# Siber Saldırıların Yıkıcılığı: Lübnan’da Yaşanılan Siber Saldırı – Emine Çelik


---

**Siber Saldırıların Yıkıcılığı: Lübnan’da Yaşanılan Siber Saldırı**

Siber saldırıların yıkıcılığı üzerine süregelen tartışmaların birçok kırılma noktası olmakla birlikte, 27 Nisan 2007’da Rusya’nın Estonya’ya düzenlediği bir dizi siber saldırıyla bu tartışmaların başka bir alana evirildiğini söylemek mümkün. Öyle ki Rusya’nın düzenlediği iddia edilen söz konusu siber saldırılar, yoğun DDoS (hizmet aksatma) ve Malware (zararlı/ kötü amaçlı yazılım) saldırılarıyla başlamış ve akabinde de Estonya’nın birçok kamu kuruluşu işlevsiz hale geldi. Estonya saldırısına kadar siber saldırılar, “görece” hasar vermeyen saldırılar olarak nitelendirilmiş olsa bile söz konusu saldırı sonrasında fiziksel askeri saldırılar

kadar yıkıcı bir etkiye sahip oldukları yönündeki tartışmalar günümüzde devam ediyor. 2007'den sonra teknoloji ve kitle iletişim araçları hızla yükselen bir ivme sergileyerek gelişti ve yaygınlaştı ve bu teknolojilerin, sosyal, ekonomik ve toplumsal hayatı kolaylaştırıcı etkisinin yanı sıra bireylerin, toplumların ve devletlerin siber alanda yeni güvenlik tehditleriyle karşı karşıya gelmesine neden oldu. Bu bağlamda devletler, ulusal siber güvenlik ve siber savunma politikalarına yönelik geniş ölçekte savunma ve saldırı planları geliştirme yolunda hızla yol almaya devam ediyor. Ancak akıllı telefonlara, çevrimiçi/dışı birçok cihaza yönelik siber saldırılar ve bu saldırıları üstlenenin olmaması gibi bir dizi anonimlik uluslararası ilişkiler bağlamında dost düşman algısında yanılgıya yol açabiliyor.

## İsrail'in Siber Saldırı Kapasitesi ve Destekçileri

Ortadoğu'da devlet sınırları tartışmalı olan İsrail'in siber uzay içinde siber saldırı ve siber terörizm konusunda da sınır tanımadığını söylemek mümkün. Bu perspektiften bakıldığında, İsrail'in jeopolitik konumu itibariyle düşman olarak nitelendirdiği devlet dışı aktörler ve ülkelere ait kritik alt yapı ve tesisler başta olmak üzere, askeri ağlar ve istihbari anlamda güvenlik açıklarından yararlanmanın yolları üzerine sürekli aktif bir şekilde çalıştığı bilinen bir gerçek. Öyle ki İsrail, söz konusu aktör ve ülkelere yönelik temel hizmetleri aksatma, iletişim ağlarına sızma, İsrail'in güvenliğini tehdit edebilecek proje ve çalışmaları sabote etme ya da varlıklarını ortadan kaldırma gibi bir dizi hedefi benimseyerek siber kapasitesini, Mossad, CIA, FBI ve günümüzde de İsrail yanlısı/ destekçisi devlet dışı aktörler ve teknoloji şirketlerinin verilerini kullanarak arttırmaktadır.

İsrail'in sansasyonel siber saldırılarının ilk dikkat çekeni hiç şüphesiz İran'a yönelik Stuxnet saldırısıdır. İsrail'in Haziran 2010'da İran'a karşı düzenlendiği bu saldırının birçok önemli parametreyi içerdiğini söylemek mümkün. Siber alanda bir kod parçasının fiziksel açıdan büyük bir yıkımla sonuçlandığı ilk saldırı olan Stuxnet solucanının, İran'da binlerce sanayi tesisinin işleyişini aksatmakla birlikte, asıl hedefi İran'ın Natanz nükleer tesislerindeki nükleer çalışmaları durdurmak ya da aksatmaktı. Saldırının düzenlendiği tarih itibariyle bakıldığında ileri düzeyde akıllı bir kod parçası olarak nitelendirilen Stuxnet'in temel hedefi, Natanz nükleer tesisinde yer alan ve Windows tabanlı santrifüjler gibi ekipmanları

çalıştıran, endüstriyel kontrol sistemlerini programlamak için kullanılan Siemens Step7'a ait yazılımın işlevini bozmaktı. İsrail'in düzenlediği Stuxnet saldırısı, İran'ın Natanz nükleer tesisinde uranyum zenginleştirmesi için bulunan 5000 santrifüjden 1000 tanesini etkisiz hale getirerek, İran'ın mevcut nükleer programında iki yıl geriye gitmesine neden oldu.  Ek olarak belirtmek gerekir ki söz konusu Stuxnet solucanın tesise çevrimiçi yerleştirilmeyip bir USB ile taşınması, kritik siber saldırılarda insan faktörünün tamamen dışarıda bırakılamayacağını ve dolayısıyla istihbari faaliyetlerin dahil edildiği saldırıların şiddetini arttırdığını göstermektedir.

**7 Ekim Sonrası Siber Saldırılar**

İsrail ve Filistin arasında devam eden savaşın yıkıcı boyutlarından biri de siber alanda kendisini gösterdi. Tıpkı Rusya Ukrayna Savaşı'nda olduğu gibi bu savaşta da siber uzay, tarafların ve tarafların destekçileri için çalışan birçok kişi ve grup için ek bir savaş alanı olarak kullanılıyor. Taraflar birbirilerinin çevrimiçi ya da dışı alanları başta olmak üzere kritik alt yapı ve diğer tesislerine yönelik saldırı alanlarını genişletmek ve yaygınlaştırmak adına büyük çaba gösteriyor. Filistin yanlısı Rus, Pakistanlı ve İranlı hackerların saldırıları genelde DDoS saldırıları olmakla birlikte Hamas'ın İsrail'e sızması için istihbari bilgileri elde etmesi, İsrail'e ait görsel, yazılı basın ve bankalara düzenlenen bir dizi siber saldırı olarak da nitelendirilebilir. Nitekim temelde herhangi bir askeri amaca hizmet etmemekle birlikte bu saldırıların, sıklıkla İsrail'in işlediği insan hakları ihlalleri, savaş suçları gibi bilgi kampanyalarıyla İsrail karşıtlığında küresel anlatıları şekillendirilmeye yönelik olduğu görülüyor. İsrail perspektifinden bakıldığında ise Gazze'deki en temel siber saldırı noktası hiç şüphesiz İsrail'in kontrol ettiği internet bağlantılı elektrik alt yapısı. Öyle ki İsrail hükümeti, interneti keserek kritik alt yapıları hedef almış ve elektrik, su şebekeleri gibi hayati önem taşıyan tesislerin işlevini ortadan kaldırmıştır. İsrail'in bu hamlesiyle, en masum bakış açısıyla bölgedeki insanları göçe zorlayarak işgalini hızlandırdığı söylenebilir.

**Lübnan'da Gerçekleşen Siber Saldırının Arka Planı**

İsrail’in son dönemdeki siber saldırıları incelendiğinde, Lübnan’da Hizbullah’a yönelik gerçekleştirdiklerinin çarpıcı düzeyde olduğu görülmektedir. Bilindiği üzere, İsrail’in Lübnan’da görülen türden karmaşık saldırılar gerçekleştirme konusunda uzun bir geçmişi var. Ancak, İsrail’in 19 Eylül 2024’de gerçekleştirmiş olduğu siber saldırı Hizbullah’ın iletişim ağlarını felç etti. Öyle ki, Hizbullah üyelerinin tam bir gizlilik içerisinde iletişim ağlarını kurduğuna yönelik mit, İsrail’in Lübnan’da 5.000’e yakın çağrı cihazına düzenlediği siber saldırı ile yerle bir oldu. Saldırının arka planına bakıldığında ise çarpıcı detayların yer aldığını söylemek mümkün. İlk olarak belirtmek gerekir ki söz konusu saldırı, Mossad destekli ve içerisinde HUMINT (insan istihbaratı ya da sahadaki insandan elde edilen istihbarat), IMINT (görüntü istihbaratı), SIGINT (sinyal istihbaratı) destekleri olan bir siber saldırı örneği olarak karşımıza çıkmakta. Uzun zamandır İsrail’in Hizbullah üyelerinin birçoğunun cep telefonlarını dinlediğine yönelik Nasrallah ve üst yönetim kadrosunun endişeleri, haberleşme için yılbaşında örgütü yeni bir arayışa yöneltti. Akabinde de Hizbullah üyelerine Tayvan merkezli Gold Apollo adlı bir markadan temin edilen AR-924 çağrı cihazları dağıtıldı. Mossad’ın ise Hizbullah’ın satın almak istediği çağrı cihazlarına ilişkin istihbari bilgiyi edindikten sonra paravan şirketler kurarak çağrı cihazlarına, örgütün cihazları üyelerine dağıtmadan önce Lübnan’daki gümrükte patlayıcı yerleştiğine dair doğrulanamayan bilgiler mevcut. Yapılan araştırmalar neticesinde, söz konusu patlayıcıların, çağrı cihazlarına gönderilen basit bir radyo sinyaliyle tetiklenerek infilak ettirildiği üzerine görüş birliği mevcut.

Çağrı cihazlarının nereden, nasıl ve hangi yollarla tedarik edildiği, sürece dahil olan aktörlerin kim olduğu ve patlayıcıların tedarik zincirinin hangi aşamasında yerleştirildiğine dair bilinmezlik, durumu daha da kritik hale getiriyor. Gelinen noktada İsrail’in gerçekleştirdiği söz konusu saldırı, Hizbullah’ın tüm iletişim ağını yok ederek üyeler arasında iletişimsizlik ve panik havasına neden oldu ve İsrail’in, bu ortamda üst kademe örgüt üyelerine düzenlediği bir dizi saldırıyla da Hizbullah’ın hazırlıksız yakalanmasıyla sonuçlandı. Yine, Netanyahu hükümetinin, Hizbullah’ı İsrail sınırından Lübnan içerisine süpürmek/ortadan kaldırmak adına kara harekatı düzenlemesi için büyük bir fırsat yarattı. Sonuç olarak, biçimi ve ilerleyişinden saldırının salt siber saldırı olmadığı, çağrı cihazlarının tedarikinden itibaren başlayan çok bileşenli bir süreç olduğunu söylemek mümkün. Ek olarak, istihbari faaliyetlerin ve siber saldırıların koordineli bir şekilde işleyişinin sağlanmasının, bölgede en kritik hamleler arasında yer aldığını söylemek de

mümkün. Siber saldırı ve istihbarat toplama tekniklerinin bir arada kullanımının pratikte nelere yol açtığını, İsrail'in hiçbir karşı müdahaleyle karşılaşmadan kara sınırından Lübnan'a rahatça girmesine ve Hizbullah'ın karşı atak için üyeleri arasında bir koordinasyon dahi kuramamasına neden olan bu saldırı göstermektedir.

---

**Emine Çelik** Lisans derecesi Anadolu Üniversitesi'nden elde edildikten sonra yüksek lisansını Necmettin Erbakan Üniversitesi Siyaset Bilimi ve Kamu Yönetimi'nde tamamlamış ve aynı üniversitede doktorasına tamamlamıştır. Halihazırda Necmettin Erbakan Üniversitesi'nde misafir öğretim üyesi olarak "Siyasal Şiddet ve Terör" dersini vermektedir. Akademik araştırma alanları arasında terörizm, radikalleşme, siber terörizm, yapay zeka ve yoksulluk bulunmaktadır.

---

**Bu yazıya atıf için:** Emine Çelik, "Siber Saldırıların Yıkıcılığı: Lübnan'da Yaşanılan Siber Saldırı" , Panorama Çevrimiçi, 11 Ekim

2024,https://www.uikpanorama.com/blog/2024/10/11/siber-saldiri-ec/

---