dipam
DİPLOMATİK İLİŞKİLER ve POLİTİK ARAŞTIRMALAR MERKEZİ
CENTER for DIPLOMATIC AFFAIRS and POLITICAL STUDIES

ANALİZ

İSRAİL SİBER SALDIRILARININ GÖLGESİNDE İRAN NÜKLEER ANLAŞMASI

Büşra ORAK

Nisan 2023 Sayı: 10

İSRAİL SİBER SALDIRILARININ GÖLGESİNDE İRAN NÜKLEER ANLAŞMASI

20.yy.da bilgi ve iletişim teknolojisindeki gelişmeler, dördüncü nesil savaş dönemi teknolojisinde önemli değişim ve dönüşüme neden olmuştur. Bu gelişim alanlarından biri de siber alandır. Beşinci savaş alanı olarak değerlendirilen siber alan, devletlerin yeni savaş alanlarından biri haline gelmiştir. Özellikle teknolojik üstünlüğe sahip devletler, hareket alanlarını genişletmek ve reel politik çıkarlarını devam ettirmek amacıyla siber saldırı, siber casusluk ve siber istihbaratı içeren siber savaş taktiklerini kullanmaktadırlar. Bu devletlerden biri olan ileri teknolojik üstünlüğe sahip İsrail, var olan tehditleri en aza indirmek ve güvenliği sağlamak için siber alanı aktif bir şekilde kullanmaktadır.

Siber Savaş'ın "Pearl Harbor'ı" olarak adlandırılan Stuxnet saldırısı, 2010'da İran ve İsrail arasında büyük bir gerilime sebep olmuştur. Stuxnet hem İran-İsrail ilişkileri hem de siber savaşlar açısından bir dönüm noktasıdır. 2010'dan günümüze kadar sayısız siber saldırıda bulunan İsrail, İran için ABD ile birlikte siber tehdidin birincil kaynağı olarak görülmüştür. Özellikle 2000'li yılların başında nükleer programını hızlandırmasıyla İran, ABD ve İsrail'in dış politika gündeminin ilk sırasında yer almasına ve yaptırımlara maruz kalmasına sebebiyet vermiştir. İran'a karşı gerçekleştirilen siber saldırıların büyük bir kısmı nükleer tesislere zarar vermek, nükleer araştırma enstitüleri ve arşivlerden belge çalmak, casusluk faaliyetleri üzerinden şekillenmiştir. Bununla birlikte İranlı nükleer bilim adamlarına karşı suikastlar düzenlenmiştir. İran hükümet yetkilileri gerçekleşen siber saldırılardan ABD ve İsrail'i sorumlu tutmuştur. İran'a karşı gerçekleşen son siber saldırılarda İsrail suçlamaları yalanlamamış ve siber saldırılar daha az gizli hale gelmiştir. (Baram, 2022)

2016 yılında İran ve P5+1 olarak bilinen BM Güvenlik Konseyi'nin beş daimi üyesi ABD, Çin, Rusya, İngiltere ve Fransa ile Almanya arasında imzalanan ve İran'ın uranyum zenginleştirme kapasitesine sınırlama öngören anlaşma, İsrail tarafından sert bir şekilde eleştirilmiştir. Bunun sonucunda 2018 yılında ABD'nin anlaşmadan çekilmesiyle sonuçlanan Kapsamlı Ortak Eylem Planı (KOEP)'na hala dönüş sağlanabilmiş değildir. İsrail'in gölgesinde gerçekleşen İran Nükleer Anlaşması, tarihsel süreci içerisinde hem reel alanda hem de siber alanda siber savaşların en önemli nedeni haline gelmiştir.

İsrail'in Siber Gücü ve Kapasitesi

20.yy.ın sonlarına doğru ortaya çıkan siber alan (Cyberspace), savaş teknolojisinden, devletin dış politika araçlarına ve savaş doktrinlerine kadar askeri, siyasi ve sosyal birçok alanın değişmesine ve dönüşmesine neden olmuştur. Uluslararası ilişkilerin geleneksel yaklaşımlarından farklı olarak güvenlik-tehdit, saldırı-savunma ya da güç-güvenlik ilişkilerini büyük ölçüde değiştirmiştir. Devletlere karşı oluşan tehditler sadece devlet düzeyinde değil, tüm analiz düzeylerinde oluşmaya başlamıştır. Bu da devletin tüm analiz düzeylerinde güvenlik stratejilerinin oluşmasını ve çeşitlenmesini mecburi hale getirmiştir. (Choucri, Clark, & Hurwitz, 2015)

Tehdidin kaynağı, türü, boyutu ve etki alanı da büyük ölçüde değişmiştir. Tehdidin kaynağı bir devlet olabileceği gibi on altı yaşında bir çocuk da olabilir. Bu nedenle devlet kontrol birimleri ve güvenlik araçları daha karmaşık ve zor bir hale gelmiştir.

Saldırı türleri ve kaynakları da çeşitlenmiştir. Bu nedenle siber saldırılar, tehdit kaynağı ve türüne göre sınıflandırılır. Devletler, casus yazılımcılar, hackerlar, kötü amaçlı yazılımcılar, teröristler, kimlik avcıları gibi devlet ve devlet dışı aktörler tehdidin kaynağı olabilir. Servis dışı bırakma saldırıları (Denial of Service Attack – DoS), Dağınık Hizmet Reddi (Distributed Denial of service- DDoS) , Truva atı (Trojan Horse), Virüs, Kötücül Yazılımlar (Malicious Software), Kurtçuk (Worms), Casus Yazılımlar (Spyware), Hackleme gibi faaliyetler bize saldırının türü hakkında bilgi vermektedir. (David, 2010)

Devletler tarafından gerçekleştirilen siber saldırılar, devlete bağlı birimler ya da özel hacker grupları tarafından gerçekleştirilmektedir. Bu siber ordular ya da özel gruplar, genellikle devletlerin kritik altyapı sistemlerini hedef almaktadır. Düşmanı yıpratma, yıldırma, korkutma veyahut gözdağı vermek amacıyla caydırıcılık unsuru olarak kullanır. İsrail'in de, siber savaş ve saldırı bilgi ve araçlarına sık sık başvurduğu görülmektedir.

İsrail hükümeti günümüz de bilgi teknolojisinde dünya lideri ve Ortadoğu'nun birinci büyük siber güç ve kapasitesine sahip olan devletidir. Siber teknolojinin bir savaş aracı olarak anılmasına ve yaygın bir şekilde kullanılmasına öncülük eden İsrail, 1990'larda siber alanda proaktif durumdan tekrar aktif hale gelmiştir. İsrailli siber güvenlik uzmanı Isaac Ben-Israel tarafından açıklanan ulusal güvenlik stratejisinde, İsrail'in bölgesel ve küresel güvenliğini sağlamak, sayısal olarak azlığını dengelemek, niteliksel üstünlüğünü artırmak için siber bilgi ve teknolojiye büyük önem verdiğini dile getirmiştir. Bu niteliksel üstünlük, bilgi teknolojisine dayanan nispeten gizli üstün silahlar olarak adlandırılmıştır. Ayrıca Isaac Ben-Israel, İsrail'in siber savaş stratejisini caydırıcılık doktrini üzerinden tanımlamıştır.

2010 yılında Isaac Ben-Israel, İsrail'in siber kapasitesini artırmak için "ulusal siber girişim" vizyonu başlatmıştır. Bu vizyondan hareketle 2011 yılında İsrail ilk ulusal siber stratejisi yayınlanmıştır. Ancak bu strateji büyük oranda kamuya açılmamıştır (McCreanor, 2021). 2017 yılına gelindiğinde Ben-Israel, ulusal siber güvenlik stratejisi savunma ve saldırı kapasitesini ve doktrinini ortaya koymuştur. Bunlar: caydırıcılık, kalıcı zafer, erken uyarı ve ittifaklar şeklinde kategorize edilmiştir. İsrail'in ulusal siber stratejisi, uluslararası siber stratejisini de kapsamaktadır. Bu strateji, küresel siber savunma mekanizmasını yaratmayı amaçlamaktadır. Strateji; küresel siber savunma için işbirliği, kapasite ve güven inşası ve yeni teknolojik çözümler olarak tanımlanmaktadır (Israel's National Cybersecurity and Cyberdefense Posture, 2020).

Bu stratejinin ötesinde kapsayıcı bir siber güvenlik örgütü, İsrail Ulusal Siber Müdürlüğü (INCD) oluşturulmuştur. INCD hükümet siber grupları arasında yer almaktadır. UNIT- 8200, ulusal bilgi güvenlik merkezi(NISA) diğer siber gruplardır. Başbakanlığın alt birimi olarak görev yapan INCD ile birlikte Mossad, Shin Bet, İsrail Ulusal Siber Olaylara Hazırlık Ekibi (CERT-IL) yer almaktadır. Ayrıca İsrail Savunma Bakanlığı ve İsrail Kamu Güvenliği Başkanlığı alt birimi olarak siber danışma organı Mat'e ha-Cyber ha, İsrail Ulusal Siber Bürosu- INCB), İsrail polisi, siber suç birimi, Ulusal Siber Güvenlik Kurumu (NCSA) şeklinde kurumlar faaliyet göstermektedir (Israel's National Cybersecurity and Cyberdefense Posture, 2020). Sadece resmi kurumlar değil, aynı zamanda siber

paralı askerleri, hacker destek grupları gibi pek çok yapı da oluşturulmuştur.

ABD ve İsrail orduları siber savunma eğitim süreçlerini birlikte yürütmekte ve siber tehditlere karşı ortak tatbikatlar yapmaktadırlar. Olası bir siber saldırıya karşı hareket kabiliyetlerini artırmaktadırlar. Bu durum bir siber saldırıda birlikte anılmalarına neden olabilmektedir. İran, İran nükleer programını hedef alan Stuxnet saldırısında hem İsrail hem de ABD'yi suçlamıştır. İran nükleer anlaşması başka bir ifadeyle kapsamlı ortak eylem planı (KOEP) sürecinde İran karşı gerçekleştirilen siber saldırılar da ABD ve İsrail'i hedef göstermiştir. İran nükleer anlaşması, İran ve İsrail arasında gerçekleşen siber saldırıların yoğunluğu bakımından önemli ipuçları verir.

İran Nükleer Anlaşması -Kapsamlı Ortak Eylem Planı (Koep)

Siber alan için hala erken bir tarih olan 2002 yılında Ali Rıza Caferzade, İran'ın Natanz ve Arak'ta iki nükleer santrale sahip olduğunu açıklamıştır. Bunun üzerine ABD, İran'ı nükleer silah geliştirme gerekçesiyle Uluslararası Atom Enerjisi Kurumu'na (UAEK) şikâyette bulunmuştur. (Çağla Gül Yesevi, 2015) ABD tarafından İran'a karşı tek taraflı uygulanan yaptırımlar, 2006-2010 arası dönemde İran'ın nükleer enerji çalışmalarına devam etmesi sonucunda BMGK'de alınan kararlarla çok taraflı yaptırımlara dönüşmüştür. 2010 Temmuz ayında H. Barack Obama tarafından imzalanan İran Yaptırım Sorumluluk ve Tecrit Yasası (İYSTC) İran'ın doğrudan petrol enerji arzını ve petrol sektörünü hedef almıştır (Rezaei, 2019).

2011- 2012 yılında BM, İran bankalarının varlığını ve petrol sektöründeki ticaretini durdurmuştur. 17 Mart 2012'de, yaptırımlara uymayan devletler, uluslararası şirketler ve tüm İran bankaları finansal işlemleri de dâhil dünyanın merkezi konumunda olan, The Society for Worldwide Interbank Financial Telecommunication (SWIFT) adlı kuruluşun dışında kalmış ve bir günde bankacılık kanallarından izole edilmiştir.

2015 yılının sonunda ABD yaptırımları, İran'da politika değişikliğine neden olmuştur. 14 Haziran 2015'de p5+1 olarak adlandırılan 6 ülke (ABD, Çin, İngiltere, Almanya, Rusya, Fransa) ve İran arasında Kapsamlı Ortak Eylem Planı (KOEP) ile karşılıklı anlaşmaya varılmıştır. Bu anlaşma İran'ın nükleer faaliyetlerine ciddi sınırlamalar getirirken 1696, 1737, 1747, 1803, 1835, 1929 sayılı yaptırım kararlarının kalkmasını sağlamıştır (Aslan, 2018).

Müzakereler iki yıldan fazla sürse de, sonunda karşılıklı olarak verilen tavizler sonucunda uzlaşma ve işbirliği sağlanabilmiştir. Müzakereler sonucunda ABD, İran enerji sektöründeki yaptırımları kaldırmıştır. Böylece, Yabancı Varlıkları Kontrol Ofisi (OFAC) öncülüğünde İran'ın finans ve bankacılık, sigortacılık, enerji ve petrokimya, gemicilik, gemi inşaatı ve liman, altın ve diğer metaller, bilgisayar programları ve otomobil sektörü üzerindeki yaptırımlar kaldırılmıştır (Rezaei, 2019). Uluslararası Enerji Ajansı(UEA) tarafından tasdik edildikten sonra anlaşma, 16 Ocak 2016 tarihinde yürürlüğe girmiştir.

ABD eski başkanı Donald Trump, seçim süreci boyunca 'tarihin en kötü anlaşması' olarak adlandırdığı İran Nükleer Anlaşması'ndan, seçildikten iki yıl sonra 8 Mayıs 2018 tarihinde tek taraflı olarak ayrılmıştır. Çin ve Rusya tarafından kabul

görmeyen bu hareket sonucunda 28 AB üyesi ülke, ABD ve İran arasında aktif bir diplomasi yürütmeye başlamıştır. Ancak Donald Trump; KOEP'in İran nükleer üretimini sadece bir süreliğine durdurduğunu ve balistik füze üretimine devam ettiği gerekçesiyle müzakereler başarıya ulaşamamıştır (Rezaei, 2019). Bu nedenle İran'da görülen ekonomik iyileşmeler ve enerji sektöründeki canlanmalar, 2015 öncesine dönmüştür. ABD, 90 ve 180 günlük iki aşamayla ülkelere çağrıda bulunarak İran ile enerji, imalat, liman, sanayi, maden sektörlerinde ticari ilişkilerini kesmesini bildirmiştir.

Trump'ın ardından Ocak 2021'de ABD başkanı seçilen Joe Biden, İran ile müzakerelere başlamaya hazır olduğunu bildirmiştir. ABD'nin KOEP anlaşmasına dönmesi için Nisan 2021'de Viyana'da başlatılan müzakereler, 8 Ağustos'ta sona ermiştir. Ancak 2022 Eylül ayında başlayan İran'daki protestolar ve artan şiddet görüntüleriyle beraber geçtiğimiz aylarda Joe Biden'ın "Nükleer Anlaşmanın öldüğünü" ima ettiği görüntülerin ortaya çıkmasıyla birlikte, tarafların tekrar müzakere masasında buluşmasının zor olduğu görülmektedir (Biden, İran ile müzakereler devam ederken nükleer anlaşmayı "ölü" ilan etmiş, 2022).

İsrail Siber Saldırılarının İran Nükleer Anlaşmasına Etkisi

1979 İran İslam devriminden önce şah yönetimiyle iyi ilişkiler kuran İsrail, devrimden sonra İran'ı varlığına bir tehdit olarak görmüştür. İran'da Ayetullah Humeyni'nin önderliğinde yapılan devrim, Şii-İslam kimliği ile bütünleşerek, İsrail'in tehdit algılarına benzer şekilde İran'ın varlığına ve kimliğine yönelik en büyük tehdit olarak ABD ve İsrail'i görmüştür (Shalom, 2016). İran'ın, Humeyni'nin doktrininden vazgeçerek İran nükleer programını başlatmasıyla birlikte, İsrail siyaseti ve beraberinde ABD siyasetinde oluşan dış baskı, önce yaptırımları, sonrasında ise İran Nükleer Anlaşması'ndaki anlaşmazlıkları beraberinde getirmiştir. Çünkü İsrail devleti ve halkının güvenliğine karşı büyük bir tehdidin varlığı ve Ortadoğu'daki güç dengesinin İsrail'in aleyhine bozulacağı endişesi, İran Nükleer Anlaşması'nın çıkmaza girmesine neden olmuştur (Oruç, 2016).

Devletler için saldırıların bir güvenlik sorunu oluşturup oluşturmayacağının önündeki en büyük engel atıf sorunu ve zamandır. Bir siber tehdit kaynağının ve türünün tespit edilmesi ciddi bir zaman kaybına neden olabilir. Tehdidin kim tarafından gerçekleştiğinin bilinmemesi de saldıran tarafın daha avantajlı bir konuma gelmesine neden olur. İsrail ve İran tarafından yapılan karşılıklı son siber saldırılar, atıf sorununu ortadan kaldırmaktadır. İsrail ve İran hükümet yetkilileri saldırıları doğrulamasa da paralelinde yapılan açıklamalar, kaynağı doğrular niteliktedir. 2010 yılından itibaren İsrail tarafından gerçekleştirilen, siber saldırı, bombalama, suikast, siber casusluk olayları İsrail'in İran'a karşı hibrit savaş taktiği yürüttüğünü ortaya koymaktadır. Bununla birlikte saldırıların hedefi de büyük oranda İran'ın nükleer programıyla bağlantılı olarak gerçekleştirilmektedir. Saldırının şekli nükleer tesislere bilgisayar virüsü bulaştırma, altyapı sistemlerini hedef alma ya da nükleer bilim adamlarına karşı düzenlenen suikastlar şeklinde kendini göstermektedir (Timeline: Israeli Attacks on Iran, 2023).

2010 yılından itibaren İsrail düzenli olarak İran'a sayısız siber saldırı da bulunmuştur. Ancak bunlar iki döneme ayrılabilir. İlki

siber saldırıların yoğunlukta yaşandığı 2010-2012 arası dönemi kapsamaktadır. Bu İran Nükleer Anlaşması'nın öncesini içermektedir (Israeli Sabotage of Iran's Nuclear Program, 2021). 2010-2012 yılları arasında çok sayıda siber saldırı olmasına karşın, karşı tarafa en zarar verici siber saldırılar Tablo.1'de sıralanmıştır.

Tablo.1: 2010-2012 Önemli Siber Saldırılar

İkincisi ise ABD'nin Nükleer Anlaşmadan çekildiği 2018 sonrası dönemi içermektedir. Ancak bu dönem hibrit savaş yöntemlerinin ağır bastığı, siber savaş yöntemlerinin yanında Mossad baskını, suikast ve drone saldırılarını da içine almaktadır. İran'ın nükleer tesislerine sayısız saldırı gerçekleştirilmiştir (Israeli Sabotage of Iran's Nuclear Program, 2021). Ancak Tablo.2'de siber boyuttaki önemli saldırılar gösterilmektedir.

Tablo.2: 2018-2021 Önemli Siber Saldırılar

2018 ve sonrasında gerçekleşen siber saldırıların, daha açık bir şekilde yapıldığı görülmektedir. 2 Temmuz 2020 tarihinde gerçekleşen patlama, İran'ın Natanz'daki ana nükleer zenginleştirme tesisinde büyük hasara yol açarak, IR-4 ve IR-6 santrifüjleri üreten fabrikaya zarar vermesi, 29 Ocak askeri bir fabrikaya ve 14 Şubat 2022 tarihinde ise altı İsrail dronunun, İran'ın insansız hava aracı üretim merkezini hedef alması gibi pek çok saldırı gerçekleştirilmiştir (İran Askeri Fabrikasına Drone Saldırısı, 2023). Bunun yanında İran'ın siber saldırıları misilleme olarak gerçekleşmekte ve ABD, İsrail ve Suudi Arabistan ağırlıklı olmak suretiyle Türkiye ve Batılı ülkeleri de hedef almaktadır. 2015 yılının ilk yarısında ve 2018 yılının son altı ayında İran'ın siber saldırılarında yoğun artış olduğu gözlenmiştir (Bulut, 2021) Bu durum, nükleer anlaşma sürecini takip etmesi bakımından manidardır.

Sonuç ve Değerlendirme

İsrail devleti kurulduktan tam beş yıl sonra, ulusal savunma strateji belgesinde bilgi teknolojisinden bahsederek, düşmandan gizli üstün nitelikli silahların geliştirilmesi gerektiğini önemini vurgulamıştır. Bu tarihten tam yarım asır sonra bölgenin en üstün teknolojik silahlarına sahip ülkesi haline gelmiştir. Siber alandaki üstün yetenekleri ve siber saldırı- savunma stratejilerini profesyonelce uygulaması sayısız siber saldırı ve siber casusluk faaliyetini gerçekleştirmesine imkân sağlamıştır.

ABD siber grupları ile ortak çalışmalar yürüten İsrail devlet ve devlet dışı siber hacker grupları, İran'a karşı düzinelerce saldırı ve casusluk faaliyetinde bulunmuştur. Ancak İsrail'in İran'a karşı düzenlediği siber saldırıların nihai hedefi İran nükleer programı çerçevesinde gerçekleştirilmiştir. İran'da gerçekleşen siber saldırılar incelendiğinde saldırılar üç nokta da kesişmektedir. Bunlar ilk olarak nükleer tesisler, nükleer çalışmaların yapıldığı enstitü ve arşivler ve İran'ın iletişim ve teknolojik altyapısıdır. Özellikle 2010 sonrası dönemde İsrail'in İran'a karşı siber saldırılarında büyük bir artış yaşanmıştır. Bu süreç, artan siber saldırı yoğunluğuna göre dönemlere ayrılmıştır. İlk dönem İran Nükleer Anlaşması öncesi, ikinci dönem ise ABD eski başkanı D. Trump'ın anlaşmadan çekildiği döneme denk gelmektedir.

İsrail, en büyük güvenlik tehdidi olarak gördüğü İran nükleer programına karşı 2010'dan günümüze kadar siber saldırı, siber casusluk, suikast, drone saldırısı, patlama şeklinde hibrit bir savaş yürütmüştür. Böylece İran'ın nükleer çalışmalarını zayıflatmış ve zaman kaybına neden olmuştur. İran da, İsrail'e karşı özellikle İsrail'in müttefiklerini hedef alacak şekilde siber saldırılar düzenlemiştir. İran ve İsrail arasında gerçekleşen siber saldırılar, dış politika stratejileri ve güvenlik algılarına göre şekillenmektedir. Bu nedenle siber alan, İran Nükleer Anlaşması'nın geleceğinin ne olacağı ve sürecin nasıl işleyeceği konusunda önemli doneler sunabilmektedir. 2018'den bu yana giderek artan siber saldırılar İran Nükleer Anlaşması'nın geleceği konusunda belirsizliği artırmakta ve nükleer müzakerelere gölge düşmesine neden olmaktadır.

KAYNAKÇA

(2020). *Israel's National Cybersecurity and Cyberdefense Posture.* Zürich: Center for Security Studies (CSS).

Israeli Sabotage of Iran's Nuclear Program. (2021). https://iranprimer.usip.org/blog/2021/apr/12/israeli-sabotage-iran%E2%80%99s-nuclear-program adresinden alınmıştır

Kasım Süleymani suikastı üzerinden bir yıl geçti ancak İran ile ABD arasındaki gerginlik azalmadı. (2021). anadolu ajansı: https://www.aa.com.tr/tr/dunya/kasim-suleymani-suikasti-uzerinden-bir-yil-gecti-ancak-iran-ile-abd-arasindaki-gerginlik-azalmadi/2096165 adresinden alınmıştır

Biden, İran ile müzakereler devam ederken nükleer anlaşmayı "ölü" ilan etmiş. (2022, aralık 20). https://www.hurriyet.com.tr/dunya/biden-iran-ile-muzakereler-devam-ederken-nukleer-anlasmayi-olu-ilan-etmis-42190798 adresinden alınmıştır

İran Askeri Fabrikasına Drone Saldırısı. (2023). https://www.voaturkce.com/a/iran-askeri-fabrikasina-drone-saldirisi/6938909.html adresinden alınmıştır

Timeline: Israeli Attacks on Iran. (2023). https://iranprimer.usip.org/blog/2022/aug/11/timeline-israeli-attacks-iran adresinden alınmıştır

Aslan, M. (2018). ABD'nin Nükleer Anlaşmadan Çekilmesinin Ekonomik Sonuçları. *İran Araştırma Merkezi(İRAM)*, 5-18.

Baram, G. (2022, july 25). *How the cyberwar between Iran and Israel has intensified*. https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/ adresinden alınmıştır

Bulut, S. (2021). İran'ın Siber Alan Faaliyetleri: Kapsamlı Ortak Eylem Planı (KOEP) SürecineDair Bulgular. *GAZİANTEP UNIVERSITY JOURNAL OF SOCIAL SCIENCES*, 166-191.

Choucri, N., Clark, D. D., & Hurwitz, R. (2015). *exploration in cyber international relation.* Cambridge: Massachusetts Institute of Technology.

Çağla Gül Yesevi. (2015). İran'ın Enerji Sektörü: İran'ın Yumuşak ve Akıllı Gücü. *İstanbul Kültür Üniversitesi*, 441-467.

David, C. (2010). Characterizing,cyberspace:,past,,present,and,future. *MIT,CSAIL*, 1-18.

McCreanor, K. (2021). The Theory, Pursuit, and Practice of Cyber power in Israel. *Centre of Military and Strategic Studies*, 2-21.

Oruç, H. (2016). ran Nükleer Anlaşması ve İsrail'in Anlaşmaya Yönelik Tepkisi. *ORTADOĞU YILLIĞI* , 484-500.

Rezaei, F. (2019). *Iran's Foreign Policy After the Nuclear Agreement.* Ankara: Palgrave Macmillan.

Shalom, Z. (2016). Israel, the United States, and the Nuclear Agreement with Iran:Insights and Implications. *Strategic Assessment*, 18-28.

YAZAR HAKKINDA

Büşra ORAK, Niğde Ömer Halisdemir Üniversitesi Siyaset Bilimi ve Uluslararası ilişkiler bölümünü tamamlamış, Hacı Bayram Veli Üniversitesi Uluslararası İlişkiler Yüksek Lisans Programına devam etmektedir. Orak, aynı zamanda DİPAM'da Odak Çalışma Grubu Stajyeri olarak görev almaktadır.
orakbusra09@gmail.com