• *ANALİZ*

ABD/İsrail-İran Savaşı: Yapay Zeka Çağında Savaşın Dönüşümü ve Uluslararası Hukuk

Mammad Ismayilov

www.setav.org

20.yıl | SETA

MAYIS 2026 SAYI 466

ABD/İSRAİL-İRAN SAVAŞI: YAPAY ZEKA ÇAĞINDA SAVAŞIN DÖNÜŞÜMÜ VE ULUSLARARASI HUKUK

MAMMAD ISMAYILOV

SETA

ISBN: 978-625-5703-42-2

Editörya: Ebrar Üzümcü, Berrin Çalışkan, Mustafa Said İşeri
Mizanpaj: Said Demirtaş

SETA | SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312 551 21 00 | Faks: +90 312 551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüpsultan 34050 İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Faks: +90 212 395 11 11

SETA | Washington D.C.
1025 Connecticut Avenue, N.W., Suite 410
Washington D.C., 20036 USA
Tel: 202 223 98 85 | Faks: 202 223 60 99
www.setadc.org | info@setadc.org | @setadc

SETA | Berlin
Kronenstraße 1, 10117 Berlin GERMANY
berlin@setav.org

SETA | Brüksel
Avenue des Arts 6, 1000 Bruxelles BELGIUM
Tel: +32 2 313 39 41

İÇİNDEKİLER

Bu analiz, ABD ve İsrail'in YZ destekli siber saldırılarını uluslararası hukukun temel parametreleri çerçevesinde incelemektedir.

ÖZET

28 Şubat 2026'da başlayan ABD/İsrail-İran savaşıyla birlikte yapay zeka (YZ) destekli siber araçlar kinetik saldırılarla eş zamanlı olarak savaş ortamında kullanılmıştır. Bu analiz söz konusu YZ destekli siber saldırıların Birleşmiş Milletler (BM) Şartı'nın 2(4). maddesi kapsamındaki kuvvet kullanma yasağı ve 51. maddesi kapsamındaki silahlı saldırı eşiğini aşıp aşmadığını, devletin uluslararası sorumluluğu bağlamında atıf sorununu ve meşru müdafaa hakkının bu çerçevedeki sınırlarını eleştirel bir perspektifle incelemektedir.

GİRİŞ

M.Ö. 490'da Perslerin Attika'ya ilerleyişini anlatan Herodot, savaş sonrasında Perslere bir kalkanla sinyal verildiği yönündeki tartışmalı olayı aktarır. Bu örnek savaşın yalnızca kinetik çatışmadan ibaret olmadığını; bilgi, işaretleşme ve algı yönetiminin çatışmanın erken aşamalarında dahi önemli rol oynadığını göstermektedir.[1] Bu kadim mantık 28 Şubat 2026'nın karanlık saatlerinde dijital bir biçimde yeniden sahnelenmiştir.

ABD Genelkurmay Başkanı Orgeneral Dan Caine 2 Mart 2026 tarihli basın toplantısında saldırıların ilk aşamasına ilişkin şu açıklamalarda bulunmuştur: ABD Siber Komutanlığı ve ABD Uzay Komutanlığı operasyonun "ilk adım atanları" olmuştur.[2] Nitekim ilk kinetik mühimmat hedeflere ulaşmadan önce gerçekleştirilen siber saldırılar İran'ın iletişim ve sensör ağlarını devre dışı bırakmış; erken uyarı radarlarını kör etmiş ve komuta kontrol altyapısını işlevsiz kılmıştır. Bu süreçte İran'ın internet trafiği saldırıların ilk saatlerinde normal seviyesinin yüzde 4'ünün altına kadar gerilemiştir.[3]

1 Herodot, *Herodot Tarihi*, çev. Müntekim Ökmen, (Türkiye İş Bankası Kültür Yayınları, İstanbul: 2019), VI. 115, VI. 124.

2 Dan Caine, "Pentagon Press Briefing on Operation Epic Fury", US CENTCOM, 2 Mart 2026, https://www.centcom.mil/Media/Press-Briefings, (Erişim tarihi: 6 Nisan 2026); Evan Grey, "The Iran Precedent: Operation Epic Fury and the Law of Armed Conflict in Space", SatNews, 4 Mart 2026, https://satnews.com/2026/03/04/the-iran-precedent-operation-epic-fury-and-the-law-of-armed-conflict-in-space, (Erişim tarihi: 6 Nisan 2026).

3 "Iran-Israel Cyber War Dashboard", SOCRadar, 28 Şubat 2026, https://socradar.io/iran-israil-cyber-conflict-dashboard, (Erişim tarihi: 6 Nisan 2026); "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran (Updated March 26)", Palo Alto Networks Unit 42, 26 Mart 2026, https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026, (Erişim tarihi: 6 Nisan 2026).

"Destansı Öfke" ve İsrail tarafından "Aslanın Kükremesi" olarak adlandırılan operasyonlar, YZ destekli siber ve istihbari sistemlerin modern savaş alanında ulaştığı yüksek hassasiyet kapasitesini ortaya koymaktadır. Geleneksel yöntemlerle aylar sürebilecek veri analiz süreçlerinin saniyelere indirgenmesi, hedef tespitinin biyometrik izleme ve sivil yoğunluk analizleri gibi çok katmanlı veriler üzerinden gerçekleştirilmesi, yüksek değerli hedeflere yönelik operasyonel etkinliği önemli ölçüde artırmaktadır. Bu gelişim, İsrail'in Gazze'deki saldırılarında kullanılan "The Gospel", "Lavender" ve "Where is Your Daddy?" gibi YZ destekli hedefleme sistemleriyle birlikte değerlendirildiğinde söz konusu teknolojilerin aşamalı bir şekilde olgunlaştığını göstermektedir.[4]

Bununla birlikte mevcut gerilimi önceki dönemlerden ayıran iki temel unsur öne çıkmaktadır. İlki YZ kullanımının artık örtülü bir operasyonel unsur olmaktan çıkarak ABD'li üst düzey askeri yetkililer tarafından açık biçimde askeri doktrinin bir parçası olarak ifade edilmesidir. İkincisi ise bu teknolojilerin yol açtığı etik ve hukuki sorumluluk tartışmalarıdır. CENTCOM Komutanlığı tarafından yapılan açıklamalarda YZ'nin operasyonel süreçlerde kullanıldığı kabul edilirken "nihai kararın insan tarafından verildiği" vurgusu, artan sivil kayıplar ve otonom sistemlerin sorumluluk rejimine ilişkin uluslararası eleştiriler karşısında hukuki ve politik bir denge kurma çabası olarak değerlendirilmektedir.[5]

"Destansı Öfke" ve İsrail tarafından "Aslanın Kükremesi" olarak adlandırılan operasyonlar, YZ destekli siber ve istihbari sistemlerin modern savaş alanında ulaştığı yüksek hassasiyet kapasitesini ortaya koymaktadır.

Bu bağlamda YZ destekli sistemlerin istihbarat ve hedefleme süreçlerine entegrasyonu yalnızca teknik bir üstünlük değil aynı zamanda insan-makine etkileşimine dayalı yeni bir savaş paradigmasının oluşumuna işaret etmektedir. Büyük veri analizi, sinyal istihbaratı ve makine öğrenmesi algoritmalarının birleşimi, operasyonel karar alma süreçlerini hızlandırmakta ve hedef tespitinde hata payını azaltmaktadır. Ancak bu durum askeri etkinlik ile hukuki sorumluluk arasındaki sınırların giderek daha tartışmalı hale gelmesine yol açmakta ve uluslararası hukuk kurallarının bu yeni teknolojilere uygulanabilirliği sorusunu ortaya çıkarmaktadır.

Bu analiz, ABD ve İsrail'in YZ destekli siber saldırılarını uluslararası hukukun temel parametreleri çerçevesinde incelemektedir. Bu kapsamda çalışmada öncelikle uluslararası hukukun siber uzaya ve buna bağlı olarak YZ teknolojilerine uygulanabilirliği ele alınmakta; ardından kuvvet kullanma yasağı, silahlı saldırı eşiği, devletin uluslararası sorumluluğu ve meşru müdafaa hakkı savaşın somut boyutları üzerinden değerlendirilmektedir.

4 Erman Akıllı, "ABD/İsrail-İran Savaşında İkinci Haftanın Ardından YZ Bilançosu", SETA, 18 Mart 2026, https://www.setav.org/abdisrail-iran-savasinda-ikinci-haftanin-ardindan-yz-bilancosu, (Erişim tarihi: 10 Nisan 2026).

5 Akıllı, "ABD/İsrail-İran Savaşında İkinci Haftanın Ardından YZ Bilançosu".

ULUSLARARASI HUKUKUN SİBER UZAY VE YZ'YE UYGULANABİLİRLİĞİ

ABD/İsrail-İran savaşı kapsamında gerçekleştirilen YZ destekli siber saldırıları uluslararası hukuk bağlamında değerlendirebilmek için öncelikle "gri" ve "kurgusal alanlar" olarak nitelendirilen siber uzay ve YZ'ye mevcut uluslararası hukuk normlarının uygulanıp uygulanamayacağı sorusunu yanıtlamak gerekir.

Siber uzay ve YZ; devletin kara, deniz ve hava egemenlik alanlarından önemli ölçüde ayrışmaktadır. Bu iki alanı diğer alanlardan ayıran en temel özellik ise insan yapımı olmalarıdır.[6] Nitekim siber uzay ve YZ bu yapay nitelikleri gereği –kara, deniz ve havanın aksine– jeopolitik veya doğal sınırlarla kısıtlanmamaktadır.[7]

Siber uzay ve YZ; devletin kara, deniz ve hava egemenlik alanlarından önemli ölçüde ayrışmaktadır. Bu iki alanı diğer alanlardan ayıran en temel özellik ise insan yapımı olmalarıdır.

Uluslararası ilişkiler literatüründe siber uzay; kara, deniz, hava ve dış uzay gibi geleneksel egemenlik alanlarına ek olarak sıklıkla "beşinci alan" olarak nitelendirilmektedir.[8] Buna karşılık YZ ise siber uzaya bağlı ve büyük ölçüde bağımlı bir yapı arz ettiğinden bağımsız bir alan olarak değerlendirilmemektedir. Eğer siber uzayı veya YZ'yi bağımsız beşinci alan olarak kabul edersek, mevcut uluslararası hukuk kurallarının bu alanlardaki faaliyetlere doğrudan uygulanması teorik olarak güçleşebilir. Bu nedenle siber uzay ve YZ'yi bu şekilde konumlandırmak isabetli bir yaklaşım olarak görülmemektedir.

Bu sonuca ulaşmak için kara, deniz, hava ve dış uzayın temel özelliklerine bakmak yeterlidir. Siber uzay ve YZ, diğer dört alanın aksine insanların fiziksel olarak bulunabileceği veya faaliyetlerini bizzat yürütebileceği bir mecra değildir; zira bu alanlara fiziksel olarak "gidilmesi" mümkün değildir. Buna karşılık insan diğer dört alan arasında fiziksel olarak seyahat edebilir ve bu alanlarda konuşlanabilir. Özel ekipman gerektirse bile deniz altına veya dış uzaya gitmek fiziken mümkündür. Bu bağlamda örneğin bir denizaltı denizin altından kara, deniz, hava veya uzaydaki bir hedefi vurmak üzere füze fırlatabilir. Oysa siber uzay veya YZ ortamında bulunan bir unsuru hedef almak için deniz altından doğrudan bu alanlara füze fırlatmak teknik olarak imkansızdır.[9]

Dolayısıyla siber uzay ve YZ, bağımsız bir alan olmaktan ziyade diğer dört alandaki nesneleri etkilemek için kullanılan bir araçtır. Siber faaliyetler veya YZ faaliyetleri nihayetinde kara, deniz, hava ve dış uzayda somut sonuçlar doğurmakta ve bu sebeple söz konusu alanlara ilişkin uluslararası hukuk normları tarafından

6 Mammad Ismayilov, *Siber Uzayda Yeni Devlet Dışı Aktörlerin Uluslararası Sorumluluğu: Atıf, Özen Yükümlülüğü ve Doğrudan Sorumluluk*, (Yetkin Yayınları, Ankara: 2026), s. 35.

7 Nils Melzer, "Cyberwarfare and International Law", UNIDIR Resources, (2011), s. 5, https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf, (Erişim tarihi: 6 Nisan 2026).

8 W. J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*, Cilt: 89, Sayı: 5, (2010), s. 97-108.

9 Christian Czosseck ve Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, (IOS Press, Amsterdam: 2009), s. 132-142.

düzenlenmektedir. Siber uzay ve YZ'nin kurgusal niteliği nedeniyle uluslararası hukukun uygulanabilirliğini sorgulamak yersizdir.[10]

Ayrıca 1945 tarihli BM Şartı gibi temel uluslararası hukuk belgeleri, siber uzay ve YZ'nin icadından önce oluşturulmuş olsalar da yalnızca o dönemdeki değil genel olarak devlet faaliyetlerini düzenlemek amacıyla öngörülmüştür. Mevcut belgelerin siber uzay ve YZ faaliyetlerine uygulanmasını engelleyen herhangi bir sınırlama bulunmamaktadır. Bu bağlamda BM Şartı, 1949 Cenevre Sözleşmeleri ve 2001 tarihli "Uluslararası Haksız Fiillerden Dolayı Devletin Uluslararası Sorumluluğu" taslak maddelerinin, sırf siber çağdan önce kaleme alınmış olmaları gerekçesiyle günümüz operasyonlarının siber boyutuna uygulanamayacağı iddia edilemez.

Bu çerçevede mevcut uluslararası hukuk kurallarının ABD/İsrail-İran savaşında gerçekleştirilen YZ destekli siber saldırılara uygulanabileceği açıktır. Nitekim uluslararası toplumun tutumu da bu yöndedir: BM Hükümet Uzmanları Grubu (GGE) 2013 ve 2015 raporlarında egemenlik, kuvvet kullanma yasağı ve iç işlerine karışmama ilkeleri gibi normların siber uzayda da geçerli olduğunu teyit etmiştir.

KUVVET KULLANMA YASAĞI

Uluslararası hukukun temel taşı olan BM Şartı'nın 2(4). maddesi devletlerin uluslararası ilişkilerinde kuvvet kullanma tehdidini ve kuvvet kullanımını kesin bir dille şöyle yasaklamaktadır:

> Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek Birleşmiş Milletler'in amaçlarıyla bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar.[11]

Bu hüküm sadece bir antlaşma kuralı değil aynı zamanda tüm devletleri bağlayan *jus cogens* (emredici kural) niteliğinde bir normdur. Ancak ABD/İsrail-İran savaşında kullanılan modern askeri müdahaleler siber unsurların ve YZ destekli sistemlerin geleneksel kuvvet kullanımı eşiğini nasıl dönüştürdüğünü tartışmaya açmaktadır. Geleneksel olarak "kuvvet" kavramı 1945'in ruhuna uygun biçimde "silahlı kuvvet" ile özdeşleştirilse de siber saldırıların fiziksel bir mermi patlamadan da egemen bir devleti felç edebilme kapasitesi bu dar yorumu sarsmaktadır. Bir siber saldırının kuvvet kullanımı teşkil etmesi için *Tallinn El Kitabı*'nın 11. Kural'ında belirtilen "kinetik eş değerlik" doktrini uyarınca eylemin ölçeği ve etkileri bakımından fiziksel bir saldırıyla karşılaştırılabilir sonuçlar doğurması

10 Ismayilov, *Siber Uzayda Yeni Devlet Dışı Aktörlerin Uluslararası Sorumluluğu*, s. 37.

11 "Birleşmiş Milletler Şartı", BM, 26 Haziran 1945, https://www.un.org/en/about-us/un-charter/full-text, (Erişim tarihi: 8 Nisan 2026).

beklenir. Bu bağlamda YZ destekli siber saldırıların hukuki statüsünü belirlemek için sadece kullanılan araca değil ortaya çıkan stratejik sonuca odaklanmak bir zorunluluk haline gelmiştir.[12]

ABD ve İsrail'in İran'a karşı gerçekleştirdiği saldırıların ilk aşaması olan "kör etme operasyonu" bu hukuki tartışmanın en somut zeminini oluşturmaktadır. ABD Siber Komutanlığının İran'ın erken uyarı radarları, iletişim ağları ve sensör sistemlerini devre dışı bırakması, ilk bakışta "geçici ve geri dönüşümlü" bir aksaklık gibi görünse de bu fiillerin oluşturduğu işlevsel sonuçlar hayati önemdedir. Geleneksel yaklaşımlar, kalıcı fiziksel hasar doğurmayan frekans karıştırma (RF jamming) veya siber sızmaları 2(4). maddenin eşiğinin altında tutma eğilimindedir; zira ortada yıkılan bir bina veya kaybedilen bir can yoktur.[13] Ancak bu sığ yaklaşım YZ destekli siber müdahalenin asıl amacı olan mağdur devleti savunma kapasitesinden tamamen yoksun bırakmayı göz ardı etmektedir.[14]

İran'ın koordine olma yeteneğinin elinden alınması, binlerce hedefin vurulması ve stratejik liderliğin etkisiz hale getirilmesine yani stratejik dekapitasyona zemin hazırlamıştır.

İran'ın koordine olma yeteneğinin elinden alınması, binlerce hedefin vurulması ve stratejik liderliğin etkisiz hale getirilmesine yani stratejik dekapitasyona zemin hazırlamıştır. Dolayısıyla YZ destekli bir siber saldırıyı kinetik saldırıdan kopuk ve bağımsız bir aksaklık olarak değil toplam askeri harekatın ayrılmaz bir öncülü ve tamamlayıcısı olarak değerlendirmek hukuki gerçekliğin bir gereğidir. YZ destekli siber saldırıların hukuki karakterini tayin etmekte kullanılan geleneksel teoriler, "Destansı Öfke" gibi çok katmanlı ve sofistike operasyonlar karşısında anakronik kalarak yetersizleşmektedir. Bu çerçevede araç temelli yaklaşım (*instrument-based approach*) zihnini sadece konvansiyonel silahların kinetik doğasına hapsettiği için dijital kodlardan oluşan yazılımsal müdahaleleri hukuki değerlendirme alanının dışına itme riski taşımaktadır. Oysa bir aracı "silah" düzeyine taşıyan unsur onun metalik gövdesinden ziyade yöneldiği stratejik amaç ve failin elinde büründüğü yıkıcı etkidir.[15]

Madalyonun diğer yüzünde yer alan hedef temelli yaklaşım (*target-based approach*) ulusal kritik altyapılara yönelik en ufak siber teması dahi kuvvet kullanımı sayarak "aşırı kapsayıcı" bir refleks sergilemekte; bu durum basit bir istihbarat faaliyetini bile savaş gerekçesine (casus belli) dönüştürebilecek tehlikeli bir belirsizlik iklimi oluşturmaktadır.[16]

12 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Sayı: 37, (1999), s. 890-895.

13 Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?", *Stanford Law & Policy Review*, Sayı: 25, (2014), s. 280-285.

14 Francois Delerue, *Cyber Operations and International Law*, (Cambridge University Press, Cambridge: 2020), s. 294-298.

15 Schmitt, "Computer Network Attack and the Use of Force in International Law", s. 890-915.

16 Russell Buchan ve Nicholas Tsagourias, *Regulating Cyber Operations: State Responsibility and the Use of Force*, (Edward Elgar Publishing, Cheltenham: 2020), s. 158-162.

Bu iki kutup arasındaki en makul liman olan "etki ve işlev temelli yaklaşım" ise YZ destekli siber müdahalenin teknik mutfağından ziyade bir devletin egemenlik haklarını ve askeri direnç kapasitesini ne ölçüde felç ettiğine odaklanır. Şayet YZ destekli bir siber saldırı, hedef devletin en temel hakkı olan meşru müdafaa refleksini dahi felç edecek bir yoğunluğa erişiyorsa; kullanılan araç ister bir füze ister bir kod satırı olsun bu eylem tartışmasız bir kuvvet kullanımıdır.

ABD ve İsrail'in İran'a karşı gerçekleştirdiği saldırılarda YZ araçlarının aktif hedefleme rolünde kullanılması, kuvvet kullanma eşiğine ilişkin tartışmalara yeni bir karmaşıklık katmanı eklemiştir. YZ güdümlü sistemlerin hedef seçimini optimize etmesi ve saldırı vektörlerini otonom olarak belirlemesi, kuvvet kullanımının "başladığı an"ın tespitini güçleştirmektedir. Otonom bir yazılımın milisaniyeler içinde gerçekleştirdiği binlerce sızma ve devre dışı bırakma eylemi, insan kontrolündeki bir saldırıdan çok daha hızlı ve yıkıcı bir sürece işaret eder. Bu noktada YZ'nin kararları üzerindeki insan denetiminin seyrelmesi, devletlerin uluslararası sorumluluğunu ortadan kaldırmaz; aksine bu teknolojileri kullanan devletlerin, sistemlerin doğuracağı sonuçlardan doğrudan sorumlu tutulmasını gerektirir. ABD/İsrail-İran savaşı YZ'nin sadece bir verimlilik aracı olmadığını aynı zamanda saldırının ölçeği ve şiddetini 2(4). madde kapsamında kuvvet niteliğine taşıyan temel bir çarpan olduğunu kanıtlamaktadır.

Bilindiği üzere BM Şartı'nın 2(4). maddesi devletlerin siyasal bağımsızlığına karşı kuvvet kullanma tehdidi ve kuvvet kullanımını kesin bir biçimde yasaklamaktadır. ABD ve İsrail'in 28 Şubat'ta gerçekleştirdiği YZ destekli kinetik saldırılar, doğrudan rejim değişikliğini hedefleyerek İran dini lideri Ayetullah Ali Hamaney'i etkisiz hale getirmeye odaklanmış ve bu yönüyle İran'ın siyasal bağımsızlığına karşı açık bir kuvvet kullanımı teşkil etmiştir.

Sonuç olarak ABD/İsrail-İran savaşında YZ ile güçlendirilmiş, kinetik harekatla bütünleşmiş ve devlet tarafından alenen üstlenilmiş olan siber saldırılar; Hamaney ve diğer üst düzey yetkililerin ölümüyle fiziksel zarar eşiğine ulaştığı, İran'ın siyasal bağımsızlığı ve askeri bütünlüğüne yönelik ağır bir müdahale teşkil ettiği için kuvvet kullanma yasağının doğrudan ihlali niteliğine bürünmüştür.

SİLAHLI SALDIRI

Uluslararası hukukun en kritik istisnalarından birini teşkil eden meşru müdafaa hakkı, BM Şartı'nın 51. maddesi uyarınca ancak bir "silahlı saldırı" meydana geldiğinde doğmaktadır. Uluslararası Adalet Divanı (UAD), Nikaragua davasında verdiği tarihi kararla her kuvvet kullanımının silahlı bir saldırı teşkil etmediğini; silahlı saldırının, kuvvet kullanımının "en ağır biçimleri" olduğunu vurgulayarak bu iki kavram arasına bir eşik yerleştirmiştir. Divan, bu ayrımı yapabilmek için

"ölçek ve etki" ölçütünü benimsemiştir.[17] ABD ve İsrail'in saldırılarının YZ ve siber boyutu, tam da bu hukuki gri alanın merkezinde yer almaktadır. Saldırının tasarımcıları, RF jamming ve siber aksamaların kalıcı donanım hasarı doğurmadığı, dolayısıyla "geçici ve geri dönüşümlü" olduğu gerekçesiyle bu eylemlerin silahlı saldırı eşiğinin altında kaldığını ileri sürmektedir. Ancak bir aracı silah kılan onun fiziksel doğası değil hangi amaçla kullanıldığı ve ortaya çıkardığı somut etkidir.[18] Eğer YZ destekli bir siber müdahale, kinetik bir saldırının etkilerine eş değer yıkım, can kaybı veya stratejik felç oluşturuyorsa kullanılan dijital kodun geleneksel bir füzeyle aynı hukuki statüde değerlendirilmesi bir zorunluluktur.

ABD ve İsrail'in saldırıları kapsamında gerçekleştirilen "siber kör etme" faaliyetleri, kinetik operasyonlardan soyutlanarak tek başına ele alındığında "silahlı saldırı" eşiğini aşmıyor gibi görünebilir. Nitekim RF jamming ve sinyal kesme eylemleri, geleneksel olarak egemenlik ihlali veya kuvvet kullanımı kapsamında değerlendirilse de nadiren silahlı saldırı olarak nitelendirilmiştir. Ancak UAD'nin Petrol Platformları davasında işaret ettiği "olayların bütünlüğü" ilkesi, siber saldırının kinetik saldırının ayrılmaz bir parçası olduğunu ortaya koymaktadır.[19] İran'ın savunma ve iletişim kapasitesinin sıfırlanması, akabinde gerçekleşen ve 1.000'den fazla hedefin vurulmasıyla sonuçlanan büyük ölçekli yıkımın zeminini hazırlamıştır. Bu bağlamda YZ destekli siber saldırıları kinetik saldırıdan kopuk, bağımsız birer "teknik aksaklık" olarak görmek hukuki bir körlük oluşturacaktır. İran'ın internet altyapısının yüzde 4 kapasiteye düşürülmesi ve 27 gün boyunca bu seviyede tutulması, meseleyi "rahatsızlık verici bir eylem" olmaktan çıkararak devletin varlığına yönelik sistematik bir saldırı düzeyine taşımaktadır.

BM Genel Kurulunun 3314 sayılı Saldırının Tanımı Kararı'nın 3(b). maddesi, saldırı eylemini "bir devletin ülkesine karşı herhangi bir silah kullanılmasını" içerecek şekilde geniş bir çerçevede tanımlamaktadır. Uluslararası hukuk literatüründe baskın olan görüş, bu maddedeki "herhangi bir silah" ifadesinin sadece kinetik araçları değil oluşturduğu ölçek ve etki bakımından fiziksel yıkıma veya stratejik felce yol açan siber araçları da kapsadığı yönündedir.[20] Kararın 2. maddesinde aranan "yeterli ağırlık" kriteri[21] ABD ve İsrail'in saldırıları bağlamında değerlendirildiğinde bahsi geçen saldırıların toplam etkisinin bu ağırlığı fazlasıyla karşıladığı görülmektedir. Kinetik saldırılarla eş zamanlı olarak yürütülen ve Hamaney dahil üst düzey yetkililerin ölümüyle sonuçlanan bu süreç, Nikaragua

17 Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, International Court of Justice Reports 1986, s. 14; 1986 I.C.J. 14 (27 Haziran 1986).

18 Karl Zemanek, "Armed Attack", *Max Planck Encyclopedia of Public International Law*, Sayı: 1, (2012), s. 599.

19 Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, I.C.J. Reports 2003, s. 161, para. 64, https://www.icj-cij.org/en/case/90, (Erişim tarihi: 8 Nisan 2026).

20 UN General Assembly, Resolution 3314 (XXIX), Definition of Aggression, 14 December 1974, Article 3(b), https://digitallibrary.un.org/record/201407, (Erişim tarihi: 8 Nisan 2026).

21 UN General Assembly, Resolution 3314 (XXIX), Definition of Aggression, 14 December 1974, Article 2, https://digitallibrary.un.org/record/201407, (Erişim tarihi: 8 Nisan 2026).

davasında öngörülen en ağır kuvvet kullanımı biçimine tekabül etmektedir. Öte yandan saldırıların bir parçası olan devlet televizyonunun ele geçirilmesi veya dua uygulamalarının manipüle edilmesi gibi psikolojik harp unsurları, tek başlarına birer silahlı saldırı teşkil etmese de operasyonun genel ölçek ve etkisi içerisinde saldırının ciddiyetini artıran bileşenler olarak okunmalıdır. Burada kritik olan sadece fiziksel yıkım değil devletin savunma refleksleri kırılarak egemenlik bütünlüğünün YZ ve siber araçlarla sistematik olarak tasfiye edilmesidir.

YZ araçlarının hedefleme sürecine dahil edilmesi, silahlı saldırı nitelendirmesinde "özel niyet" (*animus aggressionis*) unsurunun tespitini daha da karmaşıklaştırmaktadır. Uluslararası hukuk, bir eylemin silahlı saldırı sayılabilmesi için belirli bir devlete zarar verme yönünde bilinçli bir irade aramaktadır.[22] YZ destekli otonom sistemlerin hedef seçimini optimize ettiği ve saldırı vektörlerini bağımsız olarak genişlettiği bir senaryoda, niyetin kaynağı neresidir? *Tallinn El Kitabı* ve mevcut normlar, bu teknolojik özerkliği hukuki bir "niyet" çerçevesine oturtmakta yetersiz kalmaktadır.[23] Ancak ABD ve İsrail'in saldırıları bağlamında General Caine'in saldırıları alenen kabul etmesi[24] ve operasyonun stratejik hedeflerini dünya kamuoyuyla paylaşması, niyet belirsizliğini ortadan kaldırmıştır. ABD'nin en üst düzey askeri yetkilileri tarafından üstlenilen bu saldırılar, YZ'nin sadece teknik bir araç olduğunu ve stratejik niyetin ise devletin siyasi iradesine ait olduğunu kanıtlamaktadır. Dolayısıyla YZ kullanımı, sorumluluğu muğlaklaştırmak bir yana saldırının hassasiyetini ve yıkıcılığını artırarak "yeterli ağırlık" kriterinin karşılanmasını kolaylaştıran bir unsura dönüşmüştür.

> İran'ın savunma ve iletişim kapasitesinin sıfırlanması, akabinde gerçekleşen ve 1.000'den fazla hedefin vurulmasıyla sonuçlanan büyük ölçekli yıkımın zeminini hazırlamıştır.

YZ destekli siber saldırıların silahlı saldırı teşkil edip etmediğine ilişkin tartışma, ABD ve İsrail'in saldırıları bağlamında yeni bir boyut kazanmıştır. Geleneksel yaklaşım olan "Fiziksel zarar yoksa silahlı saldırı da yoktur" tezi, YZ'nin bir devleti işlevsiz hale getirebilecek kapasitesi karşısında giderek yetersiz kalmaktadır. Bu nedenle "yıkıcı etki" doğuran siber saldırıların, hedefin niteliğinden bağımsız olarak, sonuçları itibarıyla bir bombardımanla eş değer kabul edilerek "silahlı saldırı" kapsamında değerlendirilmesi gerektiği ileri sürülebilir. Bu noktada "yıkıcı etki" kavramının açıklığa kavuşturulması önem taşımaktadır.

Öncelikle belirtmek gerekir ki "yıkıcı etki" doğuran YZ destekli siber saldırılara ilişkin genel kabul görmüş bir bağlayıcı tanım bulunmamaktadır.[25] Bununla birlikte kavramın anlaşılmasına katkı sunan çeşitli tanımlar mevcuttur. Örneğin National Initiative for Cybersecurity Careers and Studies (NICCS) yıkıcı etkiyi

22 Michael N. Schmitt, "Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics", *Harvard National Security Journal*, (2013).

23 Schmitt, "The Law of Cyber Warfare: Quo Vadis?", s. 269-299.

24 Akıllı, "ABD/İsrail-İran Savaşında İkinci Haftanın Ardından YZ Bilançosu".

25 David Sanger ve John Markoff, "Obama Outlines Coordinated Cyber-Security Plan", *The New York Times*, 29 Mayıs 2009.

operasyonların veya işlevlerin kabul edilemez derecede uzun bir süre boyunca beklenmedik şekilde kesintiye uğramasına yol açan bir olay olarak tanımlamaktadır.[26] Michigan Cyber Disruption Response Strategy ise bu kavramı; elektronik bilgiye, bilgi sistemlerine, hizmetlere veya ağlara ilişkin gizlilik, bütünlük ya da erişilebilirliğin zedelenmesi sonucunda kamu ve özel sektördeki kritik işlev ve hizmetlere zarar veren veya verme ihtimali bulunan; kamu güvenliğini tehdit edebilen, kamu güvenini sarsabilen, ülke ekonomisini olumsuz etkileyebilen ya da devletin güvenliğini zayıflatabilen bir olay şeklinde açıklamaktadır.[27] Bir başka yaklaşıma göre ise yıkıcı etki; fiziksel hasar veya yaralanmaya yol açmaksızın bilgi akışını ya da bilgi sistemlerinin işleyişini kesintiye uğratan eylemleri ifade eder.[28]

ABD ve İsrail'in saldırılarında siber ve kinetik unsurların iç içe geçmesi özellikle yıkıcı etki doğuran YZ destekli siber faaliyetlerin hukuki niteliğinin yeniden değerlendirilmesini zorunlu kılmaktadır.

Bu çerçevede yıkıcı etki doğuran YZ destekli siber saldırıların temel özelliği, ortaya çıkan zararın kesintiye uğratıcı nitelikte olmasıdır. Başka bir ifadeyle bu tür saldırılar sonucunda belirli hizmetler, faaliyetler veya işlevler kullanılamaz hale gelir. Bu durum; kritik bilgi sistemlerine erişimin engellenmesi, internet bağlantısının kesilmesi, belirli ağlara ulaşılamaması veya işletim sistemlerinin işlevsiz hale gelmesi gibi çeşitli şekillerde ortaya çıkabilir. Ayrıca bu etkiler yalnızca doğrudan sonuçlarla sınırlı kalmayıp ikinci ve hatta üçüncü dereceden sonuçlar da doğurabilir.

Bunun yanında söz konusu kesintiye uğratıcı etkilerin belirli bir ağırlık ve ciddiyet düzeyine ulaşması gerekir. Zira bazı yıkıcı etkiler diğerlerine kıyasla çok daha ağır sonuçlar doğurur. Örneğin kritik devlet kurumlarına ait internet sitelerinin devre dışı bırakılması, bir e-ticaret sitesinin erişime kapatılmasına kıyasla çok daha ciddi sonuçlara neden olmaktadır.

ABD ve İsrail'in saldırılarında siber ve kinetik unsurların iç içe geçmesi özellikle yıkıcı etki doğuran YZ destekli siber faaliyetlerin hukuki niteliğinin yeniden değerlendirilmesini zorunlu kılmaktadır. Bu tür saldırılar fiziksel hasar üretmese bile kritik altyapıyı devre dışı bırakarak, kamu düzenini ciddi biçimde sarsarak ve hatta dolaylı biçimde insan hayatını tehlikeye atarak klasik silahlı saldırıların doğurduğu sonuçlara benzer etkiler ortaya çıkarabilmektedir. Bu nedenle belirleyici olan unsur, kullanılan aracın niteliğinden ziyade ortaya çıkan etkinin ağırlığıdır. Şayet bir YZ destekli bir siber saldırı yaygın, derin ve ciddi kesintilere yol açarak devletin temel fonksiyonlarını felce uğratıyorsa bu durumda söz konusu eylemin yıkıcı etki doğurduğu kabul edilmelidir. Bu durumda söz konusu fiilin uluslarara-

26 "Explore Terms: A Glossary of Common Cybersecurity Terminology", National Initiative for Cybersecurity Careers and Studies (NICCS), 10 Şubat 2015, https://definedterm.com/a/download/document/11128, (Erişim tarihi: 23 Nisan 2026).

27 "State of Michigan Cyber Disruption Response Plan", State of Michigan Executive Office, 12 Kasım 2023, https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Services/Cybersecurity/Cyber-Disruption-Response-Plan.pdf, (Erişim tarihi: 23 Nisan 2026).

28 Ido Kilovaty, "Virtual Violence - Disruptive Cyberspace Operations as 'Attacks' under International Humanitarian Law", *Michigan Telecommunications and Technology Law Review*, Cilt: 23, Sayı: 1, (2016), s. 123-124.

sı hukuk bakımından bir silahlı saldırı olarak değerlendirilmesi gerektiği yönündeki yaklaşım güç kazanmaktadır. Bu yorum aynı zamanda uluslararası hukukun statik değil teknolojik gelişmelere uyum sağlayabilen dinamik bir yapı arz ettiğini de ortaya koymaktadır.

DEVLETİN SORUMLULUĞU

Uluslararası hukukta devletin sorumluluğu, bir devletin hukuka aykırı bir fiiliyle bir başka hukuk kişisine zarar vermesi durumunda doğan hukuki ilişkiyi ifade eder. Bu sorumluluğun temel çerçevesi 2001 tarihli "Uluslararası Haksız Fiillerden Dolayı Devletin Uluslararası Sorumluluğuna İlişkin Taslak Maddeler" belgesiyle çizilmiştir. Bu belgenin 2. maddesi uyarınca bir devletin sorumlu tutulabilmesi için iki temel şartın eş zamanlı gerçekleşmesi gerekir: (i) fiilin (icrai veya ihmali) uluslararası hukuka göre devlete isnat/atıf edilebilmesi, (ii) bu fiilin devletin bir uluslararası yükümlülüğünü ihlal etmesi.[29]

Saldırıların teknik mutfağında yer alan ABD Siber Komutanlığı ve İsrail 8200 Birimi gibi yapıların konumu, uluslararası sorumluluk hukuku açısından gri alan bırakmamaktadır. 2001 tarihli belgenin 4. maddesi uyarınca bir devletin yasama, yürütme veya yargı fonksiyonlarını icra eden herhangi bir kişi veya birimin fiili o devletin fiili sayılmaktadır.

Burada kritik olan husus şudur: Bu birimler ilgili devletlerin iç hukukunda resmi olarak "devlet organı" (*de jure organ*) statüsünde tanımlandıkları için siber uzaydaki her hamleleri doğrudan devletin şahsiyetine atfedilir. Bu bağlamda YZ destekli siber saldırıların kim tarafından yapıldığını belirleme sorunu, failin anonim kaldığı vakaların aksine, resmi devlet kurumlarının açık müdahalesiyle birlikte hukuki bir "isnat edilebilirlik" kesinliğine dönüşmüştür. 2001 tarihli belgenin 4. maddesi bu tür kurumsal müdahalelerde "etkin kontrol" gibi daha karmaşık testlere ihtiyaç duymaksızın sorumluluğu doğrudan devletin üzerine yüklemektedir.

MEŞRU MÜDAFAA HAKKI

BM Şartı'nın 51. maddesiyle güvence altına alınan meşru müdafaa hakkı, YZ ve siber uzayın anonim ve hibrit doğasıyla birlikte köklü bir dönüşüm yaşamaktadır. ABD ve İsrail, askeri eylemlerini İran'ın Hamas, Hizbullah ve Husiler gibi vekil gruplar aracılığıyla uzun süredir sürdürdüğü sistematik saldırılarla bağlantılı bir güvenlik tehdidine karşı öz savunma hakkı kapsamında gerekçelendirmektedir. Bu argümanın temelinde UAD'nin Nikaragua davasında belirlediği "önemli

29 Enver Bozkurt, Yasin Poyraz ve Selcan Erdal, *Devletler Hukuku*, 11. Baskı, (Yetkin Yayınları, Ankara: 2021), s. 273.

ölçüde dahliyet" ölçütü yer almaktadır.[30] Washington ve Tel Aviv yönetimleri, Tahran'ın vekil gruplarına sağladığı stratejik ve lojistik desteğin İsrail'e yönelik saldırılarla bağlantılı olduğunu ileri sürerek 2026'daki kapsamlı operasyonu öz savunma hakkı kapsamında gerekçelendirmektedir. Ancak bu yaklaşım uluslararası hukuk literatüründe tartışmalıdır. Ayrıca YZ destekli siber saldırıların bu kinetik harekatın öncüsü olarak kullanılması, meşru müdafaanın klasik sınırlarını zorlayan yeni bir hukuki tartışmayı da beraberinde getirmiştir.

YZ destekli siber saldırıların meşru müdafaa kapsamında değerlendirilmesinde en kritik eşik, bu saldırıların "zorunluluk" ve "orantılılık" ilkelerine uygunluğudur. ABD Siber Komutanlığı siber müdahaleleri "kinetik eşiğin altında kalan destekleyici unsurlar" olarak tanımlayarak hukuki bir koruma kalkanı oluşturmaya çalışmıştır.[31] Fakat devletin temel işlevlerini felç eden, askeri komuta kontrol ağlarını çalışamaz hale getiren ve savunma kapasitesini sıfırlayan YZ destekli bir siber saldırı, fiziksel yıkım oluşturmasa dahi silahlı saldırı ile eş değer kabul edilebilir. İran'ın savunma refleksleri YZ destekli siber araçlarla kör edildikten sonra 1.000'den fazla hedefin vurulması, siber ve kinetik saldırıların birbirinden bağımsız orantılılık testine tabi tutulmasını imkansız kılmaktadır. Bu durum, YZ destekli siber saldırıların artık tek başına değil ortaya çıkardığı stratejik sonuçlar üzerinden bütünsel bir orantılılık analizine tabi tutulması gerektiğini göstermektedir.

ABD ve İsrail'in saldırılarının en dikkat çekici yönlerinden biri özel sektör mülkiyetindeki dijital altyapıların birer askeri hedefe dönüşmesidir.

ABD ve İsrail'in saldırılarının en dikkat çekici yönlerinden biri özel sektör mülkiyetindeki dijital altyapıların birer askeri hedefe dönüşmesidir. YZ destekli bir siber saldırının hedefi doğrudan bir askeri tesis olmasa bile dev bir hastane ağının veya Google gibi küresel bir veri merkezinin çökertilmesi gibi sivil sistemlere yönelik müdahaleler, yol açtığı yıkıcı etkiler nedeniyle silahlı saldırı olarak sınıflandırılabilir. Modern devletlerde kritik ulusal altyapıların büyük kısmının özel şirketlerin elinde olması, bu kurumları "dijital cephe hattı"na taşımaktadır.

ABD/İsrail-İran savaşı meşru müdafaa hakkının 21. yüzyılın teknolojik gerçekliğine göre yeniden yorumlanması gerektiğini ortaya koymaktadır. YZ destekli siber saldırılar, geleneksel mermilerden daha sessiz olsa da bir ulusu savunmasız bırakma kabiliyeti bakımından çok daha etkilidir. Eğer YZ destekli bir siber saldırı, hükümetin temel görevlerini yerine getirmesini engelliyor ve silahlı kuvvetlerin konuşlandırılmasını imkansız kılıyorsa bu saldırı 51. madde anlamında bir saldırıdır. Ancak bu noktada devletlerin "savunma" adı altında yürüttükleri saldırgan stratejilerin zorunluluk ilkesini aşmamasına dikkat etmeleri gerekir. ABD Başkanı

30 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14, para. 195.

31 *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, US Cyber Command, 23 Mart 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, (Erişim tarihi: 8 Nisan 2026).

Donald Trump'ın İran'ın altyapısını "havaya uçurma"[32] yönündeki söylemi gibi saldırgan beyanlar, meşru müdafaa hakkının sınırlarını aşarak uluslararası barışı tehlikeye atan bir kuvvet kullanımı tırmanışına dönüşme riski taşımaktadır.

SONUÇ

28 Şubat 2026'da başlatılan ABD/İsrail saldırıları, uluslararası hukukun temel taşları olan kuvvet kullanma yasağı, silahlı saldırı eşiği, devletin sorumluluğu ve meşru müdafaa hakkı gibi normların çok kapsamlı bir sınava tabi tutulduğu tarihi bir dönüm noktası olarak kayda geçmiştir. 7 Nisan 2026 itibarıyla ilan edilen ateşkesle savaşın sıcak aşaması sona ermiş olsa da bu süreçte siber saldırıların ulaştığı boyut ve YZ'nin oynadığı derin rol mevcut hukuki paradigmanın yetersizliğini açıkça ortaya koymuştur.

Savaş süresince analiz edilen tüm veriler ışığında ulaşılan temel tespitler, YZ ve siber uzayın artık yalnızca teknik bir alan olmadığını aynı zamanda uluslararası hukukun doğrudan uygulama sahası haline geldiğini ve bu alandaki gri bölgelerin ivedilikle kodifiye edilmesi gerektiğini göstermektedir.

Bu analizden çıkan ilk temel sonuç, ABD tarafından resmi olarak üstlenilen YZ destekli siber saldırıların, BM Şartı'nın 2(4). maddesi kapsamında kuvvet kullanımı eşiğine işlevsel olarak ulaştığıdır. YZ destekli siber müdahalelerin kinetik harekatla tam entegre biçimde yürütülmesi, bu eylemlerin sadece birer teknik aksaklık değil hedef devletin egemenliğine yönelik doğrudan bir saldırı olduğunu göstermektedir. Özellikle İran'ın internet altyapısının savaş boyunca fiilen neredeyse sıfırlanması ve savunma kapasitesinin felç edilmesi, YZ destekli siber saldırıların ölçek ve etki bakımından bir silahlı saldırı niteliği taşıdığına dair en somut veridir. Bu durum YZ destekli siber saldırıların fiziksel yıkım oluşturmasa dahi stratejik sonuçları itibarıyla geleneksel savaş araçlarıyla eş değer görüldüğü bir dönemi başlatmıştır.

Devletin sorumluluğu ve atıf meselesi açısından ABD/İsrail-İran savaşı geçmişteki siber çatışmaların aksine çok daha berrak ve tartışmasız bir zemin sunmaktadır. Saldırıların hem ABD hem de İsrail tarafından resmi düzeyde üstlenilmesi, klasik siber savaşların vazgeçilmez bir unsuru olan "makul inkar edilebilirlik" perdesini bu kez bütünüyle indirmiştir.

Siber mecranın doğurduğu tüm bu nevzuhur meydan okumalar ve normatif boşluklara rağmen mevcut uluslararası hukuk, bu yeni gerçeklik karşısında bütünüyle aciz ve dilsiz değildir. Aksine yerleşik teamüller ve temel ilkeler; siber uzay ve YZ'nin kaotik doğasını uluslararası hukukla evcilleştirebilecek ölçüde köklü

32 "Trump Warns a 'Whole Civilization will Die Tonight' if a Deal with Iran isn't Reached", PBS NewsHour, 7 Nisan 2026, https://www.pbs.org/newshour/amp/world/trump-warns-a-whole-civilization-will-die-tonight-if-a-deal-with-iran-isnt-reached, (Erişim tarihi: 21 Nisan 2026).

bir esneklik ve direnç kapasitesine sahiptir. Bu süreçte uluslararası hukuk, teknoloji karşısında geri çekilen değil onunla birlikte dönüşerek egemenlik haklarının dijital kalkanı olmayı başaran dinamik bir normatif yapı olarak varlığını devam ettirmektedir.

MAMMAD ISMAYILOV

Gaziantep Üniversitesi Tarih Bölümü'nden lisans ve Ceza ve Ceza Muhakemesi Hukuku Programı'ndan yüksek lisans derecelerini almıştır. Ankara Sosyal Bilimler Üniversitesi'nde uluslararası hukuk alanında doktora eğitimini tamamlamıştır. Çalışma alanları arasında uluslararası hukukta siber uzay ve uzay hukuku, uluslararası silahlı çatışmalar hukuku, uluslararası insan hakları hukuku ve uluslararası deniz hukuku yer almaktadır.

ABD/İsrail-İran Savaşı:
Yapay Zeka Çağında Savaşın Dönüşümü ve Uluslararası Hukuk

Mammad Ismayilov

28 Şubat 2026'da başlayan ABD/İsrail-İran savaşıyla birlikte YZ destekli siber araçlar kinetik saldırılarla eş zamanlı olarak savaş ortamında kullanılmıştır. Bu analiz söz konusu YZ destekli siber saldırıların BM Şartı'nın 2(4). maddesi kapsamındaki kuvvet kullanma yasağı ve 51. maddesi kapsamındaki silahlı saldırı eşiğini aşıp aşmadığını, devletin uluslararası sorumluluğu bağlamında atıf sorununu ve meşru müdafaa hakkının bu çerçevedeki sınırlarını eleştirel bir perspektifle incelemektedir.

20.yıl | SETA

ANKARA • İSTANBUL • WASHINGTON D.C. • BERLİN • BRÜKSEL

www.setav.org