İstihbarat Çalışmaları ve Araştırmaları Dergisi

Journal of Intelligence Research and Studies

Haziran 2024, Cilt: 3, Sayı: 2, ss.175-211

June 2024, Volume: 3, Issue: 2, pp.175-211

ISSN 2822-3349 (Basılı/Print) **ISSN 2822-3357 (Çevrimiçi/Online)**

Makaleye ait Bilgiler / Article Information

İnceleme Makalesi / Review Article

Makale Başvuru Tarihi / Application Date: 15 Nisan 2024 / 15 April 2024

Makale Kabul Tarihi / Acceptance Date: 03 Haziran 2024 / 03 June 2024

Makalenin Başlığı / Article Title

Siber Güvenlikte Siber Gözetim: Pegasus Projesi

Cyber Surveillance in Cyber Security: The Pegasus Project

Yazar(lar) / Writer(s)

Pınar DEMİRCİ

Atıf Bilgisi / Citation:

Demirci, P. (2024). Siber Güvenlikte Siber Gözetim: Pegasus Projesi. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 3(2), ss.175-211, DOI: 10.61314/icad.1468290

Demirci, P. (2024). Cyber Surveillance in Cyber Security: The Pegasus Project. *Journal of Intelligence Research and Studies*, 3(2), pp.175-211, DOI: 10.61314/icad.1468290

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

Research Center for Defense Against Terrorism and Radicalization Association

Adres/Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı 5387. Cadde No:15A D:58

06800 Çankaya/Ankara

www.icadergisi.com

e-posta/e-mail: editor@icadergisi.com

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2024, 3(2) : 175-211 Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2024, 3(2) : 175-211 Research Article
DOI: 10.61314/icad.1468290

SİBER GÜVENLİKTE SİBER GÖZETİM: PEGASUS PROJESİ

Pınar DEMİRCİ*

ÖZET

İsrail Hükümeti'nin siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olması kamu-özel sektör iş birliğinin kötüye kullanılmasına neden olmaktadır. Makalede 2021 yılında ortaya çıkan İsrailli NSO şirketinin Pegasus casus yazılımını satın alan hükümetlerin neden olduğu insan hakları ihlallerini içeren Pegasus Projesi vakası ele alınacaktır. Araştırma nitel bir çalışmadır. Nitel araştırma yöntemlerinden dokümantasyon incelemesi yapılacaktır. Makalenin amacı, siber güvenlik alanında kamu-özel sektör iş birliğinde İsrail Hükümeti'nin siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olmasıyla iş birliğinin kötüye kullanılmasını Pegasus Projesi üzerinden göstermektir. Bu amaç doğrultusundan makalede şu sorulara yanıt aranmıştır: Pegasus projesi kapsamında İsrail Hükümeti'nin sorumluluğu nedir? İsrail Hükümeti'nin İsrailli siber ürünlerin ihracatındaki yetkisi nedir? Söz konusu yetkiyi hangi amaçlar için kullanmaktadır? Çalışmada, NSO şirketinin tarihine, Pegasus Projesinin ortaya çıkarılışı ve sonrasındaki yaşanan sürece ve proje kapsamında İsrail Hükümeti'nin sorumluluğuna yer verilmiştir. İsrail güvenlik şirketleri tarafından üretilen casus yazılımların ülkelere satılmasında onay yetkisine sahip İsrail Hükümeti, diplomatik ilişkiler geliştirmek ve siyasi kazanımlar elde etmek için baskıcı hükümetlere casus yazılımların satılmasına izin vermektedir.

Anahtar Kelimeler: *İsrail, NSO, Siber Güvenlik, Casus Yazılım, Pegasus Projesi*

Cyber Surveıllance In Cyber Securıty: The Pegasus Project

ABSTRACT

The Israeli government's full control over the private sector in the export of cyber products causes the abuse of the cooperation between the public and private sectors. The article will discuss the case of the Pegasus Project emerging in 2021 and involving human rights violations caused by oppressive governments that purchased the Pegasus spyware of the Israeli NSO company. The research is a qualitative study. Document analysis, one of the qualitative research methods, will be conducted. The aim of the article is to show the abuse of public-private sector cooperation in cyber security as the Israeli government has full control over the private sector in the export of cyber products through the Pegasus Project. For this purpose, answers to the following questions were sought in the article. What is the responsibility of the Israeli Government within the scope of the Pegasus Project? What is the Israeli Government's authority on the export of Israeli cyber products? For what purposes does she use this authority? In the study, the history of the NSO Company, the process of revealing the Pegasus Project and its aftermath, and the responsibility of the Israeli

* Yüksek Lisans Mezunu, Milli Savunma Üniversitesi, ORCID: 0000-0003-2980-4857.

Makale Başvuru Tarihi / Application Date: 15 Nisan 2024 / 15 April 2024

Makale Kabul Tarihi / Acceptance Date: 03 Haziran 2024 / 03 June 2024

Government within the scope of the project are included. The Israeli government, which has the authority to approve the sale of spyware such as Pegasus produced by Israeli security companies to other countries, allows the sale of spyware to oppressive governments with an aim to develop diplomatic relations and attain political gains.

Keywords: *Israel, NSO, Cyber Security, Spyware, Pegasus Project*

GİRİŞ

Günümüzde, İsrail'in siber gözetim ve casus yazılım endüstrisi, İsrail Savunma Kuvvetleri'nin (Israel Defense Forces – IDF) teknik bilgi birikiminden yararlanmaktadır. IDF'in siber birim mezunları ve gazileri, kurdukları siber şirketlerle askeri teknolojik deneyimlerini ve bilgilerini özel sektöre aktarmakta, siber gözetim ve casus yazılım endüstrisinin büyümesini ve gelişimini sağlamaktadır. Birçok İsrailli casus yazılım şirketinin kurucuları ve çalışanları, IDF'in elit siber birimlerinde tecrübe kazanmıştır. Ürettiği Pegasus adlı casus yazılımla ön plana çıkan İsrailli ünlü casus yazılım şirketi NSO Grup'un üç kurucusu Omri Lavie, Shalev Hulio ve Niv Karmi, Birim 8200[1] gazileridir (Levy, 2017; Melman, 2021). Ayrıca casus yazılım şirketinin araştırma ekibinin tamamı ve çalışanlarının çoğu, başta Birim 8200 olmak üzere IDF siber birimlerinde görev aldığı medyada rapor edilmektedir (Bergman ve Mazzetti, 2022). 2014 yılında kurulan diğer bir İsrailli gözetim şirketi Candiru'nun kurucuları Eran Shorer ve Yaakov Weizman da Birim 8200'de görev almıştır (Megiddo, 2021). Siber gözetleme şirketi Intellexa'nın kurucusu Tal Dilian da, IDF'in özel harekât birimleri ve diğer savunma teşkilatları için istihbarat araçları geliştirmekten sorumlu başka bir siber birim olan Birim 81'de görev almıştır (Sadeh, 2020).

NSO başta olmak üzere İsrailli siber gözetim şirketleri, son yıllarda siber teknolojilerini birçok otoriter rejime ihraç etmektedir. Başta Pegasus olmak üzere İsrailli siber gözetleme şirketleri tarafından üretilen casus yazılımların satın alınan ülkeler tarafından farklı muhalif gruplara karşı kullanıldığı ve satılan ülkelerde başta mahremiyet ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlaline neden olduğu raporlarda yer almaktadır (Uluslararası Af Örgütü, 2021a; Kaldani ve Prokopets, 2022,

[1] Birim 8200 olarak bilinen Merkezi Toplama Birimi ya da diğer adıyla İsrail Sinyal İstihbaratı Ulusal Birimi, IDF bünyesindeki Askeri İstihbarat Müdürlüğü (AMAN)'ne bağlı askeri siber uzay operasyonlarını koordine etmek ve yönlendirmekle görevli bir siber karargâhtır. Bkz. Oren, A. (2010, Ocak). The IDF's New Battlefield Is Found In Computer Networks. *Haaretz*. Erişim Tarihi: 24 Mayıs 2023, http://www.haaretz.co.il/misc/1.1182490

ss.19-20; Goodfriend, 2021). Uluslararası Af Örgütü'nün teknik desteğiyle 17 küresel medya kuruluşunun iş birliğinde ortaya çıkarılan Pegasus Projesi skandalı kapsamında, Pegasus yazılımını satın alan müşteriler için potansiyel hedef olduğu düşünülen telefon numaralarının olduğu NSO şirketine ait bir kayıt listesi ele geçirilmiştir. Proje kapsamında ortaya çıkarılan listede, 50'den fazla ülkeden devlet başkanları, politikacılar, diplomatlar, insan hakları savunucuları, akademisyenler, iş adamları, avukatlar, doktorlar, sendika liderleri ve gazetecilerin numaralarının olduğu belirlenmiştir (Uluslararası Af Örgütü, 2021a). Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın teknik analizine göre, gazetecilerden insan hakları savunucularına birçok kişi casus yazılım tarafından hedef alınmış; hukuka aykırı şekilde casus yazılımla takip edilmiştir (Uluslararası Af Örgütü, 2021b, s.6). Mahremiyet, ifade özgürlüğü ve basın özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlali 17 medya kuruluşu tarafından rapor edilmiştir (Richard, 2021).

Silah sistemlerinin ihracatında olduğu gibi, İsrailli şirketler tarafından üretilen Pegasus gibi casus yazılımların yurt dışına ihracatlarının İsrail Savunma Bakanlığı tarafından onaylanması gerekmektedir (İsrail Savunma Bakanlığı, 2023a). 2007 tarihli İsrail yasası uyarınca, siber güvenlik ürünleri satmak isteyen şirketler, Wassenaar Düzenlemesi'ne dayalı olarak Savunma Bakanlığı'nın Savunma İhracat Kontrolleri Dairesi'nden ihracat lisansları almaktadır (İsrail Savunma Bakanlığı, 2007, s.7; Wassenaar Düzenlemesi, 2023a; Silahlı Kontrol Derneği, 2022). İsrail Savunma Bakanlığı, siber ürünlerin ihracatına yönelik kararlarda Wassenaar Düzenlemesi'ne bağlılığını ifade ederken İsrailli casus yazılımların neden olduğu insan hakları ve temel özgürlüklerin ihlali, İsrail tarafından Wassenaar Düzenlemesi'ne uyulmadığını göstermektedir.

Bu makalede günümüzde uzun dönemli siber güvenlik politikalarının geliştirilmesi ve uygulanmasında kamu-özel sektör iş birliğinin arz ettiği önem İsrail örneği üzerinden ele alınmaktadır. Gelişen teknolojiyle birlikte günümüzde siber tehdit unsurlarının niceliği ve çeşitliliği artarken tehditlerin etkisi ve yıkıcılığı da ciddi boyutlara ulaşmaktadır. Siber saldırılar devletlerin siber uzayda faaliyet gösteren sağlık hizmetleri sistemlerinden bankacılık hizmetlerine, iletişim sistemlerinden enerji tesislerine kadar tüm altyapı sistemlerinin faaliyetlerinin felce uğramasına veya sistemlerin tamamen işlevsiz kalmasına neden olmaktadır. Bu bağlamda, siber saldırılar devletler için öncelikli ulusal güvenlik sorunları olurken daha kapsamlı ve

etkili siber güvenlik politikaları yürütülmesi için farklı siber aktörlerle iş birliği yapmaktadır.

Bu çalışmada günümüzde uzun dönemli siber güvenlik politikalarının geliştirilmesi ve uygulamasında kamu-özel sektör iş birliğinin arz ettiği önem kapsamlı ve detaylı bir şekilde İsrail örneği üzerinden ele alınmaktadır. Makalede 2021 yılında, Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın teknik destek sağladığı, 17 küresel medya kuruluşu tarafından ortaya çıkarılan İsrailli NSO şirketinin Pegasus casus yazılımını satın alan hükümetlerin neden olduğu hak ihlallerini içeren Pegasus Projesi vakası ele alınmaktadır (Uluslararası Af Örgütü, 2021, s.6). İsrail güvenlik şirketleri tarafından üretilen Pegasus gibi casus yazılımların ülkelere satılmasında onay yetkisine sahip İsrail Hükümeti, diplomatik ilişkiler geliştirmek ve siyasi kazanımlar elde etmek için insan hakları ihlalleri yapan otoriter rejimlere yazılımların satılmasına izin vermektedir. 2021 yılında 11 milyar dolar ile tarihindeki en yüksek siber ihracat rakamına ulaşan İsrail, küresel siber güvenlik yatırımlarının yaklaşık %40'ını çekerek 8,8 milyar dolar yatırıma sahip olmuş; dünyada en çok siber yatırım çeken ülke olmuştur (İsrail Ulusal Siber Müdürlüğü, 2022). Diğer yandan, siber güvenlik alanında kamu-özel sektör iş birliğinde küresel alanda en çok yatırım çeken endüstriye sahip olan İsrail'de siber ihracatta hükümetin özel sektör üzerinde tam kontrol gücüne sahip olması, iş birliğinin kötüye kullanılmasına neden olmaktadır.

Araştırma nitel bir çalışmadır. Nitel araştırma yöntemlerinden dokümantasyon incelemesi yapılmıştır. Makalenin amacı, siber güvenlik alanında kamu-özel sektör iş birliğinde İsrail Hükümeti'nin siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olmasıyla iş birliğinin kötüye kullanılmasını Pegasus Projesi üzerinden göstermektir. Bu amaç doğrultusundan makalede şu sorulara yanıt aranmıştır:

- Pegasus Projesi kapsamında İsrail Hükümeti'nin sorumluluğu nedir?
- İsrail Hükümeti'nin İsrailli siber ürünlerin ihracatındaki yetkisi nedir? Söz konusu yetkiyi hangi amaçlar için kullanmaktadır?

1. LİTERATÜR TARAMASI

2022 yılında yayınlanan "*Misenformasyon & Pegasus Projesi: Hindistan Örneği*" adlı tez, ana akım Hint medyasının Pegasus Projesi sızıntısına ve bunun Twitter'daki konuşmaları yönlendirmedeki etkisine nasıl tepki verdiğini analiz etmektedir (Khurana, 2022, s.8). Tez, Hint medyasının devlete yakın bölgelerdeki yanlış bilgilerin yayılmasındaki kalıpları ortaya çıkarmayı amaçlamaktadır (Khurana, 2022, s.8). Analiz edilen medya kuruluşlarının tamamı, değişen derecelerde de olsa, haberlerinde yanlış bilgilerin kurbanı olmuştur. Tezde, ulusal medya kuruluşlarının kamuoyunu yanlış bilgiye maruz bırakmada önemli bir rol oynadığı ve kendilerinin de yanlış bilgiye yatkın olduğu sonucuna varılmaktadır (Khurana, 2022, s.67). Çalışma, nüfusun önemli bir kısmının Pegasus casus yazılımlarıyla ilgili önemli yanlış bilgilerin farkında olduğunu ortaya koymaktadır. Ancak bu anlayış medya kuruluşlarının sosyal medya (Twitter) üzerinden eylem çağrısına dönüşmemiştir. Hint medya raporları ile sosyal medya arasındaki zayıf korelasyon, incelenen Hint medya kuruluşlarının izleyiciler tarafından yapılan haberlerine güven eksikliğini göstermektedir (Khurana, 2022, s.67-69).

2022 yılında Avrupa Konseyi için hazırlanan "*Pegasus Casus Yazılım ve İnsan Hakları Üzerindeki Etkileri*" adlı rapor, Pegasus casus yazılımlarının başta mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlükler üzerindeki etkisini analiz etmektedir (Kaldani ve Prokopets, 2022, s.5). Rapor, Pegasus casus yazılımlar gibi müdahaleci gözetim teknolojilerinin, yalnızca mahremiyet hakkı ve ifade özgürlüğü üzerinde değil, onur hakkı, toplanma özgürlüğü, din özgürlüğü ve hatta bireyin fiziksel ve psikolojik bütünlüğü de dahil olmak üzere diğer insan hakları ve temel özgürlükler üzerinde yarattığı veya potansiyel olarak yaratabileceği caydırıcı etkinin altını çizmektedir (Kaldani ve Prokopets, 2022, s.19-20). Raporda ayrıca yalnızca Pegasus'a değil aynı zamanda diğer kötü amaçlı saldırılara maruz kalma olasılığını en aza indirmek amacıyla daha iyi koruma için temel kurallar da sunulmaktadır (Kaldani ve Prokopets, 2022, s.15-20).

"*Pegasus Casus Yazılım: Vataşların Gizlilik Hakkının Destekleme*" adıyla 2023 yılından yayınlanan makalenin amacı, gözetim araçlarına ilişkin şeffaflığı ve hesap verebilirliği belirlemek ve Pegasus casus yazılımları aracılığıyla verilerin korunmasına ilişkin mahkemelerin gözlemlerini analiz

etmektir (Sneha, 2023, s.453). Birçok davada Hindistan mahkemesi, mahremiyet hakkının insan haklarının inkar edilemeyecek önemli yönlerinden biri olduğuna karar vermiştir. Elektronik delilleri sırasıyla birincil veya ikincil delil olarak göstermenin tek alternatifi, aslını, kopyasını veya 1872 tarihli Hindistan Delil Yasası'nın 65B Bölümü uyarınca bir sertifikayla bağlantılı muadilini ibraz etmektir. Elektronik kayıtların kabul edilebilirliği ve hukuk, ceza ve diğer hukuki prosedürlerde delil olarak kullanışlılığı, Yüksek Mahkeme tarafından birçok önemli kararla açıkça ortaya konmuştur. Elektronik cihazlar soruşturma için değeri Hindistan Kanıt Yasası kurallarına uyup uymadıklarına bağlıdır (Sneha, 2023, s.467)

2023 yılında "*Pegasus Casus Yazılımı: Gizlilik Hakkının İhlali ve Hindistan'da Gözetim Yasalarına Tehdit*" adıyla yayınlanan makalenin amacı, Pegasus casus yazılımlarının gizlilik hakkı üzerindeki çeşitli sorunlarını ve etkilerini özetlemek ve Hindistan Anayasası'nın özel hayatın gizliliğine ilişkin hükümlerini ve gözetim ile ilgili çeşitli yasaları incelemek ve analiz etmektir (D'Souza, 2023, s.425). Makalede, casus yazılımın bireylerin mahremiyetini ve güvenliğini etkili ve kesin bir şekilde tehlikeye attığı vurgulanmaktadır (D'Souza, 2023, s.436). Hindistan'daki 2000 Bilişim Yasası ve kuralları veri korumasına ilişkin hükümler içermesine rağmen yetersiz görünmektedir (D'Souza, 2023, s.436). Zayıf yasa ve mevzuatlar mahremiyet hakkını etkilemekte ve dolayısıyla kolay gözetime olanak tanımaktadır. Müdahale türleri, ele geçirilebilecek bilgilerin ayrıntı düzeyi ve hizmet sağlayıcıların işbirliği düzeyi, yasanın çiğnenmesini kolaylaştırmakta ve devletin izlemesini desteklemektedir (D'Souza, 2023, s.433).

2023 yılında yayınlanan "*Görünmez Casusun Düzenlenmesi – Pegasus Casus Yazılımına İlişkin Gözetim Teknolojisini İnceleyen Örnek Olay İncelemesi*" adlı tezde, Pegasus casus yazılımlarına ilişkin gözetim teknolojilerinin yarattığı zorluklara teknoloji düzenleyici kurumların ulusal anayasaları, bölgesel anlaşmaları, evrensel hak ve özgürlükleri dikkate alarak ne ölçüde yanıt verdiği ele alınmıştır (Dieterle, 2023, s.4). Çalışma düzenleyici kurumların Pegasus ve benzeri casus yazılımların kötüye kullanılmasına çözüm bulma ihtiyacını kabul ettiğini ve mevcut düzenleyici çerçevelerdeki boşlukları tespit ettiğini ortaya koymuştur (Dieterle, 2023, s.34). Sivil toplum üyelerinin çalışmaları nedeniyle gözetim düzenlemesine ilişkin sorunlar küresel gündeme taşınmış ve uluslararası, bölgesel, ulusal ve özel paydaşlar sorunlara yanıt vermeye zorlanmıştır. Bu da onların bir

kontrol mekanizması, başka bir deyişle bekçi köpeği rolünü üstlenmelerini sağlamıştır. Kamu ve özel sektör paydaşları sorunlara farklı şekillerde yanıt vermişlerdir. AB gibi bölgesel paydaşlar, düzenleyici çerçevelerdeki boşlukları doldurmaya çalışarak soruşturmalar yürütürken, BM gibi uluslararası paydaşlar, evrensel haklara uyum garanti altına alınıncaya kadar gözetim teknolojisinin satışı, transferi ve kullanımı konusunda küresel bir moratoryum ilan edilmesini tavsiye etmiştir. Her iki yanıt da gözetim teknolojisine ilişkin parçalı yasal çerçeveyi ve daha fazla insan hakları ihlalini önlemek için mevcut boşlukların doldurulması ihtiyacını vurgulamaktadır (Dieterle, 2023, s.34).

2024 yılında yayınlanan "*Pegasus Casus Yazılımlarının Kapsamlı Analizi ve Dijital Gizlilik ve Güvenlik Açısından Etkileri*" adlı makale, Pegasus casus yazılımını ve bunun dijital gizlilik ve güvenlik üzerindeki etkilerini kapsamlı bir şekilde analiz etmektedir. Çalışmanın amacı, yasal, etik ve politika konularını derinlemesine inceleyerek Pegasus ve benzeri casus yazılım araçlarının yarattığı zorluklara ilişkin bütünsel bir anlayış sunmaktır. Çalışma, tehditleri azaltmaya ve kullanıcıları istilacı gözetim tekniklerinden korumaya yönelik potansiyel çözümler sunmaktadır (Kareem, 2024, s.1360). Pegasus gibi gelişmiş casus yazılımların varlığı ve yaygınlaşması, dijital teknolojilere olan güvenin erozyona uğramasına, gözetlemenin normalleşmesine ve siber güvenlikteki açıkların açığa çıkmasına neden olmuştur (Kareem, 2024, s.1366-1367). Bu zorluklar, yenilikçi çözümler geliştirmek, yasal ve düzenleyici çerçeveleri güçlendirmek ve dijital çağda sorumlu davranışı teşvik etmek için hükümetlerin, endüstrinin, akademi ve sivil toplumun ortak çabalarını gerektirmektedir (Kareem, 2024, s.1370). Pegasus ve benzeri casus yazılımların oluşturduğu tehditleri azaltmak için önerilen çözümler arasında şifreleme ve güvenli iletişim teknolojilerinin güçlendirilmesi, kamuoyunun farkındalığının artırılması ve dijital okuryazarlığın teşvik edilmesi, mahremiyet artırıcı teknolojilerin geliştirilmesi, yasal ve düzenleyici çerçevelerin revize edilmesi ve ortak norm ve kuralların geliştirilmesi için uluslararası iş birliğinin teşvik edilmesi yer almaktadır (Kareem, 2024, s.1371).

2. NSO ŞİRKETİ

NSO şirketi, 2010 yılında İsrailli üç girişimci Niv Carmi, Shalev Hulio ve Omri Lavie tarafından Tel Aviv yakınlarındaki Herzliya şehrinde kurulmuştur. Şirket adını kurucuları Niv, Shalev ve Omri'nin baş harflerinden almaktadır (Bergman ve Mazzetti, 2022). Daha önce, IDF bünyesindeki Askeri İstihbarat Müdürlüğü (AMAN)'ne bağlı siber istihbarat birimi Birim 8200'de çalışan çocukluk arkadaşları Shalev Hulio ve Omrie Lavie, 2007 yılında ilk ortak girişimlerini gerçekleştirmişlerdir. İzleyicilerin ekranda görünen ürünleri bulmasına ve satın almasına yardımcı olan ilk girişimleri olan video pazarlama şirketi MediAnd şirketini kurmuşlardır. Hulio ve Lavie'nin ilk ortak girişimi MediAnd, Eddie Shalev'in kurucusu olduğu İsrailli Genesis Partners adlı risk sermayesi şirketi tarafından fonlanmıştır (Yablonko, 2019).

2008 yılında ise Hulio ve Lavie, ikinci girişimleri olan müşterilerinin mobil telefonlarına uzaktan erişim sağlayarak teknik destek sunan mobil müşteri hizmetleri şirketi CommuniTake şirketini kurmuşlardır. CommuniTake şirketi müşterilerine mobil cihazlar için uzaktan destek sağlayarak mobil servis noktalarını ziyaret etme ihtiyacını ortadan kaldıran bir hizmet sunmuştur. İkili, diğer ortaklarla yaşanan anlaşmazlıklar nedeniyle şirketten ayrılmışlardır (Fischer ve Levy, 2016).

CommuniTech'in mobil cihazları uzaktan kontrol yeteneği, Lavie ve Hulio için mobil cihazları izinsiz olarak uzaktan kontrol edebilecekleri bir yazılım geliştirme fikrini ortaya çıkarmıştır. CommuniTake şirketinin ardından 2010 yılında Hulio ve Lavie ikilisi, Birim 8200'de ve İsrail Dış İstihbarat Servisi MOSSAD'da görev yapmış Niv Karmi ile birlikte üçüncü girişimleri olan NSO şirketini kurmuşlardır (Bergman ve Mazzetti, 2022). NSO şirketinin 1,5 milyon dolarlık ilk finansman desteği MediAnd şirketinde olduğu gibi Genesis Partners şirketi tarafından sağlanmıştır (Lipson, 2017). Kurucu ortaklardan Niv Carmi'nin şirketin kuruluşundan kısa bir süre sonra şirketten ayrıldığı medyada yer almıştır (Shahaf, 2018).

NSO şirketinin kurulmasından bir yıl sonra 2011 yılında NSO mühendisleri, ilk casus yazılımlarının ilk versiyonunun kodlamasını tamamlamıştır (Bergman ve Mazzetti, 2022). NSO kurucuları, casus yazılımlarına Pegasus[2] adını vermiştir. Pegasus, Apple ve Android mobil

[2] Pegasus, Yunan mitolojisinde dişi canavar Medusa'nın kanından doğduğuna ve kutsal yerleri koruduğuna inanılan kanatlı bir attır. Bkz. Theoi Project. (2023). *Pegasos*. https://www.theoi.com/Ther/HipposPegasos.html

işletim sistemlerindeki sıfır gün kusurlarından yararlanarak hedef cihazlara bulaşan bir yazılımdır (Bergman ve Mazzetti, 2022). Bu casus yazılım kullanıcının herhangi bir etkileşimini gerektirmeden, herhangi bir dosya ya da mobil uygulama indirmesine gerek duymadan telefona yüklenebilmektedir. Hedeflenen kişinin telefonuna, tabletine veya bilgisayarına yüklenebilmesi için kişiyi, güvenliği ihlal edilmiş bir bağlantıya veya dosyaya tıklamaya ikna etmeye dayanan geleneksel casus yazılımların aksine sıfır tıklama saldırısında casus yazılım, herhangi bir bağlantıya tıklanmadan cihazlara yüklenebilmektedir (Kaspersky, 2023). Yazılım yüklendiği telefonlardaki tüm bilgilere ulaşılabilmekte, telefon dinlenmesi yapabilmektedir. Sıfır tıklama saldırısı, mobil cihazlardaki boşluklardan yararlanarak hedeflenen sisteme girmek için veri doğrulama boşluğunu kullanmaktadır. Saldırının işleyişi, hedeflenen sistemlere gönderilen verilerin, sistem henüz verilerin güvenilir olup olmadığını kontrol edemeden harekete geçmesini sağlamaktır.[3]

Sıfır tıklamayla bulaşmada casus yazılım, hedef cihaza tam erişim sağlayabilmekte ve kullanıcı kötü amaçlı bir bağlantıya tıklamadan tüm verileri indirebilmektedir. Sıfır tıklamada sadece telefon numarasına sahip olunarak hangi cep telefonu şirketinin kullanıldığına bakılmaksızın mobil cihazlardaki tüm belgelere erişilmesine, cihazların gizlice dinlenmesine, telefon görüşmelerinin kaydedilmesine, hedefin bulunduğu yerin takip edilmesine ve tüm çağrıların, mesajların, e-postaların ve sosyal ağlardaki hareketlerin görüntülenmesine olanak sağlamaktadır (Shezaf ve Jacobson, 2018). Bu durum, mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlaline neden olmaktadır (Kaldani ve Prokopets, 2022, s.19-20).

Şirket kısa bir süre içerisinde genişleyerek farklı ülkelerde ofisler açmış; Herzliya'da bulunan genel merkezinde ve ofislerinde 700'den fazla kişiyi istihdam etmiştir. NSO şirketinde istihdam edilen araştırma üyelerinin ve personellerin büyük çoğunluğu, başta Birim 8200 olmak üzere AMAN'ın elit birimlerinde görev almış kişilerden seçilmiştir (Bergman ve Mazzetti, 2022).

[3] Detaylı bilgi için bkz. BilgiGüvende. (2020, 13 Mayıs). *Siber Güvenlik Dünyasında Bir Başka Gizli Tehdit: Zero-Click Saldırısı.* Erişim Tarihi: 29 Ağustos 2023, https://bilgiguvende.com/siber-guvenlik-dunyasinda-bir-baska-gizli-tehdit-zero-click-saldirisi/

NSO resmi web sitesinde telekomünikasyon ve istihbarat uzmanları tarafından üretilen Pegasus yazılımı, terörizm, uyuşturucu kaçakçılığı ve diğer büyük suçlarla mücadele aracı olarak tanıtılmıştır. Yazılımın, devlet kurumlarına, istihbarat teşkilatlarına ve kolluk kuvvetlerine terör saldırılarını önlemede ve suç şebekelerini dağıtmada şifrelemenin zorluklarını ortadan kaldırmak için satılan bir araç olduğu belirtilmiştir. Terörizmin ve diğer büyük suçların önlenmesinin yanı sıra yazılımın kayıp kişilerin bulunmasına ve arama kurtarma faaliyetlerine yardımcı olduğu vurgulanmıştır (NSO Grup, 2023).

NSO teknoloji şirketinin Pegasus yazılımını ilk sattığı ülke Meksika olmuştur. 2012 yılında Meksika hükümeti NSO ile Pegasus yazılımının satışı için 20 milyon dolarlık bir sözleşme imzaladığını bildirmiştir (Hirschauge ve Orpaz, 2014). NSO yetkilileri, El Chapo lakabıyla tanınan Meksikalı uyuşturucu baronu Joaquín Archivaldo Guzmán Loera'nın 2016 yılında yakalanmasında Pegasus casus yazılımının kullanıldığını ifade etmiştir (Yaron, 2020; Bergman, 2019). Aynı yıl NSO'nun, Pegasus yazılımını Panama Hükümeti'ne sattığı medyada yer almıştır (News Room Panama, 2021).

NSO şirketinin tek ürünü olan Pegasus casus yazılımının birçok yabancı hükümet tarafından ilgi gördüğü ve bundan dolayı NSO şirketinin yazılım için hükümetlerden yüksek fiyatlar talep ettiği medyada yer almıştır (Dogani, 2016). Amerika Birleşik Devletleri (ABD) merkezli New York Times gazetesinin NSO şirketinin satış sözleşmelerine dayandırdığı haberinde NSO şirketinin geleneksel yazılım şirketlerine benzer olarak gözetim araçlarını hedef sayısına göre fiyatlandırdığı ve fiyatların 500 bin dolarlık sabit bir kurulum ücretinden başladığı yer almıştır. Haberde, sabit kurulum ücretine ek olarak, NSO'nun, 10 iPhone kullanıcısını gözetlemek için devlet kurumlarından 650 bin dolar, 10 Android kullanıcısı için 650 bin dolar, 5 BlackBerry kullanıcısı için 500 bin dolar ve 5 Symbian kullanıcısı için 300 bin dolar talep ettiği belirtilmiştir. Haberde, NSO şirketinin, 100 ekstra hedef için 800 bin dolar, 50 ekstra hedef için 500 bin dolar, 20 ekstra hedef için 250 bin dolar ve 10 ekstra hedef için 150 bin dolar talep ettiği ifade edilmiştir. Ayrıca, şirketin her yıl toplam satış ücretinin yüzde 17'si kadar yıllık sistem bakım ücreti talep ettiği de haberde yer almıştır (Perltroth, 2016).

2014 yılında Hulio ve Lavie, NSO şirketinin %70 hissesini, 120 ile 130 milyon dolar arasında bir ücrete 1999 yılında kurulan Kaliforniya merkezli bir özel sermaye şirketi olan Francisco Partners şirketine satmıştır (Yablonko, 2019). Francisco Partners, NSO şirketinden önce de Kudüs merkezli Ex Libris ve Tel Aviv merkezli Dmatek teknoloji şirketlerini satın almıştır (Shezaf ve Jacobson, 2018). NSO şirketinin satın alınmasından bir yıl sonra Francisco Partners şirketinin, NSO'dan 75 milyon dolar kar elde ettiği medyada yer almıştır (Stone ve Roumeliotis, 2015).

Francisco Partners şirketi, 2017 yılında NSO'nun hisselerini resmi olarak 1 milyar dolardan fazla bir bedelle satışa çıkarmıştır (O'neill, 2017). 14 Şubat 2019'da ise Francisco Partners, NSO şirketinin sahip olduğu hisselerini tekrardan NSO'nun kurucu ortakları Hulio ve Lavie'ye satmıştır. NSO şirketinin hisselerinin 1 milyar dolara yakın bir paraya satıldığı medyada yer almıştır. NSO şirketi tarafından yapılan açıklamada Hulio ve Lavie'nin NSO şirketini Londra merkezli özel sermaye şirketi Novalpina Capital ile ortak satın aldığı, eski kurucuların ve Novalpina Capital şirketinin ayrı ayrı olarak %50'şer hisseye sahip olduğu belirtilmiştir (Solomon, 2019).

Günümüzde, sıfır tıklama teknolojili Pegasus casus yazılımı dünyadaki en gelişmiş casus yazılım araçlarından biri olarak görülmektedir (Mazzetti, Bergman ve Stevis-Gridneff, 2022). Küresel yazılım endüstrisinde adını duyuran Pegasus gibi casus yazılımları üreten İsrail siber casusluk endüstrisi, gözetleme araçları ve iletişim dinleme alanında küresel ticaretin öncüleri arasında yer almıştır. 2021 yılında 11 milyar dolar ile tarihindeki en yüksek siber ihracat rakamına ulaşan İsrail, küresel siber güvenlik yatırımlarının yaklaşık %40'ını çekerek 8,8 milyar dolar yatırıma sahip olmuş; dünyada en çok siber yatırım çeken ülke olmuştur (İsrail Ulusal Siber Müdürlüğü, 2022). Günümüzde değeri 1 milyar doların üzerinde olan NSO şirketi, faaliyetlerini halen kurucu üyeleri Hulio ve Lavie başkanlığında yürütmektedir (Brewster, 2021).

3. PEGASUS PROJESİ

18 Temmuz 2021'de, Paris merkezli Fransız kâr amacı gütmeyen medya kuruluşu olan Forbidden Stories, Uluslararası Af Örgütü'nün teknik desteğiyle NSO şirketine ait Pegasus casus yazılımının satın alan müşteriler tarafından kötüye kullandığını ortaya çıkaran bir soruşturma başlatmıştır (Forbidden Stories, 2021). Uluslararası Af Örgütü'nün Güvenlik

Laboratuvarı tarafından elde edilen veriler, Forbidden Stories medya kuruluşu tarafından 10 ülkeden 16 küresel medya kuruluşuyla paylaşılmıştır. Soruşturmanın analizleri 17 medya kuruluşunun ortak çalışmasıyla tamamlanmış; soruşturma Pegasus Projesi adını almıştır (Uluslararası Af Örgütü, 2021b, s.6). Forbidden Stories tarafından verilerin paylaşıldığı medya kuruluşları arasında ABD merkezli Organize Suç ve Yolsuzluk Raporlama Merkezi (OCCRP), Washington Post ve PBS Frontline, İngiliz gazetesi Guardian, Fransız Le Monde ve Radio France, İsrail gazetesi Haaretz, Alman Süddeutsche Zeitung ve Die Zeit, Meksika merkezli Proceso ve Aristegui Noticias, Belçika merkezli Le Soir ve Knack, Hindistan merkezli Wire, Macaristan merkezli Direkt36 ve Suriye merkezli Daraj yer almaktadır (Forbidden Stories, 2021). 17 medya kuruluşundan 80'den fazla gazeteci telefon numaralarından oluşan bu kayıtları analiz ve rapor etmiştir (Richard, 2021).

Uluslararası Af Örgütü'nün Güvenlik Laboratuvarı, listede kayıtlı telefon numaralarının kullanıldığı telefonlara yönelik adli analizler gerçekleştirmiştir. Güvenlik Laboratuvarı listede kayıtlı telefon numaralarının kullanıldığı 67 iphone telefona ulaşarak telefonları analiz etmiştir. Adli analizler sonucunda listede kayıtlı 67 telefon numarasının 37'sinde Pegasus casus yazılımına ait izler olduğu tespit edilmiştir. Yazılımın saldırılarına maruz kalan telefon numaraları Azerbaycan, Fransa, Macaristan, Hindistan ve Meksika ülkelerine ait olduğu belirlenmiştir (Pfenniger, 2023). Ayrıca, Pegasus casus yazılımının izlerinin tespit edildiği 37 telefon numarasından bazılarına çok yakın tarihlerde, Apple'ın iOS mobil işletim sistemindeki güvenlik açıklarından yararlanılarak Pegasus yazılımının bulaştığı rapor edilmiştir (Schwartz, 2021). İncelenen 67 telefonun yarısından fazlasında Pegasus casus yazılımına ait izlerin olduğunun doğrulanması, Uluslararası Af Örgütü ve Forbidden Stories tarafından ortaya çıkarılan NSO şirketine ait 50.000'den fazla telefon numarasının bulunduğu listenin Pegasus casus yazılımı için bir hedef listesi olduğu düşüncesini desteklemektedir (Pfenniger, 2023).

Forbidden Stories ve Uluslararası Af Örgütü, Kanada'daki Toronto Üniversitesi bünyesindeki Munk Küresel İlişkiler ve Kamu Siyaseti Okulu'nda disiplinlerarası bir laboratuvar olarak faaliyet gösteren Vatandaş Laboratuvarı (Citizen Lab)'ndan Uluslararası Af Örgütü Güvenlik Laboratuvarı tarafından incelenen telefon numarası örneklerinin ve ortaya çıkarılan adli metodolojinin bağımsız bir şekilde incelenmesini talep etmiştir

(Marczak, Scott-Railton, Anstis ve Deibert, 2021). Vatandaş Laboratuvarı yaptığı adli incelemeler sonucunda, Uluslararası Af Örgütü'nün adli tıp metodolojisinin, Pegasus saldırılarını doğru şekilde tespit ettiğini doğrulamıştır (Marczak, Scott-Railton, Anstis ve Deibert, 2021). Bu bağlamda, iki farklı bağımsız kuruluşunun da incelenen telefon numaralarında Pegasus yazılımına ait izlere ulaşması, erişilen NSO'ya ait listenin casus yazılım için bir hedef listesi olduğu tezinin güvenirliliğini artırdığı değerlendirilmektedir (Pfenniger, 2023).

3.1. Pegasus Projesi Kapsamında Hedef Profilleri

Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın teknik desteğiyle, 17 medya kuruluşunun Pegasus yazılımı için potansiyel hedef olduğu düşünülen telefon numaralarına yönelik inceleme ve analizlerinin sonuçları, 18 Temmuz 2021'de kamuoyuyla paylaşılmıştır (Kirchgaessner vd., 2021). Soruşturma sonucunda, 2016 yılından beri Pegasus yazılımını satın alan müşteriler tarafından potansiyel hedef olarak seçildiği düşünülen telefon numaralarının kayıtlarının olduğu listede 50'den fazla ülkeden devlet başkanları, politikacılar, diplomatlar, insan hakları savunucuları, akademisyenler, iş adamları, avukatlar, doktorlar, sendika liderleri ve gazetecilerin numaralarının olduğu belirlenmiştir (Richard, 2021). 17 medya kuruluşunun ortak soruşturmasında, NSO'ya ait listeye telefon numaraları giren ve NSO'nun müşterisi olduğu düşünülen 11 hükümet tespit edilmiştir. Listeye telefon numaraları giren hükümetler arasında Meksika, Suudi Arabistan, Birleşik Arap Emirlikleri (BAE), Hindistan, Macaristan, Azerbaycan, Bahreyn, Kazakistan, Fas, Ruanda ve Togo hükümetleri yer almaktadır (Uluslararası Af Örgütü, 2021a).

Medya kuruluşlarının incelemesine göre, 15.000'den fazla telefon numarasıyla listeye en çok telefon numarası giren ülke, farklı devlet kurumlarının Pegasus yazılımını kullandığı bilinen Meksika olmuştur. Meksika'nın ardından NSO'ya ait listeye 10.000'den fazla numara giren ülkeler BAE ve Fas gelmektedir. NSO müşterileri tarafından Avrupa Birliği (AB) ülkelerine ait 1.000'den fazla telefon numarası listeye eklenmiştir (Kirchgaessner vd., 2021). Medya kuruluşlarının incelemesine göre, 34 ülkeden 600'den fazla hükümet yetkilisi ve politikacının potansiyel hedef olarak seçildiği tespit edilmiştir (Uluslararası Af Örgütü Birleşik Krallık, 2021). Kayıtlı listede aralarında Fransa Cumhurbaşkanı Emmanuel Macron, Güney Afrika Devlet Başkanı Cryil Ramaphosa, Fas kralı 6. Muhammed el-

Sadis bin el-Hasan, Mısır Başbakanı Mustafa Kemal Madbuli, Irak eski Cumhurbaşkanı Berham Ahmed Salih, eski Belçika Başbakanı Charles Michel, eski Fransa Başbakanı Edouard Philippe, eski Lübnan Başbakanı Saad Hariri, eski Kazakistan Başbakanı Bakıtcan Abdirulı Sağıntayev, eski Fas Başbakanı Saadeddin Osmani, eski Uganda Başbakanı Ruhakana Rugunda, eski Pakistan Başbakanı İmran Khan, eski Cezayir Başbakanı Nureddin Bedevi ve Yemen Başbakanı Ahmed bin Dağr'ın olduğu 14 ülke liderinin telefon numaralarının yer aldığı tespit edilmiştir (Timberg, Birnbaum, Harwell ve Sabbagh, 2021).

Erişim sağlanan listede Fransa, Hindistan, Meksika, Macaristan ve Fas'ın aralarında bulunduğu 20 ülkeden yaklaşık 200 gazetecinin telefon numarası kaydının olduğu tespit edilmiştir (Richard, 2021). Listede, Financial Times, CNN, New York Times, France 24, Economist ve Associated Press ve Reuters gibi küresel medya kuruluşlarından yöneticilerin, muhabirlerin ve editörlerin telefon numaralarının yer aldığı tespit edilmiştir (Kirchgaessner vd., 2021). Soruşturmada, Suudi gazeteci Cemal Kaşıkçı'nın aile üyelerinin 2 Ekim 2018'de İstanbul'da yaşanan Kaşıkçı cinayeti[4] öncesinde ve sonrasında Pegasus yazılımıyla hedef alındığına dair kanıtlar ortaya çıkmıştır. İncelemeye göre, Cemal Kaşıkçı'nın aile üyelerinin numaraları cinayetin öncesi ve sonrasında Suudi Arabistan tarafından listeye eklenmiştir (Uluslararası Af Örgütü, 2021a). Cemal Kaşıkçı cinayetinden 6 ay sonra Mart 2019'da ABD merkezli CBS televizyon kanalında yayınlanan 60 dakika programına katılan NSO şirketinin kurucusu Shalev Hulio, cinayetle ilgilerinin olduğu, gazeteciyi ve ailesini hedef almak için Pegasus casus yazılımının kullanıldığına dair iddiaları reddetmiştir (CBS News, 2019). NSO şirketinin cinayetle ilgililerinin olduğuna dair iddiaları daha öncesinde reddetmesine karşın

[4] Washington Post gazetesi yazarı Suudi Arabistan vatandaşı Cemal Kaşıkçı 2 Ekim 2018'de, Suudi Arabistan'ın İstanbul'daki Başkonsolosluğu'na Türk nişanlısı Hatice Cengiz ile evlenmek için gereken belgeleri almak için geldiği sırada Suudi bir tim tarafından öldürülmüştür. Gazeteci Kaşıkçı ölmeden önce Washington Post gazetesinde Suudi yönetimini ve Suudi Veliaht Prens Muhammed bin Salman el-Suud'un politikalarını eleştiren yazılar yazmıştır. Suudi Arabistan Dışişleri Bakanlığı tarafından 19 Ekim'de yapılan açıklamada, savcılar tarafından yürütülen ön soruşturmaya göre Kaşıkçı'nın Başkonsoloslukta karıştığı kavga sonucunda öldüğü bilgisine yer verilmiştir. Ocak 2019'da Kaşıkçı cinayetiyle ilgili olarak Suudi Arabistan Riyad Ceza Mahkemesi'nde adı açıklanmayan 11 kişi yargılanmıştır. Aralık 2019'da mahkeme beş kişiyi cinayeti işledikleri gerekçesiyle idam cezasına çarptırmış; üç kişiye suçu örtbas etmekten 24 yıl hapis cezası vermiştir. Diğer üç kişi suçsuz bulunmuştur. Bkz. BBC. (2021, 24 Şubat). *Jamal Khashoggi: All You Need To Know About Saudi Journalist's Death*. Erişim Tarihi: 8 Eylül 2023, https://www.bbc.com/news/world-europe-45812399

Uluslararası Af Örgütü Güvenlik Laboratuvarı, Suudi Arabistan ve BAE'de yaşayan Kaşıkçı'nın oğlu Abdullah Kaşıkçı, Kaşıkçı'nın eski eşi Hanan Elatr ve diğer aile üyelerinin mobil cihazlarının Eylül 2017 ile Nisan 2018 arasında defalarca casus yazılımın saldırısına uğradığını tespit etmiştir. Güvenlik Laboratuvarı'nın adli analizinde, Pegasus casus yazılımının, Kaşıkçı'nın nişanlısı Hatice Cengiz'in telefonuna cinayetten dört gün sonra yüklendiği kanıtlanmıştır (Uluslararası Af Örgütü, 2021a). Adli tıp sonuçlarına göre, Kaşıkçı cinayetinden sonra, Cemal Kaşıkçı'nın yakın arkadaşı El Cezire kanalının eski yöneticisi Vaddah Hanfar'ın telefonu da Pegasus yazılımının saldırısına uğramıştır (Priest, Mekhennet ve Bouvart, 2021).

Meksika'da ise gazeteci Cecilio Pineda'nın telefonunun, 2017 yılında öldürülmesinden sadece birkaç hafta önce listeye eklendiği belirlenmiştir. Gazeteci Pineda kendi sosyal medya hesabında düzenli olarak Meksika'nın organize suç gruplarının savaş alanı olan Tierra Caliente bölgesindeki yerel yetkililer ile uyuşturucu kaçakçıları arasında bağlantı olduğunu iddia eden yayınlar yapmıştır. 2 Mart 2017'de gazeteci Pineda, Tierra Caliente bölgesindeki Ciudad Altamirano kasabasında vurularak öldürülmüştür. Soruşturmada, Pineda'nın ölüm tehditleri aldığı sıralarda telefon numarasının NSO'nun kayıt listesine Meksikalı bir müşteri tarafından eklendiği tespit edilmiştir (Lakhani, 2021). Soruşturmaya göre, 2016 ile 2017 yılları arasında en az 26 Meksikalı gazetecinin telefon numaraları potansiyel hedef olarak listeye eklenmiştir (Uluslararası Af Örgütü, 2021a).

Soruşturmaya göre, Hindistan'da 2017 ile 2021 yılları arasında büyük medya kuruluşlarından 40'tan fazla gazeteci hedef olarak listeye eklenmiştir (Uluslararası Af Örgütü, 2021b). Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın adli tıp testleriyle Hindistan'ın bağımsız medya kuruluşu The Wire'ın kurucusu Siddharth Varadarajan'ın telefonuna Nisan 2018'de Pegasus casus yazılımın bulaştığı kanıtlanmıştır (Forbidden Stories, 2021a). Güvenlik Laboratuvarı, medya kuruluşu The Wire gazetesinin diğer kurucu ortağı MK Venu'nun telefonuna ise Haziran 2021'de Pegasus casus yazılımı bulaştığını ortaya çıkarmıştır (Forbidden Stoeies, 2021b). Pegasus casus yazılımıyla yaklaşık 200 gazetecinin hedef seçilmesi, basın özgürlüğü ve gazetecilerin ifade özgürlüğünün ihlal edilmesine neden olmaktadır (Kaldani ve Prokopets, 2022, s.5).

NSO'ya ait telefon numaralarının olduğu kayıt listesinde insan hakları savunucularının ve avukatların telefon numaraları da yer almaktadır. Soruşturmada, Suudi kadın hakları savunucusu Luceyn el-Hezlul'un telefon numarasının 2018 yılında BAE'den Suudi Arabistan'a zorla geri gönderilmesinden birkaç hafta önce hedef olarak listeye eklendiği tespit edilmiştir. El-Hezlul, Suudi Arabistan yönetiminin kadınlara yönelik yasaklarının eleştiren kampanyalar yürütmüştür (Walker, Kirchgaessner, Lakhani ve Safi, 2021). Soruşturmada, birçok insan hakları davasında yer alan İngiliz avukat Rodney Dixon'un telefon numarasının da 2019 yılında hedef olarak seçildiği tespit edilmiştir. Güvenlik Laboratuvarı'nın adli tıp analizleriyle, Dixon'un telefonunun Pegasus yazılımı tarafından hedef alındığı ortaya çıkarılmıştır. İngiliz avukat Dixon'ın müvekkilleri arasında öldürülen Suudi gazeteci Cemal Kaşıkçı'nın nişanlısı Hatice Cengiz de yer almaktadır (Sabbagh, Pegg, Lewis ve Kirchgaessener, 2012). İnsan hakları davaları yürüten Fransız avukat Joseph Breham'ın telefon numarasının da Fas tarafından 2019 yılında listeye kaydedildiği tespit edilmiştir. Adli tıp analizleri sonucunda Breham'ın telefonunun casus yazılım tarafından saldırıya uğradığı ortaya çıkarılmıştır (Benjakob, 2022).

NSO'nun kullanım amaçlarını açıkladığı üzere Pegasus yazılımının terörizm, uyuşturucu kaçakçılığı ve diğer büyük suçlarla mücadelede devletlerin istihbarat teşkilatlarına ve kolluk kuvvetlerine yardımcı olmaktır (NSO Grup, 2023). Yazılımın satın alan hükümetler tarafından muhalif grupları takip etmek, yerlerini tespit etmek, faaliyetlerini gözetlemek ve üzerlerinde baskı kurmak amacıyla kullanılması, yazılımın üretim amaçlarından uzaklaştırarak yazılımı hükümetler için rakiplerine veya muhalif gruplara karşı kullandıkları bir baskı aracına dönüştürmüş; başta mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlal edilmesine neden olmuştur.

3.2. Pegasus Projesi Sonrası Yaşananlar

18 Temmuz 2021'de Pegasus Projesi soruşturmasının sonuçlarının yayınlamasının ardından NSO şirketi, avukatları aracılığıyla soruşturmayla ile ilgili kamuoyuna yaptığı açıklamada Pegasus Projesi kapsamında öne sürülen tüm iddiaları kesin olarak reddettiklerini, iddiaların Pegasus veya diğer NSO ürünlerini kullanan müşterilerin hedef listesiyle hiçbir ilgisi olmayan, HLR arama hizmetleri gibi, erişilebilir ve açık temel bilgilerden sızdırılan verilerin yanıltıcı bir şekilde yorumlanmasına dayandığını ifade

etmiştir (Guardian, 2021). Açıklamada, sözleşme koşulları ve ulusal güvenlik hususları nedeniyle NSO şirketinin, hükümet müşterilerinin isimlerini açıklamayacağı ifade edilmiştir (Kirchgaessner vd., 2021). Açıklamada, Meksika'daki bir NSO müşterisinin 2017 yılında öldürülmeden önce Meksikalı gazeteci Cecilio Pineda'yı hedeflediği haberinin doğru olsa bile NSO müşterisinin veya NSO yazılımı tarafından toplanan verilerin gazetecinin öldürülmesiyle bağlantısı olduğu anlamına gelmeyeceği ifade edilmiştir. Ayrıca, yazılımın ABD'de siber gözetim gerçekleştirmek için kullanılamayacağı ve hiçbir yabancı müşterinin ABD numaralarına sahip telefonlara erişemeyecekleri ifade edilmiştir. Şirketin, tüm kötüye kullanım iddialarını araştıracağı ve araştırmaların sonuçlarına göre, 2021 Haziran'da şirketin yayınladığı Şeffaflık ve Sorumluluk Raporu'nda belirtildiği gibi kötüye kullanım durumlarında müşterilerin sistemlerini kapatmak gibi uygun önlemleri alınacağı vurgulanmıştır (Guardian, 2021). Haziran 2021'de yayınlanan şirketin ilk Şeffaflık ve Sorumluluk Raporu'nda, insan hakları inceleme süreçlerinin bir sonucu olarak 300 milyon dolarının üzerinde satış fırsatının NSO tarafından reddedildiği; Pegasus casus yazılımının insan hakları endişeleri nedeniyle bazı ülkelere satışına izin verilmediği ifade edilmiştir (NSO Grup, 2021, s.4)

19 Temmuz 2021'de, Uluslararası Af Örgütü'nün, NSO şirketinin gözetleme faaliyetleri için ABD merkezli bulut bilişim platformu Amazon Web Services'in altyapısını kullandığını açıklamasının ardından Amazon Web Services şirketi, NSO şirketine bağlı bulut hesaplarını devre dışı bıraktığını açıklamıştır (Fung, 2021). 21 Temmuz'da Fransa Cumhurbaşkanı Macron, kendisinin, eski Fransa Başbakanı Édouard Philippe'in ve 14 Fransız Bakan'ın telefon numaralarının listede hedef olarak yer aldığının ortaya çıkmasının ardından casus yazılımla ilgili soruşturma talimatı vermiştir. Güvenlik Laboratuvarı'nın adli analiziyle eski Fransa Çevre Bakanı François de Rugby'in telefonunda casus yazılıma ait izlerin olduğu kanıtlanmıştır (Chrisafis, 2021).

24 Temmuz'da ABD merkezli anlık mesajlaşma uygulaması WhatsApp Messenger'ın Genel Müdürü Will Cathcart yaptığı açıklamada, 2019 yılında 1400 WhatsApp kullanıcısına yönelik düzenlenen saldırıların Pegasus casus yazılımıyla gerçekleştiğini ve 2019 yılındaki WhatsApp kullanıcılarına yönelik saldırı ile Pegasus Projesi kapsamında ortaya çıkarılan verilerin örtüştüğünü ifade etmiştir (Kirchgaessner, 2021). 2019 yılının Nisan ile Mayıs ayları arasında 20 farklı ülkeden aralarında üst düzey

hükümet yetkililerinin, politikacıların, gazetecilerin ve insan hakları savunucularının olduğu 1.400 WhatsApp kullanıcısının telefonlarına saldırı gerçekleşmiştir. 29 Ekim 2019'da WhatsApp şirketi, NSO şirketine WhatsApp mesajlaşma uygulamasındaki bir hatadan yararlanarak 1.400 kişinin gözetlenmesine neden olan casus yazılımı yüklemekle suçlayan bir dava açmıştır (Hopkins ve Kirchgaessner, 2019). Mahkeme belgelerinde NSO, müşterilerinin devlet müşterileri olması nedeniyle kendisine devlet dokunulmazlığı verilmesi gerektiğini savunduğu medyada yer almıştır. 9 Ocak 2023'te, ABD Yüksek Mahkemesi, NSO şirketinin daha önceki itirazını reddederek WhatsApp'ın NSO şirketine yönelik dava açmasına izin vermiştir (Reuters, 2023).

29 Ekim 2021'de İrlanda merkezli sivil toplum kuruluşu Front Line Defenders, Filistin merkezli insan hakları örgütü Al Haq kuruluşunun 6 Filistinli çalışanının telefonlarında Pegasus casus yazılımına ait izler tespit etmiştir (Front Line Defenders, 2021). Front Line Defenders kuruluşunun 6 Filistinlinin telefonlarına yönelik adli analizi, Vatandaş Laboratuvarı ve Uluslararası Af Örgütü'nün Güvenlik Laboratuvarı'nın adli analizleriyle doğrulanmıştır (Citizen Lab, 2021; Uluslararası Af Örgütü, 2021c).

3 Kasım 2021'de ABD'de Joe Biden yönetimi, NSO şirketinin ABD'nin dış politikasına ve ulusal güvenlik çıkarlarına aykırı davrandığını belirlediği NSO şirketini ve bir başka İsrail gözetim şirketi olan Candiru şirketini ABD'nin varlık listesine eklemiştir. Federal bir kara liste olan varlık listesinde yer alan şirketlerin, Amerikan şirketleriyle ticareti yasaklanmaktadır (Harwell, Nakashima ve Timberg, 2021a). ABD Ticaret Bakanlığı yaptığı açıklamada, NSO Grup ve Candiru şirketinin casus yazılımlarının, yabancı hükümetlerin ulus ötesi baskı yürütmesine ve otoriter rejimlerin muhalefeti susturmak için kendi egemenlik sınırları dışındaki muhalif politikacıları, gazetecileri ve aktivistleri hedef almasına neden olduğu; şirketlerin kara listeye alınmasının baskı için kullanılan dijital araçların yayılmasını durdurmak da dâhil olmak üzere insan haklarını, ABD dış politikasının merkezine koyma çabalarının bir parçası olduğu belirtilmiştir (Harwell, Nakashima ve Timberg, 2021a).

Candiru şirketi 2014 yılında Birim 8200 mezunu ve eski NSO çalışanları olan Eran Shorer ve Yaakov Weizman tarafından Tel Aviv'de kurulmuştur. Candiru şirketi kurulduktan kısa bir süre sonra NSO şirketinin eski yönetim kurulu üyesi Isaac Zack şirketin en büyük yatırımcısı olmuştur

(Megiddo, 2021). Temmuz 2021'de Toronto Üniversitesi bünyesindeki Vatandaş Laboratuvarı ve Microsoft Tehdit İstihbarat Merkezi'nin adli analizleri sonucunda, 10 ülkeden 100'den fazla politikacı, gazeteci ve aktivistin Candiru tarafından üretilen casus yazılımların hedefi olduğu ortaya çıkarılmıştır. Vatandaş Laboratuvarı'nın yayınladığı raporda, Candiru şirketinin casus yazılımının saldırdığı hedefler arasında Filistin, Lübnan, Türkiye, İran, İsrail, Yemen, İngiltere, Ermenistan ve Singapur yer almaktadır (Marczak, Scott-Railton, Berdan, Abdul Razzak ve Deibert, 2021, s.1).

23 Kasım 2021'de ABD merkezli teknoloji şirketi Apple, NSO şirketine Pegasus yazılımıyla kullanıcılarını gözetlemek ve hedeflemekle suçlayan bir dava açmıştır. Apple şirketi, kullanıcılarının daha fazla suiistimal edilmesini ve zarar görmesini önlemek amacıyla, mahkemeye NSO şirketinin herhangi bir Apple yazılımını, hizmetini veya cihazını kullanmasını yasaklayan kalıcı bir ihtiyati tedbir talebinde de bulunmuştur (Apple, 2021). Apple'ın yasal şikâyeti, Pegasus Projesi skandalının sonuçlarının ve Apple cihazlara sızmak için güvenlik açığından yararlanan NSO şirketinin FORCEDENTRY yazılımının Vatandaş Laboratuvarı tarafından tespit edilmesinin ardından gelmiştir (Marzczak vd., 2021a, s.1).

13 Eylül 2021'de Vatandaş Laboratuvarı, Pegasus casus yazılımının bulaştığı bir Suudi insan hakları savunucusunun telefonunun analizinde, Apple tarafından geliştirilen anlık mesajlaşma uygulaması iMessage platformunda sıfır tıklama açığı keşfetmiştir. Güvenlik Laboratuvarı tarafından FORCEDENTRY adını alan güvenlik açığı, laboratuvarın raporuna göre Apple'ın görsel işleme kütüphanesini hedef almakta ve Apple iOS, MacOS ve WatchOS cihazlarında etkili olmaktadır. Güvenlik açığının Apple şirketine bildirilmesinin ardından 13 Eylül'de Apple yeni bir güncelleme yayınlamıştır (Marczak vd., 2021a, s.1). 3 Aralık'ta ise Apple, 11 ABD Büyükelçiliği çalışanının iPhone telefonlarının Pegasus casus yazılımı tarafından saldırıya uğradığını bildirmiştir (Harwell, Nakashima ve Timberg, 2021b). 21 Aralık'ta ise Güvenlik Laboratuvarı'nda çalışan Bill Marczak, Cemal Kaşıkçı'nın eşi Hana Elatr'ın iki telefonunda da Kaşıkçı cinayetinden önce BAE tarafından hedeflenen Pegasus casus yazılımın izlerini tespit etmiştir (Priest, 2021).

Pegasus Projesinin sonuçlarının açıklanmasının ardından Vatandaş Laboratuvarı'nın yeni Pegasus casus yazılım saldırıları tespit etmesi,

WhatsApp ve Apple şirketlerinin casus yazılım saldırıları için NSO şirketini dava etmesi ve NSO şirketinin ABD'nin ticari kara listesi olan varlık listesine eklenmesi şirket için tüm dünyada olumsuz bir hava yaratmıştır. 21 Ağustos 2022'de NSO şirketi, yaptığı açıklamada şirketin kurucusu ve CEO'su Shalev Hulio'nun görevinden istifa ettiğini duyurmuş; yeniden yapılanma sürecinin bir parçası olarak 100 çalışanın da işten çıkarıldığı ifade edilmiştir (Berger, 2022). İşten çıkarılan 100 çalışanla birlikte şirketin çalışanlarının yaklaşık %13'ünü kaybettiği medyada yer almıştır. Şirket açıklamasında, yeniden yapılanmayla NATO üyesi ülkelere odaklanılarak NSO şirketinin önde gelen yüksek teknoloji siber istihbarat şirketlerinden biri olarak kalmasının sağlanmaya çalışılacağı ifade edilmiştir (Obel ve AP, 2022).

18 Temmuz 2023'te ise ABD Ticaret Bakanlığı, NSO ve Candiru'nun yanı sıra iki İsrailli siber casus yazılım şirketini daha ticari kara listesine eklediğini açıklamıştır. İsrail dışında faaliyet gösteren Yunanistan merkezli Intellexa ve Kuzey Makedonya merkezli Cytrox şirketleri, ABD'nin varlık listesinde yer almıştır (Benjakob ve Reuters, 2023). Cytrox şirketi, 2017 yılında İsrail Havacılık ve Uzay Sanayisi'nden sağlanan finansmanla Rotem Farkash tarafından Kuzey Makedonya'nın Üsküp kentinde kurulmuştur (Benjakob ve Reuters, 2023). 2019 yılında şirket, İsrail'in siber elit birimi Birim 81'in eski komutanı Tal Dillian'ın başkanlığını yaptığı Yunanistan'da faaliyet gösteren Intellexa şirketi tarafından satın alınmıştır. Cytrox şirketi hedef alınan kişinin gönderilen bağlantıya tıklamasıyla mobil cihazdaki tüm verilere ulaşan Predator casus yazılımını geliştirmiştir (Haaretz, 2023). Mart 2022'de, Vatandaş Laboratuvarı, Yunan gazeteci Thanasis Koukakis'in telefonunda Predator casus yazılımının izlerini bulmuştur (Telloglou ve Triantafillou, 2022). Temmuz 2022'de ise Avrupa Parlamentosu Laboratuvarı, Yunanistan'ın Panhelenik Sosyalist Hareket Partisi lideri Nikos Androulakis'in mobil cihazında Predator casus yazılımının yüklenmesi için gönderilen bir mesaj bulmuştur (Mildebrath, 2022). Yunan muhalif lider Androulakis ve Yunan gazeteci Koukasis'in casus yazılımla hedef alınmasını kapsayan 2022 Yunanistan dinleme skandalının ardından ABD, Intellexa ve Cytrox şirketlerini varlık listesine eklemiştir (Benjakob ve Reuters, 2023).

Birçok hükümete ülkelerinde veya egemenlik sınırları dışında muhalif grupları hedef almalarına ve muhalif gruplar üzerinde baskı oluşturmalarına neden olan casus yazılımı satmakla suçlanan NSO şirketine yönelik davalar

ve soruşturmalar günümüzde devam etmektedir. ABD'nin kara listesi olarak adlandırılan varlık listesinde bulunan şirket, ABD şirketleriyle de olası iş fırsatlarını kaybetmektedir. Nitekim casus yazılımı satın almak için NSO şirketi ile görüşmelerde bulunan Amerikalı savunma yüklenicisi L3 Harris Teknolojileri şirketi, ABD yönetiminin olası herhangi bir anlaşmanın ABD hükümeti için ciddi karşı istihbarat ve güvenlik kaygıları yaratacağına dair uyarısının ardından satın alma görüşmelerine son vermiştir (Kirchgaessner, 2022a). Mart 2023'te de ABD Hükümeti, ABD kamu kurumlarının ve departmanlarının ulusal güvenlik riskleri oluşturabilecek veya küresel olarak insan haklarını tehlikeye atacak şekilde kötüye kullanılabilecek ticari casus yazılımlar kullanmasını yasaklamıştır (ABD Beyaz Saray, 2023). Bu bağlamda, ABD kamu kurumlarının ve departmanlarının, ticari kara listesinde bulunan Pegasus casus yazılımı satın alması engellenmiştir.

3.3. İsrail Hükümeti'nin Pegasus Projesi Kapsamında Sorumluluğu

İsrail ihracat kontrolü uygulamaları, 2007 tarihli Savunma İhracatı Kontrol Kanunu'na ve takip eden resmi düzenlemelere dayanmaktadır. İsrail resmi olarak Wassenaar Düzenlemesi'nin bir üyesi değildir. Ancak, Savunma İhracatı Kontrol Kanunu, konvansiyonel silahların ve çift kullanımlı mal ve teknolojilerin transferinde şeffaflığı ve daha fazla sorumluluğu teşvik eden uluslararası Wassenaar Düzenlemesi'nin çift kullanımlı ürünler ve teknolojiler listesine atıfta bulunmaktadır (İsrail Savunma Bakanlığı, 2007, s.7; (Wassenaar Düzenlemesi, 2023a; Silahlı Kontrol Derneği, 2022). İsrail'de savunma ürünlerinin ihracat lisanslarının verilmesinden sorumlu DECA, siber gözetim ve casus yazılım ürünlerini de kapsayan çift kullanımlı ürünler ve teknolojiler için Wassenaar Düzenlemesi'ne uygun şekilde lisans vermektedir (İsrail Savunma Bakanlığı, 2007, s.7; Gross, 2021). DECA, Wassenaar Düzenlemesi'ne uymayan İsrailli siber güvenlik şirketlerinin ürünlerinin lisanslanmasını kısıtlayabilmektedir. Ayrıca, DECA, İsrailli şirketlere ait casus yazılım ürünlerini satın almak isteyen ülkelerin insan hakları kayıtları için kendi incelemesini yürütebilmektedir (Harris ve Mekhennet, 2021). Bu bağlamda, İsrail Savunma Bakanlığı, casus yazılımların yurt dışına satılmasında gözetim ve kontrol rolü üstlenmekte ve İsrailli gözetleme şirketlerinin müşteri seçimlerinde son karar yetkisine sahip olmaktadır.

Pegasus Projesi skandalının ardından 6 Aralık 2021'de DECA, siber sistemlerin ihracatına ilişkin düzenlemeyi sıkılaştırdığını duyurmuştur.

DECA, Pegasus casus yazılımı gibi siber saldırı teknolojilerini satın almak isteyen ülkelerin imzalaması gereken Nihai Müşteri Beyannamesi'nin yeni bir versiyonunu yayınlamıştır. Yeni beyannamenin şartlarına göre ülkeler, teknolojiyi yalnızca terör ve ciddi suçları önlemek için kullanacağını taahhüt etmek zorundadır. Beyannamede belirtilen yükümlülüklere uyulmaması durumunda siber sistemin kullanımının kısıtlanması veya kapatılması dâhil olası yaptırımlar açıkça belirtilmektedir (İsrail Dışişleri Bakanlığı, 2021).

Günümüzde, Pegasus ve Candiru casus yazılımlarıyla hükümet yetkililerinden avukatlara birçok kişinin hedef alınarak kişiler üzerinde hukuka aykırı gözetim yapılması, kişilerin özel hayat ve mahremiyetinin çiğnenmesi, ifade özgürlüğü basın özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlal edilmesi Wassenaar Düzenlemesi'nin bölgesel ve uluslararası güvenlik ve istikrara katkıda bulunma ve terörle mücadele gibi amaçlarıyla uyuşmamaktadır. Casus yazılımların sebep olduğu insan hakları ve temel özgürlüklerin ihlalinden casus yazılımları baskı araçları olarak kullanan hükümetlerle birlikte casus ürünleri satın almak isteyen ülkelerin insan hakları kayıtları için kendi incelemesini yürütebildiği halde yazılımların bu otoritelere satışına onay veren İsrail Savunma Bakanlığı ve İsrail Hükümeti de sorumlu olmaktadır.

Pegasus Projesinin sonuçlarının yayınlanmasının hemen ardından Haaretz gazetesi tarafından yayınlanan araştırmada, Pegasus Projesi skandalı kapsamında casus yazılımı satın aldığı ortaya çıkan aralarında Suudi Arabistan, Macaristan, Azerbaycan, Birleşik Arap Emirlikleri, Ruanda, Hindistan ve Meksika'nın yer aldığı ülkelerle İsrail'in son yıllarda önemli diplomatik ilişkiler geliştirdiği ifade edilmiştir (Ziv, 2021). Nitekim bu ülkelerden biri olan Suudi Arabistan ile Cemal Kaşıkçı cinayetinde Pegasus yazılımının kullanıldığı suçlamaları üzerine NSO şirketinin aynı yıl sözleşmesini feshettiği; ancak 2019 ortalarında NSO şirketi tekrardan Suudi Arabistan'a sistemlerini açtığı medyada yer almıştır. New York Times gazetesinin İsrailli yetkililere dayandırdığı haberinde, İsrail Hükümeti'nin NSO şirketine Suudi Arabistan ile tekrardan çalışması için baskı yaptığı ve baskı sonucu NSO şirketi yazılım sistemlerini tekrardan Suudi Arabistan'a açtığı ifade edilmiştir (Bergman ve Mazzetti, 2021b). Bu bağlamda Pegasus casus yazılımının ülkelere satışına izin veren DECA'nın İsrail'in dış politikasıyla uyumlu kararlar aldığı, İsrail'in ilişkilerini geliştirdiği ülkelere Pegasus yazılımının satışına onay verdiği değerlendirilmektedir. İsrail Hükümeti'nin Pegasus casus yazılımından diplomasi alanında kullanılabilir

bir araç olarak fayda sağlamak amacıyla ulusal çıkarları için yaşanan insan hakları ihlallerini göz ardı ederek baskıcı rejimlerin yazılımı kullanmasına onay vermesi, yazılımı üretim amacından uzaklaştırmaktadır.

SONUÇ

İsrailli siber casusluk şirketi NSO'nun son yıllarda Pegasus casus yazılımını birçok otoriter rejime ihraç ettiği ve ürünlerin devlet başkanlarından gazetecilere kadar binlerce insan üzerinde kullanıldığı Pegasus Projesi soruşturması kapsamında medyada yer almıştır (Uluslararası Af Örgütü, 2021a). Proje kapsamında listede telefon numarası yer alan politikacılardan gazetecilere birçok kişinin casus yazılım tarafından hedef alındığı, kişiler üzerinde hukuka aykırı gözetim yapıldığı, kişilerin özel hayat ve mahremiyetinin çiğnendiği, yazılımın basın özgürlüğü ve ifade özgürlüğü olmak üzere diğer insan hakları ihlallerine neden olduğu ortaya çıkmıştır (Kaldani ve Prokopets, 2022, s.19-20; Richard, 2021). Uluslararası Af Örgütü'nün Güvenlik Laboratuvarı tarafından listede kayıtlı telefon numaralarının kullanıldığı 67 telefona ulaşarak yapılan adli analizlerde, 67 telefonun yarısından fazlasında Pegasus casus yazılımına ait izlerinin olduğunun ortaya çıkarılmış, Uluslarararası Af Örgütü'nün ulaştığı sonuçlar bağımsız bir kuruluş olan Vatandaş laboratuvarı tarafından da doğrulanmıştır (Marczak, Scott-Railton, Anstis ve Deibert, 2021). İki kuruluş tarafından 67 telefonun yarısından fazlasında Pegasus casus yazılımının bulaştığının doğrulanması, Uluslararası Af Örgütü ve Forbidden Stories tarafından ortaya çıkarılan listesinin Pegasus casus yazılımı için bir hedef listesi olduğu düşüncesini güçlendirmiştir (Pfenniger, 2023).

Casus yazılımların sebep olduğu insan hakları ve temel özgürlüklerin ihlalleri doğrudan satın alan hükümetler tarafından kaynaklansa da casus ürünleri satın almak isteyen ülkelerin insan hakları kayıtları için kendi incelemesini yürütebildiği halde casus yazılımların satın alan hükümetler tarafından muhalifler üzerinde kullanılmasına izin veren İsrail Hükümeti de bu ihlallerden sorumlu olmaktadır. Casus yazılımın neden olduğu insan hakları ve temel özgürlüklerin ihlalini ortaya çıkaran Pegasus Projesi skandalı, İsrail'de kamunun siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olmasıyla kamu-özel sektör iş birliğinin kötüye kullanıldığını gösteren önemli bir örnek olmaktadır. Başta Pegasus olmak üzere casus yazılımlarla muhalif grupların hedef alınması, kişilerin hukuka aykırı takip

edilmesi, özel hayat ve mahremiyetinin ihlal edilmesi, ifade özgürlüğü ve basın özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin engellenmesi, İsrail'in Savunma Bakanlığı'nın bağlı olduğunu ifade ettiği Wassenaar Düzenlemesi'nin bölgesel ve uluslararası güvenlik ve istikrara katkıda bulunma ve terörle mücadele gibi amaçlarıyla uyuşmamaktadır.

İsrailli siber casus yazılımların devletlere satışında lisans verme yetkisine sahip olan İsrail, yazılımların satışını ulusal çıkarları için diplomatik bir araç olarak kullanabilmekte ve insan haklarını göz ardı ederek İsrail casus yazılımlarını muhalif gruplar üzerinde baskı aracı olarak kullanan otoriter rejimlere satabilmektedir. Nitekim, Haaretz gazetesi tarafından, Pegasus Projesi skandalı kapsamında casus yazılımı satın aldığı ortaya çıkan Suudi Arabistan ve BAE gibi ülkelerle İsrail'in son yıllarda önemli diplomatik ilişkiler geliştirdiği ifade edilmiştir (Ziv, 2021). İsrail Hükümeti'nin NSO şirketinin Cemal Kaşıkçı cinayetinin ardından Suudi Arabistan ile sözleşmeyi feshettiği ancak İsrail Hükümeti'nin baskısıyla yazılım sistemlerini tekrardan Suudi Arabistan'a açtığı iddiası medyada yer almıştır (Bergman ve Mazzetti, 2021b). İsrail Hükümeti'nin Pegasus casus yazılımından diplomasi alanında kullanılabilir bir araç olarak fayda sağlamak amacıyla ulusal çıkarları için mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlalini göz ardı ettiği görülmektedir.

Pegasus casus yazılım skandalın ortaya çıkmasının ardından şirket birçok olumsuz durumla karşılaşmıştır. Amazon Web Services şirketi, NSO şirketine bağlı bulut hesaplarını devre dışı bırakmış; WhatsApp ve Apple şirketlerinin casus yazılım saldırıları için NSO şirketini dava etmiştir (Fung, 2021). NSO şirketi ABD Hükümeti tarafından ABD'nin ticari kara listesi olan varlık listesine eklenirken ABD Merkezli önde gelen savunma şirketi L3 Harris Teknolojileri ABD Hükümeti'nin baskısıyla casus yazılımının satın alam işlemlerine son vermiştir (Harwell, Nakashima ve Timberg, 2021a; Kirchgaessner, 2022a). Şirket yeniden yapılanma adı altında 100 çalışanını işten çıkarırken şirketin kurucusu Shalev Hulio başkanlık görevinden istifa etmiştir. Şirket yeniden yapılanmayla hedef pazar olarak NATO üyesi ülkelere odaklandığını açıklamıştır (Obel ve AP, 2022). Pegasus Projesi skandalının ardından şirketin kendine yönelik dava, soruşturma ve ambargolardan dolayı maddi kayıplar yaşadığı görülmektedir. Şirketin yeniden yapılanmayla birlikte NATO üyesi ülkelere odaklanma stratejisiyle hem daha çok Avrupalı müşteriler kazanmak hem de yazılımları

baskı aracı olarak kullanan hükümetlere casus yazılım sattığına yönelik eleştirileri ortadan kaldırmak istediği düşünülebilir.

Pegasus Projesi skandalının ardından İsrailli yazılımlarının yurt dışına satışında onay makamı DECA, siber sistemlerin ihracatına ilişkin düzenlemeyi sıkılaştırdığını duyurmuş; yeni müşteri beyannamesinde müşteri ülkelerin teknolojini yalnızca terör ve ciddi suçları önlemek için kullanacağını taahhüt etmek zorunda olduğu belirtilmiştir (İsrail Dışişleri Bakanlığı, 2021). Bu bağlamda, Pegasus başta olmak üzere İsrailli siber gözetim yazılımlarının satın almak isteyen ülkelerin Pegasus gibi siber yazılımları muhalif gruplar üzerinde kullanılmasının önüne geçilmek istendiği görülmektedir. İsrail Hükümeti'nin siber sistemlerin ihracatına ilişkin düzenlemeyi sıkılaştırmasıyla İsrail'in kendisine yönelik Pegasus casus yazılımının neden olduğu insan hakları ve temel özgürlüklerin ihlaline göz yumduğu suçlamalarını ortadan kaldırmayı ve küresel kamuoyu baskısını azaltmayı amaçladığı düşünülebilir.

Günümüzde baskıcı otoriteler tarafından Pegasus yazılımı kullanılarak neden olunan mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlali, NSO şirketine yönelik devam eden davalar ve yazılımın Kaşıkçı ve Pineda cinayetleriyle ilişkilendirilmesi, Pegasus'un kötü bir ünle anılmasına neden olmaktadır. İsrail'in İsrailli casus yazılımların baskıcı rejimlere satılmasına izin veren politikasını sürdürmesi, İsrailli siber gözetim şirketlerinin ABD örneğinde olduğu gibi daha fazla ülke tarafından kara listeye eklenmesine, Amerikalı L3 Harris Teknoloji şirketiyle yaşananlar gibi küresel şirketlerle olası iş birliği fırsatlarının kaybedilmesi ve mali kayıpların yaşanmasına, İsrail siber endüstrisine yönelik yatırımların azalmasına ve endüstrinin dünyada en çok siber yatırım çeken endüstri pozisyonunu da kaybetmesine neden olabilir. Sonuç olarak, İsrail'de siber güvenlik alanında kamu-özel sektör iş birliğinde siber ihracatta kamunun özel sektör üzerinde tam yetkiye sahip olması, iş birliğinin kötüye kullanılmasına ve insan hakları ihlallerinin yaşanmasına neden olmaktadır.

Bu makalede, siber güvenlik alanında kamu-özel sektör ve akademi iş birliği modeli, İsrail örneği üzerinden incelenmiş ve iş birliğinde İsrail Hükümeti'nin siber ürünlerin ihracatında özel sektör üzerinde tam kontrol gücüne sahip olmasının neden olduğu kötüye kullanım Pegasus Projesi kapsamında ele alınmıştır. Çalışmada günümüz güvenlik ortamının en

önemli konularından biri olan siber güvenlik konusu özel sektör iş birliği boyutuyla incelenerek literatüre katkı sağlanması amaçlanmaktadır. Çalışma ülkemizin siber güvenlik politikalarının şekillendirilmesi konusundaki fayda sağlayabileceği ve siber güvenlik alanına yapılacak yatırımlar için ülkemize yol gösterici olabileceği gibi, benzer yazılımlara karşı güvenlik eksenli oluşturacağı farkındalık da önem taşımaktadır. Çalışmanın Türkçe literatüre kazandırılmasının akademinin yol gösterici olarak yapacağı ileri çalışmalara katkı sağlayacağı değerlendirilmektedir.

KAYNAKÇA

ABD Beyaz Saray. (2023). *Fact Sheet: President Biden Signs Executive Order To Prohibit U.S. Government Use of Commercial Spyware That Poses Risks To National Security*. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/

ABD Fas Büyükelçiliği. (2020). *December 22, 2020 a Historic Day For Morocco, Israel, and the United States*. https://ma.usembassy.gov/white-house-senior-advisor-to-the-president-jared-kushner-visit/

Apple (2021). *Apple Sues NSO Group To Curb The Abuse of State-Sponsored Spyware*. https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

BBC. (2017, 4 Temmuz). *Narendra Modi Becomes First Indian PM To Visit Israel*. Erişim Tarihi: 12 Eylül 2023, https://www.bbc.com/news/world-asia-india-40489746

BBC. (2021, 24 Şubat). *Jamal Khashoggi: All You Need To Know About Saudi Journalist's Death*. Erişim Tarihi: 8 Eylül 2023, https://www.bbc.com/news/world-europe-45812399

Benjakob, O. (2022, 5 Nisan). The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware. *Haaretz*. Erişim Tarihi: 6 Eylül 2023, http://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000

Benjakob, O. & Reuters. (2023, 18 Temmuz). U.S. Blacklists Israeli-owned Cyber Arms Firms. *Haaretz*. Erişim Tarihi: 11 Eylül 2023, https://www.haaretz.com/israel-news/security-aviation/2023-07-18/ty-

article/.premium/intellexa-cytrox-tal-dilian-u-s-blacklists-israeli-owned-cyber-arms-firms/00000189-6927-dc94-a78d-f9ef48d10000

Berger. M. (2022, 22 Ağustos). CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup. *The Washington Post*. Erişim Tarihi: 11 Eylül 2023, https://www.washingtonpost.com/world/2022/08/22/nso-pegasus-ceo-shalev-hulio-israel/

Bergman, R. (2019, 1 Ekim). Exclusive: How Mexican Drug Baron El Chapo Was Brought Down By Technology Made In Israel. *Ynetnews*. Erişim Tarihi: 31 Ağustos 2023, https://www.ynetnews.com/articles/0,7340,L-5444330,00.html [Erişim Tarihi: 31.8.2023].

Bergman R. & Mazzetti M. (2021, 17 Temmuz). Israeli Companies Aided Saudi Spying Despite Khashoggi Killing. *New York Times*. Erişim Tarihi: 13 Eylül 2023, https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

Bergman, R. & Mazzetti, M. (2022, 28 Ocak). The Battle for the World's Most Powerful Cyberweapon. *New York Times Magazine*. Erişim Tarihi: 17 Ağustos 2023, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [Erişim Tarihi:17.8.2023].

BilgiGüvende. (2020, 13 Mayıs). *Siber Güvenlik Dünyasında Bir Başka Gizli Tehdit: Zero-Click Saldırısı.* Erişim Tarihi: 29 Ağustos 2023, https://bilgiguvende.com/siber-guvenlik-dunyasinda-bir-baska-gizli-tehdit-zero-click-saldirisi/

Brewster, T. (2021, 22 Temmuz). 'If You're Not A Criminal, Don't Be Afraid'—NSO CEO On 'Insane' Hacking Allegations Facing $1 Billion Spyware Business". *Forbes*. Erişim Tarihi: 5 Eylül 2023, https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=54db5cc4472d

CBS News. (2019, 24 Mart). *CEO of Israeli Spyware-Maker NSO On Fighting Terror, Khashoggi Murder, and Saudi Arabia.* Erişim Tarihi: 8 Eylül 2023, https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/

Chrisafis, A. (2021, 21 Temmuz). Macron Orders Multiple Inquiries Into Leaked Pegasus Project Data. *Guardian.* Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/news/2021/jul/21/macron-orders-multiple-inquiries-into-leaked-pegasus-project-data

Chrisafis, A., Sabbagh, D., Kirchgaessner S., Safi M. (2021, 20 Temmuz). Emmanuel Macron Identified In Leaked Pegasus Project Data. *Guardian.* Erişim Tarihi: 7 Eylül 2023, https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

Citizen Lab. (2021). *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware.* https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/

D'Souza, J. (2023). *Pegasus Spyware: A Violation of Right to Privacy and a Threat to Surveillance Laws in India*. Journal of Legal Studies & Research, Cilt: 9, Sayı:6, ss. 424-438.

Dieterle, L. C. (2023). "Regulating The Invisible Spy – A Case Study of the Pegasus Spyware examining Surveillance Technology Regulation". University of Twente, ss.1-47.

Dogani, R. (2016, 4 Eylül). NSO charges $650,000 to hack 10 iPhones – report. *Globes*. Erişim Tarihi: 6 Eylül 2023, https://en.globes.co.il/en/article-nso-group-charges-650000-to-hack-ten-iphones-report-1001149988

Euronews. (2021, 18 Mayıs). *Hungary Only Nation Against EU Call For Israel-Hamas Ceasefire*. Erişim Tarihi: 13 Eylül 2023, https://www.euronews.com/2021/05/18/eu-fms-due-to-discuss-political-solutions-to-end-israel-gaza-conflict-as-violence-surges-o

Feldstein, S. & Kot, B. (2023). Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. *Carnegie Uluslararası Barış Vakfı.* 1-35.

Fischer, Y. & Levy, R. (2016, 29 Ağustos). The Israelis Behind History's 'Most Sophisticated Tracker Program' That Wormed Into Apple. *Haaretz*. Erişim Tarihi: 28 Ağustos 2023, https://www.haaretz.com/israel-news/business/2016-08-29/ty-article/.premium/the-most-sophisticated-tracking-program/0000017f-f70f-ddde-abff-ff6f051d0000

Forbidden Stories. (2021). *Pegasus Project – All the Articles*". Erişim Tarihi: 6 Eylül 2023, https://forbiddenstories.org/pegasus-project-articles/

Front Line Defenders. (2021, 8 Kasım). *Six Palestinian human rights defenders hacked with NSO Group's Pegasus Spyware.* Erişim Tarihi: 13 Eylül 2023, https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus

Fung, B. (2021, 19 Temmuz). Amazon Web Services Disables Cloud Accounts Linked To NSO Group. *CNN Business*. Erişim Tarihi: 10 Eylül 2023, https://edition.cnn.com/2021/07/19/tech/amazon-nso-group-pegasus-cloud-accounts/index.html

Goodfriend, S. (2021, 23 Kasım). "We Violated People's Privacy For A Living": How Israel's Cyber Army Went Corporate. *+972Magazine*. Erişim Tarihi: 25 Ağustos 2023, https://www.972mag.com/nso-surveillance-companies-israel-army/

Gross, J. A. (2021, 19 Temmuz). Israel: If NSO Group Violated Export Permits, 'Appropriate Action' Will Be Taken. *The Times of Israel*. Erişim Tarihi: 15 Ağustos 2023, https://www.timesofisrael.com/israel-if-nso-group-violated-export-permits-appropriate-action-will-be-taken/

Guardian. (2021, 20 Temmuz). *Response From NSO and Governments*. Erişim Tarihi: 30 Ağustos 2023, https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

Haaretz. (2023, 13 Temmuz). *Report: Israeli Spyware Firm, Ex-security Boss, Advised on Secret Greek Spy Agency Deal*. Erişim Tarihi: 11 Eylül 2023, https://www.haaretz.com/israel-news/security-aviation/2023-07-13/ty-article/report-israeli-spyware-firm-ex-security-boss-advised-on-secret-greek-spy-agency-deal/00000189-4e9a-da08-a5ef-defa40b20000

Harris, S. & Mekhennet, S. (2021, 20 Temmuz). U.S. And E.U. Security Officials Wary of NSO Links To Israeli Intelligence. *The Washington Post*. Erişim Tarihi: 12 Eylül 2023, https://www.washingtonpost.com/national-security/2021/07/20/nso-israel-intelligence/

Harwell, D., Nakashima, E., Timberg, C. (2021a, 3 Kasım). Biden Administration Blacklists NSO Group Over Pegasus Spyware. *The Washington Post*, Erişim Tarihi: 10 Eylül 2023, https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/

Harwell, D., Nakashima, E., Timberg, C. (2021b, 3 Aralık). Pegasus Spyware Used To Hack U.S. Diplomats Working Abroad. *The Washington Post*. Erişim Tarihi: 10 Eylül 2023, https://www.washingtonpost.com/technology/2021/12/03/israel-nso-pegasus-hack-us-diplomats/

Hirschauge, O. & Orpaz, I. (2014, 17 Şubat). U.S. Fund to Buy NSO and Its Smartphone-snooping Software. *Haaretz*. Erişim Tarihi: 30 Ağustos

2023, https://www.haaretz.com/israel-news/business/2014-02-17/ty-article/u-s-fund-to-buy-snooping-software/0000017f-f010-d223-a97f-fdddda30000

Holmes, O. (2020, 23 Kasım). Netanyahu Holds Secret Meeting With Saudi Crown Prince. *Guardian*. Erişim Tarihi: 12 Eylül 2023, https://www.theguardian.com/world/2020/nov/23/benjamin-netanyahu-secret-meeting-saudi-crown-prince-mohammed-bin-salman

Hopkins, N. & Kirchgaessner, S. (2019, 20 Ekim). Whatsapp Sues Israeli Firm, Accusing It of Hacking Activists' Phones. *Guardian*. Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones

İsrail Dışişleri Bakanlığı. (2021). *Israel Mod Tightens Control of Cyber Exports*. https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021

İsrail Ekonomi ve Sanayii Bakanlığı. (2023). *Export Control Agency, Ministry of Economy and Industry*. https://www.gov.il/en/Departments/General/duexportcontrol-info

İsrail Savunma Bakanlığı. (2007). *Defense Export Control Law, 5766-2007*. 1-32.

İsrail Savunma Bakanlığı. (2023a). *Defense Exports Control Agency (DECA)*. ,https://english.mod.gov.il/Departments/Pages/DefenseExportsControlAgency.aspx

İsrail Savunma Bakanlığı. (2023b). *Message From Director*. https://exportctrl.mod.gov.il/English/Pages/Message-from-Director.aspx

İsrail Ulusal Siber Müdürlüğü, "Israeli Cyber Security Industry Continues Growth In 2021", 20 Ocak 2022, https://www.gov.il/en/departments/general/israeli-cyber-security-industry-continues-growth-20-jan-2022 [Erişim Tarihi: 13.06.2023].

İsrail Ulusal Siber Müdürlüğü. (2022). *Israeli Cyber Security Industry Continues Growth In 2021*. Erişim Tarihi: 13 Haziran 2023, https://www.gov.il/en/departments/general/israeli-cyber-security-industry-continues-growth-20-jan-2022

Kaldani, T. & Prokopets, Z. (2022). "Pegasus Spyware And Its Impacts On Human Rights". Council of Europe, s.1-23.

Kareem, K. M. (2024). "A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security", International Journal of Intelligent Systems and Applications In Engineering, ss.1360-1373, Mart 2024.

Kaspersky. (2023). *Sıfır Tıklama Kötü Amaçlı Yazılımı Nedir ve Sıfır Tıklama Saldırıları Nasıl Gerçekleştirilir?.* Erişim Tarihi: 28 Ağustos 2023, https://www.kaspersky.com.tr/resource-center/definitions/what-is-zero-click-malware

Khurana. A. (2022). "*Misinformation & Pegasus Project: Case study of India*". Univerzita Karlova, Fakulta sociálních věd, Katedra bezpečnostních studií.

Kirchgaessner, S. (2021, 24 Temmuz). Officials Who Are US Allies Among Targets of NSO Malware, Says Whatsapp Chief. *Guardian.* Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/technology/2021/jul/24/officials-who-are-us-allies-among-targets-of-nso-malware-says-whatsapp-chief

Kirchgaessner, S. (2022b, 23 Mart). Israel Blocked Ukraine From Buying Pegasus Spyware, Fearing Russia's Anger. *Guardian*. Erişim Tarihi: 13 Eylül 2023, https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia

Kirchgaessner, S. (2022a, 10 Temmuz). US Defence Firm Ends Talks To Buy NSO Group's Surveillance Technology. *Guardian*. Erişim Tarihi: 10 Eylül 2023, https://www.theguardian.com/us-news/2022/jul/10/us-defence-firm-ends-talks-to-buy-nso-groups-surveillance-technology

Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lakhani, N., Safi, M. (2021, 18 Temmuz). Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon. *The Guardian.* Erişim Tarihi: 7 Eylül 2023, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Lakhani, N. (2021, 18 Temmuz). Revealed: Murdered Journalist's Number Selected By Mexican NSO Client. *The Guardian*. Erişim Tarihi: 8 Eylül 2023, https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

Landau, N. (2020, 15 Eylül). Full Text: The Israel-UAE-Bahrain Abraham Accords Peace Agreement. *Haaretz*. Erişim Tarihi: 13 Eylül 2023, https://www.haaretz.com/middle-east-news/.premium-full-text-the-israel-uae-bahrain-abraham-accords-declaration-1.9159509

Landau, N. & Khoury, J. (2018, 27 Ekim). Netanyahu Visits Oman, Which Has No Diplomatic Ties With Israel. *Haaretz*. Erişim Tarihi: 12 Eylül 2023, https://www.haaretz.com/middle-east-news/2018-10-27/ty-article/netanyahu-secretly-visits-oman-which-has-no-diplomatic-ties-with-israel/0000017f-dc28-d3a5-af7f-feae05340000

Levy, R. (2017, 21 Nisan). Who Makes Millions Off Israel's Top Cyber Spy Agency?, *Haaretz*. Erişim Tarihi: 21 Ağustos 2023, https://www.haaretz.com/israel-news/business/2017-04-21/ty-article/who-makes-millions-off-israels-top-cyber-spy-agency/0000017f-db2e-d3a5-af7f-fbae453c0000

Lior, I. (2017, 20 Kaım). Israel to Pay Rwanda $5,000 for Every Deported Asylum Seeker It Takes In. *Haaretz*. Erişim Tarihi: 14 Eylül 2023, https://www.haaretz.com/israel-news/2017-11-20/ty-article/israel-to-pay-rwanda-5-000-for-every-asylum-seeker-deported-there/0000017f-e9cc-da9b-a1ff-edefea800000

Lipson, N. (2017, 27 Ekim). Goodbye Uzi, Hello Big Brother: The Israelis Arming the World With Sophisticated Cyber-weapons. *Haaretz*. Erişim Tarihi: 1 Eylül 2023, https://www.haaretz.com/israel-news/2017-10-27/ty-article/the-new-face-of-israels-arms-exporters/0000017f-db9c-db22-a17f-ffbd474f0000

Marczak, B., Scott-Railton, J., Anstis S., Deibert, R. (2021, Temmuz). Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware. *The Citizen Lab*. Toronto Üniversitesi. https://citizenlab.ca/2021/07/amnesty-peer-review/

Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., Deibert, R. (2021, Temmuz). Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus. *Citizen Lab Araştırma Raporu* No.139, Toronto Üniversitesi. 1-14.

Marczak, B., Scott-Railton, J., Abdul Razzak, B., Al-Jizawi, N., Anstis, S., Berdan, K., Deibert, R. (2021a, Eylül). Forcedentry: NSO Group iMessage Zero-Click Exploit Captured in the Wild. *Citizen Lab Araştırma Raporu* No:143, Toronto Üniversitesi. 1-4.

Marczak, B., Scott-Railton, J., Abdul Razzak, B., Al-Jizawi, N., Anstis, S., Berdan, K., Deibert, R. (2021b, Aralık). Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. *Citizen Lab*. Toronto Üniversitesi. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Mazzetti, M., Bergman R., Stevis-Gridneff, M. (2022, 8 Aralık). How the Global Spyware Industry Spiraled Out of Control. *The New York*

Times. Erişim Tarihi: 4 Eylül 2023, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html

Megiddo, G. (2021, 17 Aralık). "We're on the U.S. Blacklist Because of You": The Dirty Clash Between Israeli Cyberarms Makers. *Haaretz*. Erişim Tarihi: 18 Ağusots 2023, https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/.highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fdb72e9a0000

Melman, Y. (2021, 21 Temmuz). Pegasus Scandal Turns Spotlight on Israel's Controversial Military Tech Sector. *Middle East Eye*. Erişim Tarihi: 18 Ağustos 2023, https://www.middleeasteye.net/news/pegasus-israel-scandal-military-tech-sector-spotlight

Mildebrath, H. (2022, Eylül). Greece's Predatorgate: The Latest Chapter In Europe's Spyware Scandal?. *Avrupa Parlamentosu Araştırma Servisi*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf

News Room Panama. (2021, 26 Temmuz). *'Disappeared' Pegasus Spyware Used In Panama In 2012*. Erişim Tarihi: 1 Eylül 2023, https://www.newsroompanama.com/news/disappeared-pegasus-spyware-used-in-panama-in-2012

NSO Grup. (2021). *Transparency and Responsibility Report 2021*. 1-32.

NSO Grup. (2023). *About Us*. Erişim Tarihi: 1 Eylül 2023, https://www.nsogroup.com/about-us/

Obel, A. & AP (2022, 21 Ağustos). NSO Group's Hulio Steps Down As CEO Of Spyware Firm, 100 Employees Let Go. *Haaretz*. Erişim Tarihi: 10 Eylül 2023, https://www.timesofisrael.com/nso-groups-hulio-steps-down-as-ceo-of-spyware-firm-100-employees-let-go/

O'neill, P. H. (2017, 12 Haziran). Israeli Hacking Company NSO Group Is On Sale For More Than $1 Billion. *CyberScoop*. Erişim Tarihi: 1 Eylül 2023, https://cyberscoop.com/nso-group-for-sale-1-billion-pegasus-malware/ [Erişim Tarihi: 1.9.2023].

Oren, A. (2010, Ocak). The IDF's New Battlefield Is Found In Computer Networks. Erişim Tarihi: 24 Mayıs 2023, http://www.haaretz.co.il/misc/1.1182490

Perltroth, N. (2016, 2 Eylül). How Spy Tech Firms Let Governments See Everything on a Smartphone. *The New York Times*. Erişim Tarihi: 1 Eylül 2023, https://www.nytimes.com/2016/09/03/technology/nso-

group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html

Pfenniger, K. (2023, 17 Temmuz). Pegasus Project: What Has Happened Since The Revelations?. Forbidden Stories. Erişim Tarihi: 9 Eylül 2023, https://forbiddenstories.org/pegasus-project-impacts-map/

Priest, D. (2021, 21 Aralık). A UAE Agency Put Pegasus Spyware On Phone of Jamal Khashoggi's Wife Months Before His Murder, New Forensics Show. *The Washington Post*. Erişim Tarihi: 12 Eylül 2023, https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/

Priest, D., Mekhennet, S., Bouvart, A. (2021, 18 Temmuz). Jamal Khashoggi's Wife Targeted With Spyware Before His Death. *The Washington Post*. Erişim Tarihi: 8 Eylül 2023, https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/

Reuters. (2023, 9 Ocak). *U.S. Supreme Court Lets Meta's WhatsApp Pursue 'Pegasus' Spyware Suit,* Erişim Tarihi: 10 Eylül 2023, https://www.reuters.com/legal/us-supreme-court-lets-metas-whatsapp-pursue-pegasus-spyware-suit-2023-01-09/

Richard, L. (2021, Temmuz 18). The Pegasus Project: A Worldwide Collaboration to Counter A Global Crime". *Forbidden Stories*. Erişim Tarihi: 7 Eylül 2023, https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/

Sabbagh, D., Pegg, D., Lewis P., Kirchgaessner, S. (2021, 21 Temmuz). UAE linked to listing of hundreds of UK phones in Pegasus project leak. *Guardian.* Erişim Tarihi: 7 Eylül 2023, https://www.theguardian.com/world/2021/jul/21/uae-linked-to-listing-of-hundreds-of-uk-phones-in-pegasus-project-leak

Sadeh, S. (2020, 31 Aralık). A Shady Israel Intel Genius, His Cyber-spy Van and Million Dolar Deals. *Haaretz*. Erişim Tarihi: 19 Ağustos 2023, https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000

Schwartz, M. J. (2021, 19 Temmuz). Leak of 50,000 Contact Details Tied to Spyware Targeting. *Bank of Security*. Erişim Tarihi: 7 Eylül 2023, https://www.bankinfosecurity.com/leak-50000-contact-details-tied-to-spyware-targeting-a-17097

Shahaf, T. (2018, 5 Temmuz). Verint Was Reportedly About to Buy NSO At A $1 Billion Valuation. *Globes*. Erişim Tarihi: 1 Eylül 2023,

https://en.globes.co.il/en/article-nso-cyber-weapon-co-sale-to-verint-in-jeopardy-1001244757

Shahaf, T. (2019, 11 Nisan). Technology. *Ynetnews*. Erişim Tarihi: 11 Eylül 2023, https://www.ynetnews.com/articles/0,7340,L-5618901,00.html

Shezaf, H. & Jacobson, J. (2018, 20 Ekim). Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays. *Haaretz*. Erişim Tarihi: 15 Ağustos 2023, 20 Ekim 2018, https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000

Arms Control Association. (2022). *The Wassenaar Arrangement at A Glance*. https://www.armscontrol.org/factsheets/wassenaar

Sneha. (2023, Nisan). "The Pegasus Spyware: Endorsing The Citizens' Right To Privacy". Journal of Legal Research and Juridical Sciences. Vol:2, Sayı:3, s.451-468, ISSN (O): 2583-0066.

Solomon, S. (2019, 14 Şubat). NSO Founders, Management Buy Stake In Firm From Francisco Partners. *The Times of Israel*. Erişim Tarihi: 5 Eylül 2023, https://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/

Stone M. & Roumeliotis, G. (2015, 3 Kasım). Secretive Cyber Warfare Firm NSO Group Explores Sale: Sources. *Reuters*. Erişim Tarihi: 1 Eylül 2023, https://www.reuters.com/article/us-nsogroup-m-a-idUSKCN0SR2JF20151103

Telloglou, T., Triantafillou, E. (2022, 11 Nisan). Ποιος παρακολουθούσε το κινητό του δημοσιογράφου Θανάση Κουκάκη. *Inside Story*. Erişim Tarihi: 11 Eylül 2023, https://insidestory.gr/article/poios-parakoloythoyse-kinito-toy-dimosiografoy-thanasi-koykaki

Theoi Project. *Pegasos*. Erişim Tarihi: 30 Ağustos 2023, https://www.theoi.com/Ther/HipposPegasos.html

Timberg, C., Birnbaum, M., Harwell, D., Sabbagh, D. (2021, 20 Temmuz). On The List: Ten Prime Ministers, Three Presidents And A King. *The Washington Post*. Erişim Tarihi: 16 Eylül 2023, http://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

Timberg, C., Kirchgaessner, S., Mekhennet, S., Nakashima, E., Harris, S. (2022, 23 Mart). Israel Blocked Ukraine From Getting Potent Pegasus Spyware. *The Washington Post*. Erişim Tarihi: 13 Eylül 2023, https://www.washingtonpost.com/technology/2022/03/23/urkraine-spyware-pegasus-russia/

Uluslararası Af Örgütü. (2021a). *Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally*. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

Uluslararası Af Örgütü. (2021b). *Forensic Methodology Report: How To Catch NSO Group's Pegasus*. 1-81. DOC 10/4487/2021.

Uluslararası Af Örgütü. (2021c). *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware.* https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

Ulusal Af Örgütü Birleşik Krallık. (2021). *Pegasus Project: Macron Among World Leaders Selected As Potential Targets of NSO Spyware*". https://www.amnesty.org.uk/press-releases/pegasus-project-macron-among-world-leaders-selected-potential-targets-nso-spyware

Walker, S., Kirchgaessner, S., Lakhani, N., Safi, M. (2021, 19 Temmuz). Pegasus Project: Spyware Leak Suggests Lawyers and Activists at Risk Across Globe. *The Guardian*. Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe

Wassenaar Düzenlemesi. (2023a). *About Us*, https://www.wassenaar.org/about-us/#faq

Wassenaar Düzenlemesi. (2023b). *Overview*. https://www.wassenaar.org/about-us/#faq

Yablonko, Y. (2019, 14 Şubat). Novalpina Capital and Founders Buy NSO At $1b Co Value. *Globes*. Erişim Tarihi: 1 Eylül 2023, https://en.globes.co.il/en/article-novalpina-capital-and-founders-buy-nso-for-1b-1001273312

Yaron, O. (2020, 30 Kasım). The Secret of NSO's Success in Mexico. *Haaretz*. Erişim Tarihi: 30 Ağustos 2023, https://www.haaretz.com/israel-news/tech-news/2020-11-30/ty-article/.highlight/the-secret-of-nsos-success-in-mexico/0000017f-e0f5-d568-ad7f-f3ff5cff0000

Ziv, A. (2021, 20 Temmuz). The Pegasus Project | Where Netanyahu Went, NSO Followed: How Israel Pushed Cyberweapon Sales. *Haaretz*. Erişim Tarihi: 12 Eylül 2023, https://www.haaretz.com/israel-news/tech-news/2021-07-20/ty-article/.highlight/where-bibi-went-nso-followed-how-israel-pushed-cyberweapons-sales/0000017f-e388-d7b2-a77f-e38fd45a0000