perdue, William ve Spiegel, Julia. (2012). *The Law of Cyber-Attack*, California Law Review, Cilt:100, s. 817-886. Erişim: 01.03.2020. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers

Hathaway, Oona A. ve Francis, Alexandra ve Haviland, Aaron ve Kethireddy, Srinath Reddy ve Yamamoto, Alyssa T.. (2019). *Aiding and Abeting in International Criminal Law*. Cornell Law Review, Cilt:104, s. 101-149. Erişim: 20.12.2020.

https://poseidon01.ssrn.com/delivery.php?ID=653004094099107076079024000006072095049017031083090035064100084096008125125091027121022102098031119063013103096080008000097072000020066087035098003101022064025073047043021000082028081019113118092114112081123090112098123086025019080022089110116119065&EXT=pdf&INDEX=TRUE

Heinegg, Wolff Heintschel von. (2012). *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn.

Hoisington, Matthew. (2009). *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, Boston College International and Comparative Law Review, Cilt:32, Sayı:2, Makale:16, s. 439-454.

Hruza, Petr ve Cerny, Jiri. (2017). *Cyberwarfare,* International Cenference Knowledge-Based Organization, Cilt:23, Sayı:1, s. 155-160. Erişim: 25.01.2022. https://www.researchgate.net/publication/318737253_Cyberwarfare

Jensen, Eric Talbot. (2002). *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking to Rights of Self-Defense,* Stanford Journal of International Law, Cilt:38, s. 207-240.

Jensen, Eric Talbot. (2015). *Cyber Sovereignty: The Way Ahead*. Texas International Law Journal, Cilt:50/2.

Jensen, Eric Talbot. (2017). *The Tallinn Manual 2.0: Highligts and Insights*, Georgetown Journal of International Law, Cilt:48.

Jensen, Eric Talbot ve Watts, Sean. (2017). *A Cyber Duty of Due Dilience: Gentle Civilizer or Crude Destabilizer?* Texas Law Review, Cilt:95:1555.

Kanuck, Sean. (2010). *Sovereign Discourse on Cyber Conflict Under International Law*, Texas Law Review, Cilt:88, s. 1571-1597.

Karadağ, Ulaş. (2016). *Birleşmiş Milletler Antlaşması'na Göre Meşru Müdafaa Hakkı.* İnönü Üniversitesi Hukuk Fakültesi Dergisi, Cilt:7, Sayı:2, s. 171-186.

Karakoç, İrem. (2004). *Türk Hukuk Tarihi'nde Uluslararası Andlaşmaların Uluslararası Hukukun Gelişim Sürecindeki Yeri*. DEÜ Hukuk Fakültesi Dergisi, Cilt:6, Sayı:2, s. 199-253.

Kasapoğlu, Can. (2017). *Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında*, EDAM Siber Politikalar Kâğıtları Serisi, Sayı:2. Erişim: 21.04.2020.

https://edam.org.tr/wp-content/uploads/2017/10/sibersavas_tr_rbs_logo.pdf

Kelsey, Jeffrey T.G. (Mayıs 2008). *Hacking into International Humaniterian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.* Michigan Law Review, Cilt:106, s. 1427-1452.

Kesan, Lay P. ve Hayes, Carol M. (Spring 2012). *Mitigative Counterstriking: Self-Defence and Deterence in Cyberspace*, Harvard Journal of Law & Technology, Cilt:25, Sayı:2. s. 430-543.

Khan, Kamal Ahmad. (2017). *Use of Force and Human Rights under International Law*, Athens Journal of Law, Cilt:3, Sayı:2. s. 141-164.

Kolasi, Klevis. (2017). *Savaşın Değişen Niteliği ve Jus ad bellum ve Jus in bello'ya Etkisi.* İnsan Hakları Yıllığı, Cilt:35, s. 1-29.

Korhan, Sevda. (2017). *Siber Uzayda Aktör - Güç İlişkisi*, Siber Politikalar Dergisi, Cilt:2, Sayı:3, s. 71-100. Erişim: 10.07.2022.

https://www.academia.edu/40571066/S%C4%B0BER_UZAYDA_AKT%C3%96R_G%C3%9C%C3%87_%C4%B0L%C4%B0%C5%9EK%C4%B0S%C4%B0

Lin, Herbert. (2012). *Cyber Conflict and International Humaniterian Law*, International Review of the Red Cross, Cilt:94, s. 515-531.

Lin, Herbert S. (2010). *Offensive Cyber Operation and the Use of Force*, Journal of Nationmal Security Law & Policy, Cilt:4, s. 63-86.

Mačák, Kubo. (2015). *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humaniterian Law*, Israel Law Review, Cilt:48, s. 55-80.

Mačák, Kubo. (2018). *Silent War: Applicability of the Jus in Bello to Military Spaca Operations*, International Law Studies, Cilt:94.

Orend, Briand. (September 2000). *Michael Walzer on Resorting to Force*, Canadian Journal of Political Science, Cilt:33 (3). s. 523-547.

Özarslan, Bahadır Bumin. (2014). *Soykırım Suçunun Önlenmesi ve Cezalandırılması Sözleşmesi Açısından Hocalı* Katliamı, Hacettepe HFD, Cilt:4, Sayı:1, s. 187-214.

Padmanabhan, Vijay M. (2013). *Cyber Warriors and the Jus in Bello*, Int'l L. Stud., Cilt:89, s. 288-308.

Pascucci, CDR Peter. (2017). *Distiction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, Minnesota Journal of Int'l Law, Cilt:26:2, s. 418-460.

Piatkowski, Mateusz. (2017). *The Definition of the Armed Conflict in the Condition of Cyber Warfare*, Polish Political Science Yearbook, Cilt:46 (1). s. 271-280.

Roscini, Marco. (2010). *World Wide Warfare-Jus ad bellum and the Use of Cyber Force*, Max Planck Yearbook of United Nations Law, Cilt:14, s. 85-130.

Schmitt, Michael N. (2013). *Classification of Cyber Conflict*, US Naval War Collage International Law Studies, Cilt:89, s. 233-251.

Schmitt, Michael N. (2017). *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum,* Harvard National Security Journal, Cilt:8, s. 239-282.

Shackelford, Scott J. (2010). *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Conference on Cyber Conflict, CCD COE Publications, Tallinn, s. 197-208.

Stahl, William M. (2011). *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, GA. J. INT'L & COMP. L., Cilt:40, s. 247-273.

Taddeo, Mariarosaria. (2011). *Information Warfare: A Philosophical Perspective*. Philopsophy and Geography, Cilt:25(1), s. 105-120. Erişim: 12.08.2022. https://www.researchgate.net/publication/234627039_Information_Warfare_A_Philosophical_Perspective

Türkay, Şeyda. (2013). *Siber Savaş Hukuku ve Uygulama Sorunsalı.* İÜHFM, Cilt:71, Sayı:1, s. 1177-1228.

Vida Antolin-Jenkins. (2008). *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*. 51 NAVAL L. REV. 132, 140.

Wallace, David ve Reeves, Shane R. (2013). *The Law of Armed Conflict's "Wicked Problem: Levée en Masse in Cyber Warfare*, Int'l L. Stud., Cilt:89, s. 646-668.

Weglinski, Konrad. (2016). *Cyberwarfare and Responsibility of States*, Torun International Studies, Cilt:1, Sayı:9, s. 79-86.

TEZLER

Dal, Ufuk. (2019). *Uluslararası Sorumluluk Hukukunda Uluslararası Hukuka Aykırı Eylemin Devlete Atfedilmesi*. Doktora Tezi, İstanbul, İstanbul Üniversitesi.

Erkiner, Hakkı Hakan. (2008). *Devletin Haksız Fiilinden Kaynaklanan Milletlerarası Sorumluluğu*. Doktora Tezi, İstanbul, Marmara Üniversitesi.

Güneysu, Gökhan. (2011). *Çevrenin Silahlı Çatışmalar Esnasında Korunması*. Doktora Tezi, Eskişehir, Anadolu Üniversitesi.

Pino, Beatriz. (2020). *International Responsibility of States and Artificial Intelligence*. Master Thesis, Barcelona Üniversity. Erişim: 30.12.2021. http://diposit.ub.edu/dspace/bitstream/2445/170430/1/TFM_Beatriz_Pino.pdf

Rølsåsen, Thea Helen Eriksen. (2016). *When do Cyber Operations Amount to Use of Force and Armed Attack, and What Response will They Justify?*, Master Thesis, University of Oslo. Erişim: 26.06.2020. https://www.duo.uio.no/bitstream/handle/10852/50840/723.pdf?sequence=1&isAllowed=y

Sarıca, Şermin. (2008). *Farklı Refah Devleti Modellerinde Sosyal Harcamaların Niteliği: Emekgücünün Meta Niteliği Açısından Bir Değerlendirme*. Doktora Tezi, İstanbul, İstanbul Üniversitesi.

Sönmez, Seda. (2019). *Michael Walzer ve Haklı Savaş Problemi*. Yüksek Lisans Tezi, Hacettepe Üniversitesi. Erişim: 16.12.2021. 10218355.pdf (hacettepe.edu.tr)

Uzun, Elif. (2007). *Milletlerarası Hukuka Aykırı Eylemlerinden Dolayı Devletin Sorumluluğu*. İstanbul: Beta.

İNTERNET KAYNAKLARI

Afroditi, Papanastasiou. (2010). *Application of International Law on Cyber Warfare Operations.* Erişim: 23.04.2020. https://poseidon01.ssrn.com/delivery.php?ID=904114091001094030071081005075016112117009040087024023014000092108095082074007118117124123020032031057028101069083067090119076109033095005041121095065083018093023067042082017120016093080097114086124070119127120114019021125119085097082001000124123112017&EXT=pdf

Altundağ, Zehra. (2016). *Geçmişten Günümüze Şangay İşbirliği Örgütü*. Avrasya Etüdleri, Cilt: 49, Sayı:2016/1, s. 111. Erişim: 24.01.2023 https://dergipark.org.tr/en/download/article-file/422162

Campbell, Duncan. (Ekim 1999). *Development of Surveilliance Technology and Risk of Abuse of Economic Information.* Erişim: 02.05.2020. https://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

Chandler, William M.A. (2017). *Evgeny Pasukanis: Hukukun Meta-Form Kuramı* (Çev. Furkan Yılmaz). Hukuk Kritik. Erişim: 05.11.2022. https://www.hukukkritik.com/projects/evgeny-pasukanis%3A-hukukun-meta-form-kuram%C4%B1

Çelik, Soner ve Çeliktaş, Barış. (2018). *Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar,* Cyberpolitik Journal. Cilt:3, Sayı:5. Erişim: 04.11.2022.

https://dergipark.org.tr/en/download/article-file/536201

Corn, Gary ve Jensen, Eric Talbot. (2018). *The Use of Force and Cyber Countermaesures*. 32 International & Comperative Law Journal 127. Erişim: 17.01.2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3190253

Coupland, Robin M. ve Herby, Peter. (1999). Review of the legality of weapons: a new approach The SIrUS Project, International Committee of the Red Cross. Erişim: 01.01.2022. https://www.icrc.org/en/doc/resources/documents/article/other/57jq36.htm

Department of Defence Office of General Counsel. (1999). *An Assessment of International Legal Issues in Information Operations*. Erişim: 18.08.2020. https://fas.org/irp/eprint/io-legal.pdf

Erkiner, Hakkı Hakan. (2010). *Uluslararası Hukukta Uluslararası Topluluk Kavramının Başlıca Görünümleri.* Erişim: 07.04.2020. https://www.academia.edu/33296812/HAKKI_HAKAN_ERK%C4%B0NER_MAKALE_ULUSLARARASI_HUKUKTA_ULUSLARARASI_TOPLULUK_KAVRAMININ_BA%C5%9ELICA_G%C3%96R%C3%9CN%C3%9CMLER%C4%B0

Erkiner, Hakan Hakkı. (2020). *Uluslararası Hukukta Kuvvet Kullanma Yasağının Kişi bakımından (Ratione Personae), yer Bakımından (Ratione Loci) ve Konu Bakımından (Ratione Materiae) Uygulanabilirliği*, Karadeniz 3. Uluslararası Sosyal Bilimler Kongresi, s. 283-291. Erişim: 11.09.2022. https://www.researchgate.net/publication/352826229_Uluslararasi_Hukukta_Kuvvet_Kullanma_Yasaginin_Kisi_Bakimindan_Ratione_Personae_Yer_Bakimindan_Ratione_Loci_Ve_Konu_Bakimindan_Ratione_Materiae_Uygulanabilirligi

Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defence, Lockheed Martin, s. 1-10, Erişim: 27.06.2020.
http://cdn2.hubspot.net/hubfs/91979/Gaining_the_Advantage_Cyber_Kill_Chain.pdf?t=1459783725510&utm_campaign=Commercial+Cyber&utm_source=hs_automation&utm_medium=email&utm_content=21881761&_hsenc=p2ANqtz-8cr09K-ZaN2zypp5DVXY61NM8WOUa8WolIWEbmilZIHlySlNuHD7D1cuB8wAoAqDTklkdr2mYB_jz-RhLIlVS_LjK3Zg&_hsmi=21881761

Government of Canada. (2010). *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Erişim: 11.08.2022.
https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf

Gümüşbaş, Ahmet, *Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları*. Erişim: 30.11.2020.
https://tasam.org/Files/Icerik/File/Stuxnet_ve_Aramco_Saldırıları_pdf_1acfbb35-785b-4de4-8d9a-850a695d45ac.pdf

Hartmann, Kim ve Giles, Keir. (2018). *Net Neutrality in the Context of Cyber Warfare*, 10th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, s. 139-158.

Hogan, Mel. (2015). *Data flows and water woes: The Utah Data Center*. Erişim: 12.08.2022.
https://www.researchgate.net/publication/281807399_Data_flows_and_water_woes_The_Utah_Data_Center

Inside the Slammer Worm, *Center for Applied Data Analysis*. Erişim: 28.06.2020.
https://www.caida.org/publications/papers/2003/sapphire2/sapphire.xml

Inside the Slammer Worm. (2003). *Security and Privacy Magazine*. Erişim: 13.08.2022. https://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf

Lieber Yasası'nın 14. Maddesi. Erişim: 12.11.2022. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=8FC14110FCE40830C12563CD00514A6E

Lindsay, Jon R. (2013). *Stuxnet and the Limit of Cyber Warfare*, Security Studies. s. 1-53. Erişim: 28.06.2022. https://www.scinapse.io/papers/1972914161

Kadıoğlu Kumtepe, Cemre. (2021). *Siber Uzayda Kuvvet Kullanma Yasağı ve Yasağın İstisnalarının Geçerliliği.* Erişim: 11.09.2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4083156

Kadıoğlu Kumtepe, Cemre. (2021). *Uluslararası Veri Aktarımının Kısıtlanmasına İlişkin Veri Uygunluğu İlkesinin Devletlerin Egemenliğine Etkisi*. Erişim: 11.09.2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4083162

Key Events in the Development of the First General Purpose Electronic Digital Computer, the ENIAC. Erişim: 02.11.2022. https://www.historyofinformation.com/detail.php?id=636

Mačák, Kubo. (2017). *From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law.* Erişim: 20.04.2020. https://ccdcoe.org/uploads/2018/10/Art-09-The-Impact-of-the-Development-of-the-Cyber-Law-of-War-on-General-International-Law.pdf

Melzer, Nils. (2011). *Cyberwarfare and International Law.* Erişim: 15.05.2020. https://www.files.ethz.ch/isn/134218/pdf-1-92-9045-011-L-en.pdf

Mikhail, George. *How the USA and China Trade War Caused Cybersecurity Boom*. Erişim: 11.08.2022. https://datasearchconsulting.com/how-the-us-and-china-trade-war-caused-cybersecurity-boom/

Milosevic, Nikola. (2013). *History of Malware, Digital Forensics Magazine*, 1/16, s. 58-66. Erişim: 24.04.2021. https://www.research.manchester.ac.uk/portal/files/32297162/FULL_TEXT.PDF

Mukherjee, Sourav. Cyber warfare and Implications. Erişim: 27.06.2022. https://deliverypdf.ssrn.com/delivery.php?ID=611103021078106112122000084119065112034072042037055057122116099022104008025122084096028012000000980300470220070740951191040981110250000870190020070090660251120661050660090320270790001230021220910091100771130030300970741071270160970161180051091200970 96&EXT=pdf&INDEX=TRUE

Namanya, Anitta Patience ve Cullen, Andrea ve Awan, Irfan U. ve Disso, Jules Pagna. (2018). *The World of Malware: An Overview*, IEEE 6th International Conference on Future Internet of Things and Cloud, s. 420-427. Erişim: 04.04.2021. https://www.researchgate.net/publication/327665678_The_World_of_Malware_An_Overview

Pernik, Piret (Ed.). (2022). *Cyberspace Strategic Outlook 2030 Horizon Scanning and Analysis*. Tallinn: CCDCOE Publication, s. 13. Erişim: 24.01.2023. https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_v2_170x240_220513.pdf

Position Paper. (2021). *On the Application of International Law in Cyberspace*. Erişim: 04.08.2022. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Protecting Europe against large-scale cyber-attacks. Erişim: 05.05.2021. https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf

Schreier, Fred. (2015). *On Cyberwarfare*, DCAF Horizon 2015 Working Paper, No:7. Erişim: 29.01.2022. https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

Singh, Brahmanand Pratap. (April 2022). *Cyber War,* International Journal of Innovative Research in Science, Engineering and Technology Cilt:11, Sayı:4, s. 3290-3292. Erişim: 27.06.2022. https://www.researchgate.net/publication/360005307_CYBER_WAR

Sklerov, Matthew J. (2009). *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent.* Erişim: 27.04.2020. https://www.hsdl.org/?view&did=12115

Statement by Director of National Intelligence James R. Clapper on Allegations of Ecomomic Espionage (08 Eylül 2013) Erişim: 02.05.2020. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage

Stokes, Paul. (2014). *State Responsibility for Cyber Operations: International Law Issues, Event Report*, British Institute of International and Comperative Law. Erişim: 29.08.2022. https://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf

Streltsov, Anotoly A. (2017). *Application of Internaional Humanitarian Law to Armed Conflicts in Cyberspace*. Erişim: 17.10.2020. https://digital.report/wp-content/uploads/2016/04/169747-Streltsov-ENG.pdf

Therrien-Tremblay, Anne-Marie. (2022). *The NATO 2030 Initiative: Overview and Implications for Canada.* Ottowa: Library of Parliement. Erişim: 24.01.2023. https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/HillStudies/PDF/2022-16-E.pdf

Tureng, the Multilingual Dictionary. https://tureng.com/tr/turkce-ingilizce

United Kingdom, Cabinet Office. (2009). *Cyberspace Security Strategy of the United Kingdom: safety, security and resilience in cyber space*. Erişim: 11.08.2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf

United States, Office of White House Press. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Erişim: 11.08.2022. https://nsarchive.gwu.edu/document/21424-document-28

Yousef LI.M., Ahmed. (2018). *Cyber operations between Jus Ad Bellum and below the Threshold of the use of force*, ResearchGate. Erişim: 30.08.2022. https://www.researchgate.net/publication/331639155_Cyber_operations_below_the_threshold_of_the_use_of_force_Principle_of_state_sovereignty

Wikileaks media organization and Web site. Erişim: 02.11.2022. https://www.britannica.com/technology/website

Wikipedia The Free Encyclopedia. Erişim: 05.11.2022. https://en.wikipedia.org/wiki/Real-time_data

GAZETE HABERLERİ

Borger, Jullian. (24 Eylül 2013). Brezillian president: US Surveillance 'a breach of international law'. *The Gardian.* Erişim: 02.05.2020. https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance

Collier, Kevin. (23 Eylül 2019). 27 Countries Sign Cybersecurity Pledge with Digs at China Russia, *CNN.* Erişim: 09.09.2021. https://edition.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html

Corbin, Kenneth. (16 Mayıs 2019). When Cybersecurity and Trade Wars Collide, *Forbes.* Erişim: 11.08.2022. https://www.forbes.com/sites/kennethcorbin/2019/05/16/when-cybersecurity-and-trade-wars-collide/?sh=4e0090716774

Cyberwar: war in the fifth domain, *The Economist.* (01 Temmuz 2010). Erişim: 15.11.2022. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain;

Fisher, Max. (29 Ekim 2013). Why America Spies on its Allies (and probably should), *The Washington Post.* Erişim: 09.09.2021. https://www.washingtonpost.com/news/worldviews/wp/2013/10/29/why-america-spies-on-its-allies-and-probably-should/

Hedges Chris. (06 Haziran 2003). What Every Person Should Know Abour War, *The New York Times.* Erişim: 07.02.2021. https://www.nytimes.com/2003/07/06/books/chapters/what-every-person-should-know-about-war.html#:~:text=Has%20the%20world%20ever%20been,wars%20in%20the%20twentieth%20century.

https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html Erişim: 20.03.2020.

Lawson, Sean. (7 Aralık 2016). Does 2016 Mark the End of Cyber Pearl Harbor Hysteria? *Forbes*. Erişim: 02.05.2020**.** https://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/#35dcff0522c2

Rienks, Captain Katharina J. (2020). The Plea of Necessity and Cyber Warfare, Army Lawyer, Issue:5, s. 72-81.

Sanger, David E. (01 Haziran 2012). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*. Erişim: 03.05.2020. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sanger, David E. ve Barboza, David ve Perlroth, Nicole. (18 Şubat 2013). Chinese Army Unitis Seen as Tied to Hacking Against U.S., *The New York Times*. Erişim: 12.08.2022. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Sanger, David E. ve Perlroth, Nicole. (22 Mart 2014). N.S.A. Breached Chinese Servers Seen as Security Threat. *The New York Times.* Erişim: 02.05.2020. https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html

Snowden talks industrial espianage, death threats in German interview, France 24 (27 Ocak 2014) Erişim: 02.05.2020. https://www.france24.com/en/20140127-snowden-german-interview-industrial-espionage

Straub, Jeremy ve Traylor, Terry. (2018). *Introduction Marytime Model for Cyber and Information Warfare*, International Conference on Computational Intelligence, s. 25-29.

Wathers, Richard. (13 Ocak 2006). Yahoo loses Nazi memorabilia case. *The Financial Times.* Erişim: 04.10.2020. https://www.ft.com/content/81127f12-83cb-11da-9017-0000779e2340

Waxman, Matthew C. (2011). *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* The Yale Journal of International Law, Cilt:436, s. 421-459.

Waxman, Matthew C. (2013). *Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions,* US Naval War Collage International Law Studies, Cilt:89, s. 109-122.

RAPOR VE BELGELER

BM Genel Kurulu. "Combating the Criminal Misuse of Infirmation Thecnology (A/RES/55/63)" Erişim: 05.11.2022. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement

BM Genel Kurulu, Declaration on Principles of International Law Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (24 Ekim 1970) Erişim: 12.06.2022. https://www.un.org/ruleoflaw/files/3dda1f104.pdf

BM Genel Kurulu. "Definition of Aggression (A/RES/29/3314)" Erişim: 12.06.2022. A/RES/29/3314 - Definition of Aggression - UN Documents: Gathering a body of global agreements (un-documents.net)

BM Genel Kurulu. "Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (A/RES/45/121)" Erişim: 05.11.2022.https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/565/10/IMG/NR056510.pdf?OpenElement

BM Güvenlik Konseyi, "Resolution 487 (1981) / Adopted by the Security Council at its 2288th Meeting." 19 Haziran 1981, Erişim: 12.06.2022. Resolution 487 (1981) / (un.org)

Commision of the European Communities. (2005). *Green Paper on a European Programme for Critical Infrastructure Protection,* COM 576 final, 17.11.2005, Erişim: 15.05.2020. https://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-576-EN-F1-1.Pdf

Communication from the Commission to the European Parliament, the Council, the European Economik and Social Committee and the Committe of the Regions on Critical Information Infrastructure Protection. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Convention on Cybercrime;
https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Critical Insfrustructures Protection Act of 2001, 42 U.S. Code §5195c.

DeWeese, Geoffrey S. (2015). *Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminance*, 7th International Conference on Cyber Conflict: Architecture in Cyberspace, NATO CCD COE Publications, Tallinn, s. 81-92.

European Parliament, REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), (11 Temmuz 2001) Erişim: 02.05.2020.
https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

EYUCM, "*Tadi´c Case*", 07 Mayıs 1997, Erişim: 16.07.2022. https://www.icty.org/en/press/tadic-case-verdict

Francisco Mallén (United Mexican States) v. U.S.A., Reports of International Arbitral Awards, UN General Claims Commission, Cilt:5, 1927, s. 170-190. Erişim: 27.02.2021. https://legal.un.org/riaa/cases/vol_IV/173-190.pdf

Hakemlik Kararı, "*Island of Palmas Case*", 04 Nisan 1928, Erişim: 15.07.2022. https://legal.un.org/riaa/cases/vol_II/829-871.pdf

Harvard Program on Humanitarian Policy and Conflict Research. (2010). *Commentary on the HPCR Manual on International Law Applicable to Air and Misslile Warfare.*

International Commitee of the Red Cross. (1987). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.*

International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (12 Aralık 2001), Yearbook of the International Law Commission, Cilt:2.

Hakemlik Kararı, "*Naulilaa Arbitration*", 31 Temmuz 1928, Erişim: 15.07.2022. https://www.scribd.com/document/506919046/Naulilaa-Arbitration-Portugal-vs-Germany-Google-translated

1907 IV sayılı Lahey Kara Savaşları Kuralları Sözleşmesi'ne Ek Yönetmelik. Erişim: 13.11.2022. http://askerihukuk.net/FileUpload/ds158941/File/kara_harbinin_kanunlari_ve_adetleri_hakkinda_sozlesme.pdf

1907 tarihli Kara Savaşlarında Tarafsız Kişi ve Güçlerin Hak ve Ödevleri Konulu V. Lahey Konvansiyonu. Erişim: 13.11.2022. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/200-220002?OpenDocument

Liles, Samuel ve Rogers, Marcus ve Dietz J. Eric ve Dean, Larson. (2012). *Applying Traditional Millitary Principles to Cyber Warfare,* 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, s. 169-180.

NATO Bükreş Zirvesi Bildirisi. Erişim: 09.11.2022. *https://sgp.fas.org/crs/row/RS22847.pdf*

Posecutor vs Thomas Lubanga Dyilore, Decision on the confirmation of charges, 29 Jan. 2007, Trial Chamber I, No: ICC-01/04-01/06. Erişim: 06.02.2022.

https://www.icc-cpi.int/CourtRecords/CR2007_02360.PDF

Report of the High-level Panel on Threats, Challanges and Changes, UN Doc. A/59/565.

Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Antlaşması (2009) Erişim: 17.12.2021.

Agreement_on_Cooperation_in_Ensuring_International_Information_Security_between_the_Member_States_of_the_SCO.pdf

Şangay İşbirliği Örgütü Yekaterinburg Deklerasyonu (2009) Erişim: 17.12.2021.

Yekaterinburg_Declaration_by_the_Heads_of_the_Member_States_of_the_SCO.pdf

UAD, "*Advisory Oppinion of the International Court of Justice on the Legal Consequences of the Construction of a Wall in The Occupied Palestinian Territory*", 09 Haziran 2004, Erişim: 05.11.2022. https://www.un.org/unispal/document/auto-insert-178825/

UAD, "*Case Concerning Application of The Convention on the Prevention and Punishment of the Crime of Genocide*", 26 Şubat 2007, Erişim: 16.07.2022. https://www.icj-cij.org/public/files/case-related/91/091-20070226-JUD-01-00-EN.pdf

UAD, "*Case Concerning the Gabcikovo-Nagymaros Project*", 25 Eylül 1997, Erişim: 16.07.2022. https://www.icj-cij.org/public/files/case-related/92/092-19970925-JUD-01-00-EN.pdf

UAD, "*Case Concerning Military and Paramilitary Activities in and Against Nicaragua*", 27 Haziran 1986, Erişim: 12.06.2022. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

UAD, "*Case Concerning Oil Platforms*", 06 Kasım 2003, Erişim: 12.06.2022. https://www.icj-cij.org/public/files/case-related/90/090-20031106-JUD-01-00-EN.pdf

UAD, "*Case Concerning United States Diplomatic and Consular Staf in Tehran*", 24 Mayıs 1980, Erişim: 16.07.2022. https://www.icj-cij.org/public/files/case-related/64/064-19800524-JUD-01-00-EN.pdf

UAD, "*Corfu Channel Case*", 09 Nisan 1949, Erişim: 15.07.2022. https://www.icj-cij.org/public/files/case-related/1/001-19491215-JUD-01-00-EN.pdf

UAD, "*Legality of the Threat or Use of Nuclear Weapons*", 08 Temmuz 1996, Erişim: 12.06.2022. https://www.un.org/law/icjsum/9623.htm

*The National Strategy to Secure Cyberspace. (*2003). Erişim: 18.08.2020. https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

EK 1. ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DOKTORA TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
…… ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: .../..../.....

Tez Başlığı : ……

……

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam …… sayfalık kısmına ilişkin, .../...../..... tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % ..... 'tür.

Uygulanan filtrelemeler:

1- ☐ Kabul/Onay ve Bildirim sayfaları hariç
2- ☐ Kaynakça hariç
3- ☐ Alıntılar hariç
4- ☐ Alıntılar dâhil
5- ☐ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

Adı Soyadı: _____
Öğrenci No: _____
Anabilim Dalı: _____
Programı: _____
Statüsü: ☐ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

_____
(Unvan, Ad Soyad, İmza)

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
Ph.D. DISSERTATION ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
…… DEPARTMENT

Date: …/…./……..

Thesis Title : ……

……

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on ……/……/…… for the total of …….. pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is …….. %.

Filtering options applied:

1. ☐ Approval and Decleration sections excluded
2. ☐ Bibliography/Works Cited excluded
3. ☐ Quotes excluded
4. ☐ Quotes included
5. ☐ Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Date and Signature

Name Surname: _____
Student No: _____
Department: _____
Program: _____
Status: ☐ Ph.D. ☐ Combined MA/ Ph.D.

ADVISOR APPROVAL

APPROVED.

_____
(Title, Name Surname, Signature)

EK 2. ETİK KURUL/KOMİSYON İZNİ YA DA MUAFİYET FORMU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ ÇALIŞMASI ETİK KOMİSYON MUAFİYETİ FORMU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
…… ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: .../..../.....

Tez Başlığı: ……

……

Yukarıda başlığı gösterilen tez çalışmam:

1. İnsan ve hayvan üzerinde deney niteliği taşımamaktadır,
2. Biyolojik materyal (kan, idrar vb. biyolojik sıvılar ve numuneler) kullanılmasını gerektirmemektedir.
3. Beden bütünlüğüne müdahale içermemektedir.
4. Gözlemsel ve betimsel araştırma (anket, mülakat, ölçek/skala çalışmaları, dosya taramaları, veri kaynakları taraması, sistem-model geliştirme çalışmaları) niteliğinde değildir.

Hacettepe Üniversitesi Etik Kurullar ve Komisyonlarının Yönergelerini inceledim ve bunlara göre tez çalışmamın yürütülebilmesi için herhangi bir Etik Kurul/Komisyon'dan izin alınmasına gerek olmadığını; aksi durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

Adı Soyadı: _____
Öğrenci No: _____
Anabilim Dalı: _____
Programı: _____
Statüsü: ☐ Yüksek Lisans ☐ Doktora ☐ Bütünleşik Doktora

DANIŞMAN GÖRÜŞÜ VE ONAYI

_____
(Unvan, Ad Soyad, İmza)

Detaylı Bilgi: http://www.sosyalbilimler.hacettepe.edu.tr
Telefon: 0-312-2976860 **Faks:** 0-3122992147 **E-posta:** sosyalbilimler@hacettepe.edu.tr

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
ETHICS COMMISSION FORM FOR THESIS

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
…… DEPARTMENT

Date: …/…./……..

Thesis Title: ……

……

My thesis work related to the title above:

1. Does not perform experimentation on animals or people.
2. Does not necessitate the use of biological material (blood, urine, biological fluids and samples, etc.).
3. Does not involve any interference of the body's integrity.
4. Is not based on observational and descriptive research (survey, interview, measures/scales, data scanning, system-model development).

I declare, I have carefully read Hacettepe University's Ethics Regulations and the Commission's Guidelines, and in order to proceed with my thesis according to these regulations I do not have to get permission from the Ethics Board/Commission for anything; in any infringement of the regulations I accept all legal responsibility and I declare that all the information I have provided is true.

I respectfully submit this for approval.

Date and Signature

Name Surname: _____
Student No: _____
Department: _____
Program: _____
Status: ☐ MA ☐ Ph.D. ☐ Combined MA/ Ph.D.

ADVISER COMMENTS AND APPROVAL

_____
(Title, Name Surname, Signature)