

## ÖRNEK VAKA İNCELEMELERİ ÇERÇEVESİNDE SİBER SALDIRILAR KARŞISINDA ULUSLARARASI HUKUKUN YETERSİZLİĞİ

Berke BURCU<sup>1</sup>

### Özet

21. yüzyılda devletlerarası rekabette siber tehditler, teknik bir sorun olmaktan çıkarak siyasi, hukuki ve etik boyutları olan stratejik bir meseleye dönüşmüştür. Bu çalışma, devletlerin siber saldırılara karşı aldığı önlemleri, uluslararası hukuk normları çerçevesinde bu saldırıların değerlendirilmesini ve mevcut hukuki düzenlemelerin etkinliğini incelemeyi amaçlamaktadır. Bu kapsamda çalışmada nitel araştırma yöntemi benimsenmiş olup, Estonya, Gürcistan, İran ve Ukrayna örnekleri karşılaştırmalı vaka analizi ve belge incelemesi teknikleriyle uluslararası hukuk normları ve teorik yaklaşımlar çerçevesinde incelenmiştir. Tallinn Manual gibi temel belgeler ışığında, siber saldırıların uluslararası hukukta tanımı ve devletlerin hukuki yanıtları ele alınmıştır. Bulgular, hukuk normlarının siber tehditler karşısında yetersiz olduğunu ve saldırı kaynağının tespitindeki zorlukların meşru müdafaa hakkını sınırlandırdığını göstermektedir. Siber saldırılar, devlet egemenliği ve uluslararası barış için ciddi riskler taşır. Bu nedenle siber güvenlik, teknik değil, hukuk, politika ve etik disiplinlerinin birlikte çalışmasını gerektiren disiplinlerarası bir alandır. Dijital çağda güvenlik için bağlayıcı uluslararası normlar ve çok taraflı iş birliği kritik öneme sahiptir.

**Anahtar Kelimeler:** Siber saldırı, Siber güvenlik, Uluslararası hukuk, Meşru müdafaa, Tallinn Manual.

## THE INADEQUACY OF INTERNATIONAL LAW IN THE FACE OF CYBER ATTACKS BASED ON CASE STUDIES

### Abstract

In the 21st century, cyber threats have moved beyond their technical dimension and have become strategic issues with political, legal, and ethical implications in interstate competition. This study aims to examine states' responses to cyber-attacks, the evaluation of these attacks within the framework of international law, and the effectiveness of existing legal regulations. Within this scope, the study adopts a qualitative research approach and analyzes Estonia, Georgia, Iran, and Ukraine through comparative case analysis and document review. Considering the Tallinn Manual, the United Nations Charter, NATO documents, and related legal frameworks, the study evaluates how cyberattacks are defined under international law and which legal instruments are available to states. The findings indicate that existing international legal norms remain insufficient in responding to cyber threats. In particular, the attribution problem limits the effective use of the right of self-defense under Article 51 of the United Nations Charter. Cyber-attacks pose serious risks to state sovereignty, the principle of non-intervention, and international peace. Therefore, cybersecurity should not be considered merely a technical issue but rather an interdisciplinary field requiring cooperation among law, politics, and ethics. In the digital age, binding international norms, clearer legal definitions, and stronger multilateral cooperation are essential for ensuring global cyber stability.

**Keywords:** Cyber-attack, Cybersecurity, International law, Self-defense, Tallinn Manual.

<sup>1</sup> Yüksek Lisans Öğrencisi, Aksaray Üniversitesi, Sosyal Bilimler Enstitüsü, berkeburcu70@gmail.com, ORCID: 0009-0009-9296-7190

**Bu Yayına Atıfta Bulunmak İçin:** Burcu, B. (2026). Örnek vaka incelemeleri çerçevesinde siber saldırılar karşısında uluslararası hukukun yetersizliği. *Karabük Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 6(1), 125-148. <https://doi.org/10.63233/kbuiibfdergisi.1848571>

## GİRİŞ

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, devletlerin güvenlik politikalarında köklü bir dönüşüm yaratmış ve uluslararası ilişkilerde dijital bir boyutun ortaya çıkmasına yol açmıştır. Siber uzay, yalnızca bireysel faaliyetleri değil, devletlerin dış politika önceliklerini, ulusal güvenlik stratejilerini ve askerî yapılanmalarını doğrudan etkileyen merkezi bir alan hâline gelmiştir. Devletler bu dijital alanda egemenlik iddiasında bulunmakta; ancak siber uzayın sınırlarının belirsizliği ve siber faaliyetlerin anonim doğası, etkin müdahale ve düzenleme süreçlerini ciddi biçimde zorlaştırmaktadır.

Siber saldırılar, teknik sistemlere verilen zararın ötesinde; ekonomik altyapıların çökmesi, seçim süreçlerinin manipüle edilmesi ve askerî operasyonların sektöre uğraması gibi ağır sonuçlar doğurabilmektedir. Estonya, Gürcistan, İran ve Ukrayna örnekleri, siber saldırıların yalnızca teknik eylemler olmadığını, aynı zamanda siyasi, hukuki ve stratejik etkiler yarattığını açık biçimde ortaya koymaktadır. Bu gelişmeler, geleneksel savaş hukuku ile mevcut uluslararası hukuk normlarının siber tehditleri değerlendirmekte yetersiz kaldığını göstermektedir.

Uluslararası hukuk sistemi, kuvvet kullanma yasağı, egemen eşitlik ve meşru müdafaa gibi temel ilkelere dayanmakla birlikte, bu ilkeler esasen geleneksel silahlı çatışmalar dikkate alınarak şekillendirilmiştir. Siber saldırıların kaynağının tespit edilmesi, etkilerinin ölçülmesi ve hukuki sorumluluğun belirlenmesi mevcut normlar çerçevesinde ciddi belirsizlikler yaratmaktadır. Bu durum, uluslararası hukukta yeni yorumlara ve düzenlemelere duyulan ihtiyacı açıkça ortaya koymaktadır. Tallinn Manual gibi rehber nitelikli belgeler önemli katkılar sunsa da bağlayıcı olmamaları nedeniyle devlet uygulamaları üzerinde sınırlı bir etkiye sahiptir. Nitekim Tallinn Manual 1.0, siber savaş ve silahlı çatışma hukuku açısından; Tallinn Manual 2.0 ise barış dönemi siber operasyonları, devlet sorumluluğu, egemenlik, kuvvet kullanımı ve meşru müdafaa gibi daha geniş başlıklar açısından önemli bir başvuru kaynağıdır (Schmitt, 2013; Schmitt, 2017). Bu nedenle siber güvenlik yalnızca teknik bir mesele olarak değil; hukuki, siyasi ve etik boyutlarıyla birlikte çok disiplinli bir yaklaşımla ele alınması gereken stratejik bir güvenlik alanı hâline gelmiştir. Siber saldırılar hem dijital sistemlerin kırılganlığını hem de mevcut uluslararası hukuk düzeninin sınırlarını görünür kılan yeni nesil tehdit unsurları arasında değerlendirilmektedir.

Bu çalışma, Estonya, Gürcistan, İran ve Ukrayna örneklerinden hareketle siber saldırıların yalnızca teknik değil, aynı zamanda uluslararası hukuk açısından nasıl bir meydan okuma oluşturduğunu ortaya koymayı amaçlamaktadır. Literatürde eksik kalan vaka temelli analizlere katkı sunan çalışma, uluslararası hukuk normlarının siber tehditler karşısındaki yetersizliğini; meşru müdafaa hakkı, egemenlik ve devlet sorumluluğu ilkeleri çerçevesinde yeniden değerlendirmektedir.

Bu doğrultuda, çalışmanın birinci bölümünde siber güvenlik kavramı ve siber saldırı türleri kuramsal bir çerçevede ele alınmaktadır. İkinci bölümde siber saldırıların uluslararası hukuk ve Birleşmiş Milletler Şartı bağlamındaki konumu, meşru müdafaa hakkı ve Tallinn Manual gibi normatif düzenlemeler ışığında ele alınmaktadır. Üçüncü bölümde Estonya, İran, Gürcistan ve Ukrayna örnekleri, nitel araştırma yöntemlerinden doküman incelemesi ve karşılaştırmalı vaka analizi tekniği kullanılarak, saldırıların yapısı, hedefleri ve devletlerin tepkileri ekseninde incelenmektedir. Son bölümde ise uluslararası örgütlerin siber güvenlik stratejileri ile ITU gibi kurumlar tarafından geliştirilen küresel endeksler değerlendirilerek, siber güvenliğin disiplinlerarası boyutu ortaya konulmaktadır.

Son yıllarda yapılan çalışmalar, siber güvenliğin yalnızca teknik değil, aynı zamanda siyasi ve hukuki bir mesele olduğunu açıkça ortaya koymuştur. Ancak bu çalışmaların önemli bir kısmı ya teknik tehditlere ya da genel normatif tartışmalara odaklanmış; vaka temelli ve karşılaştırmalı analizlere yeterince yer vermemiştir. Mevcut literatür, siber saldırıların uluslararası hukukta yarattığı yapısal boşlukları çoğu zaman teorik düzeyde ele almakta; ancak bu boşlukların devlet uygulamalarına nasıl yansıdığını sınırlı ölçüde değerlendirmektedir. Bu bağlamda çalışma, uluslararası hukukun devlet destekli siber saldırılar karşısında meşru müdafaa hakkını ve egemenlik ilkesini ne ölçüde koruyabildiğine ilişkin sorunun cevabını aramaktadır. Çalışmada, mevcut uluslararası hukuk normlarının “saldırı” kavramını büyük ölçüde fiziksel kuvvet kullanımı üzerinden değerlendirmesinin, dijital egemenliği hedef alan ancak fiziksel yıkım eşiğinin altında kalan siber operasyonlar karşısında bir “gri alan” oluşturduğu ileri sürülmektedir. Bu doğrultuda çalışma, söz konusu normatif boşluğun Estonya, Gürcistan, İran ve Ukrayna örnekleri üzerinden nasıl görünür hâle geldiğini inceleyerek akademik tartışmalara ve politika yapım süreçlerine katkı sunmayı amaçlamaktadır.

Çalışma, uluslararası ilişkilerde güvenlik olgusunu açıklamak için kullanılan iki temel yaklaşımı esas almaktadır: realizm ve konstrüktivizm. Realist yaklaşıma göre siber alan, devletlerarası güç mücadelesinin yeni bir cephesidir ve devletler bu alanda güvenliklerini sağlamak amacıyla kapasite artırımı, ittifaklar ve caydırıcılık politikaları geliştirmektedir. Konstrüktivist yaklaşım ise siber tehditlerin algılanma biçiminin uluslararası normlar ve devlet kimlikleri tarafından şekillendirildiğini savunmaktadır. Bu çerçevede siber saldırılar yalnızca teknik eylemler değil, aynı zamanda uluslararası ilişkilerde normatif yapıların yeniden üretildiği siyasi pratikler olarak da değerlendirilmektedir. Çalışma, incelenen dört vaka üzerinden bu iki yaklaşımı karşılaştırmalı olarak ele almaktadır.

## YÖNTEM

Bu çalışmada nitel araştırma yöntemi benimsenmiştir. Araştırmada doküman incelemesi ve karşılaştırmalı vaka analizi tekniklerinden yararlanılmıştır. Çalışmanın temel inceleme alanını oluşturan Estonya, Gürcistan, İran ve Ukrayna örnekleri; siber saldırıların devlet güvenliği, uluslararası hukuk ve meşru müdafaa hakkı üzerindeki etkilerini farklı boyutlarıyla ortaya koymaları nedeniyle seçilmiştir. Vaka seçiminde, farklı dönemlerde gerçekleşmelerine rağmen devlet destekli veya devletlerle ilişkilendirilen siber operasyonların uluslararası güvenlik üzerindeki etkilerinin gösterilmesi esas alınmıştır. Çalışmada ayrıca Birleşmiş Milletler Şartı, Tallinn Manual 1.0 ve 2.0, NATO’nun siber güvenlik strateji belgeleri ve Budapeşte Sözleşmesi gibi birincil hukuki kaynaklardan yararlanılmıştır. Bunun yanında, konuya ilişkin akademik çalışmalar, raporlar ve uluslararası kuruluş verileri karşılaştırmalı olarak analiz edilmiştir. Araştırmanın temel amacı, siber saldırıların uluslararası hukuk bağlamında ortaya çıkardığı normatif boşlukları vaka örnekleri üzerinden değerlendirmek ve mevcut hukuki düzenlemelerin yeterliliğini incelemektir.

## Güvenlik Kavramının Dönüşümü ve Siber Güvenlik

Güvenlik kavramı, uluslararası ilişkiler literatüründe uzun süre devletin askeri tehditlere karşı korunması ekseninde ele alınmıştır. Ancak Soğuk Savaş sonrası dönemde güvenliğin kapsamı genişlemiş; ekonomik istikrar, çevresel riskler, enerji arzı, insan güvenliği ve dijital altyapılar da güvenlik tartışmalarının bir parçası hâline gelmiştir. Bu dönüşüm, güvenliğin yalnızca askerî kapasiteyle değil, devletlerin teknolojik, kurumsal ve hukuki dayanıklılığıyla da ilişkili olduğunu göstermektedir. Siber güvenlik ise bu genişleyen güvenlik anlayışının dijital alandaki karşılığıdır. En genel anlamıyla siber güvenlik; bilgi sistemlerinin, ağların, dijital altyapıların ve verilerin yetkisiz erişim, zarar verme, manipülasyon ve kesintiye uğratma

girişimlerine karşı korunmasını ifade etmektedir. Bu çerçevede siber güvenlik, klasik güvenlik anlayışının ötesine geçen çok boyutlu bir güvenlik alanı olarak değerlendirilmektedir.

Dijitalleşmenin bireysel iletişimden kamu yönetimine, finansal işlemlerden askerî sistemlere kadar geniş bir alana yayılması, siber güvenliği devletler, kurumlar ve bireyler açısından kritik bir güvenlik meselesi hâline getirmiştir. Siber güvenlik yalnızca teknik savunma araçlarından ibaret değildir; stratejik planlama, kullanıcı farkındalığı, hukuki düzenlemeler, kurumsal kapasite ve uluslararası iş birliği gibi çok boyutlu unsurları da kapsamaktadır. Bu yönüyle siber güvenlik, bireysel gizliliğin korunmasından ulusal savunmaya kadar uzanan geniş bir güvenlik alanı oluşturmaktadır (Tunca, 2019). Bu durum, siber güvenliğin yalnızca bilişim uzmanlarının ilgi alanı olmadığını, aynı zamanda devletlerin güvenlik politikalarının temel unsurlarından biri hâline geldiğini göstermektedir. Dolayısıyla siber güvenlik, uluslararası sistemde giderek daha belirleyici bir stratejik unsur olarak öne çıkmaktadır.

Siber tehditler, bireyler ve özel kuruluşlar açısından da ciddi riskler yaratmaktadır. Bireyler açısından kimlik hırsızlığı, kişisel verilerin ele geçirilmesi, dolandırıcılık, mahremiyet ihlalleri ve dijital şantaj gibi sonuçlar ortaya çıkabilmektedir. Özel kuruluşlar açısından ise veri sızıntıları, üretim süreçlerinin durması, finansal kayıplar, itibarın zedelenmesi ve müşteri güveninin azalması gibi etkiler söz konusu olmaktadır. Bu nedenle siber güvenlik, yalnızca devletlerin ulusal güvenlik politikalarıyla sınırlı değil; ekonomik istikrar, toplumsal güven ve dijital hizmetlerin sürdürülebilirliği açısından da stratejik bir zorunluluk olarak değerlendirilmektedir (Sertçelik, 2018). Siber tehditlerin etkisi yalnızca teknik zararlarla sınırlı kalmamakta; ekonomik ve toplumsal düzen üzerinde de doğrudan etkiler yaratmaktadır. Bu yönüyle siber güvenlik, modern toplumların sürdürülebilirliği açısından kritik bir güvenlik alanı hâline gelmiştir.

Siber saldırıların fiziksel sınır tanımaması, devletleri ve kritik altyapıları sürekli olarak risk altında bırakmaktadır. Kamu kurumları, enerji sistemleri, finansal ağlar, sağlık hizmetleri, ulaşım altyapıları ve iletişim sistemleri siber saldırganlar için öncelikli hedefler arasında yer almaktadır. Bu alanlara yönelik saldırılar yalnızca teknik aksamalara yol açmamakta; kamu hizmetlerinin kesintiye uğraması, ekonomik faaliyetlerin zarar görmesi ve toplumsal düzenin bozulması gibi geniş kapsamlı sonuçlar doğurabilmektedir. Bu nedenle siber güvenlik, bireysel bir tehdit alanı olmaktan çıkarak devletlerin ulusal güvenliğini doğrudan etkileyen bir unsur hâline gelmiştir. Avrupa Birliği'nin siber güvenlik alanında ortak standartlar geliştirmeye yönelmesi de dijital altyapıların korunmasının artık uluslararası düzeyde ele alınan bir güvenlik meselesi olduğunu göstermektedir (Nezgitli ve Benzer, 2020). Bu gelişmeler, devletlerin yalnızca ulusal düzeyde değil, uluslararası iş birliği mekanizmaları aracılığıyla da hareket etmek zorunda olduğunu ortaya koymaktadır. Siber tehditlerin sınır aşan yapısı, ortak güvenlik politikalarının önemini giderek artırmaktadır.

Siber tehditlerle mücadele yalnızca yazılımsal çözümlerle sağlanamaz. Etkili bir siber güvenlik politikası; teknik savunma sistemlerinin yanında kurumsal koordinasyon, kriz yönetimi, hukuki düzenleme ve uluslararası iş birliği kapasitesini de gerektirmektedir. Gençoğlu'na göre siber olaylara müdahale süreçleri, her olayın kendine özgü yapısı dikkate alınarak yürütülmelidir (2021: 479). Bu bağlamda ülkelerin siber olaylara müdahale ekiplerine, yani Computer Emergency Response Team (CERT) yapılarına yatırım yapmaları ve artan küresel tehditler karşısında uluslararası iş birliklerini güçlendirmeleri önem taşımaktadır. Uluslararası ilişkiler açısından bakıldığında, siber güvenlik giderek bir diplomasi, caydırıcılık ve güç kapasitesi alanına dönüşmektedir. Devletlerin siber kapasite geliştirme yarışına girmesi ve bu alanda çeşitli ittifaklar oluşturması, siber alanın yeni bir rekabet zemini hâline geldiğini

göstermektedir (Güntay, 2018). Bu durum, siber güvenliğin yalnızca savunma politikalarının değil, dış politika stratejilerinin de önemli bir parçası hâline geldiğini göstermektedir. Dolayısıyla siber kapasite, devletlerin uluslararası sistemdeki konumunu etkileyen stratejik unsurlardan biri olarak değerlendirilmektedir.

Uluslararası kuruluşlar, siber güvenlik alanında ortak standartlar oluşturma ve devletler arasında iş birliğini artırma çabası içindedir. NATO'nun siber güvenlik stratejileri ve bu kapsamda kurulan NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), bu kurumsallaşma sürecinin önemli örnekleri arasında yer almaktadır. Bu tür yapılar, devletlerin siber güvenlik kapasitelerini geliştirmelerine katkı sağlamakta ve uluslararası normların oluşumunu desteklemektedir (Kışman ve Güleç, 2021). Buna karşın siber güvenlik alanı, uluslararası hukukla tam uyumlu ve bağlayıcı bir yapıya henüz kavuşmuş değildir. Siber olayların mevcut hukuk normlarıyla tam anlamıyla örtüşmemesi, caydırıcılığı azaltmakta ve failerin cezalandırılmasını zorlaştırmaktadır. Bu nedenle siber saldırıların hukuki açıdan daha açık biçimde tanımlanması, devletlerarası iş birliğini ve uluslararası caydırıcılığı güçlendirme bakımından kritik önem taşımaktadır (Gürkaynak ve İren, 2011). Mevcut hukuki boşluklar, siber saldırıların uluslararası sistemde neden tartışmalı bir alan olarak kaldığını açıkça göstermektedir. Bu nedenle siber güvenlik alanında daha kapsamlı ve bağlayıcı uluslararası düzenlemelere duyulan ihtiyaç giderek artmaktadır.

### ***Siber Saldırı ve Siber Sabotaj Kavramları***

Dijitalleşmenin hız kazanmasıyla birlikte çevrimiçi tehditlerin niteliği ve kapsamı da önemli ölçüde değişmiştir. Siber saldırı ve siber sabotaj kavramları, bilgi sistemlerini hedef alan zararlı faaliyetleri ifade etmekle birlikte; amaçları, yöntemleri ve ortaya çıkardıkları sonuçlar bakımından farklı özellikler taşımaktadır. Siber saldırılar genel olarak veri ele geçirmek, sistem işleyişini aksatmak, hizmet kesintisi oluşturmak veya dijital altyapılara zarar vermek amacıyla gerçekleştirilen kötü niyetli müdahaleler olarak tanımlanmaktadır (Yayla, 2014). Siber sabotaj ise daha çok kritik sistemleri işlevsiz hâle getirmeyi, fiziksel hasar oluşturmayı veya ekonomik süreçleri sekteye uğratmayı hedefleyen yıkıcı operasyonları ifade etmektedir (Acar, 2019: 15). Bu yönüyle siber sabotajın, klasik siber saldırılara kıyasla daha stratejik ve uzun vadeli sonuçlar doğurabildiği görülmektedir.

Kritik altyapıların dijital sistemlerle bütünleşmesi, siber sabotaj faaliyetlerinin ulusal güvenlik açısından daha ciddi sonuçlar doğurmasına neden olmuştur. Enerji santralleri, ulaşım ağları, sağlık sistemleri, iletişim altyapıları ve finansal ağlar gibi alanlar, siber saldırganlar açısından öncelikli hedefler arasında yer almaktadır. Özellikle endüstriyel kontrol sistemlerine yönelik saldırılar, yalnızca veri kaybına değil; fiziksel ekipmanların devre dışı kalmasına, üretim süreçlerinin durmasına ve kamu hizmetlerinde ciddi aksamalara yol açabilmektedir. Nitekim İran'ın nükleer tesislerini hedef alan Stuxnet saldırısı, siber sabotajın fiziksel sonuçlar doğurabileceğini gösteren en önemli örneklerden biri olarak değerlendirilmektedir. Bu tür saldırılar, siber tehditlerin yalnızca teknik bir güvenlik problemi olmadığını; aynı zamanda ekonomik, siyasi ve stratejik sonuçlar doğurabilen hibrit tehdit unsurları hâline geldiğini göstermektedir.

Siber saldırıların çoğu zaman sınır aşan bir yapıya sahip olması, tehditlerin uluslararası boyut kazanmasına neden olmaktadır. Devlet destekli gruplar, organize suç ağları ve bağımsız hacker toplulukları tarafından gerçekleştirilen saldırılar, hedef ülkelerin kamu düzenini ve ulusal güvenliğini doğrudan etkileyebilmektedir. Özellikle kritik altyapılara yönelik saldırılar, enerji arzının kesintiye uğraması, finansal işlemlerin durması ve iletişim sistemlerinin çökmesi gibi sonuçlar doğurarak toplumsal istikrarı tehdit edebilmektedir. Bu durum, devletlerin

güvenlik politikalarında siber tehditlere karşı daha kapsamlı savunma stratejileri geliştirmesini zorunlu hâle getirmiştir (Sandilaç, 2022). Dolayısıyla siber saldırılar, yalnızca dijital sistemlere yönelik teknik müdahaleler olarak değil, uluslararası güvenlik dengelerini etkileyebilen stratejik operasyonlar olarak da değerlendirilmektedir.

Bu gelişmeler, siber güvenliğin yalnızca teknik önlemlerle sınırlandırılmayacağını açıkça ortaya koymaktadır. Siber saldırılar ve siber sabotaj faaliyetleri, hukuki düzenlemelerden kurumsal koordinasyona, toplumsal farkındalıktan uluslararası iş birliğine kadar uzanan çok boyutlu tedbirleri gerekli kılmaktadır. Teknik savunma mekanizmalarının yanında hukuki ve diplomatik araçların geliştirilmesi de siber tehditlerle mücadelede giderek daha önemli hâle gelmektedir. Çünkü siber tehditler yalnızca bilgi sistemlerini değil; ekonomik düzeni, kamu güvenliğini ve bireylerin temel haklarını da doğrudan etkileyebilecek kapasiteye sahiptir (Cengiz, 2021; Çakır ve Taşer, 2023: 348). Bu nedenle siber saldırılar, çağdaş güvenlik çalışmalarının merkezinde yer alan çok boyutlu bir güvenlik sorunu olarak değerlendirilmektedir.

### ***Siber Saldırı Türleri***

Dijital teknolojilerin gelişmesiyle birlikte siber saldırı yöntemleri de çeşitlenmiş ve daha karmaşık bir yapıya dönüşmüştür. Günümüzde siber saldırılar yalnızca bireysel kullanıcıları değil; devlet kurumlarını, askerî sistemleri, enerji altyapılarını, finans kuruluşlarını ve iletişim ağlarını da hedef alabilmektedir. Bu durum, siber saldırıların uluslararası güvenlik açısından stratejik bir tehdit unsuru hâline gelmesine neden olmuştur. Özellikle devlet destekli siber operasyonların artış göstermesi, siber uzayın klasik savaş alanlarının ötesinde yeni bir mücadele alanı olarak değerlendirilmesine yol açmıştır.

Siber saldırılar, verileri ele geçirmek, sistemleri devre dışı bırakmak, kritik altyapıları hedef almak, kamu düzenini bozmak veya stratejik üstünlük sağlamak amacıyla gerçekleştirilebilmektedir. Bu saldırılar bağımsız hacker grupları, organize suç örgütleri veya doğrudan devlet destekli yapılar tarafından gerçekleştirilebilmektedir (Özdemir, 2025). Özellikle kritik altyapılara yönelik saldırılar, yalnızca dijital sistemleri değil; ekonomik istikrarı, kamu güvenliğini ve toplumsal düzeni de etkileyebilecek sonuçlar ortaya çıkarmaktadır. Bu nedenle siber saldırılar, yalnızca teknik bir problem değil; aynı zamanda siyasi, ekonomik ve stratejik boyutları bulunan çok katmanlı güvenlik tehditleri olarak değerlendirilmektedir.

Siber saldırı yöntemleri zaman içerisinde gelişmiş, teknik kapasiteleri artmış ve daha geniş ölçekli sonuçlar doğurmaya başlamıştır. Günümüzde en yaygın siber saldırı türleri arasında hizmet dışı bırakma saldırıları, zararlı yazılımlar, siber casusluk faaliyetleri ve sistemlere gizlice yerleştirilen arka kapı mekanizmaları yer almaktadır. Bu saldırı türleri, hedef alınan sistemin yapısına göre farklı sonuçlar doğurabilmekte ve devletlerin güvenlik politikalarını doğrudan etkileyebilmektedir.

Saldırı yöntemleri zaman içinde çeşitlenmiş, karmaşıklaşmış ve etkileri artmıştır. Başlıca siber saldırı türleri şu şekilde sıralanabilir:

- **Hizmet Dışı Bırakma (DDoS) Saldırıları:** Belirli bir sistemi aşırı trafikle hedef olarak hizmet veremez hâle getirmeyi amaçlayan saldırılardır. Bu tür saldırılarda genellikle devlet kurumları, bankalar ve medya kuruluşları hedef alınmaktadır (Öztürk vd., 2025).

- Zararlı Yazılımlar: Bilgi sistemlerine zarar vermek veya veri ele geçirmek amacıyla geliştirilen virüs, solucan, Truva atı ve rootkit gibi yazılımlar kullanılmaktadır (Kara, 2015).
- Siber Casusluk: Bilgi toplama amacıyla gerçekleştirilen gizli siber saldırılar olup, özellikle devletlerin kritik ve stratejik verileri hedef alınmaktadır (Kara, 2015).
- Mantık Bombaları ve Arka Kapılar: Sistemlere gizlice yerleştirilen ve belirli koşullar gerçekleştiğinde zararlı etki yaratan yazılımlar olarak tanımlanır (Kara, 2015).

Zararlı yazılımlar yalnızca hedef sistemlere doğrudan zarar vermekle sınırlı kalmamakta, aynı zamanda saldırıların yayılma hızını ve etki alanını da artırmaktadır. Solucanlar, botnetler ve keyloggerlar gibi araçlar, saldırganlara geniş ağlara erişim sağlama, kullanıcı bilgilerini ele geçirme ve sistemleri uzaktan kontrol etme imkânı vermektedir. Bu durum, siber saldırıların teknik kapasitesini artırmakta ve tekil bir güvenlik ihlalinin kısa sürede daha geniş ölçekli bir krize dönüşmesine neden olabilmektedir. Bu nedenle zararlı yazılımlar ve DDoS saldırıları siber güvenlik literatüründe en yaygın ve etkili saldırı türleri arasında değerlendirilmektedir.

Siber saldırılar yalnızca sanal ortamda sonuç doğuran müdahaleler değildir; bazı durumlarda fiziksel dünyada da ciddi güvenlik riskleri ortaya çıkarabilmektedir. İnternet altyapıları, enerji santralleri, ulaşım sistemleri, sağlık ağları ve askerî savunma yapıları siber saldırıların hedefi hâline geldiğinde, saldırının etkisi dijital sistemlerin ötesine taşmaktadır. Özellikle kritik altyapılara yönelik saldırılar, kamu hizmetlerinin kesintiye uğramasına, ekonomik faaliyetlerin zarar görmesine ve toplumsal güvenliğin zayıflamasına yol açabilmektedir. Bu nedenle siber saldırıların doğası, yalnızca dijital değil; fiziksel, ekonomik ve stratejik sonuçlar doğurabilen çok boyutlu bir güvenlik tehdidi olarak değerlendirilmelidir.

### **Uluslararası Hukuk ve BM Şartı Ekseninde Siber Saldırıları ve Meşru Müdafaa**

Siber saldırılar, klasik savaş hukuku çerçevesinde tam olarak tanımlanamadığından uluslararası hukuk açısından tartışmalı bir alan oluşturmaktadır. Siber uzayda gerçekleştirilen eylemler; silahlı saldırı, casusluk, sabotaj veya propaganda gibi farklı nitelikler taşıyabilmektedir. Ancak bu eylemlerin hangi koşullarda uluslararası hukuk ihlali sayılacağı konusunda ortak bir görüş bulunmamaktadır. Özellikle Birleşmiş Milletler Şartı'nın 2. maddesi, kuvvet kullanma yasağı ve devletlerin egemen eşitliği ilkeleri açısından 51. maddesi, silahlı saldırı hâlinde meşru müdafaa hakkı bakımından temel bir hukuki çerçeve sunmaktadır (United Nations, 1945, arts. 2, 51). Buna rağmen, fiziki bir saldırı ile siber bir saldırının hukuki açıdan eşdeğer olup olmadığı hâlâ tartışmalıdır. Uluslararası hukukta “silahlı saldırı” kavramı çoğunlukla fiziksel kuvvet kullanımıyla sınırlandırılarak dar bir biçimde yorumlanmaktadır (Gürkaynak ve İren, 2011). Bu nedenle siber saldırıların silahlı saldırı kapsamında değerlendirilmesi, genellikle ciddi altyapı hasarı veya can kaybı gibi sonuçların ortaya çıkmasıyla ilişkilendirilmektedir. Tallinn Manual'a göre bir siber operasyonun meşru müdafaa hakkını doğuran “silahlı saldırı” seviyesine ulaşmış olması, saldırının ölçeği ve etkileri dikkate alınarak değerlendirilmelidir (Schmitt, 2013; Schmitt, 2017). Bu belirsizlik, meşru müdafaa hakkının uygulanması konusunda önemli tartışmalara yol açmakta ve normatif düzenleme ihtiyacını artırmaktadır (Karadağ, 2016).

NATO'nun siber güvenlik alanındaki yaklaşımı, özellikle 2016 Varşova Zirvesi sonrasında daha kurumsal bir boyut kazanmıştır. NATO'nun 8–9 Temmuz 2016 tarihli Warsaw Summit Communiqué belgesinde, siber uzayın kara, deniz ve hava gibi ayrı bir “operasyon

alanı” olarak kabul edildiği açıklanmıştır (NATO, 2016, para. 70). Belgede ayrıca siber saldırıların modern toplumlar açısından konvansiyonel saldırılar kadar yıkıcı sonuçlar doğurabileceği vurgulanmış ve siber savunmanın NATO’nun kolektif savunma politikalarının önemli bir parçası olduğu ifade edilmiştir. Bu yaklaşım, ciddi siber saldırıların belirli koşullar altında NATO’nun ortak savunma mekanizmalarını gündeme getirebileceğini göstermektedir. Bununla birlikte, hangi tür siber saldırıların kolektif savunmayı tetikleyecek düzeyde değerlendirileceği konusu hâlen uluslararası hukuk ve güvenlik literatüründe tartışmalı bir alan olarak varlığını sürdürmektedir. Bu durum, siber saldırıların hukukî niteliğinin belirlenmesinde yaşanan belirsizliklerin devam ettiğini göstermektedir.

Uluslararası hukuk açısından siber saldırılar üzerine tartışılan bir diğer temel mesele, saldırının hangi aktör tarafından gerçekleştirildiğinin tespit edilmesidir. Siber saldırıların failinin belirlenmesindeki güçlük, uluslararası hukuki sorumluluğun ortaya konulmasını önemli ölçüde zorlaştırmaktadır. Saldırıların çoğu zaman üçüncü taraflar, sahte IP adresleri, botnet ağları veya vekil aktörler üzerinden gerçekleştirilmesi, hedef devletin doğrudan sorumluluk atfetmesini güçleştirmektedir. Bu durum, devletlerin karşılık verme, yaptırım uygulama veya meşru müdafaa hakkına başvurma kapasitesini sınırlamaktadır (Sandilaç, 2022). Failin kesin biçimde tespit edilememesi, yalnızca devletlerin değil, NATO gibi kolektif savunma mekanizmalarının da caydırıcılık kapasitesini zayıflatmaktadır (Dilek vd., 2023). 2007 Estonya saldırıları bu duruma çarpıcı bir örnek teşkil etmektedir. Saldırıların Rusya ile ilişkilendirilmesine rağmen doğrudan bir devlet sorumluluğu ortaya konulamaması, siber alanda isnat sorununun uluslararası hukuk bakımından ne kadar kritik olduğunu göstermiştir. Bununla birlikte, bu olay NATO ve Avrupa Birliği başta olmak üzere uluslararası kuruluşların siber güvenlik alanında daha kurumsal ve proaktif düzenlemelere yönelmesine zemin hazırlamıştır.

Siber saldırılar, devletlerin egemenlik haklarını ve uluslararası hukuk çerçevesinde sahip oldukları meşru müdafaa hakkını zorlayan yeni bir tehdit unsuru olarak öne çıkmaktadır. BM Şartı’nın 2. maddesi, devlet egemenliğine saygıyı temel ilke olarak düzenlemekte ve bir devletin başka bir devletin içişlerine müdahalesini yasaklamaktadır. Ancak dijital çağda kritik altyapıları hedef alan siber saldırılar fiilî bir müdahale niteliği taşıyabilmektedir. Şart’ın 51. maddesi ise silahlı saldırı hâlinde meşru müdafaa hakkını tanımaktadır. Günümüzde enerji santrallerinin devre dışı bırakılması gibi ağır sonuçlar doğuran siber saldırıların, belirli koşullarda silahlı saldırı kapsamında değerlendirilebileceği kabul edilmektedir. Bununla birlikte, saldırının kaynağının tespitindeki zorluk bu hakkın fiilen kullanılmasının önündeki en büyük engeli oluşturmaktadır. Dijital ortamda gerçekleşen müdahaleler, fiziki saldırılar kadar yıkıcı sonuçlar doğurabilmekte ve uluslararası hukuku bu yeni gerçekliğe uyum sağlamaya zorlamaktadır (Karadağ, 2016).

Meşru müdafaa, devletlerin varoluşsal bir hakkı olmakla birlikte, siber saldırıların görünmez ve karmaşık yapısı bu hakkın uygulanmasını güçleştirmektedir. Failin belirlenmemesi ve karşılık verme eyleminin orantılılık ilkesiyle uyumlu olup olmadığı gibi temel kriterler, dijital ortamda daha tartışmalı hâle gelmektedir. Özellikle devlet destekli siber saldırılarda teknik izlerin silinmesi, hedef devletin meşru müdafaa gerekçesiyle gerçekleştireceği karşı hamlenin hukukiliğini belirsizleştirmektedir. Bu durum, teknolojik gelişmelerle birlikte meşru müdafaa kavramının uluslararası hukuk içindeki konumunun giderek daha karmaşık hâle geldiğini göstermektedir. Dijital çağda “saldırı” kavramının yalnızca fiziksel müdahalelerle sınırlı kalmaması, uluslararası güvenlik anlayışında önemli bir dönüşüm yaratmıştır. Bu durum, uluslararası hukuk normlarının dijital tehditlere uyum sağlayacak şekilde yeniden değerlendirilmesini zorunlu kılıyor.

## Küresel Örneklerle Siber Saldırıları ve Etkileri

Siber saldırılar artık yalnızca teknik bir sorun değil, uluslararası siyasetin ve güvenliğin merkezine oturmuş bir tehdit türüdür. Günümüzde hiçbir ülke bu dijital tehditlerden tamamen bağımsız değildir. Bu nedenle küresel düzeyde yaşanan örnekler, bu meselenin boyutlarının daha iyi anlaşılmasına katkı sağlamaktadır. Dünyada artan dijitalleşme süreci, siber güvenlik sorunlarını küresel bir öncelik hâline getirmiştir. Özellikle devlet ve hacker grupları arasında yaşanan siber saldırılar, yalnızca teknik değil; aynı zamanda siyasi ve hukuki krizlere de neden olabilmektedir. Bu bölümde ele alınacak örnekler, siber saldırıların ne kadar stratejik, yıkıcı ve çok boyutlu etkiler doğurabileceğini göstermesi açısından önemlidir (Şafak, 2020). Özdemir’e göre siber alanın sınır tanımayan yapısı, siber saldırıları yalnızca teknik bir sorun olmaktan çıkarmış; ulusal güvenlik ve uluslararası istikrar açısından stratejik bir tehdit hâline getirmiştir. Bu nedenle siber tehditlerin yalnızca teknik önlemlerle değil, hukuk, diplomasi ve savunma stratejileriyle birlikte ele alınması gerektiği belirtilmektedir (Özdemir, 2025). Bu durum, siber güvenliğin çok disiplinli bir yaklaşım gerektirdiğini ve devletlerin yalnızca teknolojik önlemlerle yetinmemesi gerektiğini açıkça göstermektedir. Ayrıca, uluslararası arenada iş birliği ve hukuki düzenlemelerin öneminin giderek arttığına dikkat çekmektedir.

### *Estonya*

Estonya’da 2007 yılında yaşanan siber saldırılar, dijital çağda güvenlik anlayışının dönüşümünü gösteren en önemli örneklerden biri olarak değerlendirilmektedir. Bu saldırılar, siber güvenliğin yalnızca teknik bir mesele olmadığını; siyasi, hukuki ve stratejik sonuçlar doğuran çok boyutlu bir güvenlik sorunu olduğunu ortaya koymuştur. Estonya örneği, birçok devletin savunma politikalarını dijital tehditleri de kapsayacak biçimde yeniden değerlendirmesine zemin hazırlamıştır.

Dilek, Talih ve Bensghir’e göre 2007 yılında Estonya’da yaşanan siber saldırılar, dijital altyapısı gelişmiş bir devletin kamu kurumları, bankacılık sistemi, medya kuruluşları ve iletişim ağları üzerinden eş zamanlı biçimde hedef alınabildiğini gösteren modern dönemde devlet ölçeğinde gerçekleşen ilk geniş çaplı siber saldırı örneklerinden biri olarak değerlendirilmektedir. Saldırıları, Estonya hükümetinin başkent Tallinn’de bulunan Sovyetler Birliği dönemine ait “Bronz Asker” heykelini şehir dışına taşıma kararı almasının ardından başlamıştır. Bronz asker heykeli, Sovyetler Birliği döneminde II. Dünya Savaşı’nda hayatını kaybeden Kızıl Ordu askerlerini anmak amacıyla dikilmiş bir savaş anıtıdır. Ancak bu anıt, Estonya toplumunda farklı tarihsel anlamlara sahiptir. Estonya’daki Rus azınlık açısından Nazi Almanyası’na karşı kazanılan zaferi ve Sovyet savaş hafızasını temsil ederken, birçok Estonyalı için Sovyet işgalini ve baskı dönemini hatırlatan tartışmalı bir sembol olarak görülmektedir. Bu nedenle heykelin Tallinn merkezinden taşınması, yalnızca idari bir karar değil; Estonya’nın ulusal hafızası, kimlik politikası ve Rusya ile ilişkileri açısından sembolik bir kırılma noktası olmuştur (Contested Histories, 2021). Bu karar, ülkedeki Rus azınlığın protestolarına ve Moskova’nın sert tepkisine neden olmuş; kısa süre sonra Estonya’nın devlet kurumları, parlamentosu, medya kuruluşları, bankaları ve diğer kritik dijital altyapıları yoğun DDoS saldırılarına maruz kalmıştır (Dilek, Talih ve Bensghir, 2023). Nitekim Estonya örneği, tarihsel hafıza krizinin kısa sürede dijital güvenlik krizine dönüşebildiğini ve siber saldırıların uluslararası siyasette sembolik gerilimlerle doğrudan ilişkilendirilebildiğini göstermektedir.

Bu gelişmeler, Estonya vakasının yalnızca teknik bir siber saldırı örneği olarak değil, uluslararası güvenlik ve hukuk açısından dönüştürücü bir olay olarak değerlendirilmesini gerekli kılmaktadır. 2007 saldırıları, Sovyet dönemine ait Bronz Asker heykelinin taşınmasıyla başlayan tarihsel hafıza ve kimlik krizinin kısa sürede dijital alana taşınmasıyla ortaya çıkmıştır.

Bu yönüyle saldırılar, siber güvenliğin yalnızca teknik bir altyapı meselesi olmadığını; tarihsel gerilimler, ulusal kimlik, azınlık politikaları ve devletlerarası ilişkilerle doğrudan bağlantılı olduğunu göstermiştir.

Saldırıların hedefleri oldukça geniş bir alana yayılmıştır. Estonya'nın hükümet ve parlamento siteleri, bakanlık portalları, medya kuruluşları, internet servis sağlayıcıları, bankacılık sistemleri ve bazı iletişim altyapıları eşzamanlı biçimde hedef alınmıştır. Saldırıların önemli bir bölümü DDoS niteliği taşımış; yoğun trafik yönlendirmesiyle kamu hizmetlerine, haber akışına ve çevrim içi bankacılık işlemlerine erişim zorlaştırılmıştır. CCDCOE tarafından yayımlanan analizlerde, saldırıların çoğunun kamuya açık web siteleri ve e-posta hizmetleri gibi alanlara yöneldiği; ancak çevrim içi bankacılık ve DNS gibi daha kritik hizmetlerin de hedef alındığı belirtilmektedir (Ottis, 2008). Bu nedenle Estonya vakası, dijitalleşmiş bir devletin kamu hizmetleriyle finansal altyapısının aynı anda hedef alınması bakımından erken dönem ve çarpıcı bir örnek oluşturmıştır.

Saldırıların arkasında doğrudan Rusya Federasyonu'nun bulunduğu ilişkin güçlü siyasi şüpheler ortaya çıkmış; ancak uluslararası hukuk açısından devlet sorumluluğunu kesin biçimde ortaya koyabilecek doğrudan deliller sunulamamıştır. Bu durum, Estonya vakasını siber saldırılarda “isnat sorunu” açısından klasik örneklerden biri hâline getirmiştir. Siber saldırıların farklı ülkelerden yönlendirilmesi, botnet ağlarının kullanılması ve saldırganların kimliklerini gizleyebilmesi, failin tespitini zorlaştırmıştır. Bu belirsizlik, meşru müdafaa hakkının kullanımı, devlet sorumluluğunun belirlenmesi ve caydırıcılık stratejilerinin uygulanması bakımından ciddi bir hukuki boşluk doğurmuştur.

Estonya saldırılarının en önemli sonuçlarından biri, NATO'nun siber güvenlik alanındaki kurumsal kapasite geliştirme sürecini hızlandırmasıdır. Her ne kadar Estonya, NATO'ya katıldıktan sonra 2004 yılında bir siber savunma mükemmeliyet merkezi kurulması fikrini önermiş olsa da 2007 saldırıları bu ihtiyacın somut ve acil olduğunu göstermiştir. Bu süreç sonucunda NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Estonya'nın girişimi ve Almanya, İtalya, Letonya, Litvanya, Slovakya ve İspanya'nın katılımıyla 14 Mayıs 2008'de Tallinn'de kurulmuştur. Merkez, aynı yıl NATO tarafından akredite edilmiş ve uluslararası askerî örgüt statüsü kazanmıştır (CCDCOE, n.d.). Bu nedenle Estonya saldırıları, NATO'nun siber savunma yaklaşımında bir kırılma noktası olarak değerlendirilmektedir.

CCDCOE'nin kurulması, yalnızca teknik savunma kapasitesinin artırılması açısından değil, siber saldırıların uluslararası hukuk açısından nasıl değerlendirileceği sorusunun kurumsal düzeyde tartışılması bakımından da önemlidir. Nitekim Tallinn Manual süreci, siber operasyonlara uygulanabilir uluslararası hukuk kurallarının açıklığa kavuşturulması amacıyla uluslararası hukuk uzmanlarının katkısıyla geliştirilmiştir. Tallinn Manual 1.0, siber savaş ve silahlı çatışma hukuku bakımından; Tallinn Manual 2.0 ise barış zamanı siber operasyonları, egemenlik, devlet sorumluluğu, kuvvet kullanımı ve meşru müdafaa gibi daha geniş başlıklar bakımından önemli bir referans noktası oluşturmıştır (Schmitt, 2013; Schmitt, 2017). Bu çerçevede Estonya vakası, yalnızca bir saldırı örneği değil, siber güvenliğin uluslararası hukuk ve NATO güvenlik mimarisi içinde kurumsallaşmasını hızlandıran bir dönüm noktasıdır.

Bu vaka teorik açıdan değerlendirildiğinde, krizin tarihsel hafıza ve kimlik tartışması üzerinden başlaması konstrüktivist yaklaşım açısından önemlidir. Bronz Asker heykeli etrafında şekillenen sembolik gerilim, siber saldırıların yalnızca teknik çıkar veya askerî kapasite üzerinden değil, kimlik, algı ve tarihsel anlamlar üzerinden de şekillenebildiğini göstermektedir. Buna karşılık saldırı sonrasında NATO'nun kurumsal kapasitesini artırması,

CCDCOE'nin kurulması ve Tallinn Manual sürecinin hız kazanması, realist açıdan devletlerin ve ittifakların yeni tehdit alanlarına karşı güvenlik kapasitelerini güçlendirme eğilimini ortaya koymaktadır. Bu nedenle Estonya örneği, siber güvenliğin hem normatif hem de stratejik boyutlarını birlikte gösteren kurucu vakalardan biri olarak değerlendirilebilir.

### *İran – Stuxnet*

Siber saldırılar, günümüzde yalnızca dijital sistemlerde veri kaybına yol açan teknik tehditler olmaktan çıkmış; kritik altyapıları hedef alabilen ve fiziksel sonuçlar doğurabilen stratejik güvenlik risklerine dönüşmüştür. Bu dönüşümün en dikkat çekici örneklerinden biri Stuxnet saldırısıdır. Stuxnet vakası, siber operasyonların yalnızca bilgi sistemlerini değil, doğrudan fiziksel altyapıları da hedef alabileceğini göstermesi bakımından uluslararası güvenlik literatüründe önemli bir kırılma noktası olarak değerlendirilmektedir.

2010 yılında İran'ın Natanz Nükleer Tesisi'nde tespit edilen Stuxnet adlı zararlı yazılım, Siemens tarafından geliştirilen SCADA sistemlerini hedef alacak şekilde tasarlanmıştır. Yazılım, uranyum zenginleştirme sürecinde kullanılan santrifüjlerin çalışma hızını manipüle ederek sistemlerin fiziksel olarak zarar görmesine yol açmıştır. İranlı yetkililer, saldırı sonucunda santrifüjlerin yaklaşık beşte birinin işlevsiz hâle geldiğini açıklamıştır (Sandilaç, 2022). Bu durum, siber saldırıların yalnızca veri ihlali veya sistem kesintisi oluşturmadığını; enerji ve nükleer tesisler gibi kritik altyapılar üzerinde doğrudan fiziksel tahribat yaratabildiğini göstermiştir.

Natanz Tesisi, İran'ın nükleer programının en önemli merkezlerinden biri olarak kabul edilmektedir. Tesiste yürütülen uranyum zenginleştirme faaliyetleri, İran'ın nükleer kapasitesinin geliştirilmesinde stratejik bir rol oynamaktadır. Bu nedenle tesisin hedef alınması, yalnızca teknik bir sabotaj girişimi değil; İran'ın nükleer programını yavaşlatmaya yönelik stratejik bir müdahale olarak değerlendirilmiştir. Her ne kadar saldırının sorumluluğu resmî olarak hiçbir devlet tarafından üstlenilmemiş olsa da, uluslararası literatürde operasyonun ABD ve İsrail iş birliğiyle gerçekleştirildiğine ilişkin güçlü iddialar bulunmaktadır. Özellikle “Olympic Games Operasyonu” kapsamında geliştirildiği ileri sürülen Stuxnet'in, devlet destekli ilk büyük ölçekli siber sabotaj operasyonlarından biri olduğu değerlendirilmektedir.

Stuxnet saldırısı sonrasında İran, kritik altyapılarının siber güvenliğini artırmaya yönelik daha kapsamlı politikalar geliştirmeye başlamıştır. İran yönetimi, saldırıyı yalnızca teknik bir güvenlik sorunu olarak değil, doğrudan ulusal güvenliği hedef alan stratejik bir tehdit olarak değerlendirmiştir. Bu süreçte İran'ın yerli siber güvenlik kapasitesini geliştirmeye, kritik tesislerde dışa bağımlılığı azaltmaya ve siber savunma altyapısını güçlendirmeye yönelik adımlar attığı görülmektedir. Böylece Stuxnet saldırısı, yalnızca hedef alınan sistemler üzerinde değil, İran'ın güvenlik politikaları ve savunma anlayışı üzerinde de uzun vadeli etkiler yaratmıştır.

Saldırının ardından uluslararası hukuk literatüründe, bu tür siber operasyonların “silahlı saldırı” kapsamında değerlendirilip değerlendirilemeyeceği yoğun biçimde tartışılmıştır. Bu bağlamda Schmitt'in etki temelli yaklaşımı ile Tallinn Manual'de ortaya konan fiziksel yıkım ölçütü çerçevesinde yapılan değerlendirmelerde, Stuxnet'in santrifüjlerde doğrudan maddi hasar meydana getirmesi nedeniyle “silahlı saldırı” kategorisine dâhil edilebileceğini savunan görüşler ön plana çıkmıştır (Nezgitli ve Benzer, 2020). Nitekim Tallinn Manual'de fiziksel hasar doğuran siber operasyonların belirli koşullar altında kuvvet kullanımı veya silahlı saldırı kapsamında değerlendirilebileceği ifade edilmektedir (Schmitt, 2013; Schmitt, 2017). Buna karşın saldırının arkasında doğrudan bir devletin bulunduğu kesin biçimde

kanıtlanamaması, meşru müdafaa hakkının sınırlarını daha tartışmalı hâle getirmiştir. Bu durum, siber saldırılarda “isnat sorununun” uluslararası hukuk açısından ne kadar kritik olduğunu göstermektedir.

Stuxnet vakası sonrasında devletlerin kritik altyapı güvenliğine yönelik yaklaşımı önemli ölçüde değişmiştir. Enerji tesisleri, ulaşım sistemleri, nükleer altyapılar ve endüstriyel kontrol mekanizmaları siber güvenlik politikalarının merkezine yerleşmiştir. Bu olay, siber operasyonların fiziksel yıkım oluşturabilme kapasitesi nedeniyle klasik güvenlik anlayışını dönüştürmüş ve devletlerin siber caydırıcılık stratejilerine daha fazla yatırım yapmasına yol açmıştır. Böylece Stuxnet, yalnızca teknik bir siber operasyon değil; uluslararası hukuku, devletlerin güvenlik politikalarını ve stratejik savunma anlayışını etkileyen küresel ölçekte bir dönüm noktası hâline gelmiştir.

Bu vaka teorik açıdan değerlendirildiğinde, Stuxnet saldırısı realist yaklaşımın siber güvenlik alanındaki açıklayıcılığını güçlendirmektedir. Çünkü saldırı, devletlerin rakiplerinin stratejik ve askerî kapasitesini doğrudan savaş ilan etmeden zayıflatmak amacıyla siber araçları kullanabildiğini göstermektedir. İran’ın nükleer programının hedef alınması, siber alanın devletlerarası güç mücadelesinin yeni bir cephesine dönüştüğünü ortaya koymaktadır. Konstrüktivist açıdan bakıldığında, Stuxnet İran’ın nükleer faaliyetlerinin uluslararası toplumda nasıl bir tehdit algısı ürettiğini ve bu algının siber müdahaleleri meşrulaştıran bir güvenlik söylemine dönüşebildiğini göstermektedir. Bu nedenle Stuxnet vakası, siber saldırıların hem maddi güç dengeleri hem de tehdit algıları üzerinden şekillendiğini ortaya koyan önemli bir örnek olarak değerlendirilebilir.

### ***Gürcistan***

Siber saldırılar, modern çatışmalarda yalnızca teknik sistemleri hedef alan araçlar olmaktan çıkmış; konvansiyonel askerî operasyonlarla eş zamanlı yürütülen hibrit savaş stratejilerinin önemli bir unsuru hâline gelmiştir. Gürcistan örneği, siber alanın doğrudan savaş süreçlerine entegre edildiğini gösteren ilk önemli vakalardan biri olarak değerlendirilmektedir. Bu yönüyle 2008 Rusya-Gürcistan Savaşı, siber operasyonların askerî harekâtla koordineli biçimde kullanılmasına dikkat çekici bir örnek teşkil etmiştir.

2008 yılının ağustos ayında başlayan Rusya-Gürcistan savaşı sırasında Gürcistan’ın devlet kurumlarına ait internet siteleri yoğun siber saldırılara maruz kalmıştır. Başta Gürcistan Cumhurbaşkanlığı internet sitesi olmak üzere birçok kamu kurumu, medya kuruluşu ve iletişim ağı erişilemez hâle gelmiştir. Bunun yanında finans merkezleri, haberleşme sistemleri ve bazı kritik altyapılar ciddi aksaklıklar yaşamıştır (Şenol, 2016). Bu saldırılar, siber operasyonların yalnızca destekleyici faaliyetler olmadığını, doğrudan savaşın işleyişini etkileyebilen stratejik araçlara dönüştüğünü göstermiştir.

Siber saldırıların kara harekâtı ile eş zamanlı yürütülmesi, Gürcistan örneğini hibrit savaş kavramı açısından önemli hâle getirmiştir. Özellikle iletişim altyapısının hedef alınması, bilgi akışının yavaşlatılması ve devlet kurumlarının dijital kapasitesinin zayıflatılması, savaş sürecinde psikolojik baskı oluşturmayı amaçlayan çok katmanlı bir stratejinin parçası olarak değerlendirilmiştir. Bu durum, modern savaşlarda siber alanın yalnızca teknik bir boyut değil; psikolojik harp, bilgi savaşı ve algı yönetimi süreçleriyle doğrudan bağlantılı bir güvenlik alanı hâline geldiğini göstermektedir (Şenol, 2016).

Saldırıların hedefleri arasında yalnızca devlet kurumları değil, medya kuruluşları ve haberleşme altyapıları da yer almıştır. Bu durum, kamuoyunun bilgiye erişimini zorlaştırmış ve

savaş sürecinde Gürcistan'ın uluslararası kamuoyuyla iletişim kurma kapasitesini sınırlamıştır. Böylece siber operasyonların yalnızca teknik sistemleri devre dışı bırakmayı değil, aynı zamanda bilgi akışını kontrol ederek stratejik üstünlük sağlamayı da amaçladığı görülmüştür. Özellikle DDoS saldırıları yoluyla internet trafiğinin yoğunlaştırılması, Gürcistan'ın dijital altyapısında ciddi kesintilere neden olmuştur (Şenol, 2016). Bu durum, siber saldırıların savaş dönemlerinde yalnızca teknik bir destek aracı olarak değil, doğrudan bir stratejik baskı unsuru olarak da kullanılabildiğini göstermektedir. Gürcistan örneği, bilgi akışının kontrol edilmesinin modern çatışmalarda askerî başarı kadar önemli hâle geldiğini ortaya koymaktadır.

Rusya Federasyonu saldırıların doğrudan sorumluluğunu resmî olarak kabul etmemiştir. Ancak uluslararası kamuoyunda saldırıların Rusya bağlantılı gruplar tarafından organize edildiğine yönelik güçlü değerlendirmeler yapılmıştır. Bu durum, Estonya örneğinde olduğu gibi Gürcistan vakasında da “isnat sorununun” uluslararası hukuk açısından önemli bir problem olduğunu göstermiştir. Failin kesin biçimde tespit edilememesi, devlet sorumluluğu ve meşru müdafaa hakkı gibi konuların uygulanmasını daha karmaşık hâle getirmiştir (Gürkaynak ve İren, 2011). Bu belirsizlik, siber saldırıların uluslararası hukukta neden gri alan oluşturduğunu açıkça göstermektedir. Dolayısıyla Gürcistan vakası, siber saldırılarda failin belirlenmesinin yalnızca teknik değil, aynı zamanda hukuki ve siyasi bir mesele olduğunu ortaya koymaktadır.

Gürcistan saldırıları sonrasında NATO ve Batılı ülkeler, siber saldırıların konvansiyonel savaş süreçleriyle birlikte kullanılabilmek kapasitesini daha ciddi biçimde değerlendirmeye başlamıştır. Özellikle kritik altyapıların korunması, askerî iletişim ağlarının güvenliği ve hibrit tehditlere karşı dayanıklılık konuları NATO'nun güvenlik stratejilerinde daha fazla önem kazanmıştır. Bu süreç, devletlerin yalnızca fiziksel sınırlarını değil, dijital altyapılarını da ulusal güvenliğin ayrılmaz bir parçası olarak görmeye başladığını ortaya koymuştur (Bıçakçı, 2014). Bu nedenle Gürcistan örneği, NATO'nun siber güvenlik ve hibrit tehditler konusundaki kurumsal farkındalığını artıran vakalardan biri olarak değerlendirilebilir. Ayrıca bu vaka, devletlerin savaş hazırlıklarında dijital dayanıklılığı temel bir güvenlik kapasitesi olarak ele almaları gerektiğini göstermektedir.

Bu vaka teorik açıdan değerlendirildiğinde, Rusya'nın askerî harekâtı ile siber saldırıları eş zamanlı biçimde yürütmesi, realist yaklaşımın güç mücadelesi ve güvenlik maksimizasyonu anlayışıyla örtüşmektedir. Siber operasyonların konvansiyonel savaşın stratejik bir çarpanı olarak kullanılması, devletlerin rakiplerinin askerî ve iletişim kapasitesini zayıflatmak amacıyla çok boyutlu güvenlik araçlarına yöneldiğini göstermektedir. Konstrüktivist açıdan bakıldığında ise Gürcistan vakası, bilgi savaşı, algı yönetimi ve kamuoyu etkisinin modern çatışmalarda ne kadar önemli hâle geldiğini ortaya koymaktadır. Bu nedenle Gürcistan örneği, siber saldırıların hibrit savaş stratejileri içerisinde nasıl merkezi bir rol üstlenebildiğini gösteren önemli vakalardan biri olarak değerlendirilebilir.

### ***Ukrayna***

Ukrayna örneği, siber saldırıların doğrudan sivil halkı ve kritik altyapıları etkileyebildiğini açık biçimde ortaya koyan en önemli vakalardan biri olarak değerlendirilmektedir. Özellikle enerji altyapısına yönelik saldırılar, siber operasyonların yalnızca dijital sistemlerle sınırlı kalmadığını; toplumun günlük yaşamını, kamu hizmetlerini ve ekonomik faaliyetleri doğrudan etkileyebildiğini göstermiştir. Bu yönüyle Ukrayna vakası, siber güvenliğin ulusal güvenlik ve kritik altyapı koruması açısından stratejik önemini ortaya koyan önemli örneklerden biri hâline gelmiştir.

2015 ve 2016 yıllarında Ukrayna'nın enerji altyapısına yönelik gerçekleştirilen siber saldırılar, ülke genelinde büyük ölçekli elektrik kesintilerine yol açmıştır. Özellikle 2015 yılının aralık ayında gerçekleştirilen saldırı sonucunda yaklaşık 225 bin kişinin elektriksiz kaldığı belirtilmektedir (Çağlar, 2016). Saldırılarda BlackEnergy adlı zararlı yazılımın kullanıldığı ve enerji dağıtım sistemlerinin uzaktan manipüle edildiği ifade edilmektedir. Bu durum, siber saldırıların yalnızca veri sistemlerini değil, fiziksel altyapıları da işlevsiz hâle getirebildiğini göstermiştir. Enerji altyapısının hedef alınması, elektrik hizmetinin toplumun günlük yaşamı ve kamu düzeni açısından ne kadar kritik olduğunu bir kez daha ortaya koymuştur.

Saldırıları sonrasında yapılan incelemelerde, Ukrayna'nın enerji şebekesinde bulunan güvenlik açıklarının saldırganlar tarafından etkili bir biçimde kullanıldığı anlaşılmıştır. Bu olay, kritik altyapıların siber saldırılar karşısında ne derece savunmasız kalabileceğini göstermesi bakımından uluslararası güvenlik literatüründe önemli bir örnek olarak değerlendirilmiştir. Ayrıca saldırılar, siber operasyonların yalnızca teknik sistemlere zarar vermediğini; kamu hizmetlerinin sürekliliğini, ekonomik faaliyetleri ve toplumsal güvenliği doğrudan etkileyebildiğini ortaya koymuştur.

Ukrayna hükümeti saldırılar sonrasında enerji altyapısının güvenliğini artırmaya yönelik çeşitli reformlar gerçekleştirmiş ve siber savunma kapasitesini güçlendirmeye yönelik yeni politikalar geliştirmiştir. Kritik altyapıların korunması, enerji ağlarının dijital güvenliğinin artırılması ve acil müdahale kapasitesinin güçlendirilmesi bu süreçte öncelikli alanlar arasında yer almıştır. Bunun yanında NATO ve Batılı ülkeler de Ukrayna'ya siber güvenlik alanında teknik destek sağlamış; özellikle hibrit tehditlere karşı dayanıklılık, kriz yönetimi ve kritik altyapı güvenliği konularında iş birliği süreçleri hız kazanmıştır (Özdemir, 2025). Bu durum, siber saldırıların kolektif savunma anlayışı açısından da önemli bir güvenlik meselesi hâline geldiğini göstermektedir.

Ukrayna vakası, devlet destekli olduğu iddia edilen siber saldırıların yalnızca hedef ülkenin iç işleyişini değil, bölgesel güvenlik dengelerini de etkileyebildiğini göstermiştir. Özellikle enerji altyapısının hedef alınması, siber operasyonların sivil yaşam üzerindeki doğrudan etkisini açık biçimde ortaya koymuştur. Bu nedenle uluslararası toplum açısından siber saldırılara karşı ortak normların geliştirilmesi ve kolektif tepki mekanizmalarının güçlendirilmesi giderek daha önemli hâle gelmiştir. Nitekim Ukrayna saldırıları, NATO'nun hibrit tehditler ve kritik altyapı güvenliği konularına daha fazla önem vermesine de katkı sağlamıştır (Paltacı, 2022).

Bu vaka teorik açıdan değerlendirildiğinde, kritik altyapıların hedef alınması ve enerji sistemlerinin doğrudan devre dışı bırakılması realist yaklaşımın güç mücadelesi ve stratejik üstünlük anlayışıyla örtüşmektedir. Siber operasyonların enerji altyapısı gibi hayati sistemleri hedef alması, devletlerin rakiplerinin toplumsal ve ekonomik kapasitesini zayıflatmaya yönelik çok boyutlu güvenlik stratejileri geliştirdiğini göstermektedir. Konstrüktivist açıdan bakıldığında ise sivil altyapının hedef alınması, uluslararası normlar, etik tartışmalar ve siber saldırıların meşruiyeti konusunda yeni tartışma alanları ortaya çıkarmıştır. NATO'nun Ukrayna'ya yönelik siber savunma desteği ise devletlerin dijital tehditler karşısında ittifak ilişkileri ve kolektif güvenlik anlayışı çerçevesinde hareket ettiğini göstermektedir.

**Tablo 1.** İncelenen Siber Saldırı Vakalarının Karşılaştırmalı Analizi

| Vaka      | Yıl       | Hedef                                         | Saldırı Türü                       | İsnat Durumu                                                    | Hukuki Tartışma                                                                         | Devlet / Uluslararası Tepki                                                |
|-----------|-----------|-----------------------------------------------|------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Estonya   | 2007      | Devlet kurumları, bankalar, medya kuruluşları | DDoS saldırıları                   | Rusya bağlantısı iddia edilmiş ancak kesin kanıt sunulamamıştır | Egemenlik ihlali, isnat sorunu, siber saldırının kuvvet kullanımı sayılıp sayılmayacağı | NATO CCDCOE kuruldu, Estonya siber savunma kapasitesini güçlendirdi        |
| Gürcistan | 2008      | Devlet siteleri, haberleşme altyapısı         | DDoS ve bilgi savaşı operasyonları | Rusya bağlantılı gruplar suçlanmıştır                           | Hibrit savaş, devlet sorumluluğu, siber operasyonların savaşla entegrasyonu             | NATO hibrit tehditlere yönelik stratejilerini geliştirdi                   |
| İran      | 2010      | Natanz Nükleer Tesisi                         | Zararlı yazılım / SCADA saldırısı  | ABD ve İsrail iddiaları bulunmasına rağmen resmî kabul yoktur   | Silahlı saldırı eşiği, fiziksel hasar, meşru müdafaa tartışmaları                       | İran kritik altyapı güvenliğini artırmaya yönelik reformlar gerçekleştirdi |
| Ukrayna   | 2015-2016 | Enerji altyapısı                              | Zararlı yazılımlar                 | Rusya bağlantılı aktörler suçlanmıştır                          | Kritik altyapı güvenliği, kolektif savunma, isnat sorunu                                | NATO ve Batılı ülkeler Ukrayna'ya siber güvenlik desteği sağladı           |

**Kaynak:** Çalışmada ele alınan Estonya, Gürcistan, İran ve Ukrayna vakalarına ilişkin bulgular esas alınarak yazar tarafından hazırlanmıştır.

### Siber Saldırı Tehditleri Karşısında Uluslararası Hukuktaki Gelişmeler

Estonya, Gürcistan, İran ve Ukrayna örnekleri, siber saldırıların yalnızca teknik sistemleri hedef alan dijital tehditler olmadığını, devlet egemenliği, kritik altyapı güvenliği, uluslararası barış ve meşru müdafaa hakkı gibi konular üzerinde doğrudan etkiler yarattığını göstermiştir. Özellikle kritik altyapıların hedef alınması, siber operasyonların fiziksel sonuçlar doğurabilmesi ve devlet destekli saldırılarda failin tespit edilmesini zorlaştıran isnat sorunu, uluslararası hukukta önemli tartışmaları beraberinde getirmiştir. Bu süreçte NATO, Birleşmiş Milletler ve çeşitli uluslararası kuruluşlar siber güvenliğe ilişkin yeni stratejiler geliştirmeye yönelmiş; siber operasyonların mevcut uluslararası hukuk kuralları çerçevesinde nasıl değerlendirileceği konusu giderek daha fazla önem kazanmıştır. Bu bağlamda Tallinn Manual çalışmaları, siber operasyonlara uygulanabilecek uluslararası hukuk normlarını sistematik biçimde açıklamaya yönelik en önemli girişimlerden biri olarak öne çıkmaktadır.

Siber güvenliğin devletlerarası ilişkilerde giderek daha kritik bir alan hâline gelmesi, uluslararası hukuk normlarının siber operasyonlara nasıl uygulanacağı sorusunu önemli hâle

getirmiştir. Özellikle devlet destekli siber operasyonların artması, mevcut hukuk kurallarının dijital alanda ne ölçüde uygulanabileceğine ilişkin tartışmaları yoğunlaştırmıştır. Bu bağlamda Tallinn Manual çalışmaları, siber savaş ve siber operasyonlar alanında uluslararası hukuk kurallarının nasıl yorumlanabileceğini ortaya koyan temel başvuru kaynakları arasında yer almaktadır. Tallinn Manual 1.0 ve Tallinn Manual 2.0, NATO Cooperative Cyber Defence Centre of Excellence'in (CCDCOE) katkılarıyla uluslararası hukuk uzmanları tarafından hazırlanmış ve Michael N. Schmitt editörlüğünde yayımlanmıştır (Schmitt, 2013; Schmitt, 2017). Tallinn Manual sürecinin temelleri, özellikle 2007 Estonya saldırıları sonrasında NATO bünyesinde siber güvenlik alanında artan farkındalıkla birlikte atılmıştır. İlk çalışma olan Tallinn Manual 1.0, 2013 yılında yayımlanmış; daha sonra kapsamı genişletilerek Tallinn Manual 2.0 adıyla 2017 yılında güncellenmiştir (CCDCOE, n.d.). Bu çalışmalar, siber operasyonların uluslararası hukuk açısından değerlendirilmesine yönelik en kapsamlı girişimler arasında kabul edilmektedir. Ayrıca Tallinn Manual çalışmaları, devletlerin siber operasyonlara karşı ortak hukukî yaklaşımlar geliştirme ihtiyacının bir sonucu olarak ortaya çıkmıştır.

Tallinn Manual 2.0'da yer alan ilk kurallardan biri, devlet egemenliğinin siber uzayda da geçerli olduğunu ortaya koymaktadır. Bu yaklaşım, devletlerin kendi dijital altyapıları ve siber ağları üzerinde egemenlik yetkisine sahip olduğunu kabul eder. Böylece egemenlik kavramı yalnızca kara, deniz ve hava sahasıyla sınırlı görülmemekte; dijital alan da devletin yetki alanının bir parçası olarak değerlendirilmektedir (Oğurlu, 2023; Schmitt, 2017). Bu durum, uluslararası hukukta egemenlik ilkesinin dijital ortama uyarlanması açısından önemli bir normatif genişleme sağlamaktadır. Aynı zamanda devletlerin kritik altyapılarının siber saldırılara karşı korunmasının neden ulusal güvenlik meselesi hâline geldiğini de açıklamaktadır. Bu nedenle siber uzayın devlet egemenliği kapsamında değerlendirilmesi, uluslararası hukukta yeni güvenlik tartışmalarının ortaya çıkmasına yol açmıştır.

2013 yılında yayımlanan Tallinn Manual 1.0, siber savaş durumlarında uluslararası hukukun nasıl uygulanabileceğini sistematik biçimde ele alan ilk kapsamlı çalışmalardan biri olmuştur. Manual'de özellikle siber operasyonların hangi koşullarda “kuvvet kullanımı” veya “silahlı saldırı” kapsamında değerlendirilebileceği üzerinde durulmuştur. Uluslararası insancıl hukuk ve silahlı çatışma hukukunun siber operasyonlara uygulanabilirliği ayrıntılı biçimde tartışılmıştır (Schmitt, 2013). Bu yaklaşım, siber operasyonların tamamen hukuk dışı bir alan olmadığı; mevcut uluslararası hukuk kurallarının belirli ölçülerde dijital ortama da uygulanabileceği anlayışını güçlendirmiştir. Böylece Tallinn Manual 1.0, siber çatışmaların hukuk normları çerçevesinde değerlendirilmesine yönelik önemli bir zemin oluşturmıştır. Bunun yanında, çalışma siber saldırıların uluslararası hukuk açısından nasıl sınıflandırılması gerektiğine ilişkin tartışmaların akademik ve hukukî düzeyde daha sistematik biçimde yürütülmesine katkı sağlamıştır.

2017 yılında yayımlanan Tallinn Manual 2.0 ise ilk çalışmanın kapsamını genişleterek yalnızca savaş dönemindeki siber operasyonları değil, barış zamanında gerçekleştirilen siber faaliyetleri de uluslararası hukuk açısından değerlendirmiştir. Manual'de egemenlik, devlet sorumluluğu, insan hakları, kuvvet kullanımı, müdahale yasağı ve meşru müdafaa gibi konular siber operasyonlar bağlamında ayrıntılı biçimde ele alınmıştır (Schmitt, 2017). Bu yönüyle Tallinn Manual 2.0, siber güvenlik alanında uluslararası hukukun uygulanabilirliğini açıklamaya çalışan en kapsamlı referanslardan biri olarak kabul edilmektedir. Bununla birlikte, Tallinn Manual çalışmaları bağlayıcı bir uluslararası antlaşma niteliği taşımamaktadır. Daha çok uzman görüşlerine dayanan rehber metinler olarak değerlendirilmekte ve devlet uygulamalarına yön vermeyi amaçlamaktadır. Bu durum, siber güvenlik alanında hâlen bağlayıcı ve ortak kabul gören uluslararası normların tam olarak oluşmadığını göstermektedir. Dolayısıyla Tallinn Manual çalışmaları, uluslararası hukukta siber güvenlik alanındaki normatif

boşlukları tamamen ortadan kaldırmaya da devletlerin ve uluslararası kuruluşların ortak hukukî çerçeve geliştirme çabalarına önemli katkı sağlamaktadır.

### **Uluslararası Kurumlar ve Anlaşmaların Siber Güvenlikteki Etkisi**

Teknolojinin hızlı gelişimiyle birlikte siber güvenlik, yalnızca bireysel ya da ulusal bir mesele olmaktan çıkmış; uluslararası barış ve güvenlik açısından kritik bir öncelik hâline gelmiştir. Siber tehditlerin sınır aşan niteliği, devletlerin bu alanda tek başına hareket etmesini yetersiz kılmaktadır. Bu nedenle uluslararası örgütler ve anlaşmalar, siber tehditlere karşı kolektif direnç oluşturmak, ortak normlar geliştirmek ve devletler arasında iş birliğini güçlendirmek bakımından önemli roller üstlenmektedir.

Siber güvenliğin giderek daha karmaşık ve çok boyutlu hâle gelmesi, Birleşmiş Milletler, Avrupa Konseyi, NATO, Avrupa Birliği ve ITU gibi uluslararası aktörlerin bu alandaki rolünü artırmıştır. Bu kurumlar, siber güvenlik alanında ortak normların oluşmasına katkı sunmakta, devletlerarası iş birliğini teşvik etmekte ve kapasite geliştirme süreçlerini desteklemektedir. Gündoğdu'ya göre siber güvenlik, artık yalnızca teknik bir mesele değil; uluslararası barış, istikrar ve diplomasi açısından da öncelikli bir konu hâline gelmiştir (Gündoğdu, 2023). Bu durum, siber tehditlerle mücadelede yalnızca ulusal politikaların yeterli olmadığını göstermektedir. Dolayısıyla siber güvenlik, uluslararası kurumların koordinasyon kapasitesini zorunlu kılan çok taraflı bir güvenlik alanına dönüşmüştür.

Budapeşte Sözleşmesi, sınır ötesi siber suçlarla mücadelede en önemli uluslararası belgelerden biridir. Avrupa Konseyi tarafından hazırlanan ve 23 Kasım 2001'de imzaya açılan sözleşme, siber suçlarla mücadelede maddi ceza hukuku, usul hukuku ve uluslararası iş birliği boyutlarını birlikte düzenlemektedir (Council of Europe, 2001). Sözleşme, yalnızca siber suçları tanımlamakla kalmamakta, aynı zamanda taraf devletler arasında hızlı ve etkili adli yardımlaşma mekanizmalarının kurulmasını da hedeflemektedir. Elektronik delillerin kolayca silinebilmesi veya farklı ülke sunucularında bulunabilmesi, klasik adli yardımlaşma yöntemlerini yetersiz bırakmaktadır. Bu nedenle Budapeşte Sözleşmesi, dijital delillerin korunması ve sınır ötesi soruşturmaların hızlandırılması açısından önemli bir iş birliği modeli sunmaktadır (Council of Europe, 2001; Bıçakcı, 2014: 110). Bu yönüyle sözleşme, siber suçlarla mücadelede uluslararası hukukun pratik işleyişini güçlendiren temel belgelerden biri olarak değerlendirilmektedir.

NATO'nun siber güvenlik yaklaşımı özellikle 2016 Varşova Zirvesi sonrasında daha kurumsal bir nitelik kazanmıştır. NATO'nun 8–9 Temmuz 2016 tarihli Warsaw Summit Communiqué belgesinin 70. paragrafında, siber saldırıların modern toplumlar için konvansiyonel saldırılar kadar zararlı olabileceği belirtilmiş ve siber uzay kara, deniz ve hava gibi bir “operasyon alanı” olarak tanınmıştır (NATO, 2016, para. 70). Bu gelişme, dijital saldırıların belirli koşullar altında kolektif savunma kapsamında değerlendirilebileceğini göstermektedir. NATO açısından siber savunmanın kolektif savunma görevinin bir parçası hâline gelmesi, ittifakın güvenlik paradigmasının dijital tehditler doğrultusunda yeniden şekillendiğini ortaya koymaktadır. Bu nedenle siber saldırılar artık yalnızca bireysel ya da teknik tehditler değil, kolektif güvenlik stratejilerinin merkezinde yer alan ciddi bir risk unsuru hâline gelmiştir (Bıçakcı, 2014: 117-118).

Avrupa Birliği, 2019 yılında yürürlüğe giren Siber Güvenlik Yasası ile siber güvenlik alanındaki kurumsal kapasitesini güçlendirmiştir. Bu düzenleme, ENISA'ya kalıcı ve güçlendirilmiş bir görev alanı sağlamış; aynı zamanda bilgi ve iletişim teknolojileri ürünleri, hizmetleri ve süreçleri için Avrupa çapında siber güvenlik sertifikasyon çerçevesi oluşturmuştur

(ENISA, 2019). ENISA, Avrupa genelinde yüksek ve ortak bir siber güvenlik düzeyi oluşturmayı amaçlayan temel kurumlardan biri hâline gelmiştir. Nezgıtlı ve Benzer'e göre Avrupa Birliği'nin bu yöndeki düzenlemeleri, üye devletler arasında daha koordineli ve güçlü bir siber güvenlik yapısı kurulmasına katkı sağlamaktadır (Nezgıtlı ve Benzer, 2020). Bu çerçeve, Avrupa Birliği'nin siber güvenliği yalnızca teknik bir koruma meselesi olarak değil, dijital pazarın güvenliği ve ekonomik istikrar açısından da stratejik bir alan olarak gördüğünü göstermektedir.

ENISA tarafından hazırlanan rehber belgeler, özellikle Nesnelerin İnterneti gibi yeni teknolojilerin güvenliğinin sağlanması açısından önem taşımaktadır. ENISA'nın "Guidelines for Securing the Internet of Things" raporu, IoT sistemlerinde güvenlik risklerinin azaltılması ve güvenli tasarım ilkelerinin geliştirilmesi açısından yol gösterici bir çerçeve sunmaktadır (ENISA, 2020). Bu tür rehberler, Avrupa Birliği'nin siber güvenliği yalnızca hukukî düzenlemelerle değil, teknik standartlar ve uygulama rehberleriyle de desteklediğini göstermektedir. Böylece AB düzeyindeki siber güvenlik politikaları hem kurumsal hem de teknik düzeyde daha bütüncül bir yapıya kavuşmaktadır.

Siber güvenlik alanında uluslararası standartlar ve performans ölçümleri geliştirilmesi de devletlerin kapasitelerini değerlendirmeleri açısından önemlidir. Bu bağlamda Uluslararası Telekomünikasyon Birliği tarafından hazırlanan Küresel Siber Güvenlik Endeksi, ülkelerin siber güvenlik alanındaki taahhütlerini karşılaştırmalı biçimde ölçen önemli araçlardan biridir. ITU'ya göre Küresel Siber Güvenlik Endeksi, ülkeleri hukukî önlemler, teknik önlemler, kurumsal kapasite, kapasite geliştirme ve iş birliği olmak üzere 5 temel sütun üzerinden değerlendirmektedir (International Telecommunication Union, 2026). Bu yapı sayesinde ülkeler kendi siber güvenlik durumlarını değerlendirebilmekte, eksiklerini görebilmekte ve diğer ülkelerin iyi uygulamalarından yararlanabilmektedir. Bu nedenle GCI, yalnızca teknik bir sıralama aracı değil, devletlerin siber direnç kapasitelerini geliştirmelerine katkı sağlayan uluslararası bir politika göstergesi olarak da değerlendirilebilir.

Bu çerçevede uluslararası kurumlar ve anlaşmalar, siber güvenliğin normatif ve kurumsal altyapısının gelişmesinde belirleyici rol oynamaktadır. Budapeşte Sözleşmesi, sınır ötesi siber suçlarla mücadelede hukukî iş birliğini güçlendirirken NATO, siber savunmayı kolektif güvenlik anlayışına dâhil etmiş; Avrupa Birliği ise ortak standartlar ve sertifikasyon mekanizmalarıyla siber direnç kapasitesini artırmaya yönelmiştir. ITU'nun Küresel Siber Güvenlik Endeksi ise ülkelerin performansını karşılaştırmalı biçimde ölçerek uluslararası farkındalığı artırmaktadır. Bu gelişmeler, siber güvenliğin artık yalnızca teknik bir savunma alanı değil, uluslararası hukuk, diplomasi ve çok taraflı yönetim mekanizmalarının merkezinde yer alan stratejik bir konu olduğunu göstermektedir.

## SONUÇ VE ÖNERİLER

Siber saldırılar, günümüzde devletlerin egemenlik anlayışını, güvenlik algılarını ve uluslararası sistem içindeki davranış biçimlerini doğrudan etkileyen çok katmanlı bir tehdit alanı hâline gelmiştir. Bu çalışma kapsamında incelenen Estonya, İran, Gürcistan ve Ukrayna örnekleri, siber saldırıların artık yalnızca dijital ağlara yönelik teknik müdahaleler olmadığını; devlet kapasitesini zayıflatan, toplumsal düzeni aksatan ve uluslararası güvenliği etkileyen stratejik araçlara dönüştüğünü açık biçimde ortaya koymuştur. Özellikle Estonya vakası, dijital altyapıya yüksek düzeyde bağımlı devletlerin kısa sürede yönetsel ve iletişimsel krizlerle karşı karşıya kalabileceğini gösterirken, Ukrayna örneği, siber saldırıların enerji altyapıları üzerinden doğrudan sivil halkı etkileyen fiziksel sonuçlar doğurabileceğini somut biçimde ortaya koymuştur.

Bu bulgular, siber güvenliğin artık ikincil düzeyde teknik bir politika alanı olarak değerlendirilemeyeceğini; aksine ulusal güvenlik stratejilerinin merkezinde yer alması gereken yapısal bir mesele hâline geldiğini göstermektedir. Mevcut güvenlik paradigmaları büyük ölçüde fiziksel kuvvet kullanımına dayalı tehdit algıları üzerine inşa edildiğinden, siber operasyonların yarattığı düşük yoğunluklu ancak yüksek etkili saldırılar karşısında yetersiz kalmaktadır. Bu durum, uluslararası hukuk sisteminin de benzer bir uyumsuzluk yaşadığını göstermektedir. Özellikle Birleşmiş Milletler Şartı'nın kuvvet kullanma yasağını düzenleyen 2/4. maddesi ile meşru müdafaa hakkını düzenleyen 51. maddesi, siber saldırılar bağlamında yeniden yorumlanması gereken temel hukuk normları hâline gelmiştir. Çünkü günümüzde birçok siber operasyon, fiziksel savaş ilan olmadan ciddi stratejik sonuçlar doğurabilmektedir. Bu nedenle kuvvet kullanma yasağı, meşru müdafaa hakkı ve devlet sorumluluğu gibi temel ilkelerin siber saldırıların anonim, sınır aşan ve eşik altı niteliği karşısında uygulanabilirliği önemli ölçüde zorlaşmaktadır.

Budapeşte Sözleşmesi ve Tallinn Manual gibi normatif metinler, siber alanın hukuki çerçevesini belirleme konusunda önemli katkılar sunsa da bu düzenlemelerin bağlayıcı nitelikten yoksun olması, devlet uygulamalarında ciddi boşluklar yaratmaktadır. Özellikle Tallinn Manual'ın yol gösterici niteliği, devletlerin siber saldırıları kendi ulusal çıkarları doğrultusunda yorumlayabilmesine imkân tanımakta; bu durum uluslararası sistemde normatif parçalanmayı derinleştirmektedir. Çalışmanın teorik çerçevesini oluşturan realizm ve konstrüktivizm yaklaşımları bu noktada tamamlayıcı bir analiz sunmaktadır. Realist perspektif, siber alanı devletlerarası güç mücadelesinin yeni bir cephesi olarak değerlendirirken, konstrüktivist yaklaşım, tehdit algılarının ve hukuki yorumların devlet kimlikleri, normlar ve söylemler aracılığıyla inşa edildiğini ortaya koymaktadır. Böylece siber güvenliğin yalnızca teknik kapasite meselesi değil, aynı zamanda siyasal algılar ve uluslararası normlarla şekillenen çok boyutlu bir güvenlik alanı olduğu anlaşılmaktadır.

Bu bağlamda çalışmanın temel argümanı, mevcut uluslararası hukuk düzeninin siber saldırıların yarattığı “gri alan” karşısında işlevsel ve caydırıcı bir mekanizma üretmekte yetersiz kaldığıdır. Fiziksel yıkım eşiğinin altında kalan ancak stratejik sonuçlar doğuran siber operasyonlar, devletlerin meşru müdafaa hakkını etkili biçimde kullanmasını zorlaştırmakta ve saldırgan aktörler açısından düşük maliyetli bir hareket alanı oluşturmaktadır. Bu durum yalnızca hedef alınan devletlerin güvenliğini değil, aynı zamanda uluslararası sistemin öngörülebilirliğini ve istikrarını da olumsuz etkilemektedir.

Bu sorunların aşılabilmesi için öncelikle siber saldırıların “silahlı saldırı” eşiğinin uluslararası düzeyde daha net biçimde tanımlanması gerekmektedir. Tallinn Manual'de yer alan etki temelli kriterlerin, Birleşmiş Milletler Şartı ile uyumlu ve daha bağlayıcı normatif düzenlemelere dönüştürülmesi önem taşımaktadır. Bunun yanında isnat (attribution) sorununun aşılması amacıyla NATO veya Avrupa Birliği çatısı altında, ortak delil paylaşımına dayalı ve hukuki sonuç doğurabilecek uluslararası adli bilişim mekanizmalarının geliştirilmesi kritik bir ihtiyaç hâline gelmiştir. Kurumsal düzeyde ise kritik altyapıların korunması yalnızca ulusal güvenlik politikalarıyla sınırlı kalmamalı; sınır ötesi tehdit istihbaratının paylaşımını esas alan uluslararası “Siber Erken Uyarı ve Müdahale Merkezleri” kurulmalıdır.

Son olarak, devletlerin siber güvenlik yaklaşımını yalnızca pasif bir savunma anlayışıyla sınırlandırmaması gerekmektedir. Siber caydırıcılık, yalnızca teknik kapasite artırımıyla değil; diplomatik baskı, ekonomik yaptırımlar, uluslararası iş birliği ve normatif maliyetler üreten çok boyutlu stratejiler çerçevesinde ele alınmalıdır. Bu doğrultuda geliştirilecek bütüncül politikalar, yalnızca devletlerin ulusal güvenliğini güçlendirmeyecek; aynı zamanda küresel barışın, dijital hakların ve uluslararası hukukun sürdürülebilirliğine de katkı sağlayacaktır.

## EXTENDED ABSTRACT

In the 21st century, rapid advancements in information and communication technologies have fundamentally transformed states' security policies, introducing a strategic digital dimension to international relations. Cyberspace has become a central domain that directly influences not only individual activities but also foreign policy priorities, national security strategies, and military configurations. Cyberattacks have evolved from mere technical disruptions into strategic security threats capable of collapsing economic infrastructure, manipulating election processes, and disrupting military operations. However, the traditional international legal system, based on fundamental principles such as the prohibition of the use of force, sovereign equality, and the right of self-defense, was primarily designed for conventional armed conflicts. Consequently, identifying the source of cyber-attacks, measuring their impacts, and determining legal responsibility create profound uncertainties within the current normative framework. Although guiding documents such as the Tallinn Manual make substantial contributions to addressing these gaps, their non-binding nature limits their practical impact on state behavior. Therefore, cybersecurity has transcended its technical boundaries, becoming an interdisciplinary strategic domain encompassing legal, political, and ethical dimensions. The primary purpose of this study is to examine the inadequacy of international legal norms in the face of cyber threats and to re-evaluate the principles of self-defense, sovereignty, and state responsibility through comparative case studies.

This study adopts a qualitative research methodology, using document review and comparative case analysis. The research focuses on four distinct cases—Estonia, Georgia, Iran, and Ukraine—selected because they demonstrate the multifaceted impacts of cyber-attacks on state security, international law, and the right of self-defense across different contexts and periods. Primary legal sources, including the United Nations Charter (specifically Articles 2 and 51), the Tallinn Manual 1.0 and 2.0, NATO cybersecurity strategy documents, and the Budapest Convention, are thoroughly analyzed. Theoretically, the study relies on realism and constructivism. From a realist perspective, cyberspace is viewed as a new frontier for interstate power struggles, where states develop capacity-building, alliances, and deterrence policies to ensure their security. Conversely, the constructivist approach argues that perceptions of cyber threats are shaped by international norms, state identities, and historical contexts, framing cyber-attacks as political practices that reproduce normative structures in international relations.

The comparative analysis of the selected cases reveals that cyberattacks serve as multidimensional strategic tools capable of paralyzing digitized states. In the 2007 Estonia case, a political crisis surrounding the relocation of a Soviet-era monument rapidly escalated into a massive Distributed Denial of Service (DDoS) attack targeting government portals, media, and banking systems. This case demonstrated that historical tensions could trigger devastating digital crises and highlighted the critical "attribution problem" in international law, as the inability to definitively prove state responsibility hindered Estonia's legal right to self-defense. However, this crisis acted as a catalyst for institutionalizing cyber defense, leading to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

The 2010 Stuxnet attack in Iran marked a critical turning point, demonstrating that cyber operations could inflict physical destruction on critical infrastructure. By targeting the SCADA systems at the Natanz Nuclear Facility, Stuxnet physically damaged uranium enrichment centrifuges. This unprecedented event sparked intense legal debates on whether a cyber operation could be classified as an "armed attack" based on its physical effects. Stuxnet proved

that cyberspace could be weaponized for strategic sabotage, reinforcing the realist paradigm of hidden power struggles.

The 2008 Russia-Georgia War provided an early example of hybrid warfare, in which cyber-attacks were synchronized with conventional military operations. By paralyzing Georgian government websites and communication infrastructure, the attackers sought to disrupt the flow of information and exert psychological pressure. This case underscored the integration of cyber operations into comprehensive military strategies and highlighted the necessity for states to incorporate digital resilience into their war-readiness frameworks.

Furthermore, the 2015-2016 cyber-attacks on Ukraine's energy infrastructure illustrated the severe threat posed to civilian populations. Using the Black Energy malware, attackers caused massive blackouts that affected hundreds of thousands of people. The Ukraine case emphasized the vulnerability of critical infrastructure and demonstrated that cyber-attacks can directly disrupt daily civilian life, public services, and economic stability, thereby catalyzing collective defense initiatives with NATO and Western allies.

The study concludes that the current international legal order remains highly inadequate at producing effective and deterrent mechanisms against the "grey area" created by modern cyberattacks. Cyber operations that cause strategic disruptions but fall short of physical destruction make it incredibly difficult for states to effectively exercise their inherent right of self-defense, thereby providing low-cost maneuvering space for malicious actors. While normative texts like the Budapest Convention and the Tallinn Manual provide essential legal guidance, their lack of binding enforcement leads to normative fragmentation in state practices.

To address these structural deficiencies, the threshold for defining a cyber operation as an "armed attack" must be more clearly articulated and universally accepted at the international level. The effect-based criteria proposed in the Tallinn Manual should be transformed into binding normative regulations compatible with the United Nations Charter. Furthermore, to overcome the persistent attribution problem, the establishment of international digital forensics mechanisms based on shared evidence, potentially under the umbrella of NATO or the European Union, is critically needed. Institutionally, international "Cyber Early Warning and Response Centers" based on cross-border threat intelligence sharing should be established. Finally, states must adopt comprehensive cyber deterrence strategies integrating diplomatic pressure, economic sanctions, international cooperation, and the imposition of normative costs, thereby ensuring global cyber stability and the sustainability of international law.

## KAYNAKÇA

- Acar, Ü. (2019). Sabotaj eylemleri ve acil durum yönetimi. *Uluslararası Sosyal Bilimler ve Eğitim Dergisi*, 1(1), 1-23. <https://izlik.org/JA68ES53WD>
- Bıçakcı, S. (2014). NATO's emerging threat perception: Cyber security in the 21st century. *Uluslararası İlişkiler Dergisi*, 10(40), 100-130. <https://izlik.org/JA38KM49NA>
- CCDCOE. (n.d.). *Tallinn Manual*. [https://ccdcoe.org/research/tallinn-manual/?utm\\_source=](https://ccdcoe.org/research/tallinn-manual/?utm_source=)
- Cengiz, G. (2021). Siber suçlar, sosyal medya ve siber etik. *İletişim Çalışmaları Dergisi*, 7(3), 407-424. <https://izlik.org/JA65KH98YS>
- Contested Histories. (2021). *Estonia: Bronze soldier in Tallinn*. Contested Histories Case Study. [https://contestedhistories.org/wp-content/uploads/Estonia\\_-Bronze-Soldier-in-Tallinn.pdf](https://contestedhistories.org/wp-content/uploads/Estonia_-Bronze-Soldier-in-Tallinn.pdf)
- Council of Europe. (2001). *Convention on Cybercrime*. [https://www.coe.int/en/web/cybercrime/the-budapest-convention?utm\\_source=](https://www.coe.int/en/web/cybercrime/the-budapest-convention?utm_source=)
- Çağlar, N. (2016). Elektriğe siber saldırı ABD'yi nasıl panikletti? Enerji Günlüğü. <https://www.enerjigunlugu.net/elektrige-siber-saldiri-abdyi-nasil-panikletti-19506yy.htm>
- Çakır, H., & Taşer, M. (2023). Türkiye'de yapılan siber güvenlik faaliyetlerinin ve eğitim çalışmalarının değerlendirilmesi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 11(2), 347-366. <https://doi.org/10.29109/gujsc.1165131>
- Dilek, E., Talih, Ö., & Bensghir, T. (2023). Estonya 2007 siber saldırılarının incelenmesi ve ülkelerin ulusal siber güvenlik politikalarına etkileri. *Bilgi Yönetimi*, 6(2), 332-347. <https://doi.org/10.33721/by.1392577>
- ENISA. (2019). *Cybersecurity Act* [https://certification.enisa.europa.eu/about-eu-cyber-certification/eu-regulatory-context/cybersecurity-act\\_en?utm\\_source=](https://certification.enisa.europa.eu/about-eu-cyber-certification/eu-regulatory-context/cybersecurity-act_en?utm_source=)
- ENISA. (2020). *Guidelines for securing the internet of things*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>
- Gençoğlu, M. T. (2021). Siber olaylara müdahale ve analiz süreci. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 33(2), 471-479. <https://doi.org/10.35234/fumbd.865117>
- Gündoğdu, S. (2023). Uluslararası politikada bir etki aracı olarak siber güvenlik ve Türkiye'nin siber güvenlik politikası uygulaması: Ulusal siber olaylara müdahale merkezi (USOM). *Fırat University Journal of Social Sciences*, 33(3), 1325-1337. <https://doi.org/10.18069/firsbed.1261707>
- Güntay, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri Dergisi*, 14(27), 79-111. <https://doi.org/10.17752/guvenlikstrjtj.432151>
- Gürkaynak, Y., & İren, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararası ilişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(2), 263-279. <https://izlik.org/JA58TK87TF>
- International Telecommunication Union (ITU). (2026). *Global Cybersecurity Index (GCI)*. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- Kara, İ. (2015). Türkiye'de zararlı yazılımlarla mücadelenin uygulama ve hukuki boyutunun

- değerlendirilmesi. *Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi*, 52, 87-98. <https://izlik.org/JA34PT52ML>
- Karadağ, U. (2016). Birleşmiş Milletler antlaşması'na göre meşru müdafaa hakkı. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 7(2), 171-186. <https://doi.org/10.21492/inuhfd.291295>
- Kişman, Z. A., & Güleç, Ö. (2021). Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri. *Akademik Açı*, 1(1), 127-154. <https://izlik.org/JA32PL45HZ>
- NATO. (2016). *Warsaw Summit Communiqué*. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique>
- Nezgitli, S., & Benzer, R. (2020). Avrupa Birliği siber güvenlik kanunu. *Journal of Information Systems and Management Research*, 2(1), 10-17. <https://izlik.org/JA24CJ27NW>
- Oğurlu, E. (2023). International law in cyberspace: An evaluation of the Tallinn Manuals. *Annales de la Faculté de Droit D'Istanbul*, 73, 327-344. <https://doi.org/10.26650/Annales.2023.73.0010>
- Ottis, R. (2008). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective*. [https://ccdcoe.org/uploads/2018/10/Ottis2008\\_AnalysisOf2007FromTheInformationWarfarePerspective.pdf](https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf)
- Özdemir, G. (2025). Uluslararası güvenlikte siber tehditlerin yükselişi ve stratejik savunma politikaları. *Elektronik Sosyal Bilimler Dergisi*, 24(1), 1-20. <https://doi.org/10.17755/esosder.1459973>
- Öztürk, D., Aktolun, A., Emektar, M., & Harmancı, F. M. (2025). Dağıtık siber saldırıların internet hizmetlerinin kullanılabilirliği üzerindeki etkisi: Ddosphere ile deneysel bir analiz. *Alpha Journal of Engineering and Applied Sciences*, 3(1), 35-50. <https://doi.org/10.70988/ajeas.1628985>
- Paltacı, B. M. (2022). Ukrayna-Rusya savaşı bağlamında siber güvenlik ekosisteminde yaşanan gelişmeler ve değerlendirmeler. *Orta Doğu ve Orta Asya-Kafkaslar Araştırma ve Uygulama Merkezi Dergisi*, 2(2), 1-19. <https://izlik.org/JA36YA48CR>
- Sandilaç, N. (2022). Siber suç, siber terör ve siber savaş üçgeninde siber dünya. *Bilişim Hukuku Dergisi*, 4(1), 81-140. <https://doi.org/10.55009/bilisimhukukudergisi.1119881>
- Sertçelik, A. (2018). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi*, 2(3), 25-42. <https://izlik.org/JA67ZG53HY>
- Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge University Press
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press
- Şafak, E. (2020). Uluslararası hukukta değişen güvenlik algısı ve saldırı suçu bağlamında siber saldırılar. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 28(1), 127-160. <https://doi.org/10.15337/suhfd.640029>
- Şenol, M. (2016). Siber güçle caydırıcılık ama nasıl? *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2(2), 10-17. <https://doi.org/10.18640/ubgmd.303581>
- Tunca, S. (2019). Modern çağda siber güvenlik kavramı. *Dumlupınar Üniversitesi İİBF Dergisi*, 3-4, 1-7. <https://izlik.org/JA23RB59YU>

- United Nations. (1945). *Charter of the United Nations*. <https://www.un.org/en/about-us/un-charter/full-text>
- Yayla, M. (2014). Siber savař ve siber ortamdaki kötü niyetli hareketlerden farkı. *Hacettepe Hukuk Fakóltesi Dergisi*, 4(2), 181-200. <https://izlik.org/JA57HE86CL>