GELENEKSEL İSTİHBARATIN SINIRINDA SİBER OPERASYONLAR: MOSSAD'IN HİZBULLAH'A YÖNELİK ÇAĞRI CİHAZI SALDIRISI

Necati YILDIZ[*]

ORCID ID: 0009-0005-6023-396X

Declaration[*]

Özet

Bu çalışma, geleneksel istihbarat yöntemleri ile siber operasyonlar arasındaki etkileşimi incelemeyi amaçlamakta olup, temel araştırma sorusuna odaklanmaktadır: Fiziksel ve dijital unsurları bünyesinde barındıran hibrit siber operasyonlar, geleneksel istihbarat uygulamalarını ne ölçüde dönüştürmekte ve bu dönüşüm uluslararası güvenlik dinamiklerini nasıl yeniden şekillendirmektedir? Bu soruyu yanıtlamak üzere çalışmada, nitel vaka analizi yöntemi benimsenmiş; Mossad'ın Hizbullah'a yönelik gerçekleştirdiği çağrı cihazı saldırısı, açık kaynak istihbaratı (OSINT) verileri, güvenlik raporları ve ilgili akademik çalışmalar çerçevesinde incelenmiştir. Analiz sonucunda ulaşılan temel bulgu, siber operasyonların artık yalnızca istihbarat toplama veya elektronik gözetleme aracı olmaktan çıktığı; tedarik zinciri zafiyetlerinin istihbarat örgütleri tarafından operasyonel bir silah olarak kullanılmasıyla, doğrudan fiziksel ve stratejik sonuçlar doğuran bir güç unsuru haline geldiği incelenmektedir. Çalışmanın özgün katkısı ise, çağrı cihazı saldırısını yalnızca teknik bir vaka olarak ele almanın ötesinde hem geleneksel istihbaratın hem de siber operasyonların hibrit model olarak bütünleştirilmiş bir yapı haline geldiğini analiz etmektedir. Bu bağlamda çalışma, siber operasyonlar ile geleneksel istihbaratın kesişiminde ortaya çıkan ikilemler ve stratejik belirsizlikler tartışarak, gelecekteki araştırmalar için kavramsal zemin hazırlamayı hedeflemektedir.

Anahtar Kelimeler: Geleneksel İstihbarat, Siber Operasyonlar, Mossad, Hizbullah, Güvenlik Dinamikleri, Çağrı Cihazı Saldırısı

[*] Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi Lisanüstü Eğitim Enstitüsü Uluslararası İlişkiler Anabilim Dalı Yüksek Lisans Öğrencisi. nctyldzz@gmail.com

[*] Bu çalışmanın hazırlanma sürecinde, ilgili literatürün taranması ve potansiyel kaynakların tespit edilmesi aşamasında yapay zekâ destekli bir dil modelinden (Claude, Anthropic) faydalanılmıştır. Bütün sorumluluk yazarın kendisine aittir.

Abstract

This study aims to conduct an in-depth examination of the interaction between traditional intelligence methods and cyber operations, focusing on the following central research question: To what extent are hybrid cyber operations which incorporate both physical and digital elements—transforming traditional intelligence practices, and how is this transformation reshaping international security dynamics? To answer this question, the study employs a qualitative case study methodology; the Mossad's pager attack against Hezbollah was examined within a comprehensive framework through a critical discourse analysis of open-source intelligence (OSINT) data, security reports, and relevant literature. The key finding resulting from the analysis is that cyber operations have moved beyond serving merely as tools for intelligence gathering or electronic surveillance; by exploiting supply chain vulnerabilities as an operational weapon, they have become a power factor that directly produces physical and strategic consequences. The study's original contribution lies in analyzing how, beyond treating the pager attack merely as a technical case, both traditional intelligence and cyber operations have merged into an integrated hybrid model. In this context, the study aims to lay the groundwork—both conceptual and methodological for future research by discussing the dilemmas and strategic uncertainties that arise at the intersection of cyber operations and traditional intelligence.

Keywords: Traditional Intelligence, Cyber Operations, Mossad, Hezbollah, Security Dynamics, Pager Attack.

Giriş

Geleneksel istihbarat, bilgi toplama ve düşmanın faaliyetlerini önceden tespit etme faaliyetleridir. Bu nedenle istihbarat örgütleri uzun zamandır gizli ve doğrudan insan kaynakları yahut teknik yöntemlerle operasyonlar yapmaktadır (Lowenthal M. M., 2020). Fakat teknoloji hızla gelişirken, siber alanlar yeni bir operasyon bölgesi olmaya başlamıştır. Siber operasyonlar; bilgiye erişim, veri değişikliği, iletişim kesintisi gibi amaçlarla yapılmaktadır. Bunlar, geleneksel yöntemlere göre daha ucuzdur, daha az fiziksel tehlike barındırır ve daha gizli şekilde gerçekleştirilebilir. Bu durum, istihbarat faaliyetlerini genişletmiş ve operasyonların şeklini değiştirmiştir. Ayrıca, istihbarattaki bu değişim, kamu ve özel sektör arasındaki iş birliklerinin artmasına da neden olmuştur (Daricili & Erendor, 2021). Bu iş birlikleri, kaynakların daha verimli kullanılmasını ve siber tehditlere karşı daha

etkili önlemler alınmasını sağlamaktadır. Yeni yaklaşımlar, istihbarat toplama süreçlerini dönüştürmekte ve siber alanlarda daha fazla veri analizi yapılmasına olanak tanımaktadır.

Siber istihbarat operasyonlarının geleneksel istihbarattan farkı, fiziksel müdahale yerine dijital müdahale ve manipülasyonların tercih edilmesidir. Ayrıca, siber ortamlar genişleme ve anonimlik açısından avantaj sağlamakta; bu da operasyonların kim tarafından gerçekleştirildiğini tespit etmeyi zorlaştırmaktadır. Ancak, bu yeni ortam aynı zamanda uluslararası hukuk ve etik kurallar açısından çeşitli tartışmaları da beraberinde getirmektedir. Geleneksel istihbarat yöntemleri genellikle açıkça tanımlanabilir sınırlar ve kurallar çerçevesinde yürütülürken, siber operasyonlar bu sınırların ötesine geçerek etik ve hukuki kuralların sorgulanmasına neden olmaktadır (Cohen, 2024).

Buna karşılık, geleneksel yöntemlerin sınırları karmaşık ve erişim güçlüğü arz eden hedeflerde yetersiz kalabilmekte olup, siber operasyonlar bu noktada önemli bir alternatif olarak görülmektedir. Dolayısıyla hem geleneksel hem de siber istihbarat faaliyetleri, ulusal güvenlik politikalarının vazgeçilmez unsurları haline gelmiş, birbirleriyle etkileşimi ve sınırları sürekli olarak yeniden tanımlanmıştır (Lowenthal M. M., 2016). Bu süreçte teknolojik altyapıya ve hukuki çerçeveye uygun hareket etmek, operasyonların başarıyla sonuçlanması açısından önem arz etmektedir.

Araştıma sorusunda belirtildiği üzere hibrit siber saldırılar, geleneksel istihbarat metodlarını değiştirmektedir. Fakat bu tamamen yeni teknolojiler geleneksel istihbaratın yerini almış demek değildir. Çağrı cihazı saldırılarında, insan istihbaratı, karşı istihbarat, paravan şirketler, tedarik zincirine sızma, teknik mühendislik ve uzaktan tetikleme tek bir operasyon içinde bütünleşmiştir.

Çalışmada, nitel vaka analizi yöntemi benimsenmiştir. Örnek olay olarak, Mossad'ın Hizbullah'a yönelik gerçekleştirdiği çağrı cihazı saldırısı seçilmiştir. Bu vakanın tercih edilmesinin nedeni, siber müdahale ile fiziksel sonuç arasındaki doğrudan bağı en çarpıcı şekilde sergileyen yakın dönem istihbarat operasyonu olmasıdır. Veri toplama sürecinde açık kaynak istihbaratı (OSINT) verileri, akademik çalışmalar ve uluslararası güvenlik raporları kullanılmıştır.

Bu çalışma, mevcut literatürden farklı olarak, siber operasyonları sadece bir araç olarak değil, geleneksel istihbaratın ayrılmaz parçası olarak kabul etmekte ve çağrı cihazı saldırısı özelinde siber istihbarat operasyonlarının kavramsal çerçevesini istihbarat disiplinine kazandırmayı

hedeflemektedir. Çalışmanın özgün katkısı, bu tür hibrit saldırıların sadece teknik bir müdahale değil; aynı zamanda geleneksel istihbaratın gizlilik, güvenilirlik ve istihbarat döngüsü aşamalarını nasıl yeniden tanımladığını sistematik olarak ortaya koymasıdır. Böylece, gelecekteki akademik çalışmalara siber istihbarat faaliyetlerinin değerlendirilebilmesine katkı sağlamayı amaçlamaktadır.

Geleneksel İstihbarat ve Siber İstihbaratın Etkileşimi ile Farklılıkları

Modern çatışma ortamında istihbarat disiplini, jeopolitik rekabetin evrimiyle birlikte yapısal bir dönüşüm geçirmektedir. Tarihsel olarak şekillenen geleneksel istihbarat, ulusal güvenliği tehdit eden unsurları tespit etmek için insan istihbaratı (HUMINT), sinyal istihbaratı (SIGINT) ve coğrafi istihbarat (GEOINT) gibi belirli fiziksel ve beşeri kanallara dayanmaktadır (Troy Mattern, 2014). Geleneksel istihbarat faaliyetleri genellikle sınırlı insani ve teknik araçlar kullanarak belirli bölgesel veya ulusal tehditleri tespit etmek ve karşı önlemler geliştirmek amacıyla yürütülmektedir. Bu yöntemler, uzun yıllara dayanan güvenlik geleneklerine dayanmakta olup, genellikle somut istihbarat toplama, insan kaynağıyla operasyonlar ve teknik izleme gibi temel unsurlara odaklanmaktadır (Johnson, 2010).

Siber istihbarat ise modern teknolojinin sunduğu dijital altyapıyı kullanarak gizlilik ve hızlılık avantajı sağlamaktadır (Gioe, 2020). Siber alan, geleneksel yöntemlere kıyasla daha geniş çaplı ve karmaşık tehditleri tespit edip engellemeye imkan tanımakta olup, operasyonların sanal ortamlarda yürütülmesi, fiziksel sınırların ötesine geçme esnekliği sunmaktadır. Geleneksel ve siber istihbarat arasındaki temel farklardan biri, siberin bir “amaç” mı yoksa “araç” mı olduğu tartışmasında yatmaktadır. Mark Lowenthal’a (2020) göre siber, başlı başına yeni bir istihbarat disiplini (INT) değil; tıpkı uydular gibi çeşitli istihbarat türlerini mümkün kılan ve bütün toplama disiplinlerinin ortak paydası olan bir teknolojidir (Austin, 2025).

Bu iki alan arasındaki temel farklar, uygulama biçimleri ve araç setleriyle ilişkilidir. Geleneksel istihbarat genellikle fiziki takip ve iletişim dinleme gibi yöntemlerle çalışırken, siber operasyonlar dijital izleri kullanır ve çok daha hızlı iletişim ve bilgi akışına olanak sağlar. Ayrıca, siber operasyonlar, genellikle anonimlik ve sızma kabiliyetleriyle öne çıkar; bu da geleneksel istihbarat yöntemlerine kıyasla daha az görünür ve daha az doğrudan müdahale gerektirir (Devanny, 2021). Bu bağlamda, siber alanın doğası, geleneksel istihbaratın sınırlarını aşmasına ve yeni nesil tehditlerle karşı karşıya kalmasına neden olmaktadır (Cunliffe, 2021).

Bununla birlikte, her iki yaklaşımın da amaç ve hedefleri benzerdir; ulusal güvenliği sağlamak, potansiyel tehditleri önceden tespit etmek ve karşı önlemler geliştirmektir (Bonfanti, 2018). Ancak, siber operasyonların hızlı gelişimi ve teknolojik karmaşıklıkları, geleneksel yöntemlerin üstünlüklerini ve sınırlarını yeniden sorgulamaya yol açmaktadır. Bu nedenle, modern güvenlik yapıları, her iki alanın entegrasyonunu ve uyumunu sağlayarak, karşı karşıya kalınan tehditlere karşı daha etkili ve esnek stratejiler geliştirmektedir. Birlikte kullanım hem fiziksel hem de dijital tehdit ortamını kapsayan bütünsel bir güvenlik yaklaşımını mümkün kılmaktadır (Kravetz, 2025).

Mossad ve Hizbullah: Tarihsel Gelişmeler ve Operasyonel Bağlamda Önemli Noktalar

Mossad ve Hizbullah arasındaki ilişki, bölgesel güvenlik dinamikleri ve istihbarat faaliyetleri açısından oldukça karmaşık ve köklüdür (Hazbun, 2026). Mossad, İsrail'in istihbarat kurumu olarak, 1949 yılında kurulduktan sonra, bölgedeki güvenlik çıkarlarını koruma ve tehditleri önleme amacıyla çeşitli operasyonlar yürütmüştür. Mossad'ın özellikle Hizbullah ile olan mücadelesi, tarihsel süreç içinde önemli bir yer tutmaktadır. Hizbullah, Lübnan'da 1980'lerin başında özellikle, 1982 İsrail'in Lübnan'ı işgali sonrası Şii direniş hareketi olarak ortaya çıkmış ve hızla bölgesel etkisini artırarak İran tarafından desteklenen güçlü bir yapı haline gelmiştir. İran'ın direniş ekseni doktrininde önemli yer tutan Hizbullah, İran'ın direniş eksenindeki vekil gücüdür (Gök, 2021). "Direniş Ekseni, İran liderliğindeki devlet ve devlet dışı aktörlerin bir koalisyonudur. ABD, İsrail ve müttefiklerine güçlü bir şekilde karşı çıkan aktörlerden oluşur (Cingöz, 2024)." Bu yapının faaliyetleri, İsrail'in güvenliğine doğrudan tehdit teşkil etmektedir ve bu nedenle Mossad'ın askeri ve istihbarat operasyonları bu bölgede yoğunlaşmıştır.

İki taraf arasındaki ilişkiler, zaman zaman gizli operasyonlar ve karşı saldırılar şeklinde seyretmiş; Mossad, Hizbullah'ın hassas bölgelerine sızmayı ve istihbarat toplamayı amaçlayan çeşitli misyonlar gerçekleştirmiştir (Heavy Nala Estriani, 2023). Zaman içerisinde istihbarat mücadelesi sadece bilgi toplama sınırını aşmış, aynı zamanda teknik operasyonlar ve siber saldırılarla yeni bir boyut kazanmıştır (Bonfanti, 2018). Özellikle, Hizbullah'ın iletişim altyapılarına karşı gerçekleştirilen siber operasyonlar ve özel cihazlar kullanımı, karşılıklı gizli savaşların bir parçası olmuştur (Sobelman, 2025). Bu bağlamda, Mossad'ın bölgedeki faaliyetleri, politik ve askeri hesapların yanı sıra teknolojik gelişmeleri de yakından takip ederek, düşman unsurların iletişim ve komuta süreçlerini bozmak üzere tasarlanmıştır.

Sonuç olarak, Mossad ve Hizbullah arasındaki tarihî ve operasyonel bağlam, bölge güvenliği ve istihbarat taktikleri açısından dikkat çekici bir örnek teşkil etmektedir. Her iki taraf da karşı tarafı zayıflatmak adına çeşitli taktiklere ve teknolojik araçlara başvurmuş, bu da bölgedeki çatışmaların sınırlarını hem fiziksel hem de siber alanlarda genişletmiştir. Bu ilişkiler, geleneksel üslerin ötesine geçerek yeni savaş alanlarını ve teknikleri içermekte olup, bölgedeki güç dengelerine yön vermeye devam etmektedir.

Çağrı Cihazı Saldırısının Teknik Özellikleri

Lübnan'da 2024 yılında yaşanan çağrı cihazı patlamaları, siber-fiziksel güvenlik alanında eşi benzeri görülmemiş bir saldırı olarak değerlendirilmektedir. Bu olay, günlük hayatta kullanılan elektronik cihazların fiziksel birer silaha dönüştürülerek toplumsal paniğe ve ciddi zayiatlara yol açabileceğini göstermiştir. Saldırılar, 17 ve 18 Eylül 2024 tarihlerinde iki dalga halinde gerçekleşmiştir. İlk dalgada Hizbullah üyeleri tarafından kullanılan binlerce çağrı cihazı (pager) eş zamanlı olarak patlatılmış; ertesi gün ise ikinci bir dalgada telsizler ve diğer bazı elektronik cihazlar hedef alınmıştır (AlBadawi, 2025) . Olaylar sonucunda 42 kişi hayatını kaybetmiş, 3500'den fazla kişi yaralanmıştır. (C. Sheng, 2024).

2024 Lübnan saldırılarının operasyonel başarısı, geleneksel siber saldırıların ötesine geçerek donanım ve yazılımın eş zamanlı manipüle edildiği karmaşık bir teknik tasarıma dayanmaktadır (Crypto Museum, 2024). Çalışmanın bu kısmında, Hizbullah tarafından kullanılan Gold Apollo AR-924 model çağrı cihazlarının nasıl birer kinetik silaha dönüştürüldüğü açıklanmaya çalışılacaktır. Çağrı cihazı saldırısının tasarımı ve teknik özellikleri, operasyonun başarıyla gerçekleştirilmesi adına detaylı ve hassas mühendislik çalışmaları gerektirmiştir. Bu tür saldırılar genellikle hedefin iletişim altyapısındaki zayıf noktaları istismar ederek, gizlilik ve sızma kabiliyetlerini artırmayı amaçlar. Saldırıda kullanılan çağrı cihazı, sıradan bir iletişim aracından farklı olarak, özel olarak tasarlanmış ve manipüle edilmiş yazılım ve donanım unsurlarını içermektedir (Cohen, 2024). Saldırıda hedef alınan ana donanım, Tayvan merkezli Gold Apollo firmasının lisansıyla üretilen ancak paravan şirketler (BAC Consulting ve Norta Global) aracılığıyla tedarik zincirine sokulan AR-924 model alfanümerik çağrı cihazlarıdır (Sarker, 2025). Teknik incelemeler, bu cihazların standart donanımının milimetrik bir hassasiyetle modifiye edildiğini ortaya koymuştur:

Batarya Modifikasyonu: Cihazların içerisine yerleştirilen LI-BT783 model özel tasarım lityum-iyon bataryaların katmanları arasına, yaklaşık 3 ila 6 gram miktarında askeri sınıf PETN (Pentaeritritol tetranitrat) patlayıcı dolgusu yerleştirilmiştir (Crypto Museum, 2024).

Fiziksel Gizleme: Patlayıcı düzeneği, standart X-ray taramaları veya görsel denetimlerle fark edilemeyecek şekilde batarya ünitesinin içine ve Koruma Devre Modülü (PCM) ile entegre biçimde gizlenmiştir. PETN gibi plastik patlayıcıların düşük atom numarası, yoğunluk tabanlı tarama sistemlerinde kontrast farkı yaratmayarak tespit edilmesini neredeyse imkansız kılmıştır (Crypto Museum, 2024).

Teknik anlamda, cihazın tasarımında minimal bileşen kullanımı ve yüksek taşınırlık ön plandadır. Çalışma esnasında fark edilme riskini azaltmak adına, düşük güç tüketimi ve sessiz iletişim modları tercih edilmiştir. Ayrıca, saldırıda kullanılan çağrı cihazı, şifrelenmiş ve anlık veri aktarım yeteneklerine sahip olacak şekilde geliştirilmiştir. Aynı zamanda, cihazın uzaktan kontrol edilebilmesi ve güncellenebilmesi, operasyonel esneklik sağlamaktadır (AlBadawi, 2025).

Saldırıda kullanılan cihazların üretiminde yüksek uzmanlık seviyeleri ve özel malzemeler kullanılır. Bu malzemeler, gizlilik ve dayanıklılık açısından yüksek standartlara sahiptir. Ayrıca, iletişim sırasında oluşturulan sinyallerin tespiti ve engellenmesi için anti-dinleme ve anti-tespit mekanizmaları entegre edilmiştir. Bu teknik özellikler, operasyonun ileri düzey elektronik karıştırma ve müdahale teknikleriyle desteklenmesini mümkün kılar (Sarker, 2025). Sonuç olarak, çağrı cihazı saldırısının tasarımı ve teknik bileşenleri, hedef alınan yapıda ciddi hasarlara yol açmıştır. Elektronik cihazların da fiziksel bir silaha dönüşebileceği gerçeği, siber güvenlik ve istihbarat alanında son derece önemli bir gelişme olmuştur.

Çağrı cihazı operasyonu yalnızca bir siber saldırı değildir; insan istihbaratı, hedef analizi, aldatma, tedarik zincirine sızma, donanım manipülasyonu ve fiziksel sabotajın bütünleştiği hibrit bir istihbarat operasyonudur.

Sorunlar ve Sınırlılıklar

Eylül 2024'te Lübnan'da yaşanan çağrı cihazı patlamaları, modern güvenlik anlayışlarının bilgi temellerini ve teknolojik aletlerin özne-nesne ilişkisi içindeki yerini köklü bir biçimde sorgulayan, karmaşık ve çok taraflı bir kriz olarak tanımlanmaktadır. Bu olayı besleyen en derin teknik ve sistemik sorun, küresel üretim sistemlerinin giderek daha fazla modüler hale gelmesi ve coğrafi olarak dağılmış alt yüklenici ağlarına bağlanmasıyla ortaya çıkan tedarik

zincirinde kontrol dengesizliğidir. Çünkü günümüz üretim ortamlarında tasarım, prototip oluşturma, parça tedariki, montaj ve lojistik süreçleri arasındaki neden-sonuç bağı, araya giren çok katmanlı taşeron ilişkileri yüzünden giderek daha belirsiz bir hale gelmekte; bu da kontrol mekanizmalarının etkisizleşmesine ve ulusal güvenlik açısından önemli olan teknolojik ürünlerin bütünlüğünün doğrulanamamasına neden olmaktadır (Buchar, 2024). Bu durum, geleneksel siber güvenlik yaklaşımlarının sadece yazılım tehditlerine odaklanan dar kapsamını aşarak, donanım düzeyinde ve üretim aşamasında önleyici müdahaleyi zorunlu kılan yeni bir güvenlik anlayışının inşasını gündeme getirmektedir.

Operasyonel riskler arasında yanlış hedefleme, siber saldırının yayılması ve beklenmedik sonuçların ortaya çıkması yer alır. Yanlış tespitler, hassas bölgelerde sivil altyapıyı veya masum bireyleri hedef alma riski taşır; bu da hem etik hem de hukuki açıdan ciddi sorunlara yol açar. Ayrıca, siber saldırıların izlerinin kaybolması veya saldırganın kimliğinin tespiti zorluğu, operasyonun sürdürülebilirliğini ve sorumluluğun belirlenmesini güçleştirir (Kravetz, 2025).

Sonuç

Geleneksel istihbarat ve siber operasyonlar arasındaki sınırların belirsizliği, modern güvenlik ortamında yeni bir anlayış gerektirmiştir. Bu bağlamda, teknik ve operasyonel yaklaşımların entegrasyonu, istihbarat toplama ve müdahale süreçlerinde artan bir önem kazanmıştır. Mossad'ın Hizbullah'a karşı yürüttüğü çağrı cihazı saldırısı, bu entegrasyonun somut bir örneğini teşkil etmektedir. Bu operasyon hem geleneksel yöntemlerin hem de siber araçların kullanılmasıyla, bilgi edinme ve karşı tarafın iletişim altyapısını hedef alma açısından yeni standartlar belirlemiştir. Saldırının tasarımında, yüksek hassasiyetli teknikler ve detaylı planlamalar öne çıkarken, operasyonun başarısı risk yönetimi ve uyum konularında dikkatli bir denge kurulmasını zorunlu kılmıştır. Güvenlik önlemleri ve savunma stratejilerinin geliştirilmesi ise, olası saldırıların önünü kesmek ve ulusal çıkarları korumak amacıyla sürekli güncellenen bir süreçtir. Sonuç olarak, geleneksel istihbaratın sınırlarını genişleten ve siber alanın sunduğu imkanları en iyi şekilde kullanan operasyonlar, modern güvenlik paradigmasının temel unsurlarını oluşturmaktadır. Bu gelişmeler hem ulusal hem de uluslararası güvenlik ortamında yeni denge ve dengeli politikaların tesis edilmesine ihtiyaç olduğunu göstermektedir.

Çalışmanın temel bulguları, Mossad'ın Hizbullah'a yönelik çağrı cihazı saldırısı özelinde, hibrit operasyonların iki stratejik sonuç doğurduğunu göstermektedir. Tedarik zincirinin

yalnızca bir lojistik unsur değil, doğrudan operasyonel bir silah olarak kullanılabileceğini, siber müdahale ile geleneksel insan istihbaratının iç içe geçmesinin, stratejik etkisini artırdığını kanıtlamıştır.

Çalışma tek bir vaka analizine (Mossad-Hizbullah çağrı cihazı saldırısı) dayanmakta olup, operasyonun perde arkasındaki istihbarat karar alma süreçlerine ve gizli teknik detaylara doğrudan erişim imkânı bulunmadığından, bulgular büyük ölçüde açık kaynak verileri, güvenlik raporları ve ikincil literatürle sınırlıdır. Netice olarak, geleneksel istihbaratın sınırlarını genişleten ve siber alanın sunduğu imkanları birleştiren operasyonlar, modern güvenlik anlayışının önemli parçalarını oluşturmaktadır; bu gelişmeler hem ulusal hem de uluslararası güvenlik ortamında yeni denge ve dengeli politikaların kurulması ihtiyacını zorunlu kılmaktadır.

Kaynakça

AlBadawi, Habib. "Hezbollah's Military Setback: From Strategic Strength to Political Dilemma—A Comprehensive Analysis." *The Journal of Social Encounters* 9.2 (2025): 107-123.

Austin, J. (2025). Exploring the Evolution of Cyber Intelligence (CYINT): A Disciplinary Debate and Practical Implications. National Intelligence University - Intelligence Studies Summit 2025.

Bonfanti, M. E. (2018). Cyber Intelligence: in pursuit of a better understanding for an emerging practice. *Cyber, Intelligence, and Security*, 2(1), 105-121.

Buchar, J. (2024). Lessons from exploding pagers in Lebanon: The West must protect its supply chains. Defense Magazine. Retrieved from: https://www.defensemagazine.com/ (Accessed time: 10 July 2026)

Sheng, C., Ma, W., Han, Q. L., Zhou, W., Zhu, X., Wen, S., ... & Wang, F. Y. (2024). Pager explosion: Cybersecurity insights and afterthoughts. *IEEE/CAA Journal of Automatica Sinica*, 11(12), 2359-2362.

Cingöz, M., Özkan, F., Alkan, Y. S., & İzol, R. (2024). Iran's axis of resistance through the lens of ontological security. *Third World Quarterly*, 45(13), 1963-1980.

Cohen, A. &. (2024). “Well, it depends”: The explosive pagers attack revisited. Lieber Institute West Point. Retrieved from: https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/ (Accessed Time: 10 July 2026)

Crypto Museum. (2024). Retrieved from: https://www.cryptomuseum.com/covert/radio/apollo/ar924/ (Accessed Time: 03 July 2026)

Cunliffe, K. S. (2021). Hard target espionage in the information era: new challenges for the second oldest profession. Intelligence and National Security, 36(7), 1018-1034.

Daricili, A. B., & Erendor, M. E. (2021). The cyber security strategy of Israel. *Voprosy Istorii,* *11*(3), 233–246.

Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy,* 6(3), 429-450.

Gioe, D. V., Goodman, M. S., & Stevens, T. (2020). Intelligence in the cyber era: Evolution or revolution?. *Political Science Quarterly,* 135(2), 191-224.

Gök, A. (2021). Vekâlet Savaşlarında İstihbarat Örgütlerinin Rolü: Kudüs Gücü Örneği. *Ekonomi Politika ve Finans Araştırmaları Dergisi*, 6(3), 728-747.

Hazbun, W. (2026). Israel, the Axis of Resistance, and the end of deterrence. Project on Middle East Political Science. Retrieved from: https://pomeps.org/israel-the-axis-of-resistance-and-the-end-of-deterrence (Accessed Time: 02 July 2026)

Estriani, H. N., Dewanto, P. A., & Asyidiqi, H. (2023). Asymmetric and Hybrid Warfare in Postmodern Times: Lesson from Hezbollah-Israeli War 2006. *Andalas Journal of International Studies (AJIS),* 12(1), 27-37.

Johnson, L. (2010). Evaluating “Humint”: The role of foreign agents in US security. *Comparative Strategy*, 29(4), 308-332.

Kravetz MSc, J. R. (2025). The Cyber Deterrence Dilemma: Parallels Between Cyber and Intelligence Special Operations. *Joint Force Quarterly*, 119(4), 72-81.

Lowenthal, M. M., & Clark, R. M. (Eds.). (2015). The five disciplines of intelligence collection. Sage.

Lowenthal, M. M. (2025). Intelligence: From secrets to policy. CQ press.

Force, C. I. T. (2013). Operational levels of cyber intelligence. The Intelligence and National Security Alliance (INSA), Tech. Rep, 9.

Sarker, P. P. (2025). When everyday devices become weapons: A closer look at the pager and walkie-talkie attacks. arXiv preprint arXiv:2501.17405.

Sobelman, D. (2025). Axis of Resistance: Asymmetric deterrence and rules of the game in contemporary Middle East conflicts. SUNY Press.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, 27(4), 702-719