DİJİTAL CEPHE: İSRAİL VE İRAN ARASINDAKİ YAPAY ZEKÂ DESTEKLİ SİBER SAVAŞ

THE DIGITAL FRONT: AI-SUPPORTED CYBER WARFARE BETWEEN ISRAEL AND IRAN

Yusuf DİNÇEL

71

Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
Yıl: 2026 Sayfa: 1-17
https://dergipark.org.tr/tr/pub/cusosbil

DOI: 10.35379/cusosbil.1670774

Geliş Received: **06.04.2025**
Kabul Accepted **15.12.2025**

DİJİTAL CEPHE: İSRAİL VE İRAN ARASINDAKİ YAPAY ZEKÂ DESTEKLİ SİBER SAVAŞ

THE DIGITAL FRONT: AI-SUPPORTED CYBER WARFARE BETWEEN ISRAEL AND IRAN

Anahtar Kelimeler:
Siber Savaş,
Yapay Zekâ,
Siber Güvenlik,
İsrail,
İran.

Keywords:
Cyber War,
Artificial Intelligence,
Cybersecurity,
Israel,
Iran.

Yusuf DİNÇEL [1]

ÖZ

Teknolojik gelişmelerin her geçen gün hızlı bir şekilde artması, bir yönüyle gündelik hayatı kolaylaştırırken, diğer yönüyle yeni güvenlik tehditlerini de beraberinde getirmektedir. Dünya tarihinde bugüne kadar cereyan eden savaşlara bakıldığında, savaşların çoğunlukla geleneksel yöntemlerle icra edildiği görülmektedir. Ancak son yıllarda, savaşlara yeni bir boyut eklenmiş olup, siber ortamda devletler arasında çatışmalar yaşanmaktadır. İsrail ve İran, Ortadoğu'da birbirlerine rakip iki önemli güçtür. Son dönemde İsrail ile İran arasında doğrudan konvansiyonel askeri çatışmalar yaşanmış ve buna paralel olarak siber uzay da savaşın tamamlayıcı ve stratejik bir cephesi hâline gelmiştir. Bu çalışmanın amacı, İsrail ve İran arasındaki siber savaşın hangi vasıtalar aracılığıyla ve ne şekilde icra edildiğini ortaya koymaktır. Bu çalışmada, İsrail ve İran'ın hangi sektörlere yönelik siber saldırılar gerçekleştirdikleri ve yapay zekâdan hangi adımlarda istifade ettikleri analiz edilmiştir. Bu araştırmanın örnekleri, siber güvenlik ve yapay zekâ konularında yayımlanmış güncel haber içerikleri, politika belgeleri ve düşünce kuruluşlarının analiz raporları temel alınarak oluşturulmuştur. Bulgulara göre, İsrail-İran mücadelesinde siber saldırılar hem kritik altyapıları işlevsiz hale getirmeyi hedefleyen bir operasyonel araç hem de kamuoyu algısını yönlendiren, psikolojik harp ve bilgi operasyonlarını icra eden stratejik bir güç unsuru olarak kullanılmaktadır.

ABSTRACT

The rapid acceleration of technological advancements not only facilitates various aspects of daily life but also introduces new security threats. A review of wars that have occurred throughout world history shows that they were predominantly conducted through conventional means. However, in recent years, a new dimension has emerged, with states increasingly engaging in conflicts within the cyber domain. Israel and Iran are two major rival powers in the Middle East. In recent years, direct conventional military confrontations have occurred between the two states, and in parallel with these developments, the cyber domain has increasingly evolved into a complementary and strategic front of warfare. The aim of this study is to examine the mechanisms and methods through which cyber warfare between Israel and Iran has been conducted. The research analyzes the sectors targeted by both states in their cyber operations and the specific stages at which artificial intelligence technologies are employed. The cases investigated in this study are based on recent news reports, policy documents, and analytical reports published by think tanks specializing in cybersecurity and artificial intelligence. According to the findings, cyberattacks in the Israel-Iran rivalry function both as an operational tool aimed at disabling critical infrastructure and as a strategic instrument employed in psychological warfare and i-formation operations to shape public perception. These results highlight the growing centrality of cyber capabilities and AI technologies in contemporary interstate conflicts.

[1] Dr. Öğr. Üyesi, Yusuf DİNÇEL, Polis Akademisi, İç Güvenlik Fakültesi, Uluslararası İlişkiler Bölümü, dncl_10@hotmail.com, ORCID: 0000-0002-2615-6025

Alıntılamak için/Cite as: Dinçel Y. (2026) Dijital Cephe: İsrail Ve İran Arasındaki Yapay Zekâ Destekli Siber Savaş, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, s.1-17

GİRİŞ

Günümüzde dijital teknolojiler yalnızca hayatı kolaylaştırmakla kalmayıp, devletler arası rekabetin doğasını da radikal biçimde dönüştürmektedir. Siber uzay, artık hem bir çatışma alanı hem de stratejik etki yaratma sahası haline gelmiştir. Özellikle Ortadoğu'daki bölgesel güçler olan İsrail ve İran arasındaki ilişkiler, bu yeni dijital çatışma biçiminin en belirgin örneklerinden birini sunmaktadır.

Teknolojinin hızlı bir şekilde ilerlemesi neticesinde, uluslararası güvenlik dinamikleri önemli bir dönüşüm sürecine girmiştir. Siber savaşlar, geleneksel güvenlik algılarını sarsmış ve devletlerin savunma stratejilerini yeniden şekillendirmelerine yol açmıştır. Bu kapsamda, İsrail ve İran arasındaki siber çatışma örneği, dijital teknolojilerin devletler arası rekabeti nasıl etkilediğini ve uluslararası güvenlik yaklaşımlarını nasıl yeniden şekillendirdiğini ortaya koymaktadır.

Bu makale, İsrail ve İran arasındaki siber savaşın dinamiklerinin ne olduğu ve yapay zekânın bu süreçte nasıl bir rol üstlendiği sorularına cevap aramaktadır. Özellikle yapay zekâ teknolojilerinin hem saldırı hem de savunma mekanizmalarını dönüştürücü etkisi, bu makalenin merkezinde yer almaktadır. Bu kapsamda, makalenin hipotezi, İsrail ve İran arasındaki siber çatışmaların çok katmanlı bir karaktere sahip olduğu; sadece teknik altyapılara yönelik saldırılarla sınırlı kalmayıp, aynı zamanda devletlerin güvenlik stratejilerini, dış politika yaklaşımlarını ve kamuoyunu şekillendirme biçimlerini de doğrudan etkilediğidir. Bu çerçevede makale, iki ülke arasındaki siber mücadelenin tarihsel gelişimini, yöntemlerini ve etkilerini örnek olaylar üzerinden kapsamlı bir şekilde değerlendirmektedir. Türkiye'de yayımlanan akademik çalışmalar arasında, yapay zekâ destekli siber operasyonları ele alan araştırmalar sınırlıdır. Bu makale, siber savaşın teknik boyutlarını stratejik, politik ve toplumsal etkilerle birlikte değerlendirmesi ve yapay zekânın çatışmalar üzerindeki dönüştürücü rolünü bütüncül bir perspektifle incelemesi bakımından literatürdeki boşluğu dolduran nadir çalışmalardan biri niteliğindedir.

Makalede, siber savaşın yalnızca teknik bir güvenlik problemi olarak değerlendirilemeyeceği ortaya koyulmaktadır. Siber savaş, günümüzde artık salt bir bilişim güvenliği meselesi olmaktan çıkmış; hibrit savaş doktrinleri, stratejik caydırıcılık yaklaşımları, enformasyon savaşı pratikleri ve siber güç mücadelesiyle iç içe geçmiş, çok boyutlu bir güvenlik alanı hâline gelmiştir. Yapay zekânın siber alandaki kullanımı, devletlerin yalnızca savunma kapasitelerini değil, aynı zamanda algı yönetimi, psikolojik harekât ve stratejik üstünlük kurma çabalarını da dönüştürmektedir. Bu yönüyle çalışma, İsrail-İran siber çatışmasını yalnızca operasyonel bir rekabet olarak değil; bilgi temelli güç mücadelesinin güncel bir yansıması olarak ele almakta ve literatürdeki klasik siber güvenlik yaklaşımlarından farklı bir bakış açısı ortaya koymayı amaçlamaktadır.

YÖNTEM

Bu makale, nitel araştırma yaklaşımı benimsenmek suretiyle ele alınmıştır. Makale, örnek olay (case study) araştırma yöntemi çerçevesinde değerlendirilmiş ve karşılaştırmalı analiz yöntemi kullanılarak, İsrail ve İran'ın siber savaş pratikleri sistematik biçimde ortaya konmuştur. Makalede, iki ülke arasındaki siber çatışmaların temel unsurları, yapay zekâ teknolojilerinin bu süreçteki rolü ve siber operasyonların hedef aldığı alanlar karşılaştırmalı bir bakış açısıyla detaylandırılmıştır. Araştırmada kullanılan veriler, konuyla ilgili geçmiş ve güncel haberler, devletlerin yayınlamış olduğu resmî belgeler ve düşünce kuruluşlarının analiz raporları bağlamında elde edilmiştir. Böylece ortaya konan bilgiler siber güvenlik, yapay zekâ ve İsrail-İran ilişkileri alanında yayın yapan önemli kaynaklar taranarak temin edilmiştir. Veri seçiminde, İsrail ve İran arasındaki doğrudan siber çatışmaları içermesi, kritik altyapılar, devlet kurumları veya toplumsal güvenlik üzerinde etkisinin bulunması kıstas alınmıştır. Yapay zekâ destekli siber operasyonlara dair teknik ve stratejik bilgiler ile akademik açıdan güvenilir kaynaklar, bu makalede temel ölçüt olarak kabul edilmiştir.

Toplanan veriler içerik analizi tekniği ile ele alınmıştır. Bu çerçevede, İsrail ve İran'ın siber saldırı türleri, hedef aldıkları alanlar, savunma kapasiteleri ve yapay zekâ kullanım yöntemleri tematik olarak sınıflandırılmıştır. Akabinde, bu temalar üzerinden her iki ülkenin siber stratejileri, saldırı ve savunma pratikleri karşılaştırmalı

analiz yöntemi ile incelenmiştir. Çalışmanın temel sınırlılığı, analizlerin açık kaynak verileri ile kısıtlı olmasıdır. Siber saldırılar ve istihbarat faaliyetleri büyük ölçüde gizlilik unsurları barındırdığından dolayı, devletlerin tüm operasyonel kapasitelerine doğrudan erişim mümkün değildir. Bunun yanı sıra siber savaş ve yapay zekâ alanlarının hızla değişen ve dönüşen yapısı nedeniyle elde edilen bulguların, içerisinden geçtiğimiz bu dönem için tartışılması yerinde olacaktır. Bu durum araştırmanın metodolojik sınırlılıklarını oluşturmaktadır.

SİBER SAVAŞIN KAVRAMSAL ÇERÇEVESİ

Tarih boyunca devletler, uluslararası güç dengelerine yön verebilmek için kendi ulusal gündemleri doğrultusunda savaşlara müdahil olmuşlardır. Geçmişte kılıç ile yapılan savaşlardan, günümüzdeki insansız hava aracı saldırılarına kadar, uluslararası arenadaki güç dengesi, teknoloji tarafından değişime zorlanmaktadır. Bu kapsamda, devletler rakiplerine karşı güç üstünlüğünü ele geçirebilmek için yenilikçi yollara başvurmaktadırlar (Robinson vd., 2015). Son yirmi yılda modern toplumların, bilgisayar tabanlı sistemlere bağımlılıkları son derece artmıştır. Ülkelerin kritik altyapılarında önemli rol oynayan teknoloji, aynı zamanda ulusal güvenliğe tehdit olabilecek unsurları içerisinde barındırmaktadır (Smith, 2013). Siber kavramı literatürde, bilgisayar ve elektromanyetik hususları vurgulamak için kullanılır. Siber alan ise, interneti, fiber optik kablo teknolojisini ve uzay ölçeğindeki iletişim ağlarını kapsamaktadır (Nye, 2011). Siber savaş, dijital ve teknolojik metotlar kullanılarak, ülkelerin kritik altyapılarına yönelik yapılan saldırıların tamamına verilen isimdir. Siber savaş, bu yolla, istihbarat toplama ve toplumlar nezdinde algı oluşturma çabaları gibi görevler de üstelenir (Çalışkan, 2023). Bu tanımlar ışığında siber savaş, yalnızca teknik bir güvenlik tehdidi olarak değil, aynı zamanda siyasi karar alma süreçlerini, kamuoyunu ve uluslararası güç dengelerini etkileyen çok katmanlı bir mücadele alanı olarak değerlendirilmektedir. Siber saldırılar sebebiyle, dijital ortamda bulunan bilgilerin gizliliği ve bütünlüğü tehlikeye girmektedir (Hodges & Creese, 2015). Siber saldırılar ile veriler ve kontrol sistemleri hedef alınır. Verilere yönelik saldırılar sayesinde, hedef alınan kurum veya kişinin bilgileri ele geçirilmeye çalışılır. Kontrol sistemlerine yönelik saldırılarda ise su kaynakları, elektrik hatları ve demiryolu gibi fiziksel altyapıları yöneten bilgisayar sistemlerinin devre dışı bırakılması amaçlanır (Rosenfield, 2009).

Her yıl, milyonlarca hedefe yönelik siber saldırı gerçekleştirilmektedir. Maryland Üniversitesi tarafından 2024 yılında yapılan bir araştırmaya göre, Amerika Birleşik Devletleri (ABD) bünyesindeki kuruluşlar, her hafta 1636 saldırıya maruz kalmaktadır. Siber saldırılar, 2024'ün ikinci çeyreğinde %30 oranında artış göstermiştir. Ayrıca Uluslararası Para Fonu (IMF)'nun bir raporuna göre, siber suçların 2027 yılında dünya genelinde 23 trilyon dolar zarara sebep olacağı tahmin edilmektedir (Nye, 2017; SentinelOne, 2025). Bu çerçevede, siber saldırının, modern güvenlik anlayışında giderek daha önemli bir tehdit unsuru haline geldiği söylenebilir. Özellikle devletlerin kritik altyapılarına yönelik gerçekleştirilen bu tür saldırılar, yalnızca maddi kayba sebep olmakla kalmayıp, toplumsal düzeni sarsma potansiyeline sahiptir. Siber savaşın, doğrudan fiziksel yıkımdan çok, sistemlerin işleyişini bozarak kaos yaratma amacı taşıdığı göz önünde bulundurulmalıdır. Bu nedenle, devletlerin siber savunma kapasitelerini geliştirmeleri ve bu alandaki tehditlere karşı daha proaktif stratejiler benimsemeleri hayati bir önem taşımaktadır.

Jason Healey, siber savaşın tarihini üç aşamaya ayırmıştır. Buna göre, siber savaş kavramı, 1980'li yıllarda ilk defa gündeme gelmeye başlamıştır. 1998'den 2003 yılına kadar, siber savaş yükseliş dönemine girmiştir. Son olarak 2003'ten günümüze kadar olan kısımda ise, siber savaşın militarizasyon dönemi yaşanmaktadır (Mazanec, 2015). 1990'lı yılların sonunda ABD'de cereyan eden DoS (Denial of Service) saldırıları sebebiyle, ABD Hükümeti, bilgisayar güvenliği ve siber savaş tehdidine karşı önlemler almaya başlamıştır. Bu dönemde, dünya genelinde de siber saldırıların yaşanmaya başladığı bilinmektedir. 1998 yılında "Tamil Hacker"ları adlı bir grup, Sri Lanka'nın yurtdışındaki büyükelçiliklerini hedef alarak e-posta yoluyla siber saldırılar gerçekleştirmiştir. Ayrıca 1999 yılında Çinli "hacker"lar, Pekin'deki ABD Büyükelçiliğinin web sayfasına saldırmışlardır. 2000 yılında ise, İsrailli "hacker"lar, Hizbullah'ın resmi internet sitesine saldırırken; Filistinliler, İsrail Dışişleri Bakanlığı'nın web sayfasına siber saldırı düzenlemişlerdir. Estonya'nın

başkenti Talin'de 26 Nisan 2007'de Estonya Hükümeti'nin talimatını yerine getirmek için bir parka giden işçiler, Kızıl Ordu askerlerini temsil eden bir heykeli parktan kaldırmışlardır. Estonya Hükümeti'nin bu hamlesine karşılık olarak, kendini Rusya'ya yakın hisseden çok sayıda protestocu bir araya gelerek, hükümeti protesto etmiştir. Bu gelişmelerin akabinde, 27 Nisan'da başlayan ve Mayıs ayının ortasına kadar devam eden siber saldırılar, Estonya Hükümeti'ni zor durumda bırakmıştır. Bu siber saldırılar kapsamında, medya organları, bankacılık sektörü ve siyasi parti web siteleri zarar görmüştür. Estonya'daki siyasiler ve askeri yetkililer, bu topyekûn siber saldırılardan dolayı Rusya'yı sorumlu tutmuşlar ve Rusya'nın, Estonya'ya siber savaş ilan ettiğini açıklamışlardır. Yaşanan bu durum, Batı ülkelerini endişeye sevk etmiştir. Estonya Hükümeti, bu durumu ülkenin bağımsızlığından itibaren karşılaştığı en büyük güvenlik tehdidi olarak ilan etmiştir. Bu olay, literatürde modern anlamda kayda geçen ilk siber saldırı vakası olarak değerlendirilmektedir (Kaiser, 2015; Stiennon, 2015).

Yakın tarihte gerçekleşen siber saldırılara örnek olarak, Mart 2019'da Venezuela'nın elektrik altyapısını hedef alan saldırı gösterilebilir. Venezuela'daki siber saldırılar, yaklaşık 4 gün boyunca devam etmiş ve birçok mağaza ile restoran kapanmak zorunda kalmıştır. Toplu taşıma sisteminin işlevsiz hâle gelmesi, bireylerin iş yerlerine ulaşmalarını ciddi ölçüde engellemiştir. Bunun yanı sıra, çok sayıda yağma vakası yaşanmış ve elektrik yetersizliği sebebiyle hastanelerde 17 kişi hayatını kaybetmiştir (Libicki, 2020). Venezuela örneğinden de anlaşılacağı üzere, siber savaş saldırılarında gerçek güç kullanımı, karmaşık ve dolaylı bir şekilde gerçekleşmekte olup, sonuçta büyük zararlara ve can kayıplarına yol açmaktadır (Rid, 2012). Siber savaşın iç politikayı yönlendirerek, ulusal güvenliği tehdit eden bir yönü de bulunmaktadır. 2016 yılında ABD'deki başkanlık seçimleri sırasında Rusya'nın, sahte mesajlar yayarak Amerikan seçimlerini etkilediği iddiası, buna örnek olarak gösterilir (Kober, 2019). Bu olaylar, siber savaşın modern güvenlik anlayışında ne kadar kritik bir rol oynadığını ortaya koymaktadır. Ayrıca, siber saldırıların yalnızca bireysel "hacker" girişimlerinden ibaret olmadığı, aksine devlet destekli organize eylemler şeklinde, bir savaş aracı olarak kullanılabileceği gerçeği uluslararası toplumu endişeye sevk etmiştir.

Siber saldırılar, kötü amaçlı kullanılan yazılım türleri (solucanlar, virüsler, truva atları) aracılığıyla gerçekleştirilebileceği gibi, ağların izlenmesi ve güvenlik açıklarının tespit edilmesi şeklinde de gerçekleşebilir (Tabansky, 2011). Ayrıca, bilgisayar sistemlerine sızılarak yerleştirilen zararlı yazılımlar aracılığıyla sistemler çökertilebilir veya veriler silinebilir. Bu saldırı yöntemine mantık bombaları denilmektedir. Bunun yanı sıra tuzak kapıları yöntemi ile, yabancı sistemlere tekrar duhul edebilmek için sistemde kod parçaları bırakılmaktadır. Bir diğer önemli saldırı türü ise Botnet'tir. Bu yöntem ile, herhangi bir ağın yabancı biri tarafından uzaktan yönetilmesi amaçlanmaktadır. Bu yöntemler dikkate alındığında, siber saldırıların düşük maliyetle gerçekleştirilebildiği ve hedef alınan sistemlerde ciddi zararlara yol açabildiği anlaşılmaktadır. DoS ve DDoS (Distributed denial of Service) saldırıları, siber saldırılar sırasında en çok kullanılan yöntemlerin başında gelmektedirler. DoS saldırılarında temel amaç, hedef unsurun bilgisayara erişimini tamamen engellemektir. Hedefin bilgisayarına çok sayıda veri gönderilerek, sistemin çökmesi sağlanır. DDoS saldırılarında ise, internet siteleri veya sunucuları kullanıcıların erişimine kapatılır (Yenal & Akdemir, 2020). Buradaki siber operasyonlardaki amaç, hedefin bilgisayar faaliyetlerini bozmak veya yok etmektir (Smeets, 2018). Siber savaşta başarı, hedef ülkeye yönelik hızlı ve yüksek etki yaratan operasyonların hayata geçirilmesine bağlıdır (Kallberg, 2016). Bu çerçevede, siber operasyonların icra edilebilmesi maliyetli olup, operasyonu gerçekleştirenlerin sürekli kendilerini geliştirmeleri gerekmektedir (Lund, 2025).

İnternetin casusluk amacıyla kullanılması siber savaşın bir başka boyutunu oluşturmaktadır. WikiLeaks belgelerinin ortaya çıkmasıyla beraber, çok gizli nitelikteki bilgilerin devlet tarafından saklanmasının ve korunmasının oldukça zor olacağı bir sürece girilmiştir. Casusluk tarihine bakıldığında, casusluğun fiziksel bir faaliyet olduğu görülmektedir. Ancak, internetin yaygınlaşmasıyla beraber, casuslar uzaktan bilgi derleme süreci içerisine girmişlerdir. "Hacker"lar kendilerini destekleyen devletin topraklarından ayrılmadan, bilgi toplayabilmekte ve bu durum, siber

casusların yakalanmalarını zorlaştırmaktadır. Siber casuslar, devletlerin sırlarını maddi talep gözetmeksizin kamuya açıklayabildikleri gibi, kâr amaçlı casusluk faaliyetlerini de yaygın bir şekilde icra etmektedirler (Gartzke, 2013). Siber savaşta "hacker"lar hem bireysel düzeyde hareket edebilir hem de organize gruplar içinde görev alabilirler (Khalil vd., 2024). Dijital teknolojilerin yaygınlaşmasından önce, devletler gizli bilgilerini kâğıt ortamında tutmaktaydılar. Ancak zamanla, elde edilen büyük veriler, dijital ortama aktarılmaya başlanmıştır. Bu durum, rakip devletlerin birbirlerine karşı siber casusluk yapmalarına sebep olmuştur.

Siber uzay; internet, telekomünikasyon ağları, bilgisayar sistemleri başta olmak üzere, bilgi teknolojisi altyapılarını bünyesinde barındıran küresel bir alana işaret etmektedir (Biernacik, 2018). Siber uzaydaki çatışmalar "hacker"lık, casusluk, dezenformasyon ve gözetleme gibi yüksek etkili hususlara yoğunlaşır (Cristiano vd., 2023; Baezner & Cordey, 2022). Siber uzay çatışmaları sırasında "hacker"lar, telefonları dinleyebilirler (Buchanan, 2020). Siber uzayda insanlar fiziksel olarak çatışmalara doğrudan müdahil olmadıkları için gelişmeler teknik düzeyde değerlendirilir. Ancak bu durumda bile devletler, taktik ve stratejik açıdan birçok hamlede bulunmak zorundadırlar (Guyonneau & Le Dez, 2019). Siber savaşın temel yapısının anlaşılmasının ardından, bu çatışma biçiminin dönüşümünde önemli rol oynayan yapay zekâ teknolojisinin etkisi bir sonraki bölümde detaylı biçimde ele alınacaktır.

YAPAY ZEKÂNIN SİBER SAVAŞTAKİ ROLÜ

Son yıllarda yapay zekâ, çeşitli alanlarda dikkate değer dönüşümlere yol açmıştır. Bu hızlı dönüşüm ve gelişim sebebiyle, literatürde yapay zekânın tek bir tanımı bulunmamaktadır. Stamova ve Draganov'a göre yapay zekâ, "insan davranışlarını taklit eden bir yazılım türü" iken; bir diğer tanıma göre ise, bilgisayarların yardımı ile var olan büyük verilerden anlamlı bir sonuç elde etme işlemidir. Ayrıca yazılım, donanım, veri toplama ve veri depolama gibi süreçleri de kapsar (Paliszkiewicz vd., 2024; Davis, 2019). Ekonomik kalkınma ve teknolojik inovasyon süreçlerinde önemli rol oynayan yapay zekâ, özellikle sağlık, eğitim ve bilimsel araştırma alanlarında verimliliği artırıcı etkiler sunmaktadır. Öte yandan, yapay zekâ siber alandaki değişim ve dönüşüm sürecine kayıtsız kalmamıştır. Yapay zekânın günlük hayatı kolaylaştıran bir yönü olmasına rağmen, ulusal güvenliği tehdit eden bir başka yönü de bulunmaktadır. Kötü niyetli yapay zekâ kullanıcıları, hedef kişiye ait verileri ele geçirerek doğrudan siber saldırılar gerçekleştirebilir. Ayrıca yapay zekâ, hedef kişileri taklit etmek ve onlar hakkında bilgi edinmek için botlar kullanabilir (Montasari, 2022). Örneğin, 24 Şubat 2022 tarihinde başlayan Rusya-Ukrayna savaşının ilk haftalarında, Rusya Devlet Başkanı Putin ve Ukrayna Devlet Başkanı Zelensky'e ait görüntüler kullanılarak, deepfake teknolojisiyle sahte videolar oluşturulmuş ve kamuoyuna servis edilmiştir. Zelensky'e atfedilen sahte bir videoda, Ukrayna halkına silah bırakma çağrısı yapılmıştır. Bir diğer sahte videoda ise Putin'in Ukrayna ile barış sağlandığını ilan ettiği görülmektedir (Nixon, 2022). Son yıllarda siber güvenlik hem teknolojik hem de operasyonel açıdan önemli değişiklikler geçirmektedir. Bunun yanı sıra, siber ortamda devletler her an dezenformasyon, manipülasyon ve siber tehditler ile karşı karşıya kalmaktadırlar (Lande & Danyk, 2025; Ofusori vd., 2024). Yapay zekâ, siber güç sahibi olan ülkeleri siber operasyonlar icra etmeye teşvik etmektedir (Karamchand & Aramide, 2025). Örneğin, online olarak mevcut verileri tarayıp, anlık olarak bilgi derlemek veya biyometrik yüz tanıma teknolojisi için yapay zekâya başvurulmaktadır (Rosli, 2025)

Makine öğrenimi, kuantum hesaplama ve derin öğrenme gibi yapay zekâ teknolojileri, askeri ve istihbarat kurumlarına tehditlerin kaynağını tespit etme ve bunlara karşı koyma konusunda önemli katkılar sağlamaktadır (Cristiano vd., 2023). Yapay zekâ, geniş halk kitlelerini yönlendirmede, manipülatif içerik üretmede ve toplumların olaylara karşı verdikleri tepkileri ölçüp, bunları analiz etmede önemli görevler üstlenmektedir (Lande & Danyk, 2025). Siber uzayda meydana gelen çatışmalar sırasında yapay zekâ teknolojisi, verilerin zamanında ve doğru bir şekilde analiz edilmesine önemli katkılar sunmaktadır. Bu durum, siber uzaydaki çatışmaların daha öngörülebilir olmasına ve tehditlere karşı savunma mekanizmaların geliştirilmesine olanak sağlamaktadır (Cristiano vd., 2023). Yapay zekâ, bu gelişmelerde önemli roller üstlenmektedir; ancak siber savaşta tek başına stratejik

bir oyun kurucu olarak görülmemelidir. Ayrıca, yapay zekâ destekli silahların varlığı devletleri cezbetmektedir. Ancak, nükleer silahlar gibi yüksek önemdeki konular ile ilgili güvenilir olmayan ve hata yapan yapay zekâ teknolojilerini kullanmak felaketle sonuçlanabilir (Johnson, 2020). Son yıllarda devletler, hedef ülkede dezenformasyon yaymaktan, hedef ülkenin askeri stratejik noktalarını tespit etmeye kadar birçok aşamada yapay zekâdan faydalanmaktadır.

Orduların kullandığı silahların yapay zekâ ile desteklenmesi, geleneksel silahların daha verimli hale getirilmesini amaçlamaktadır. Mevcut durumda, yapay zekânın silahlandırılmasıyla ilgili kararları insan vermektedir ancak gelecekte yapay zekânın daha çok kontrol sahibi olacağı öngörülmektedir. Bu sebepten ötürü, yapay zekâ destekli uygulamalar kontrol altında tutulmalı ve ihtiyaçlara göre düzenlenmelidir. Ayrıca devletler, siber güvenliği arttırmak istiyorlarsa, makine öğrenimi araçlarını kullanmak zorundadırlar (Yamin vd., 2021). Son teknolojik gelişmeler incelendiğinde, otonominin farklı silah gruplarına entegre edilmesi süreci olduğu görülmekte ve böylece yapay zekânın silah sistemlerinde etkisi artmaktadır (Benouachane, 2024). Devletler siber saldırılara maruz kaldıklarında, saldırının kaynağının öğrenilmesi açısından yapay zekâ teknolojisinden istifade edebilirler (Guyonneau & Le Dez, 2019).

ABD'de Obama yönetiminde Department of Defense adında bir birim kuruldu ve bu birim, teknolojilerin geliştirilmesinden sorumluydu. Bu kapsamda, 13 Haziran 2018'de ABD'de Ortak Yapay Zekâ Merkezi ihdas edilmiştir. Bu merkez, Şubat 2019'da Yapay Zekâ Strateji belgesini yayınlamıştır. Buna göre, yapay zekânın askeri alanlarda kullanımının en çok otonom araçlar vasıtasıyla gerçekleştiği görülmektedir (Davis, 2019). Örneğin, askeri operasyonlar sırasında arazi şartlarının zor olduğu bölgelerde, dronlar sayesinde düşman unsurların yer tespiti kolay bir şekilde yapılabilmektedir. Günümüzün uzaktan kontrol edilebilen robotları ile gelecekteki otonom robotların kullanımının, etik sorunları da beraberinde getireceği tahmin edilmektedir. Ayrıca gelecekte orduların bir kısmının veya tamamının otonom robotlardan oluşması, siyasi ve stratejik açıdan önemli sonuçlar doğuracaktır. Böylece, robotlar aracılığıyla yürütülmek istenen bir savaş, yapay zekânın kinetik savaş alanına uygulanması ihtimalini ortaya çıkarmaktadır (Shadle, 2020).

ABD, yapay zekânın siber alandaki yeteneklerini geliştirmeye yönelik çalışmalar yürütmektedir. Yapay zekânın siber güvenliği gelecekte nasıl dönüştüreceği sorusu ise yalnızca teknik değil, aynı zamanda politik bir mesele olarak değerlendirilmektedir. Bunun yanı sıra, yapay zekânın siber saldırıda mı yoksa siber savunmada mı daha etkili olduğu tartışmasından uzaklaşarak, her iki alanda da etkin kullanımına odaklanmak gerekmektedir (Jun, 2025). Yapay zekâ, siber güvenlikte önemli bir unsur olmanın yanı sıra, büyük miktardaki verileri analiz etme ve tehditleri tespit etme açısından da kritik bir rol oynamaktadır. Yapay zekâ, verileri analiz etme yeteneği sayesinde, daha önce karşılaşılmamış saldırı türlerine bile uyum sağlayarak, çözüm önerileri sunabilmektedir. Yapay zekânın siber güvenliğe entegre edilmesi sayesinde, gelişmiş karar alma yeteneklerinin ortaya çıktığı görülmektedir (Salem vd., 2024). Devletler, istihbarat kurumları aracılığıyla siber casusluk alanında yapay zekâ tekniklerini kullanmak suretiyle terör saldırılarını minimize edebilir (Ifeanyi-Ajufo & Rosli, 2024). Bu çerçevede, yapay zekâ destekli uygulamaların önemi giderek artmakta ve askeri stratejilerin önemli bir unsuru haline gelmektedir. Ancak, bu teknolojilerin etik boyutları ve potansiyel riskleri göz önünde tutulmalıdır. Yapay zekâ teknolojisi, savaşlar ve siber güvenlik alanında önemli fırsatlar sunmaktadır. Ancak bu teknolojinin kötüye kullanım riski, uluslararası düzeyde etkin düzenleme ve denetim mekanizmalarının oluşturulmasını zorunlu kılmaktadır.

Dijital savaş alanında ciddi eksiklikler bulunmaktadır ve bu nedenle belirli kuralların tanımlanması gerekmektedir. Bu bağlamda, siber savaşı anlayabilmek için geleneksel savaş mantığına vurgu yapmakta fayda vardır. Böylece, siber savaş ile geleneksel savaş arasındaki benzerlikler/farklılıklar ortaya konulabilir. General Ferdinand Foch, 20. yüzyılın başında, Fransa'nın kara ordusunun başarısının üç ilkeye bağlı olduğunu ifade etmiştir. Bu ilkeler şunlardır: hareket serbestliği, savaş gereçleri ekonomisi ve mücadelenin yoğunlaştırılması. Hareket serbestliği ile savaş gereçleri ekonomisi unsurlarının siber taktikler ile doğrudan bir ilişkisi vardır. Hareket serbestliği kavramı ile, görevin başarılmasına odaklanılmaktadır. Ayrıca,

fiziksel savaşların uzun sürmesi gibi, siber savaşlar da uzun bir dönem devam edebilir. Mevcut koşullarda, siber savaş alanı hala insanlar tarafından yönetildiği için savaş gereçleri ekonomisi önemini korumaktadır. Siber savaşta zaman faktörü ise, hız ve siber mühimmatın çokluğu ile ölçülemez. Bu nedenle, siber savaşta mücadelenin yoğunlaştırılması kavramı, fiziksel savaştan farklılık gösterebilir (Guyonneau & Le Dez, 2019). Bunun yanı sıra, siber uzayda dünyanın herhangi bir bölgesindeki bilgisayar sistemlerine saldırmak mümkün olsa da devlet destekli siber çatışmalar genellikle komşu devletler arasında gerçekleşmektedir (Shadle, 2020).

Günümüzde siber güvenliğin, devlet yetkilileri, özel kurumlar ve devlet dışı aktörler ("hacker"lar veya suç örgütleri) aracılığıyla hem saldırı hem savunma amaçlı ve yapay zekâ teknolojilerini kullanacak şekilde dizayn edildiği bilinmektedir. Yapay zekâdan siber saldırıda istifade edildiği gibi, savunma amaçlı faaliyetlerde de faydalanılır (Bonfanti, 2022). Yapay zekâ teknolojisi, sosyal ağların analizini kısa bir sürede gerçekleştirmektedir. Bu kapsamda, içerik düzenleme algoritmaları aracılığıyla sosyal medya kullanıcılarının davranışları izlenmekte ve yönlendirilebilmektedir. Örneğin, terör grupları, yaptıkları eylemlerin etkisini arttırabilmek için sosyal medya platformlarında yapay zekâdan istifade edebilirler. Sonuç olarak, siber suç işleyenlerin kullanmış olduğu bütün sosyal mühendislik yöntemlerinin etkisi, yapay zekâ sayesinde arttırılabilir (Montasari, 2022). Siber savaşın geleneksel savaş ilkeleriyle benzerlikler taşıdığı ancak kendine özgü dinamiklerinin olduğu söylenebilir. Yapay zekânın siber savaşlardaki yükselen rolü dikkate alındığında, bu teknolojiden en yoğun biçimde faydalanan aktörlerden olan İsrail ve İran'ın siber kapasitesini ayrı ayrı değerlendirmek gerekmektedir.

İSRAİL'İN VE İRAN'IN SİBER GÜÇ KAPASİTELERİ

İsrail ve İran'ın siber güvenlik alanındaki kapasitelerinin belirlenmesi, aralarındaki siber savaşın dinamiklerinin analizine temel oluşturmaktadır. İsrail, siber alanda yaşanan gelişmelere paralel olarak, 1990'lı yıllardan itibaren dijital altyapı ve teknoloji alanlarında yatırımlar yapmaya başlamıştır (Kırık, 2025). Teknik alanlarda yapılan yenilikler, siber güvenlik için hayati öneme sahiptir. İsrail'deki araştırma üniversiteleri, siber alanla ilgili temel araştırmalarda bulunurlar ve akabinde uygulamalı faaliyetler içerisinde yer alırlar. Tel-Aviv Üniversitesi bünyesinde bulunan Blavatnik Disiplinlerarası Siber Araştırma Merkezi, siber uzay konusunda hükümet-üniversite iş birliği çerçevesinde çalışmalarını yürütmektedir. İsrailli güvenlik şirketlerinin, siber güvenlik pazarında aktif bir şekilde yer aldıkları bilinmektedir. İsrailli şirketlerin Ar-Ge için ayırmış oldukları bütçenin yüksek olması, dikkat çeken bir diğer gelişmedir. Görüldüğü üzere İsrail, siber güvenlik alanında eğitim, bilim ve araştırma alanlarına yatırım yaparak, kendisine rakip gördüğü ülkelere karşı üstünlük kurmayı amaçlamıştır. Bilimsel ve ekonomik gelişmenin, siber savunma kabiliyeti üzerinde olumlu etkileri mevcuttur (Tabansky, 2016).

İsrail Hükümeti'nin, Beer-Sheva'daki Ben-Gurion Üniversitesi ile Soroka Tıp Merkezi ve İsrail Savunma Kuvvetleri (IDF)'nin teknoloji birimlerini Negev çölüne transfer etme projesi, Başbakan Netanyahu'nun Beer-Sheva'yı siber başkent yapma fikri ile paralellik göstermektedir. Bu çerçevede Beer-Sheva'da "CyberSpark" adında siber faaliyetlerin yürütüldüğü bir merkez inşa edilmiştir (Tabansky & Ben Israel, 2015). CyberSpark'ın geliştirilmesi ve kalkındırılması için IBM, Lockheed Martin, Deutsche Telecom, PayPal, EMC ve JVP gibi şirketlerin önemli katkıları olmuştur. İsrail Hükümeti, ABD'deki Silikon Vadisi'nin bir benzerini İsrail'de kurabilmek için CyberSpark'taki faaliyetleri dikkatle takip etmektedir (Adamsky, 2017). İsrail, siber güvenliğe bu derece ehemmiyet vermesi ile karşılaştığı siber güvenlik tehditlerinin doğru orantılı olduğunu iddia etmektedir. Örneğin, Çinli "hacker"lar, 2014 yılında İsrail'in çokça övündüğü Demir Kubbe füze savunma sistemindeki bilgileri çalmışlardır (Keck, 2014). İsrail, siber tehditlere karşı hükümet-üniversite-özel sektör arasında bir uyum yakalayarak, siber tehditlerle mücadele etme yöntemini benimsemiştir. Bu noktada, siber alanın sadece teknik bir mesele olmadığı ve ulusal güvenlik ile ekonomik refah konularıyla yakından irtibatlı olduğu görülmektedir.

İsrail'deki siber güvenlik uzmanları ve mühendisler, ordu bünyesinde bulunan 8200 adlı birim tarafından eğitimlerini

alırlar. Bu birim, sinyal istihbaratı konusunda uzmanlaşmış olup, "siber güvenlik okulu" şeklinde tanımlanmaktadır. Askerlik hizmetini bu birimde ifa eden kişiler, sivil hayatta siber güvenlik alanında girişimlerde bulunmaktadırlar. Ayrıca, İsrail Ulusal Siber Direktörlüğü hem kamu hem de özel sektör ile iş birliği geliştirerek, siber güvenlik alanında öncü faaliyetlerde bulunmayı amaç edinmiştir. Bu direktörlük, siber güvenlik şirketlerini ve araştırma merkezlerini maddi olarak desteklemektedir. Ayrıca, Ulusal Siber Direktörlüğü tarafından bir ulusal acil durum merkezi ihdas edilmiştir. Siber saldırıya uğrayan İsrailli vatandaşlar, bu merkeze başvurarak, yardım alabilmektedirler. İsrail'de 400'den fazla siber güvenlik şirketi bulunmakta olup, İsrail'in 2022 verilerine göre, siber güvenlik alanındaki toplam iş hacmi 8,8 milyar doları aşmıştır ve bu rakam küresel pazarın yaklaşık %20'sine tekabül etmektedir. Check Point Software Technologies, CyberArk ve SentinelOne adlı siber güvenlik şirketleri, güvenlik duvarı teknolojileri, kimlik tespiti ve yapay zekâ destekli tehditlerin ortaya çıkarılması gibi alanlarda faaliyet göstermektedirler. Deep Instinct and Vdoo adlı siber güvenlik şirketlerinin odaklandıkları ana konu ise, yapay zekâ teknolojilerini kullanarak siber saldırı tehditlerini önceden tespit etmek ve bunlara yönelik önlem almaktır. İsrail menşeili siber güvenlik şirketleri, bilgi paylaşmak ve ortak çözümler üretebilmek için Microsoft, Google ve Cisco gibi ABD'li şirketler ile iş birliği geliştirmektedirler (Editorial INTI, 2024; Unna, 2019). İsrail'i siber alanda ön plana çıkaran bir diğer faaliyeti ise Pegasus adlı casus yazılımdır. Pegasus, Apple iOS ve Google Android işletim sistemlerine uzaktan yüklenebilen bir casus programdır. İsrail menşeili NSO adlı siber şirket tarafından geliştirilen yazılım, telefonlarda yapılan tüm hareketleri izleyebilmektedir. Bu çerçevede program, uzaktan ses ve video kaydedebilmesinin yanı sıra, şifreli WhatsApp mesajlaşmalarını ve GPS bilgilerini elde edebilir (Chawla, 2021). Siber güvenlik alanında ordu tarafından eğitim verilmesi, İsrail'in insan kaynağını spesifik alanlara yönlendirerek, verimli bir şekilde kullanmaya çalıştığını göstermektedir.

İran, askeri teknoloji ithal etmek ve bunu geliştirme noktasında uluslararası yaptırımlara maruz kaldığı için asimetrik mücadele yöntemini benimsemektedir. Bu çerçevede, askeri havacılıkta yaşanan gelişmeleri yakalayamadığını düşünen İran, balistik füze teknolojisine ağırlık vermiştir. Aynı nedenle, konvansiyonel kara ordusuna yoğun yatırım yapmak yerine, Ortadoğu'da başta Hizbullah olmak üzere bazı örgütlere maddi ve silah desteği sağlamayı tercih etmiştir. Bunun yanı sıra, siber uzaydaki gelişmeler göz önüne alındığında, İran'ın siber alandaki asimetrik güç ilişkilerinde önemli bir rol üstlenebileceği söylenebilir. Bu bağlamda, 2015 yılında ABD Ulusal İstihbarat Direktörü James Clapper, İran'ın siber uzaydaki faaliyetlerini şu şekilde özetlemiştir: İran, rakip devletlere yönelik asimetrik ancak orantılı karşılık verebilmek için siber saldırılarda bulunmaktadır (Iran's Cyberattacks Capabilities, 2020).

İnternetin ve çevrimiçi hizmetlerin yaygınlaşmaya başlamasıyla birlikte İran, 2005 yılından itibaren ulusal bir internet ağı geliştirmeye yönelik yeni politikalar oluşturmaya çalışmıştır. Özellikle 2009 yılında yaşanan protesto gösterilerinin ardından, Tahran yönetimi yabancı ağlara olan bağımlılığı azaltmak amacıyla yerel bir internet ağı kurma çabalarını hızlandırmıştır. ABD ve İsrail gibi devletler ile siber alanda yaşanan çatışmalar sebebiyle İran, bu süreçte ulusal güvenliğine zarar gelmemesi için siber altyapıya yatırım yapmıştır. İran Enformasyon ve İletişim Teknolojileri Bakanı Settar Haşimi, Ağustos 2024'te yaptığı açıklamada, İran'da ulusal bir internet ağı geliştirilmesi projesinin %60'ının tamamlandığını duyurmuştur. İranlı yetkililer, Google ve WhatsApp gibi uygulamaların, casusluk tehdidi nedeniyle İranlılar tarafından kullanılmasının doğru olmadığını açıklamaktadır. İran, ulusal internet ağı konusunda henüz sonuç alamamış olsa da ulusal siber güvenliği sağlamak için Dijital Kale (Dejfa) adlı bir güvenlik mekanizması geliştirmiştir. Ayrıca, İran siber güvenlik ve internet konularında devlet destekli yerel uygulamalar üretmeye çalışmış, ancak ekonomik yaptırımlar ve sınırlı maddi imkanlar nedeniyle istediği sonucu elde edememiştir (Çahmutoğlu, 2021; Tahran Insider, 2024). İran, askeri alandaki eksikliklerine bir denge unsuru olacak şekilde siber faaliyetlere ağırlık vermektedir. İran'ın ulusal internet ağını oluşturma gayreti, siber güvenliğini sağlama ve dış tehditlerden korunma şeklinde açıklanabilir. Yetersiz teknoloji transferi ve ekonomik ambargolar gibi sebeplere

rağmen, İran'ın siber alanda asimetrik bir güç çerçevesinde yenilikçi politikalar izlediği görülmektedir.

İran'ın siber saldırılarında, İran Devrim Muhafızları Ordusu (IRGC), Basij ve İran Pasif Savunma Örgütü (NPDO) olmak üzere üç önemli aktör faaliyet göstermektedir. IRGC; ABD, İsrail ve Suudi Arabistan'ın kritik alt yapılarına yönelik siber saldırıları yönetmektedir. Basij ise, binlerce gönüllü siber korsanlardan müteşekkil, paramiliter bir örgüttür. NPDO, İran'a yönelik siber saldırıları önlemeye yönelik faaliyetler yürütür (Gotsiridze, 2020). İran'ın siber yetenekleri, ABD, Çin veya Rusya'ya göre daha sınırlı olsa bile, siber alana yapmış olduğu yatırım azımsanmayacak ölçüdedir. İran, siber alana yaklaşık 1 milyar dolarlık yatırım yapmış; hedef ülkelere ve kurumlara yönelik siber saldırılar gerçekleştirmek amacıyla İran Siber Ordusu'nu (ICA) kurmuştur. Google yöneticisi Eric Schmidt, 2011 yılında İran'ın, Danimarka'ya düzenlediği siber saldırıdan sonra, İran'ın siber savaşta yetenekli olduğunu ifade etmiştir. ICA'nın eylemlerine bakıldığında, web sitelerini ele geçirmek ve 2009'daki İran protestolarına karşı mesaj vermek amacıyla hareket etmiştir. Bu kapsamda, 2009 yılında Twitter'a siber saldırı düzenlemiş ve bir yıl sonra Çin'in en büyük arama motoru olan Baidu, İranlı "hacker"lar tarafından ele geçirilmiştir. İran'ın bu hamlesi, Çin ile aralarında bir süre boyunca siber çatışmalara sebep olmuştu. Ayrıca Şubat 2012'de İranlı "hacker"lar, İran rejimi aleyhine yayın yapan Jaras News'e yönelik bir siber saldırı gerçekleştirmiştir (Farwell & Arakelian, 2013).

İran'ın 2012 yılında Suudi Aramco'ya düzenlediği "Shamoon" siber saldırısı sonucunda yaklaşık 30.000 bilgisayar devre dışı kalmıştı. Benzer şekilde, 2020'de COVID-19 salgını sırasında İranlı "hacker"lar, Gilead Sciences adlı ilaç şirketini hedef alarak, aşıya dair hassas verileri ele geçirmeye çalışmıştır. İran İstihbarat ve Güvenlik Bakanlığı (MOIS)'na bağlı olarak çalıştığı düşünülen MuddyWatter, hedef aldığı kişilere, içerisinde kötü amaçlı yazılımlar içeren ZIP dosyasını göndererek, hedeflerin bilgisayarlarını ele geçirmeyi amaçlamaktadır. MuddyWatter, 2017 yılından beri siber saldırılarda görev almaktadır ve Ortadoğu ülkelerine yönelik faaliyet yürütmektedir. İran hükümeti tarafından desteklenen ve 2014 yılından itibaren aktif olduğu bilinen APT35 adlı tehdit grubu, ABD, İsrail ve Ortadoğu ülkelerindeki resmî kurumlar ile enerji şirketlerini hedef alarak, siber casusluk faaliyetleri yürütmektedir. APT35'te, hedeflere gönderilen bağlantıların tıklanması suretiyle bilgisayarlara sızılmaktadır (Provecho vd., 2024). Yukarıdaki örnekler, İran'ın siber uzayda saldırı kabiliyetinin gelişmiş olduğunu göstermektedir. Devletin desteklediği hacker gruplarının gerçekleştirmiş oldukları eylemlere bakıldığında, organize ve sistematik bir şekilde hareket ettikleri görülmektedir.

Daha önce vurgulandığı gibi, İran siber uzaydaki faaliyetlerini asimetrik bir güç unsuru olarak kullanmaktadır. İran'ın yaptığı siber saldırıların casusluk, gizli verilere elde etme ve propaganda gibi amaçlarının olduğu görülmektedir (Iran's Cyberattacks Capabilities, 2020). FBI, CISA, NSA ve diğer kurumlar tarafından ilan edilen siber güvenlik duyurusunda, İsrail ve Filistin arasında Ekim 2023'te vuku bulan çatışmaların akabinde, İranlı "hacker"ların, hassas sistemlere yetkisiz erişim gerçekleştirdikleri ve çok faktörlü kimlik doğrulama (MFA) sistemlerindeki güvenlik açıklarından istifade ettikleri vurgulanmıştır. Ayrıca bu güvenlik kurumları, İran'ın fidye yazılım saldırıları, veri hırsızlığı ve kritik altyapılarda yarattığı kesintiler gibi faaliyetleri sebebiyle, tehdit seviyesinin yükseldiğini belirtmişlerdir (Malik, 2024). İran'ın siber kapasitesini geliştirmesine destek olan başlıca güçlerin başında Rusya ve Çin gelmektedir. Rusya ile İran arasında 2015 yılında siber iş birliğini içeren anlaşmalar imzalanmıştır. Ayrıca 2019-2020 yıllarında, İran'ın yüz tanıma sistemlerine kavuşması ve yapay zekâda iş birliğinin arttırılması konularında Rusya ve İran arasında çalışma grupları kurulmuştur. Son olarak 2021 yılında İran ile Rusya arasında "Bilgi Güvenliği İş birliği Paktı" imzalanmıştır. Buna göre, İran'daki muhaliflerin veya rakip ülkelerdeki üst düzey kişilerin telefonlarına ve bilgisayarlarına siber saldırı düzenleyebilmek için Rusya İran'a teknoloji transfer edecektir. Ayrıca Ukrayna'daki savaş sebebiyle İran ve Rusya arasındaki stratejik iş birliğinin siber alanı da kapsadığı düşünülmektedir. Aynı şekilde Çinli şirketler Huawei ve ZTE, İran'ın teknolojik alt yapısına yönelik önemli yatırımlar yapmışlardır. Çin ve İran arasında 2021 yılında, 25 yıl geçerli olacak şekilde stratejik iş birliği anlaşması imzalanmıştır. Buna göre, Çin, İran'da 5G teknolojisi için yatırım yapacak ve

Çinli şirketler kamera ve yapay zekâ teknolojilerini İranlı şirketlere satacaktır. Bu anlaşma ile, İran'ın siber alanda daha fazla yetkinliğe sahip olması amaçlanmıştır (Freilich, 2024). İki ülkenin siber altyapı ve kapasite farklılıkları göz önüne alındığında, bu potansiyelin pratikte nasıl bir çatışma alanına dönüştüğü İsrail-İran siber savaş örneği üzerinden analiz edilecektir.

İSRAİL VE İRAN ARASINDAKİ SİBER SAVAŞ

İsrail ve İran arasındaki mücadele, Ortadoğu'daki bölgesel istikrarsızlığın artmasında büyük bir etkendir. İsrail, İran'ın nükleer bir güç olmasını, Ortadoğu'daki grupları desteklemesini ve İran'ın İsrail'i yok edeceği yönündeki çağrılarını kendisi açısından "varoluşsal bir tehdit" olarak görmektedir. Aynı şekilde İran, kendi ulusal güvenliğine İsrail'in tehdit oluşturduğunu ve nükleer programını engellemeye çalıştığını düşünerek, İsrail'i bölgedeki en büyük tehditlerden biri olarak görmektedir (Amaliya, 2025). İran, nükleer programına önem verdiği gibi, siber faaliyetlere de aynı derecede ehemmiyet atfetmektedir. İran Genelkurmay Başkanlığı Siber Karargâh Komutanı Behrouz Esbati 2015 yılında Defa Press'e yaptığı açıklamada, siber güvenlik ile ilgili yapılan faaliyetlerin en az nükleer program kadar önemli olduğunu belirtmiştir. Bu yorum, İran'ın siber güvenlik konusuna oldukça önem verdiğini göstermektedir. İsrail ile İran'ın siber uzayda karşı karşıya geldiği en önemli olaylardan biri, Temmuz 2010 tarihinde kamuoyuna duyurulan ve ABD-İsrail ortaklığıyla gerçekleştirildiği iddia edilen Stuxnet saldırısıdır. Bu saldırı kapsamında, Stuxnet adlı kötü amaçlı bir bilgisayar virüsü, İran'ın nükleer programına duhul etmiştir (Cohen, 2019). Stuxnet saldırısı, casusluk faaliyetinin yanı sıra etkileri bakımından siber savaş tarihinde önemli bir dönüm noktası olarak kabul edilmektedir. Üzerinden uzun yıllar geçmiş olmasına rağmen Stuxnet saldırısı, siber savaş literatüründe hâlen referans niteliğinde bir vaka olarak değerlendirilmektedir (Lindsay, 2025).

Stuxnet aracılığıyla gerçekleştirilen siber saldırı sonucunda, İran'ın Natanz bölgesindeki nükleer tesiste bulunan santrifüjlerin yaklaşık beşte biri devre dışı kalmıştır (Siboni vd., 2020). Stuxnet saldırısı ilk olarak 2007 yılında planlanmış ve Natanz'a sızması için Hollanda İstihbarat Servisi için çalışan bir ajan kullanılmıştır. Bu ajan, ABD ve İsrail tarafından kurulan paravan bir şirkette çalışan teknisyen rolü ile tesiste görev almış ve belli bir süre geçtikten sonra, Stuxnet virüsünü bir USB aracılığıyla tesisteki sisteme yüklemiştir. Ayrıca İran, sistemlerinde Eylül 2011'de Duqu ve Mayıs 2012'de Flame adlı iki farklı casus yazılım tespit etmiştir. Stuxnet saldırısı sonucunda, İran'ın nükleer programındaki faaliyetler sekteye uğramış ve yaklaşık 18 aylık çalışması boşa gitmiştir. Stuxnet saldırısı, İran'ın nükleer programındaki bilgisayarlara zarar vermenin yanı sıra, fiziksel yıkıma da sebep olmuştur (Çahmutoğlu, 2021; Bahgat, 2020). Stuxnet saldırısı literatürde, kritik altyapıların endüstriyel kontrol sistemlerini hedef alan ve devlet destekli olduğu düşünülen ilk siber saldırı örneği olarak kabul edilmektedir (Barzashka, 2013).

Stuxnet'ten önceki siber saldırılar, fiziksel altyapıya yönelik doğrudan ve hassas etkiler oluşturma kapasitesine sahip değildi; bu nitelikteki ilk örnek Stuxnet saldırısıyla ortaya çıkmıştır (Denning, 2012). İsrail, İran'ın Ortadoğu'da nükleer bir güce sahip olmasına izin vermemek için çaba sarf etmekteydi. Stuxnet hadisesinin ardından, İran 2011 yılında internet ortamında sahte kimlikler oluşturarak İsrail'deki hükümet kurumlarına ait bilgisayar sistemlerine siber saldırılar düzenlemiştir. Bu saldırılar sonucunda, İsrail'in sistemlerinden sınırlı da olsa bazı bilgilere erişilmiştir (Amaliya, 2025). İsrail, bu saldırı sonucunda istihbarat destekli bir savunma modeli geliştirmesi gerektiğine inanmış ve siber saldırılar başlamadan önce bu alanda önlemler almasının zaruri olduğunu düşünmüştür. Ayrıca İran'ın siber saldırılarından kaçınmak için İsrail'in bölgedeki diğer devletler ile iş birliği yapmasının önemi bir kez daha ortaya çıkmıştı (Siboni & Kronenfeld, 2012). Stuxnet örneği, literatürde yalnızca bir siber saldırı vakası olarak değil, aynı zamanda siber caydırıcılığın ilk somut tezahürlerinden biri olarak da değerlendirilmektedir.

Stuxnet saldırısından sonra İran, siber yetkinliklerini artırmaya çalışmış ve bu doğrultuda yeni siber eylemlere ağırlık vermiştir. Bu çerçevede, Nisan 2020'de İran, İsrail'deki atık su arıtma tesislerine siber saldırı düzenleyerek, sudaki klor seviyesini arttırmayı

hedeflemiştir. Böylece İran, İsrail'de genel sağlığı etkileyebilecek bir siber saldırı gerçekleştirmeyi amaçlamıştır. Bu siber saldırı kapsamında İranlı "hacker"lar, öncelikle İsrail'de endüstriyel işlemlerin takibinin yapılması ve veri toplamak için oluşturulan SCADA yazılım sistemini hedef almışlardır. Bu saldırı, İsrailli yetkililer tarafından tespit edilmiş ve İsrail Ulusal Siber Direktörlüğü, su sektöründeki kurumlara gönderdiği bir mesajda; atık su arıtma tesisleri, su pompalama istasyonları ve kanalizasyon sistemlerine yönelik bir siber saldırı girişimi olduğunu bildirmiştir. Bu kapsamda, bu işletmelerdeki internet kullanımının azaltılması ile kullanılan yazılımların ve şifrelerin güncellenmesi gerektiği yönünde uyarılar yapılmıştır. İranlı yetkililer, bu saldırının sorumluluğunu üstlenmemişlerdir. Ancak İsrail istihbaratına ve Batılı yetkililere göre, İran düzenlediği bu siber saldırı ile rakiplerine gözdağı vermeyi amaçlamıştır. Böylece İran, siber alandaki kapasitesini ve yeteneklerini göstermeye çalışmıştır (Haroon, 2024; Kovacs, 2020). İran'ın gerçekleştirdiği bu saldırı, doğrudan fiziksel bir çatışma başlatmaksızın, düşman olarak belirlenen bir aktörün kritik altyapısına zarar verme potansiyeli taşıdığı için, konvansiyonel savaş stratejileri kapsamında "stratejik hedeflere saldırı düzenleme" yaklaşımının çağdaş bir uzantısıdır. İran'ın, İsrail'deki su arıtma tesisine yönelik gerçekleştirdiği siber saldırı sonrasında, İsrail tarafından 9 Mayıs 2020'de İran'ın güneyindeki Bender Abbas'taki Şahid Recai limanına siber saldırı düzenlenmiştir. Bu saldırı neticesinde limanda gemilerin hareketlerini yöneten bilgisayar sistemi çökmüş ve buna bağlı olarak limandaki faaliyetler birkaç gün sekteye uğramıştır (Siman-Tov & Even, 2020).

İsrail ile İran arasındaki siber çatışmalar sırasında sadece kritik önemi haiz kuruluşlar veya altyapılar zarar görmemekteydi ayrıca bu saldırılar önemli kişileri de hedef almaktaydı. Bu kapsamda, İran'ın baş askeri nükleer uzmanı ve İran'daki silah programının yürütücüsü Mohsen Fakhrizadeh, Kasım 2020'de, Mossad tarafından üretilen uzaktan kumandalı yapay zekâ ile çalışan bir keskin nişancı tüfeği ile suikasta uğramış ve hayatını kaybetmiştir (Bob, 2021).

İsrail ile İran arasında süregelen siber çatışmalar hem kapsamı hem de etkileri bakımından giderek daha karmaşık ve yıkıcı bir nitelik kazanmaktadır. Aralık 2020'de İranlı "hacker"lar tarafından İsrail'deki 80 şirkete yönelik fidye yazılımı içeren siber saldırılar gerçekleştirilmiştir. Bu kapsamda, İsrail'deki sigorta, lojistik ve endüstriyel sektördeki şirketlerin verileri çalınmıştır. "Hacker"lar, şirketlerin BitCoin üzerinden ödeme yapmadıkları takdirde, verilerinin ifşa edileceğini duyurmuşlardır. İran'ın buna benzer eylemleri, İsrail toplumunda korku ve endişeye sebep olmaktadır. Bu saldırıya karşılık olarak İsrail'in, Natanz'daki nükleer zenginleştirme tesisinde büyük bir patlamaya neden olduğu iddia edilmiştir. Saldırıda, tesisteki santrifüjleri çalıştıran sistem devre dışı kalmıştır. Bunun yanı sıra İran ve İsrail arasındaki siber savaş sırasında İsrail istihbarat teşkilatının önleyici müdahalede bulunduğunu gösteren olaylar yaşanmıştır. Mayıs 2022'de İsrail iç istihbaratından sorumlu olan Shin Bet, İsrailli iş adamlarına ve akademisyenlere yönelik İran tarafından siber operasyonlar yapıldığını ve böylece İran'ın çevrimiçi elemanlama faaliyetlerinde bulunduğunu tespit etmiştir. Operasyonda İranlı ajanlar, güvenilir kişilerin e-postalarından mesaj göndererek, iş adamlarını veya akademisyenleri İsrail dışında gerçekte olmayan bir konferansa davet etmişlerdir. Shin Bet tarafından İran'ın siber operasyonu açığa çıkartılmış ve bu kişilerin yurtdışına çıkışları engellenmiştir (United Against Nuclear Iran, 2024).

7 Ekim 2023'ten itibaren, İran kaynaklı İsrail'e yönelik siber saldırılarda belirgin bir artış yaşandığı görülmektedir. Bu karşılıklı saldırılar, siber çatışmaların artık dönemsel krizlerle sınırlı olmadığını, aksine süreklilik arz eden bir stratejik rekabet alanına dönüştüğünü göstermektedir. Microsoft'un Siber Güvenlik İstihbarat Merkezi tarafından hazırlanan bir rapora göre, İran; sosyal medya operasyonları, hedefli saldırılar, sahte haberler ve yapay zekâ teknolojisini kullanarak gerçekleştirdiği siber faaliyetlerle, İsrail toplumunda iç kargaşa ve güvensizlik ortamı yaratmayı hedeflemektedir (Ben Shushan, 2024). İsrail'de siber güvenliğin tehdit edildiği olayların sayısı hızla artmaktadır. İsrail Ulusal Siber Direktörlüğü, 2023 yılında 367 tane siber saldırı uyarısı aldıklarını belirtirken, bu sayı 2024 yılında 736'ya çıkmıştır (Nelson, 2025). İran, yapmış olduğu bu siber saldırılar sırasında yapay zekâ teknolojisinden istifade etmektedir. Ayrıca deepfake

teknolojisini kullanarak, siyasi açıdan etkili kişiler hakkında propaganda amaçlı videolar üretmektedir. Nisan 2025'te yayımlanan ve İran kaynaklı olduğu öne sürülen bir deepfake videosunda, İsrail'in eski Savunma Bakanı Yoav Gallant'a ait yapay zekâ ile üretilen sahte bir görüntü kullanılmıştır. Söz konusu videoda Gallant, ABD'nin Yemen'deki Husilere karşı başarı elde etmesinin mümkün olmadığını ifade etmiştir (Amitay, 2025).

İran, sosyal medya hesaplarından yapay zekâ sayesinde İsrail ve Batılı devletler aleyhine haber içerikleri oluşturmaktadır (Haroon, 2024). İran, 7 Ekim'den sonra İsrail'in iç kamuoyunu etkilemeye yönelik yapay zekâ destekli sosyal medya operasyonları gerçekleştirmiştir. Bu operasyonlarda, Storm-1364 adlı grup, Tears of War persona adı altında, İsrail vatandaşlarının Benyamin Netanyahu'ya karşı miting düzenlemelerini organize etmeye çalışmıştır. Bu durum, İsrailli siber uzmanlar tarafından tespit edilmiştir (Mieses vd., 2024). İsrail, karşılık olarak İran'da günlük hayatı etkileyecek siber saldırı operasyonları icra etmiştir. İsrail ile bağlantılı Gonjeshke Darande adlı hacker grubu, Aralık 2023'te İran'daki benzin istasyonlarından hizmet almayı engelleyen bir siber saldırı düzenlemiştir. Aynı hacker grubu, bir önceki yıl İran'da devlete ait Khuzestan Steel Co adlı çelik üretim tesisine siber saldırıda bulunmuştu ve üretimi aksatmıştı. Benzin istasyonlarına yapılan saldırı, İran halkını paniğe sevk etmiş ve birçok İranlı benzin istasyonlarına akın etmiştir. Olayla ilgili İran Petrol Bakanlığı tarafından yapılan açıklamada, İran'da toplam 33.000 benzin istasyonunun olduğu ve bunların yaklaşık %33'ünün çalıştığı belirtilmiştir. Böylece bu saldırı ile İran'daki benzin istasyonlarının yaklaşık %70'i kullanılamaz hale gelmiştir (Summer, 2023). Enerji altyapısına yönelik bu tür siber saldırılar, fiziksel bir saldırıya başvurmaksızın, bir ülkenin ikmal zincirini, iç güvenliğini ve hükümetin halk desteğini sarsmayı hedeflemektedir. Özellikle yakıt dağıtım ağının etkisiz hale getirilmesi, sadece ulaşım ve lojistik açısından değil, aynı zamanda temel kamu hizmetlerinin (örneğin sağlık, gıda tedariki ve acil müdahale hizmetleri) işleyişi açısından da yıkıcı etkiler doğurabilmektedir. Önümüzdeki yıllarda, İran ve İsrail arasındaki siber çatışmaların daha çok artacağı ve yapay zekânın etkili bir şekilde kullanılması ile saldırıların daha karmaşık bir yapıya evrileceği söylenebilir (Mieses vd., 2024). Görüldüğü üzere, siber uzay artık sadece bir savaş alanı olmaktan çıkmış ve siber saldırılar, kamuoyunun yönlendirilmesi veya algıların şekillendirilmesi amacıyla stratejik bir enstrüman haline gelmiştir.

7 Ekim 2023'ten itibaren İsrail Başbakanı Benyamin Netanyahu, Ortadoğu genelinde daha agresif bir politika izlemeye başlamıştı. Haziran 2025'te İsrail ile İran arasında sıcak çatışma meydana gelmiştir. İsrail jetleri, İran'daki nükleer, askeri ve enerji tesisler başta olmak üzere birçok hedefi bombalarken; İran füze saldırıları ile, İsrail'in hava savunma sistemini delmeyi başarmış ve bazı askeri tesisler ile Hayfa'daki petrol rafine tesisini hedef almıştır. ABD'nin, İran'daki nükleer tesislere saldırı düzenlemesine karşılık olarak İran, Katar'daki El Udeyd üssünü vurmuştur. İsrail ve İran arasında devam eden 12 günlük çatışma süreci sonucunda ateşkes anlaşması imzalanmıştır. Saldırılar sırasında her iki ülke de karşılıklı olarak siber saldırı yöntemlerine başvurmuştur (Geranmayeh, 2025). Bu olaylar zincirine bakıldığında, İsrail ile İran arasındaki çatışmanın hem konvansiyonel askeri alanda hem de siber uzayda eş zamanlı olarak yürütüldüğü ve çatışmaların toplumsal hayata çok boyutlu yansımalarının olduğu görülmektedir.

13-25 Haziran 2025 tarihleri arasında İsrail ile İran arasındaki yoğun çatışma ortamında, siber uzayda da önemli gelişmeler yaşanmıştır. Gonjeshke Darande hacker grubu, İran Bankası, "Bank Sepah"ın sistemini çökertmiştir. Ayrıca aynı grup, İran'daki kripto borsası Nobitex'e siber saldırı düzenleyerek, yaklaşık olarak 90 milyon doları ele geçirmiştir. Böylece İran'ın finans sektörü hedef alınarak, fon akışı aksatılmıştır. İsrail'in siber saldırılarına karşılık olarak İran, DDoS saldırıları ve sahte veriler üzerinden siber faaliyetlerini yürütmüştür. İran ile İsrail arasında çatışmalar yaşanmadan önce İran, DDoS saldırılarına başlamıştı. Çatışmanın başlamasından sonra ise, İran'ın siber saldırılarında %700'lük bir artış meydana gelmiştir. İran, İsrail toplumunu korku ve paniğe sevk edecek psikolojik harp tekniklerini kullanmış ve genel olarak ekonomik sabotaj eylemlerinde bulunmuştur. Neticede bu savaş, insansız hava araçları, savaş uçakları ve hacker gruplarının dahil olduğu, çok yönlü bir mücadele

sahasında cereyan etmiştir. Siber güç, modern savaşın önemli bir unsuru olduğunu bir kez daha göstermiş ve bu durum, konvansiyonel bir çatışmada siber saldırılardan kritik noktalarda yararlanılabileceğine işaret etmektedir (Baram & Peer, 2025).

SONUÇ

Bu çalışma, İsrail ve İran arasındaki siber savaşın unsurlarını ve yapay zekânın bu mücadeledeki rolünü kapsamlı bir şekilde analiz etmiştir. Araştırmanın bulguları, siber uzaydaki çatışmaların yalnızca teknik bir boyuta sahip olmadığını, bunun yanı sıra stratejik, siyasi ve toplumsal sonuçlar yarattığını ortaya koymaktadır. İki ülke arasındaki siber mücadele, kritik altyapıların hedef alınması, istihbarat faaliyetleri ve özellikle sosyal medya aracılığıyla toplumsal manipülasyon yaratma gibi çok yönlü bir savaş alanı oluşturmaktadır.

2010 yılında ortaya çıkartılan Stuxnet virüsü saldırısı ile İran'daki Natanz nükleer tesisi hedef alınarak, kritik altyapı tesisinde tahribat yaratılmak istenmiştir. Nisan 2020'de İran'ın İsrail'deki su arıtma tesislerine yönelik saldırısı, aynı şekilde kritik altyapı tesisini hedef alan bir eylemdir. İsrail'in bu saldırıya misilleme olarak 9 Mayıs 2020'de İran'ın Bender Abbas limanına düzenlediği siber saldırı ile deniz taşımacılığı hedef alınmıştır. İran'daki silah programının yürütücüsü Mohsen Fakhrizadeh, Kasım 2020'de, uzun süreli yürütülen istihbarat faaliyetleri sonucunda Mossad tarafından suikasta uğramış ve hayatını kaybetmiştir. Aralık 2020'de İranlı "hacker"lar tarafından İsrail'deki 80 şirkete yönelik siber saldırı düzenlenmesi, lojistik ve endüstriyel alanlarda faaliyet gösteren şirketlerin işleyişlerinde aksaklıkları beraberinde getirmiştir. İsrail adına faaliyet gösteren Gonjeshke Darande adlı grubun, 2022 yılında İran'daki Khuzestan Steel Co'ya yönelik saldırısı, sanayi sektörünü olumsuz etkilemiştir. Aynı grubun, Aralık 2023'te İran'daki benzin istasyonlarına yönelik saldırısı, enerji altyapısına yönelik doğrudan bir sabotaj girişimidir.

Bu saldırıların yanı sıra, Ekim 2023 tarihinden itibaren İran, sosyal medya üzerinden sahte haberler yaymak suretiyle İsrail halkını korku ve endişe sevk etmeye çalışmaktadır. Storm-1364 adlı grubun gerçekleştirdiği sosyal medya operasyonları, doğrudan İsrail kamuoyunu etkilemeyi ve İsrail Başbakanı Netanyahu'ya karşı sokak protestolarını teşvik etmeyi amaçlayan bir psikolojik harekât kapsamında değerlendirilmelidir. Nisan 2025'te İran kaynaklı olduğu iddia edilen deepfake videosu, İsrail eski Savunma Bakanı Gallant'a, yapay zekâ ile hazırlanmış beyanlar atfederek, sosyal medya aracılığıyla toplumsal manipülasyon yaratmayı hedeflemiştir. Son olarak Haziran 2025'te İsrail ile İran arasında cereyan eden konvansiyonel çatışmada, her iki tarafın da siber saldırılar aracılığıyla, toplumsal huzursuzluğu arttırıcı eylemlere giriştiği söylenebilir.

Bu örnekler değerlendirildiğinde, siber saldırıların büyük çoğunluğunun enerji, ulaşım, sanayi ve su altyapısı gibi kritik altyapıların işlevsiz bırakılmasına yönelik olduğu görülmektedir. Dolayısıyla saldırıların ağırlık merkezini, fiziksel altyapının siber yöntemlerle devre dışı bırakılması oluşturmaktadır. Sosyal medya manipülasyonları ise özellikle son dönemlerde ön plana çıkmış ve kamuoyu algısının yönlendirilmesi hedeflenmiştir. Bu durum, siber savaşın yalnızca kritik altyapılara yönelik zararlarla sınırlı kalmadığını, aynı zamanda psikolojik harp unsurlarını da içerdiğini göstermektedir.

Yapay zekânın siber savaşa entegrasyonu hem saldırı hem de savunma mekanizmalarında önemli değişikliklere sebep olmuştur. İsrail, yapay zekâ destekli proaktif savunma sistemlerine ve gelişmiş siber güvenlik şirketlerine sahip olmasıyla öne çıkarken; İran, asimetrik stratejiler ve devlet destekli hacker gruplarıyla dijital alanda faaliyet yürütmektedir. Özellikle Stuxnet saldırısı ve sonrasında yaşanan gelişmeler, siber savaşların fiziksel etkilerinin yanı sıra psikolojik ve politik sonuçlarının da olduğunu kanıtlamıştır. Çalışmanın bir diğer önemli bulgusu, yapay zekânın siber operasyonlarda giderek artan bir rol üstlendiğidir.

Sonuç olarak, İsrail ve İran arasındaki siber savaş, modern çatışmaların doğasını yeniden tanımlamaktadır. Bu mücadele, devletlerin siber savunma kapasitelerini geliştirmelerinin yanı sıra, yapay zekâ gibi yenilikçi teknolojileri stratejik bir şekilde kullanmalarının gerekliliğini vurgulamaktadır. Gelecekte, siber çatışmaların daha karmaşık ve yıkıcı boyutlara ulaşabileceği öngörülmekte, bu da uluslararası iş birliği ve düzenlemelerin önemini bir kez daha ortaya koymaktadır.

KAYNAKLAR

Adamsky, D. D. (2017). The Israeli odyssey toward its national cyber security strategy. *The Washington Quarterly, 40*(2), 113-127. http://dx.doi.org/10.1080/0163660X.2017.1328928

Amaliya, L. R. (2025). A cyber war of Iran-Israel: A geopolitical rivalry. *Proceedings of the International Conference on Strategic and Global Studies (ICSGS 2024),* (s. 45-56). Atlantis Press.

Amitay, N. (2025, Nisan 14). Iranian deepfake of Israeli defense minister airs live - and how clarity caught it instantly. https://www.getclarity.ai/ai-deepfake-blog/iranian-deepfake-of-israeli-defense-minister-airs-live----and-how-clarity-caught-it-instantly

Baezner, M. & Cordey, S. (2022). Influence operations and other conflict trends. M. D. Cavelty & A. Wenger (Ed.), *Cyber security politics: Socio-technological transformations and political fragmentation* içinde (ss. 17-31). Routledge.

Bahgat, B. (2020). Iran and its neighbors face risks and opportunities in cyber security. *Orbis, 64*(1), 78-97.

Baram, G. & Peer, N. (2025, Temmuz 18). How Israel and Iran brought cyber conflict to centre stage. https://bindinghook.com/how-israel-and-iran-brought-cyber-conflict-to-centre-stage/

Barzashka, I. (2013). Are cyber-weapons effective? Assessing stuxnet's impact on the Iranian enrichment programme. *The RUSI Journal, 158*(2), 48-56.

Benouachane, H. (2024). Cyber security challenges in the era of artificial intelligence and autonomous weapons. M. E. Erendor (Ed.), *Cyber security in the age of artificial intelligence and autonomous weapons* içinde (ss. 24-42). CRC Press.

Ben Shushan. (2024, Şubat 7). 'Netanyahu is the target': Microsoft report reveals Iran's cyber war on Israel. https://www.jpost.com/breaking-news/article-785566

Biernacik, B. (2018). The fifth dimension of war–cyberspace. How to secure this area: The approach of selected states and international organizations to cybersecurity. *Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu, 83*(6), 63-84.

Bob, Y. J. (2021, Eylül 19). Mossad assassinated Iran's chief nuke scientist with remote AI gun – report. https://www.jpost.com/middle-east/mossad-assassinated-irans-chief-nuke-scientist-with-remote-ai-gun-report-679751

Bonfanti, M. E. (2022). Artificial intelligence and the offense–defense balance in cyber security. M. D. Cavelty & A. Wenger (Ed.), *Cyber security politics: Socio-technological transformations and political fragmentation* içinde (ss. 64-79). Routledge.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Chawla, A. (2021). Pegasus spyware 'a privacy killer'. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890657

Cristiano, F., Broeders, D., Delerue, F., Douzet, F. & Géry., A. (2023). Artificial intelligence and international conflict in cyberspace: Exploring three sets of issue. F. Cristiano, D. Broeders, F. Delerue, F. Douzet & A. Géry (Ed.), *Artifical intelligence and international conflict in cyberspace* içinde (ss. 1-15). Routledge.

Çahmutoğlu, E. (2021). *Iran's cyber power*. İRAM yayınları.

Çalışkan, A. (2023). Siber savaş: Bilgi krizi mi yoksa güvenliği mi?. *SAVSAD Savunma ve Savaş Araştırmaları Dergisi*, *33*(1), 1-32. https://doi.org/10.54078/savsad.1188851

Cohen, S. (2019). Iranian cyber capabilities: Assessing the threat to Israeli financial and security interests. *Cyber, Intelligence, and Security, 3*(1), 71-94.

Davis, Z. (2019). Artificial intelligence on the battlefield: Implications for deterrence and surprise. *PRISM, 8*(2), 114-131.

Denning, D. E. (2012). Stuxnet: What has changed?. *Future Internet, 4*(3), 672-687.

Editorial INTI. (2024, Eylül 09). What is Israel's secret to building a global cybersecurity ecosystem?. https://intimedia.id/read/what-is-israels-secret-to-building-a-global-cybersecurity-ecosystem-66defc9fd1cc7

Farwell, J. P. & Arakelian, D. (2013). What does Iran's cyber capability mean for future conflict?. *The Whitehead Journal of Diplomacy and International Relations*, *14*(1), 49-65.

Freilich, C. (2024). The Iranian cyber threat: The institutions and praxis of Iran's cyber strategy, *Institute for National Security Studies*, 5-123. https://www.inss.org.il/publication/iranian-cyber/

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41-73.

Geranmayeh, E. (2025). *Israel and Iran on the brink: Preventing the next war.* European Union Institute for Security Studies.

Gotsiridze, A. (2020, Ocak 15). Iran's cyber capabilities. https://gfsis.org/en/irans-cyber-capabilities-2/

Guyonneau, R. & Le Dez, A. (2019). Artificial intelligence in digital warfare: Introducing the concept of the cyberteammate. *The Cyber Defense Review*, *4*(2), 103-116.

Haroon, A. (2024). AI and cyber drove warfare in the Israeli-Iran conflict and its impact on gulf states' security. *Journal of Politics and International Studies, 10*(2), 145-163.

Hodges, D. & Creese, S. (2015). Understanding cyber-attacks. J. A. Green (Ed.), *Cyber warfare: A multidisciplinary analysis* içinde (ss. 33-60). Routledge.

Ifeanyi-Ajufo, N. & Rosli, W. R. W. (2024). Artificial intelligence and cyber espionage delineating emergent warfare and international security. M. E. Erendor (Ed.), *Cyber security in the age of artificial intelligence and autonomous weapons* içinde (ss. 70-86). CRC Press.

Iran's cyberattacks capabilities. (2020, Ocak). Special report. *King Faisal Center for Research and Islamic Studies.* https://kfcris.com/en/view/post/258

Johnson, J. S. (2020). Artificial intelligence: A threat to strategic stability. *Strategic Studies Quarterly, 14*(1), 16-39.

Jun, J. (2024, Nisan 30). How will AI change cyber operations?. https://warontherocks.com/2024/04/how-will-ai-change-cyber-operations/

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*, 46, 11–20. https://doi.org/10.1016/j.polgeo.2014.10.001

Kallberg, J. (2016). Strategic cyberwar theory-A foundation for designing decisive strategic cyber operations. *The Cyber Defense Review*, *1*(1), 113-128.

Karamchand, G. & Aramide, O. O. (2025). AI and cyberwarfare. *Journal of Tianjin University Science and Technology. 58*(8), 835-851. https://doi.org/10.5281/zenodo.16948349

Keck, Z. (2014, Ağustos 02). Chinese hackers target Israel's iron dome. https://thediplomat.com/2014/08/chinese-hackers-target-israels-iron-dome/

Khalil, A., Bitar, M. & Raj, S. A. K. (2024). A new era of armed conflict: The role of state and non-state actors in cyber warfare with special reference to Russia-Ukraine war. *TalTech Journal of European Studies, 14*(2), 49-72. https://doi.org/10.2478/bjes-2024-0016

Kırık, A. M. (2025). Siber savaşların gölgesinde İsrail'in teknolojik gücü ve etik sorunlar. *Avrasya Dosyası*, *15*(2), 1-23.

Kober, A. (2019). Israel's security model. S. A. Cohen & A. Klieman (Ed.), *Routledge handbook on Israeli security* içinde (ss. 225-237). Routledge.

Kovacs, E. (2020, Nisan 27). Israel says hackers targeted SCADA systems at water facilities. https://www.securityweek.com/israel-says-hackers-targeted-scada-systems-water-facilities/

Lande, D. & Danyk, Y. (2025). Competitive artificial intelligence in information and cyber warfare. Available at SSRN: http://dx.doi.org/10.2139/ssrn.5084698

Libicki, M. (2020). Cyberwar is what states make of it. *The Cyber Defense Review*, *5*(2), 77-88.

Lindsay, J. R. (2025). Stuxnet revisited: From cyber warfare to secret statecraft. *Journal of Strategic Studies, 48*(3), 1-40. https://doi.org/10.1080/01402390.2025.2481447

Lund, M. S. (2025). Hybrid threats in cyberspace: What do Russia's cyberspace operations in Ukraine tell us?. O. J. Borch & T. Heier (Ed.), *Preparing for hybrid threats to security: Collaborative preparedness and response* içinde (ss. 69-83). Routledge.

Malik, S. (2024, Ekim 18). Iranian cyber actors target critical infrastructure: FBI, CISA, and NSA warn. https://www.capacitymedia.com/article/2dwnjgpyaqfqcheztbjeo/news/iran-cyber-actors

Mazanec, B. M. (2015). *The Evolution of cyber war: International norms for emerging-technology weapons.* Potomac Books.

Mieses, M., Kerr, N. & Jahanbani, N. (2024, Ekim 9). Artificial intelligence is accelerating Iranian cyber operations. https://www.lawfaremedia.org/article/artificial-intelligence-is-accelerating-iranian-cyber-operations

Montasari, R. (2022). Cyber threats and national security: The use and abuse of artificial intelligence. A. J. Masys (Ed.), *Handbook of security science* **içinde** (ss. 679-700). Springer International Publishing.

Nelson, N. (2025, 3 Nisan). Israel enters 'stage 3' of cyber wars with Iran proxies. https://www.darkreading.com/threat-intelligence/israel-stage-3-cyber-wars-with-iran-proxies

Nixon, G. (2022, 20 Mart). Zelensky, Putin videos provide glimpse of evolving deepfake threat, experts say. https://www.cbc.ca/news/world/zelensky-putin-ukraine-war-deepfake-video-1.6391033

Nye, J. S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4), 18-38.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44-71.

Ofusori, L., Bokaba, T. & Mhlongo, S. (2024). Artificial intelligence in cybersecurity: A comprehensive review and future direction. *Applied Artificial Intelligence*, *38*(1), https://doi.org/10.1080/08839514.2024.2439609

Paliszkiewicz, J., Chen, K. & Goluchowski, J. (2024). Privacy in social media: Future directions. J. Paliszkiewicz, K. Chen & J. Goluchowski (Ed.), *Privacy, trust and social media* içinde (ss. 3-13). Routledge.

Provecho, E. F., Phuc, P. D. & Fokker, J. (2024, Eylül 19). The Iranian cyber capability. https://www.trellix.com/blogs/research/the-iranian-cyber-capability/

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5-32. http://dx.doi.org/10.1080/01402390.2011.608939

Robinson, M., Jones, K. & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, 49, 70-94.

Rosenfield, D. K. (2009). Rethinking cyber war. *Critical Review*, *21*(1), 77-90. https://doi.org/10.1080/08913810902812156

Rosli, W. R. W. (2025). Waging warfare against states: The deployment of artificial intelligence in cyber espionage. *AI and Ethics, 5,* 47-53. https://doi.org/10.1007/s43681-024-00628-x

Salem, A.H., Azzam, S. M., Emam, O. E. & Abohany, A. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11*(105), https://doi.org/10.1186/s40537-024-00957-y

SentinelOne. (2025, Mayıs 15). Key cyber security statistics for 2025. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/#industry-specific-cyber-security-statistics

Shadle, M. A. (2020). Killer robots and cyber warfare: Technology and war in the twenty-first century. T. Winright (Ed.), *T&T Clark handbook of christian ethics* içinde (ss. 215-224). Bloomsbury Publishing.

Siboni, G., Abramski, L. & Sapir, G. (2020). Iran's activity in cyberspace: Identifying patterns and understanding the strategy. *Cyber, Intelligence, and Security, 4*(1), 21-40.

Siboni, G. & Kronenfeld, S. (2012). Iran's cyber warfare. *Institute for National Security Studies*, https://www.inss.org.il/publication/irans-cyber-warfare/

Siman-Tov, D. & Even, S. (2020). A new level in the cyber war between Israel and Iran. *Institute for National Security Studies*, https://www.inss.org.il/publication/iran-israel-cyber-war/

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly, 12*(3), 90-113.

Smith, T. E. (2013). Cyber warfare: A misrepresentation of the true cyber threat. *American Intelligence Journal, 31*(1), 82-85.

Stiennon, R. (2015). A short history of cyber warfare. J. A. Green (Ed.), *Cyber warfare: A multidisciplinary analysis* içinde (ss. 7-32). Routledge.

Summer, D. (2023, Aralık 20). Israel linked to cyberattack that closed 70% of Iran's gas stations. Israel Linked To Cyberattack That Closed 70% Of Iran's Gas Stations | IBTimes UK

Tabansky, L. (2011). Basic concepts in cyber warfare. *Military and Strategic Affairs*, *3*(1), 75-92.

Tabansky, L. ve Ben Israel, I. (2015). *Cybersecurity in Israel.* Springer International Publishing.

Tabansky, L. (2016). Towards a theory of cyber power: The Israeli experience with innovation and strategy. 2016 8th International Conference on Cyber Conflict (CyCon) (ss. 51-63). IEEE.

Tehran Insider. (2024, Ağustos 22). The final straw: Iranians dread plans for a 'national' internet. https://www.iranintl.com/en/202408218106

United against nuclear Iran. (2024, Haziran). The Iranian cyber threat. https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents

Unna, Y. (2019). National cyber security in Israel. *Cyber, Intelligence, and Security, 3*(1), 167-173.

Yamin, M. M., Ullah, M., Ullah, H. & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications,* 57, 1-14.

Yenal, S. & Akdemir, N. (2020). Uluslararası ilişkilerde yeni bir kuvvet çarpanı: Siber savaşlar üzerine bir vaka analizi. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(1), 414-450.