GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 415-447
DOI: 10.17752/guvenlikstrtj.1695757

Araştırma Makalesi
Research Article

Çağrı Cihazı Saldırıları Sonrası Siber Tehdit İstihbaratı için Yeni Bir Perspektif ve Model Önerisi

A New Perspective and Model Proposal for Cyber Threat Intelligence after Pager Attacks

Tuncay DOĞANTUNA*

Onur CERAN**

* Doktora Öğrencisi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Ana Bilim Dalı (Disiplinlerarası), Ankara, Türkiye, e-posta: tidituna@gmail.com
ORCID: 0000-0003-4135-7690

** Dr. Öğr. Üyesi, Gazi Üniversitesi, Uygulamalı Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Ankara, Türkiye, e-posta: onur.ceran@gazi.edu.tr
ORCID: 0000-0003-2147-0506

Geliş Tarihi / Submitted: 09.05.2025

Kabul Tarihi / Accepted: 13.11.2025

Öz

Bu çalışma, hibrit savaş çerçevesinde Siber Tehdit İstihbaratı (CTI) için genişletilmiş bir model önermek amacıyla, Eylül 2024'te Hizbullah'a yapılan çağrı cihazı saldırılarını bir vaka çalışması olarak incelemektedir. Son derece koordineli bir İsrail operasyonuna atfedilen saldırı, yalnızca siber unsurları değil, aynı zamanda Elektronik Harp (EH), Sinyal İstihbaratı (SIGINT) ve manipüle edilmiş tedarik zincirlerini de içermektedir. Binlerce çağrı cihazı ve telsizin senkronize bir şekilde patlatılmasıyla göze çarpan olay, kinetik ve siber yeteneklerin entegrasyonuna örnek teşkil ederek geleneksel tehdit istihbaratı modellerine meydan okumaktadır. Araştırma, MITRE ATT&CK (Rakip Taktikler, Teknikler ve Genel Bilgi) çerçevesinin mevcut sınırlamalarını, özellikle Radyo Frekansı (RF) tabanlı ve analog hedefli saldırıları yeterli şekilde yakalayamamasını eleştirmektedir. Buna karşılık, EH ve SIGINT kaynaklı tehditleri daha iyi temsil etmeyi amaçlayan iki yeni teknik önermektedir: "Spektrum Tabanlı Sinyal Enjeksiyonu" ve "RF Mesaj Enjeksiyonu ve Manipülasyonu". İyileştirme stratejileri, RF anomali tespiti, güvenli haberleşme protokolleri ve entegre SIGINT olay müdahalesini içerir. Çalışma, modern çatışmalarda düşük teknolojili cihazların güvenlik açıklarının ve tedarik zinciri zafiyetlerinin stratejik kullanımını vurgulayarak fiziksel ve dijital savaş arasındaki bulanık sınırları inceler. RF değişkenli vektörleri CTI çerçevelerine entegre eden önerilen model, hibrit tehditleri tespit ve önlemek için daha kapsamlı bir yaklaşım sunabilir, dijital çağda tehdit istihbaratını ve savunma politikasını yeniden şekillendirir.

Anahtar Kelimeler: Elektronik Harp, RF, Siber Tehdit İstihbaratı, Sinyal İstihbaratı, Tedarik Zinciri

Abstract

This study explores the September 2024 pager attacks on Hezbollah as a case study to propose an expanded model for Cyber Threat Intelligence (CTI) within the framework of hybrid warfare. Attributed to a highly coordinated Israeli operation, the attack involved not only cyber elements but also Electronic Warfare (EW), Signals Intelligence (SIGINT), and manipulated supply chains. The incident marked by the synchronized detonation of thousands of pagers and radios exemplifies the integration of kinetic and cyber capabilities, challenging conventional threat intelligence models. The research critiques the current limitations of the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, especially its inability to adequately capture Radio Frequency (RF)-based and analog-targeted attacks. In response, it proposes two new techniques: "Spectrum-Based Signal Injection" and "RF Message Injection & Manipulation", aiming to better represent EW and SIGINT-driven threats. Mitigation strategies include RF anomaly detection, secure communication protocols, and integrated SIGINT incident response. The study investigates the strategic use of low-tech device vulnerabilities and supply chain compromises in modern conflicts, highlighting the blurred boundaries between physical and digital warfare. Integrating RF variable vectors into CTI frameworks, the proposed model may offer a more comprehensive approach to detect and prevent hybrid threats, reshaping threat intelligence and defense policy in the digital age.

Keywords: Cyber Threat Intelligence, Electronic Warfare, RF, Signal Intelligence, Supply Chain

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License.

Extended Summary

This study examines the sophisticated pager attacks as a case study to propose a new perspective and model for cyber threat intelligence within the context of hybrid warfare. It analyzes how Electronic Warfare (EW), including Signals Intelligence (SIGINT) and Radio Frequency (RF) capabilities, can be integrated with cyber threats. The research investigates the exploitation of supply chain security and the complexity of these attacks, proposing a model based on the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework to better detect RF and EW-based attack traces. The aim is to bridge digital and physical security, expanding threat intelligence and enabling more proactive defense strategies. The proposed methodology, using an expanded MITRE ATT&CK matrix, seeks to enhance attack analysis and prevention for hybrid threats. This approach aims to reshape threat intelligence and security policies in cyber and electronic warfare, promoting proactive threat hunting.

The impetus for the study is the simultaneous detonation of thousands of pagers and radios used by Hezbollah in Lebanon and Syria in September 2024, attributed to an Israeli operation. While initially speculated as purely cyber, expert analysis suggests a broader involvement of electronic warfare, signal intelligence, supply chain security, and intelligence operations. The experts also compare the incident to the Stuxnet attack, which demonstrated the vulnerability of critical infrastructure even in the presence of air gaps. A key research question is whether Cyber Threat Intelligence (CTI) or MITRE ATT&CK could have detected such an attack beforehand. Investigative reports indicate a sophisticated Mossad operation involving explosives placed in pager batteries and introduced via manipulated supply chains. This highlights the strategic use of intelligence and technology, leveraging Hezbollah's shift to pagers. The pager attack underscores the instrumentalization of intelligence in asymmetrical warfare and the need for interdisciplinary approaches combining EW, SIGINT, and cyber-attack vectors. The study addresses how these elements can be integrated into threat intelligence frameworks and how physical operation preparations related to EW and supply chains can be incorporated into the MITRE ATT&CK framework.

The study defines key terms: Cyber Threat Intelligence (CTI) for predicting and neutralizing digital threats, Cyber Intelligence for strategic and operational information gathering in the digital realm, MITRE ATT&CK as a knowledge base for adversary tactics and techniques, Supply Chain Security for protecting against risks within the supply chain, Signal Intelligence (SIGINT) for intelligence from electronic communications, Electronic Warfare (EW) for military activities using the electromagnetic spectrum, Intelligence for information gathering and analysis for national security, and Covert Operations as clandestine state activities.

The literature review examines the pager attack as a case study, emphasizing the need to understand adversary TTPs (Tactics, Techniques & Procedures) and adapt security practices beyond standard frameworks. It highlights the supply chain as a key vulnerability and the need for better security in connected and even low-tech devices. It also discusses the importance of threat-informed defense, social engineering, insider threats, and integrating creativity with threat intelligence. The attack is considered a paradigm shift in cyber-physical warfare, blurring the lines between cyber and kinetic domains and demonstrating the weaponization of everyday objects.

The study analyzes the existing MITRE ATT&CK framework, noting that although it includes supply chain compromise techniques, these are primarily oriented towards

traditional IT platforms. The ICS matrix offers a more relevant, though less detailed, technique. The study argues that the current framework is insufficient to fully capture the nuances of attacks featuring significant RF and EW components targeted at analog or hybrid systems. To address this gap, the study proposes new techniques within the MITRE ATT&CK framework. The first, "T1569.xx – Spectrum-Based Signal Injection" under the "Execution" tactic, describes injecting fake messages into pager networks. Mitigation techniques include encryption, digital signatures, RF anomaly detection, and multi-factor authentication. The second proposed technique, "T1602.xx – RF Message Injection & Manipulation" under the "Impact" tactic, focuses on targeting RF-based analog or hybrid communication systems using EW and SIGINT capabilities to inject or manipulate messages or disrupt communication. Mitigation strategies involve secure communication protocols, RF signal filtering, FHSS/LFM (Frequency Hopping Spread Spectrum / Linear Frequency Modulation) usage, multi-layered authentication, and integrated SIGINT/incident response teams.

The discussion emphasizes how the pager operation demonstrates the strategic integration of EW, SIGINT, and supply chain attacks. It highlights the multi-layered planning and the blurring boundaries between digital and traditional military operations. It also underscores the vulnerability of low-tech devices and the weaponization of supply chains. The study concludes that the MITRE ATT&CK framework needs to evolve to include techniques for manipulating and tampering with both digital and analog devices. The synchronized pager explosions likely involved complex engineering with RF signals and firmware manipulation due to the devices' lack of modern security features. The security analysis recognizes that hybrid threats blur the lines between EW and cyber, highlighting the necessity of integrating RF and EW-based threats into threat intelligence. However, directly mapping these to existing MITRE ATT&CK tactics might be challenging. The proposed models aim to integrate these aspects without disrupting the framework's functionality. A limitation acknowledged is the potential ineffectiveness against sophisticated state-sponsored intelligence operations.

In conclusion, this study provides a strategic perspective on hybrid warfare in cybersecurity, analyzing the integration of electronic warfare and cyber threats. It proposes a model based on MITRE ATT&CK to better detect supply chain attacks involving RF and EW techniques. The suggested model promotes new methodologies for predicting and preventing future hybrid threats. Integrating RF and EW-based attack categories offers a more comprehensive threat analysis, bridging digital and physical security. This approach can reshape security policies and enhance proactive threat hunting. The Pager attack serves as a clear example of the blurred lines between cyber and kinetic operations in a hybrid threat environment.

Giriş

17 ve 18 Eylül 2024 tarihlerinde, Hizbullah tarafından kullanımda olan binlerce çağrı cihazı ve yüzlerce telsiz, İsrail'in saldırısı sonucu Lübnan ve Suriye'de eş zamanlı olarak patlatılmış ve akabinde kamuoyunun gündeminde günlerce yer almıştır. Bu saldırıların bazı kaynaklar tarafından siber saldırı teknikleri aracılığıyla gerçekleştirilmiş olduğu iddia edilmiştir.[1] Ancak saldırıların arka planı çeşitli teknik forum ve profesyonel sosyal ağlarda ele alındığında, birçok farklı uzmanın baskın görüşü "sadece siber saldırı teknikleriyle patlamanın

1 Twitter (X), https://x.com/hashtag/pagerexplosions?src=hashtag_click, erişim 19.09.2024.; LinkedIn, https://www.linkedin.com/search/results/all/?keywords=%23pagerexplosion&origin=HASH_TAG_FROM_FEED&sid=Q3u, erişim 20.09.2024.

gerçekleştirildiği*"* argümanı, çok zayıf bir ihtimale indirgenmiştir.[2] Vakanın ilk ortaya çıktığı andan, en son belirgin hale geldiği kritik noktaya kadar geçen süreçte sadece siber güvenlik veya siber istihbarat değil, aynı zamanda "Elektronik Harp", "Sinyal İstihbaratı", "Tedarik Zinciri Güvenliği" ve "İstihbarat Operasyonu" gibi çeşitli benzer disiplinlerin vaka özelinde dahli olduğu değerlendirilmektedir. Dolayısıyla bu saldırılar, devletlerin ve devlet dışı aktörlerin konvansiyonel ve gayrinizami yöntemleri nasıl entegre edebileceğini, teknolojiyi nasıl bir güç çarpanı olarak kullandığını ve bu tür eylemlerin bölgesel güvenlik dinamikleri ile uluslararası normlar üzerindeki potansiyel etkilerini gözler önüne sermektedir.

Lübnan'da Hizbullah'a karşı gerçekleştirilen çağrı cihazları saldırısı gibi spesifik ve planlı bir saldırı operasyonu, 2010 yılında İran'ın nükleer programını sekteye uğratmak amacıyla İsrail tarafından StuxNet zararlı yazılımı aracılığıyla gerçekleştirilen başka bir operasyonu hatırlatmaktadır.[3] O dönemki StuxNet zararlı yazılımıyla gerçekleşen siber saldırı, siber uzaydaki güvenliğin dönüşümü için bir dönüm noktası sayılmaktaydı.[4] Çünkü Stuxnet, kritik altyapıyı yöneten bilgisayar sistemlerine yönelik saldırıların en gelişmiş ve önemli ilk örneklerinden birisi konumundadır. SCADA (Supervisory Control and Data Acquisition – Denetleyici Kontrol ve Veri Toplama) sistemlerinin doğrudan internete bağlı olmamaları, yani bir hava boşluğu (*air gap*) ile izole edilmeleri, uzun süre siber saldırılara karşı koruma sağladığı düşünülen bir önlem olarak kabul edilmiştir. Ancak Stuxnet, bu inanışı kökten sarsarak, fiziksel altyapının internet bağlantısından ayrılmasının tek başına yeterli bir güvenlik tedbiri olmadığını ortaya koymuştur. Özellikle kritik altyapıların siber güvenliği, Stuxnet saldırısının ardından, nükleer emniyetin sürekliliğini sağlamak açısından kritik bir önem arz eder hale gelmiştir.[5]

Lübnan'daki çağrı cihazları saldırısının hangi aşamasında siber saldırı tekniklerinin yer aldığı veya yer almış olup olmadığı bu çalışmanın devam ettiği tarih itibarıyla kesin bir netlik kazanmamış durumdadır. Bu açıdan saldırının herhangi bir aşamasında siber saldırı tekniklerinin yer aldığını varsaydığımızda, ilgili teknik ya da taktiklere veyahut saldırı hazırlığına ilişkin emarelere siber uzayda rast gelip gelmeyeceği, bu çalışmanın araştırma sorusunu temellendirmektedir. Siber uzayda saldırıları tasnifleyerek hangi saldırının hangi APT (*Advanced Persistent Threat* – Gelişmiş Kalıcı Tehdit) grubuyla ilişkili olduğunu etiketleyen MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge* – Rakip Taktikler, Teknikler ve Genel Bilgi) Çerçevesi, siber güvenlik profesyonelleri tarafından çokça başvurulan bir başucu kaynağına dönüşmüştür. Özellikle de Rus, Çin, İran ve Kuzey Kore devlet destekli APT grupları, bu çerçeve ve Siber Tehdit İstihbaratı (CTI) kapsamında tasnif edilmekte ve incelenmektedir.[6] Benzer durumu İsrail'in Mossad veya Unit 8200 örgütleri tarafından gerçekleştirildiği iddia edilen çağrı cihazı saldırılarına uyarlarsak, CTI teknikleri veya MITRE ATT&CK Çerçevesi ile bu saldırıları, öncesinde tespit etmenin mümkün olup olmayacağı hususunun altını çizmek gerekecektir.

Saldırıların ardından yaklaşık bir ay geçtikten sonra, dikkat çekici bir araştırma gazeteciliği yayını Reuters tarafından 16 Ekim 2024 tarihinde yayınlanmıştır.[7] Araştırma

2 Reddit, https://www.reddit.com/r/geopolitics/comments/1fjnx3y/israel_planted_explosives_in_5000_hezbollah/, erişim 19.09.2024.; Medium, https://medium.com/search?q=%23pagerexplosion, erişim 20.09.2024.

3 Ekonomi ve Dış Politika Araştırmalar Merkezi, "Nükleer Tesislerin Siber Güvenliğine Giriş", *Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM)*, 20 Nisan 2016, https://edam.org.tr/siber-politikalar-ve-dijital-demokrasi/nukleer-tesislerin-siber-guvenligine-giris, erişim 01.02.2025.

4 IEEE Spectrum, "The Real Story of Stuxnet", *IEEE Spectrum*, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet, erişim 01.02.2025.

5 Ekonomi ve Dış Politika Araştırmalar Merkezi, "Nükleer Tesislerin Siber Güvenliğine Giriş", s. 104.

6 MITRE, "MITRE ATT&CK Groups", https://attack.mitre.org/groups/, erişim 05.01.2025.

7 Maya Gebeily, James Pearson ve David Gauthier-Villars, "How Israel's bulky pager fooled Hezbollah", *Reuters Graphics*, 16 Ekim 2024, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/, erişim 17.10.2024.

haberi, saldırıya ilişkin olarak birçok uzmanın argümanını destekler nitelikte bulgular ortaya koymaktadır. Haberde Lübnan'ın güneyindeki Beyrut ve diğer Hizbullah kalelerinde, binlerce çağrı cihazının eşzamanlı olarak patlaması, İsrail istihbarat servisi Mossad'ın Hizbullah'a yönelik sofistike bir operasyonunun sonucu olduğu belirtilmiştir. Ayrıca çağrı cihazlarının pillerine, X-ray cihazları tarafından tespit edilemeyen plastik patlayıcılar ve yenilikçi ateşleyicilerin yerleştirildiği ve bu cihazların sahte çevrimiçi mağazalar ve uydurma geçmişlerle desteklenerek Hizbullah'ın güvenlik kontrolleri atlatıldığı ifade edilmiştir. Bu olayın İsrail'in Hizbullah'a karşı istihbarat ve teknoloji kullanarak gerçekleştirdiği karmaşık operasyonların bir örneği olduğuna dikkat çekilmektedir. Hizbullah'ın cep telefonu iletişiminin İsrail tarafından dinlenildiğini fark ederek çağrı cihazlarına geçmesi, bu operasyonun planlama aşaması için etkili olduğu değerlendirilmektedir.[8]

Lübnan'da Hizbullah üyelerine yönelik gerçekleştirilen çağrı cihazları ve telsizlerin patlatılmasıyla sonuçlanan saldırılar özelinde basına yansıyan diğer bir kritik haber ise CBS televizyonuna konuşan iki eski Mossad ajanının açıklamaları üzerinden ortaya çıkmıştır.[9] Bu saldırıların operasyonel boyutunu ve planlama süreçlerini gözler önüne seren haberde, ajanların ifadelerine göre, saldırılar on yıllık bir stratejik planlama sürecinin ürünü olduğu ve cihazlara yerleştirilen patlayıcıların İsrail'de üretildiği belirtilmiştir.[10] İlgili operasyonda, Mossad'ın sahte şirketler aracılığıyla Hizbullah üyelerine cihaz tedarik ettiği ve bu cihazlara yalnızca kullanıcıya zarar verecek miktarda patlayıcı yerleştirdiği bildirilmiştir.[11] Özellikle göğse yakın taşınan telsizler ve çağrı cihazları seçilerek, patlamaların etkinliğinin arttırıldığı, operasyonun Tayvan merkezli Gold Apollo gibi gerçek şirketler kullanılarak maskelendiği ve reklam stratejileri ile hedef grupların bu cihazları tercih etmesinin sağlandığı aktarılmıştır. Ajanların açıklamaları, söz konusu operasyonun, İsrail istihbaratının karmaşık paravan ağlar oluşturmadaki yetkinliğini sergilediğini ortaya koymaktadır.[12]

Saldırılar, asimetrik savaş bağlamında istihbaratın araçsallaştırılmasını ve bunun uluslararası hukuktaki sonuçlarını ele alan literatür için önemli bir vaka çalışma ortamı sunmaktadır. Asimetrik bir savaşta hibrit saldırı teknik ve taktiklerinin uygulanabilmesi için "Elektronik Harp", "Sinyal İstihbaratı" ve "Siber Atak Vektörleri" gibi unsurların ve kabiliyetlerin nasıl uyumlu bir biçimde kullanıldığı araştırmacılar için ilgi ve merak uyandırıcı olmaya devam etmektedir. Bu açıdan, klasik elektronik harp ve sinyal istihbaratı taktiklerinin, modern siber saldırı teknikleriyle bir arada kullanılması, stratejik kazanımlar açısından karar vericilerin dikkatini bu alana çekmektedir. Ancak ortaya çıkan bilgilere ve kanıtlara göre, bu vakayı sadece tek başına elektronik, sinyal veya siber tekniklerle ilişkilendirmek hatalı bir yaklaşım olacaktır. Bu noktada süreci daha iyi anlamak adına bu çalışmada, aşağıda geçen araştırma sorularına cevap aranmaktadır:

1. Tehdit İstihbaratının hibrit savaşlarda kullanımı açısından Elektronik Harp (EH), Sinyal İstihbaratı (SIGINT) ve fiziksel müdahaleler, bir bütün olarak siber tehditlerle birlikte nasıl değerlendirilebilir?

8 Age.
9 Lesley Stahl, "Israel's spy agency, Mossad, spent years orchestrating Hezbollah walkie-talkie, pager plots", *CBS News*, 22 Aralık 2024, https://www.cbsnews.com/news/israeli-mossad-pager-walkie-talkie-hezbollah-plot-60-minutes/, erişim 06.01.2025.
10 Age.
11 Lesley Stahl, "Former Mossad Agents Detail Explosive Pagers, Hezbollah Terrorists Plot - 60 Minutes Transcript", *CBS News*, 8 Haziran 2025, https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/, erişim 09.06.2025.
12 İkbal Muhammet Arslan, "BM: Lübnan ve Suriye'de Eş Zamanlı Çağrı Cihazı Patlamaları Şok Edici", *Anadolu Ajansı (AA)*, 18 Eylül 2024, https://www.aa.com.tr/tr/dunya/bm-lubnan-ve-suriyede-es-zamanli-cagri-cihazi-patlamalari-sok-edici/3333807, erişim 07.01.2025.

2. MITRE ATT&CK çerçevesi, elektromanyetik spektrum ve tedarik zinciri güvenliği boyutları eklenerek nasıl genişletilebilir?
3. Bu genişletme ulusal güvenlik politikaları için ne tür stratejik/politik çıkarımlar üretir?

Bu çalışmanın katkısı iki düzeydedir. Birinci olarak "Çağrı Cihazı" saldırılarındaki vakadan yola çıkarak siber güvenlikte hibrit savaş konseptine yönelik stratejik bir bakış açısı sunmayı ve elektronik harp (SIGINT ve RF dahil) ile siber tehditlerin birlikte değerlendirilmesinin sağlanmasını hedeflemektedir. Bu kapsamda, MITRE ATT&CK çerçevesine tedarik zincirinin güvenliğine yönelik istismarı incelenerek, benzer saldırıların izlerinin tespit edilmesine yönelik bir modeli ortaya koyulacaktır. Bu bağlamda çalışma, MITRE ATT&CK çerçevesi içerisinde mevcutta yer alan tedarik zinciri güvenliğinin yanında ilave teknik tedbirlere dair bir model sunmayı hedeflemektedir. Tehdit istihbaratının geleneksel sınırlarını genişleterek, Elektronik Harp (SIGINT ve RF) tekniklerini de kapsayacak bir perspektif ortaya koyacaktır. İkinci olarak bu teknikleri ulusal güç, kurumsal dayanıklılık ve psikolojik etki katmanlarında politik/stratejik önerilerle ilişkilendirerek hibrit tehditlere disiplinler arası bir yanıt sunmaktadır.

1. Kavramsal Çerçeve

Bu bölümde konunun anlaşılması için gerekli kavramsal çerçeve sunulacaktır.

1.1. Hibrit Savaş

Hibrit savaş, savaşın ve savaş yöntemlerinin farklı seviyelerde, farklı alanlarda ve etki sahalarında, özellikle bilişsel ve moral etki sahalarında, çeşitli aktörlerin bir araya gelerek belirli bir zaman ve mekân düzenlemesiyle, savaşın tüm seviyelerinde hedeflere ulaşmayı amaçlayan, çeşitli yöntem ve teorilerin birleşimidir.[13] Bir devletin veya devlet dışı aktörün, stratejik hedeflerine ulaşmak amacıyla askerî ve gayriaskerî araçları (örneğin, konvansiyonel askerî operasyonlar, düzensiz harp taktikleri, siber saldırılar, dezenformasyon kampanyaları, ekonomik baskı, diplomatik manevralar ve örtülü operasyonlar) eş zamanlı ve senkronize bir şekilde kullandığı karmaşık çatışma türüdür.[14] Hibrit savaşın temel özelliği, belirsizliği arttırarak, sorumluluğu gizleyerek ve hasmın karar alma süreçlerini felç ederek avantaj sağlamaktır. Lübnan'daki çağrı cihazı saldırıları gibi olaylar, konvansiyonel olmayan yöntemlerin, istihbarat operasyonlarının ve teknolojik zafiyetlerin hibrit savaş konsepti içinde nasıl etkin bir şekilde kullanılabileceğine dair önemli bir örnek teşkil etmektedir.

1.2. Siber Güvenlik

Siber güvenlik, ulusal güvenliğin sağlanmasında kritik bir kuvvet çarpanı olarak kabul edilmektedir. Siber güvenlik sadece teknik bir disiplin olmanın ötesinde, bir ülkenin kritik altyapılarının (enerji, iletişim, finans ve sağlık gibi) korunması, devlet kurumlarının işleyişinin devamlılığı, ekonomik istikrarın sürdürülmesi ve toplumsal düzenin muhafazası için hayati öneme sahiptir. Siber uzaydaki tehditlerin artması ve çeşitlenmesi, devletleri siber savunma kapasitelerini geliştirmeye, ulusal siber güvenlik stratejileri oluşturmaya ve siber olaylara müdahale yeteneklerini arttırmaya yöneltmektedir.[15] Güçlü bir siber güvenlik

13 Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, School of Advanced Military Studies, United States Army Command and General Staff College, 2009, s. 8-10.

14 Erik Reichborn-Kjennerud ve Patrick Cullen, *What is Hybrid Warfare?*, Norwegian Institute for International Affairs (NUPI), 2022, s. 1-4.

15 Solange Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture", *2010 International Conference on Availability, Reliability and Security*, IEEE, Şubat 2010, s. 370-373.

altyapısı, bir ülkenin caydırıcılığını arttırır, operasyonel üstünlük sağlar ve hibrit tehditlere karşı direncini yükseltir.[16] İnsanların psikolojik zafiyetlerinden, güven eğilimlerinden veya dikkatsizliklerinden faydalanarak gizli bilgilere erişmek, belirli eylemleri gerçekleştirmelerini sağlamak veya güvenlik sistemlerini atlatmak amacıyla gerçekleştirilen manipülasyon tekniklerinin bütünü olarak tanımlanabilen sosyal mühendislik saldırıları da hibrit savaşta ön alınması gereken unsurlar arasında yer almaktadır.[17]

1.3. Siber Tehdit İstihbaratı (CTI)

Siber Tehdit İstihbaratı (*Cyber Threat Intelligence*, CTI), dijital tehditlerin öngörülmesi, tanımlanması ve etkisiz hale getirilmesi amacıyla toplanan, analiz edilen ve yorumlanan stratejik, operasyonel ve taktiksel bilgileri kapsayan bir disiplindir.[18] CTI, siber saldırganların motivasyonlarını, tekniklerini, prosedürlerini ve potansiyel hedeflerini anlamaya yönelik verilerden oluşur ve güvenlik ekiplerine risk bazlı savunma stratejileri geliştirme imkânı sunar. Bu kavram, yalnızca mevcut tehditleri izlemekle kalmayıp gelecekteki saldırıları önleme ve güvenlik mimarisini proaktif şekilde iyileştirme amacını taşır. CTI'nin etkili kullanımı, tehdit aktörleri hakkında derinlemesine bilgi sağlamanın yanı sıra güvenlik olaylarının analizinde daha hızlı ve doğru müdahaleler için de kritik önem taşır.[19]

1.4. Siber İstihbarat

Siber İstihbarat (*Cyber Intelligence*), dijital ortamda gerçekleşen tehditler, saldırılar ve güvenlik açıkları hakkında stratejik ve operasyonel düzeyde bilgi toplamayı, analiz etmeyi ve bu bilgileri kullanarak proaktif güvenlik önlemleri geliştirmeyi hedefleyen bir bilgi toplama sürecidir.[20] Geleneksel istihbarat disiplinlerinden türeyen siber istihbarat, teknik ve insan kaynaklı verilerin bir araya getirilmesiyle oluşturulan, aktörlerin motivasyonları, kapasiteleri, taktikleri ve hedefleri hakkında kapsamlı bilgi sağlar. Bu süreçte elde edilen bilgiler, risk yönetimi, siber savunma stratejileri ve karar alma mekanizmalarının güçlendirilmesinde kullanılır.[21]

1.5. MITRE ATT&CK

MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge* – Rakip Taktikler, Teknikler ve Genel Bilgi), siber tehdit aktörlerinin saldırılarını nasıl gerçekleştirdiğine dair detaylı bir bilgi tabanı ve çerçeve sunan, tehdit odaklı bir modeldir. Bu çerçeve, siber güvenlik topluluğu için saldırıların tanımlanması, analiz edilmesi ve önlenmesine yönelik standartlaştırılmış bir referans sağlar.[22]

MITRE ATT&CK, saldırganların kullandığı taktikler (hedefler), teknikler (hedeflere ulaşmak için kullanılan yöntemler) ve prosedürler (belirli bir tekniği uygulamak için izlenen

16 Artem Bratko, Denys Zaharchuk ve Valentyn Zolka, "Hybrid Warfare-A Threat to the National Security of the State", *Revista de Estudios en Seguridad Internacional*, 7:1, 2021, s. 147-160.

17 Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare*, NATO Strategic Communications Centre of Excellence, 2016, s. 9-11.

18 Ignacio M. G. Urbini, Paula Venosa, Patricia Bazán ve Nicolás Del Río, "Distributed Cybersecurity Strategy, Applying the Intelligence Operations Theory", *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, Haziran 2022, s. 1-6.

19 Nan Sun, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai ve Jun Zhang, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", *IEEE Communications Surveys & Tutorials*, 25:3, 2023, s. 1748-1774.

20 Randy Borum, John Felker, Sean Kern, Kristen Dennesen ve Tonya Feyes, "Strategic Cyber Intelligence", *Information & Computer Security*, 23:3, 2015, s. 317-332.

21 Ross W. Bellaby, "Justifying Cyber-Intelligence?", *Journal of Military Ethics,* 15:4, 2016, s. 299-319.

22 Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington ve Cody B. Thomas, "MITRE ATT&CK: Design and Philosophy", *Technical Report*, McLean, VA: The MITRE Corporation, 2018, s. 1-6.

süreçler) gibi unsurları ayrıntılı biçimde sınıflandırır. Savunma stratejilerinin geliştirilmesinde önemli bir kaynak olan bu model, siber tehdit istihbaratında tehditlerin analiz edilmesi, güvenlik açıklarının tespit edilmesi ve olay müdahale süreçlerinin geliştirilmesi için rehberlik eder.[23] Özellikle tehdit avcılığı, güvenlik kontrollerinin değerlendirilmesi ve tehdit modelleme süreçlerinde yaygın olarak kullanılmaktadır. Mitre çerçevesinde yer alan TTP (*Tactics, Techniques & Procedures*); teknik, taktik ve prosedür kelimelerinin kısaltmasıdır.[24] APT (*Advanced Persistent Threat*) ise, gelişmiş kalıcı tehditler anlamına gelen İngilizce ifadenin kısaltılmış halidir.[25] Ayrıca APT kavramı, ilgili tehditleri kendilerine has saldırı yöntemleri ve motivasyonlarıyla bir araya gelen saldırgan grupları tanımlamak için de kullanılır. Genellikle APT grupları olarak isimlendirilir. Hem TTP hem APT kavramları bölüm 4.1 içerisinde pratik örneklerle ele alınacaktır.

1.6. Tedarik Zinciri Güvenliği

Tedarik zinciri güvenliği, bir organizasyonun tedarik zincirinde yer alan tüm bileşenlerin, süreçlerin ve üçüncü tarafların siber saldırı ve bilgi güvenliği risklerine karşı korunmasını sağlama sürecidir.[26] Bu kavram, donanım, yazılım ve hizmetlerin geliştirilmesinden teslimatına kadar olan tüm aşamalarda güvenlik açıklarını ve potansiyel tehditleri ele alır. Tedarik zinciri güvenliği, özellikle dış kaynak kullanımı ve üçüncü taraflarla yapılan iş birlikleri nedeniyle karmaşık bir yapıya sahiptir. Saldırganlar, doğrudan hedefe yönelik saldırılar yerine zayıf halkalar üzerinden sisteme erişim sağlamayı tercih edebilir. Bu bağlamda, tedarik zinciri güvenliği; güvenilir tedarikçi seçimi, bileşenlerin doğrulanması, şeffaflık sağlanması ve güvenlik kontrollerinin düzenli olarak uygulanması gibi proaktif önlemleri içerir. Kritik altyapıların ve hassas verilerin korunması açısından, tedarik zinciri güvenliği modern siber güvenlik stratejilerinin temel unsurlarından biridir.[27]

1.7. Sinyal İstihbaratı (SIGINT)

Sinyal İstihbaratı (*Signals Intelligence*, SIGINT), elektronik haberleşme sistemlerinden elde edilen verilerin toplanması, analiz edilmesi ve yorumlanması yoluyla elde edilen istihbarat türüdür.[28] SIGINT, genellikle askerî ve ulusal güvenlik bağlamında kullanılmakla birlikte, modern siber güvenlik stratejilerinde de önemli bir rol oynar. Bu istihbarat türü, iletişim istihbaratı (COMINT) ve elektronik istihbarat (ELINT) gibi alt kategorilere ayrılır; birincisi haberleşme trafiğini, ikincisi ise radar ve diğer elektronik sinyalleri hedef alır.[29]

---

23 Nitin Naik, Paul Jenkins, Paul Grace ve Jingping Song, "Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model", *2022 IEEE International Symposium on Systems Engineering (ISSE)*, IEEE, Ekim 2022, s. 1-7.

24 Bir tehdit aktörünün davranışını temsil eder. Taktik, davranışın en üst düzey açıklamasıdır; teknikler, taktik bağlamda davranışın daha ayrıntılı bir açıklamasını sunar; prosedürler ise teknik bağlamda davranışın daha düşük düzeyli, oldukça ayrıntılı bir açıklamasını sunar. Bknz.: National Institute of Standards and Technology, "Tactics, Techniques, and Procedures", *National Institute of Standards and Technology (NIST)*, https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures, erişim 22.04.2025.

25 APT (*Advanced Persistent Threat*): Gelişmiş kalıcı tehdit, hedef ağ veya sistem içerisinde fark edilmeden ve kalıcı bir varlık sürdürmek için gizli saldırı tekniklerini kullanan, böylece uzun süre boyunca tespit edilmeden hedeflerine ulaşmalarını sağlayan gelişmiş bir saldırgandır. Bknz.: PICUS Security, "What is Advanced Persistent Threat (APT)?", *Picus Security*, 2025, https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt, erişim 05.05. 2025.

26 Heinrihs K. Skrodelis ve Andrejs Romanovs, "Cyber-Physical Risk Security Framework Development in Digital Supply Chains", *2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, IEEE, Ekim 2021, s. 1-5.

27 Badis Hammi, Sherali Zeadally ve Jamel Nebhen, "Security Threats, Countermeasures, and Challenges of Digital Supply Chains", *ACM Computing Surveys*, 55:14s, 2023, s. 1-40.

28 David L. Christianson, "Signals Intelligence", Gerald W. Hopple ve Bruce W. Watson (ed.), *The Military Intelligence Community*, New York, Routledge, 2019, s. 39-54.

29 D. Curtis Schleher, *Electronic Warfare in the Information Age*, Norwood MA, Artech House Inc., 1999, s. 27-35.

1.8. Elektronik Harp (EH)

Elektronik Harp (EH), elektromanyetik spektrumu kullanarak düşman iletişim, algılama ve yönlendirme sistemlerini engellemek, yanıltmak veya bozmak ve aynı zamanda kendi sistemlerinin bu tür tehditlerden korunmasını sağlamak amacıyla yürütülen askerî faaliyetlerdir.[30] Elektronik Harp, elektronik taarruz (*Electronic Attack*, EA), elektronik destek (*Electronic Support*, ES) ve elektronik koruma (*Electronic Protection*, EP) olmak üzere üç temel bileşene ayrılır. Elektronik taarruz, düşman sinyallerini hedef alan saldırı faaliyetlerini içerirken, elektronik destek, tehditlerin tespit edilmesi ve izlenmesi için sinyal toplama ve analiz süreçlerini kapsar. Elektronik koruma ise dost sistemlerin elektromanyetik spektrum tehditlerine karşı savunulmasını sağlar. Modern savaş ortamında giderek daha stratejik bir rol üstlenen elektronik harp, özellikle siber güvenlik ve sinyal istihbaratı ile iç içe geçmiş bir yapıdadır ve askerî operasyonların başarısı için kritik bir avantaj sunar.[31]

1.9. İstihbarat ve Örtülü Operasyonlar

İstihbarat, devletlerin ulusal güvenlik, dış politika ve stratejik çıkarlarını koruma amacıyla bilgi toplama, analiz etme ve yayma süreçlerini kapsayan disiplinler arası bir faaliyettir.[32] İstihbarat, karar alıcıların bilinçli ve etkili politikalar geliştirmesine yardımcı olacak bilgileri sağlamak için kullanılır. Bu süreç; insan kaynaklı istihbarat (HUMINT), sinyal istihbaratı (SIGINT), görüntü istihbaratı (IMINT) ve ölçüm ile imza istihbaratı (MASINT) gibi farklı disiplinlerden gelen verilerin toplanmasını ve bu verilerin anlamlı bir şekilde işlenmesini içerir.[33] Etkin bir istihbarat süreci, yalnızca tehditlerin tespit edilmesini değil, aynı zamanda fırsatların belirlenmesini ve risk yönetiminin güçlendirilmesini mümkün kılar.[34] İstihbarat faaliyetleri, devletlerin güvenlik stratejilerinin temel unsurlarından biri olup askerî, ekonomik ve siyasi alanlarda avantaj sağlamak amacıyla kullanılır.

Örtülü operasyonlar ise bir devletin resmi olarak üstlenmediği veya kamuya açıklamadığı faaliyetlerdir. Genellikle gizlilik gerektiren stratejik hedeflere ulaşmak için uygulanır.[35] Bu tür operasyonlar, rejim değişikliği sağlamak, rakip devletlerin etkisini zayıflatmak veya terörist faaliyetleri engellemek gibi amaçlarla gerçekleştirilebilir.[36] Örtülü operasyonların en belirgin özelliklerinden biri, operasyonun sponsoru olan devletin kimliğinin gizlenmesidir.[37] Örtülü operasyonların başarısı, planlama, gizlilik ve bilgi güvenliği unsurlarının etkili bir şekilde yönetilmesine bağlıdır.[38]

2. Literatür

Çağrı cihazları patlatılması olaylarının hemen akabinde, olayın sıcaklığıyla ilgili çeşitli teknik yorumlar, sosyal mecralarda günlerce yayılmıştı. Ancak çalışmanın araştırma probleminde vurgulanan konuya değinen sınırlı sayıda kaynak, bazı internet makalelerinde ele alınmış

30 Age, s. 37.
31 Ali Al-Khawaja ve Sattar B. Sadkhan, "Intelligence and Electronic Warfare: Challenges and Future Trends", *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, IEEE, Ağustos 2021, s. 118-123.
32 Len Scott, "Secret Intelligence, Covert Action and Clandestine Diplomacy", Christopher Andrew, Richard J. Aldrich ve Wesley K. Wark (ed.), *Secret Intelligence*, London, Routledge, 2019, s. 526-544.
33 Age, s. 527.
34 Age, s. 528.
35 Michael Warner, "A Matter of Trust: Covert Action Reconsidered", *Studies in Intelligence*, 63:4, 2019, s. 33-39.
36 Age, s. 57.
37 Peter Gill, "Intelligence, Threat, Risk and the Challenge of Oversight", *Intelligence and National Security*, 27:2, 2012, s. 206-222.
38 Age, s. 209.

görünmektedir. Literatür incelemesinde özellikle şu analizin dikkat çekici olduğunu değerlendirmekteyiz.[39]

> *"Çağrı cihazlarıyla yapılan bu saldırı, siber güvenlik için doğrudan bir paralellik sunuyor: tıpkı askerî alanda olduğu gibi, düşman hakkında derin bilgi sahibi olmak çok önemlidir. Siber güvenlikte, kötü niyetli grupların Taktiklerini, Tekniklerini ve Prosedürlerini (TTP) sürekli olarak gözlemlememiz ve bunları güvenlik uygulamalarımıza dahil etmemiz gerekir. Bu, yalnızca NIST, CIS Kontrolleri ve ISO 27001 gibi yerleşik çerçeveleri benimsemek anlamına gelmez, aynı zamanda bunları karşı karşıya olduğumuz gerçek tehditlere göre ayarlamak anlamına da gelir".*

Araştırmamız kapsamında ele alınan diğer bir makale, Hizbullah'a yönelik 2024 yılında gerçekleşen ve grubun üyelerince kullanılan çağrı cihazlarının aynı anda infilak ettiği saldırıyı incelemektedir.[40] Olay, yüzlerce cihazın içerisine patlayıcı yerleştirilip uzaktan tetiklenmesi ile gerçekleşmiştir. İsrail'in operasyonun ardındaki güç olduğu öne sürülmüş, patlamalar ciddi can kaybına ve yaralanmalara yol açmıştır. Patlamalarda kullanılan cihazların Tayvan merkezli Gold Apollo tarafından üretilmiş olması, dikkatleri tedarik zinciri güvenliğine yöneltmiştir. Tedarik zincirine sızılarak, söz konusu çağrı cihazlarının hedef gruplara toplu olarak ulaştırıldığı anlaşılmaktadır. Uzmanlar, patlamaların pillerden kaynaklanmadığını, ancak uzaktan tetikleme kabiliyetlerinin kamuya açık dijital ağlar üzerinden gerçekleştirilebileceğini belirtmiştir.[41] Saldırı, bağlı cihazların güvenliği ve üreticilerin bu tür tehditlere karşı sağlam testler yapmasının gerekliliği konusunda ciddi bir uyarı olarak ele alınmaktadır.

Diğer bir çalışmada ise İsrail'in Hizbullah'a yönelik çağrı cihazlarını kullanarak düzenlediği saldırının, siber güvenlik stratejileri için sunduğu dersleri analiz etmektedir.[42] Yazar, istihbarat operasyonlarının sürpriz, yenilik ve düşman bilgisine dayandığını vurgularken, çağrı cihazları ve daha önce Yahya Ayyaş'a yönelik suikast gibi olaylardan örnekler vermektedir. Siber güvenlik bağlamında, saldırı taktiklerini anlamanın ve tehdit bilincine dayalı savunma mekanizmaları geliştirmenin önemine dikkat çekilmektedir. Makalede ayrıca, sosyal mühendislik saldırılarına ve içeriden gelen tehditlere karşı güvenlik programlarının önemi, tedarik zinciri güvenliğine yönelik riskler ve kullanıcı farkındalığını arttırma stratejileri ele alınmaktadır. Savaşta ve siber güvenlikte yaratıcılık ile tehdit istihbaratının entegre bir güvenlik yaklaşımındaki kritik rolü vurgulanmaktadır.[43]

Bu ilk değerlendirmeler, olayın hemen ardından yapılan ve daha çok teknik boyutlara odaklanan yorumları yansıtmaktadır. Ancak bu saldırının sadece bir cihaz güvenliği veya tedarik zinciri zafiyeti meselesi olmadığı, aynı zamanda karmaşık bir istihbarat operasyonunun ve hibrit savaş taktiklerinin bir parçası olduğu göz ardı edilmemelidir. Nitekim, Lima'nın çalışmasında vurgulanan "*düşman hakkında derin bilgi sahibi olma*" gerekliliği[44] ve ilgili yazar tarafından işaret edilen "*tehdit bilincine dayalı savunma mekanizmaları geliştirme*" ihtiyacı,[45] bu tür olayların analizinde siber güvenlik disiplininin istihbarat ve stratejik

39 Marcelo Lima, "Israeli Pager Attack: Cybersecurity Lessons", *LinkedIn*, 29 Eylül 2024, https://www.linkedin.com/pulse/israeli-pager-attack-cybersecurity-lessons-security-marcelo-kcjxf, erişim 21.10.2024.
40 Information Security Buzz Staff Reporter, "Hezbollah Pager Attack: A Wake-up Call to Tech Manufacturers to Secure their Supply Chains?", *Information Security Buzz (ISB)*, 19 Eylül 2024, https://informationsecuritybuzz.com/hezbollah-pager-attack-a-wake-up-call/, erişim 20.10.2024.
41 Age.
42 Lima, "Israeli Pager Attack: Cybersecurity Lessons".
43 Age.
44 Age.
45 Age.

çalışmalar gibi sosyal bilim alanlarıyla ne kadar iç içe geçtiğini göstermektedir. Çağrı cihazlarının hedef alınması, sadece teknik bir zafiyetin istismarı değil, aynı zamanda hedef grubun iletişim alışkanlıkları, operasyonel güvenliği ve psikolojisi üzerine kurulu kapsamlı bir istihbarat çalışmasının ürünü olduğunun göstergesidir.

Singh'in internet makalesi, modern siber-fiziksel savaşın sınırlarını zorlayan ve askerî stratejide yeni bir paradigma sunan Hizbullah'a yönelik stratejik çağrı cihazı saldırısını incelemektedir.[46] Onun analizine göre, Hizbullah'ın elektronik gözetimden kaçınmak amacıyla kullandığı çağrı cihazlarına, tedarik zinciri manipülasyonu yoluyla patlayıcılar yerleştirilmiş ve bu cihazlar uzaktan senkronize şekilde patlatılarak ciddi kayıplar verilmiştir. Saldırının başarısı, PETN (*Pentaeritritol Tetranitrat*) patlayıcısı içeren cihazların fiziksel ve siber güvenlik açıklarını bir araya getiren sofistike bir istihbarat operasyonuna dayanmaktadır. Ayrıca, saldırının iletişim altyapısına zarar vermesi ve Hizbullah'ın operasyonel güvenini sarsması, tedarik zinciri güvenliği ile siber-fiziksel sistemlerin bütüncül olarak yeniden değerlendirilmesinin önemini vurgulamaktadır. Singh, bu olayın, teknolojiyle silahlandırmanın yeni bir dönemini işaret ettiğini ve savaşın geleneksel siber ve kinetik sınırlarının bulanıklaştığını savunarak, modern çatışmaların geleceğinde siber güvenliğin kritik rolüne dikkat çekmektedir.[47]

Singh, saldırıyı "*siber-fiziksel savaşın sınırlarını zorlayan ve askerî stratejide yeni bir paradigma sunan*" bir olay olarak nitelendirirken bu paradigmanın sadece teknolojik bir dönüşümü değil, aynı zamanda savaşın doğasına ilişkin geleneksel anlayışları sorguladığını da belirtmektedir. Tedarik zinciri manipülasyonu yoluyla fiziksel ve siber güvenlik açıklarının bir araya getirilmesi, devletlerin ve devlet dışı aktörlerin yıkıcı kapasitelerini nasıl arttırabileceğini göstermektedir. Bu noktada, saldırının sadece Hizbullah'ın operasyonel güvenini sarsmakla kalmayıp, aynı zamanda genel olarak teknolojiye olan güveni ve kritik altyapıların (iletişim altyapıları dahil) güvenliğine ilişkin endişeleri de arttırdığı söylenebilir.[48] Singh'in vurguladığı gibi "*savaşın geleneksel siber ve kinetik sınırlarının bulanıklaşması*", uluslararası ilişkiler ve güvenlik çalışmaları literatüründe uzun süredir tartışılan hibrit tehditler kavramıyla doğrudan örtüşmektedir. Bu tür bir saldırı, ulusal güvenlik stratejilerinin sadece askerî kapasitelere değil, aynı zamanda siber dayanıklılığa, tedarik zinciri direncine ve toplumsal farkındalığa da odaklanması gerektiğini bir kez daha teyit etmektedir.

Diğer bir analiz çalışmasında Mark Lacy, modern çatışmaların yeni boyutlarını ve teknolojik araçların silahlandırılmasını ele almaktadır.[49] Yazar, iletişim cihazlarının patlayıcı düzeneklere dönüştürülmesini, devlet dışı aktörler tarafından geliştirilen yıkıcı teknolojilerin artan erişilebilirliği bağlamında tartışmaktadır. Bu saldırılar, iletişim güvenliğinin savaşlarda her zamankinden daha kritik hale geldiği bir dönemde yaşanmış ve sıradan nesnelerin dahi savaş aracı olarak kullanılabileceğine işaret etmiştir. Lacy, Mark Galeotti ve Audrey Kurth Cronin gibi güvenlik uzmanlarının görüşlerine atıfta bulunarak, "*her şeyin silahlandırılması*" konseptinin tehditkâr gerçekliğe dönüştüğünü vurgulamaktadır.[50] Makale, gelecekteki çatışmaların daha yaratıcı ve uzaktan gerçekleştirilen saldırılarla şekilleneceği bir dünyada,

46 Inder Singh, "New Paradigm in Cyber Warfare: Strategic Pager Attack on Hezbollah", *Medium*, 18 Eylül 2024, https://inderbarara.medium.com/new-paradigm-in-cyber-warfare-strategic-pager-attack-on-hezbollah-d100247bd9ec, erişim 22.10.2024.

47 Singh, "New Paradigm in Cyber Warfare: Strategic Pager Attack on Hezbollah".

48 Tobias B. Back, "Weaponising 'Apparently Harmless Portable Objects': Emerging Categorisations of Trust and Risk in Post 'Pager Attacks' Lebanon", *Small Wars & Insurgencies*, 36:6, 2025, s. 1025-1048.

49 Mark Lacy, "Lebanon Pager Attacks: The Weaponisation of Everything has Begun", *The Conversation*, 19 Eylül 2024, https://theconversation.com/lebanon-pager-attacks-the-weaponisation-of-everything-has-begun-239423, erişim 23.10.2024.

50 Age.

devletlerin ve güvenlik kurumlarının yeni zorluklara karşı savunmasız kalabileceğini belirtir. Özellikle devlet dışı aktörlerin geleneksel caydırıcılık stratejilerine karşı daha az duyarlı olmaları, bu tehdidi daha karmaşık hale getirmektedir. Lacy, hızla değişen teknolojik ortamda jeopolitik dengelerin de yeniden tanımlanabileceğini öne sürerek belirsizliğin, çağdaş güvenlik anlayışının temel bir özelliği olarak kaldığını savunmaktadır.

Lacy, "*her şeyin silahlandırılması*" konseptinin tehditkâr bir gerçekliğe dönüştüğünü vurgularken, bu durumun uluslararası güvenlik ortamında öngörülebilirliği azalttığını ve devletlerin yanı sıra devlet dışı aktörlerin de asimetrik avantajlar elde etmesine olanak tanıdığını belirtmek önemlidir. İletişim cihazlarının patlayıcı düzeneklere dönüştürülmesi, sadece teknolojik bir yenilik değil, aynı zamanda psikolojik bir etki yaratma ve korku yayma amacı da taşıyabilir. Bu tür saldırılar geleneksel caydırıcılık stratejilerinin etkinliğini sorgulatmakta ve devletleri yeni savunma mekanizmaları geliştirmeye zorlamaktadır. Sivil teknolojiler kullanılarak gerçekleştirilen bu saldırıların savaşçı olmayanları da hedef alabileceğinden yola çıkarak insan hakları yasalarına aykırılık teşkil edeceğinin tartışıldığı bir ortamda[51], özellikle devlet dışı aktörlerin bu tür yıkıcı teknolojilere erişiminin artması, uluslararası normların ve çatışma hukukunun bu yeni gerçekliğe nasıl uyum sağlayacağı sorusunu da beraberinde getirmektedir.

Pytlak, Siebens ve Lad'ın Lübnan'daki çağrı cihazı saldırılarını incelediği çalışması, modern çatışmaların karmaşıklığını ve hibrit savaşın dinamiklerini aydınlatmaya çalışmaktadır.[52] Özellikle eski teknolojilere yapılan saldırıların, siber operasyonların ve kinetik sabotajların kesişim noktalarını nasıl temsil ettiğine odaklanmaktadır. Çağrı cihazlarının hedef alınması, çift kullanımlı teknolojilerin silahlandırılmasının ve tedarik zincirlerine yönelik müdahalelerin güvenlik üzerindeki etkilerini çarpıcı biçimde göstermektedir. Yazarlar, geleneksel siber tehditlerin ötesinde, sorumluluk atfetmenin zorluklarını ve kısa raf ömrüne sahip hibrit silahların operasyonel sınırlamalarını analiz ederek, siber savaşın benzersiz olmadığını ve geçmişten miras alınan güvenlik açmazlarını tekrar ettiğini vurguluyor. Bu olay, hibrit savaşın insan maliyeti ve güvenlik açıkları açısından yalnızca siber alanla sınırlı olmayan daha geniş bir tehdit çerçevesine sahip olduğunu hatırlatmaktadır.[53]

Pytlak ve arkadaşları, çağrı cihazı saldırılarının "*siber operasyonların ve kinetik sabotajların kesişim noktalarını*" temsil ettiğini belirtirken, bu kesişimin sadece teknik bir birleşme olmadığını, aynı zamanda stratejik ve operasyonel bir entegrasyonu da ifade ettiğini vurgulamak gerekir.[54] Yazarların, "*hibrit savaşın insan maliyeti ve güvenlik açıkları açısından yalnızca siber alanla sınırlı olmayan daha geniş bir tehdit çerçevesine sahip olduğu*" tespiti, bu tür olayların analizinde sadece teknolojik zafiyetlere odaklanmanın yetersiz kalacağını göstermektedir.[55] Bu analiz, çalışmamızın önerdiği MITRE ATT&CK çerçevesinin genişletilmesi gerekliliğini, sadece yeni teknikler eklemekle kalmayıp, aynı zamanda bu tür hibrit saldırıların karmaşık doğasını ve sosyopolitik bağlamlarını da içerecek şekilde yapılması gerektiğini desteklemektedir.[56]

51 Andrea Lavazza ve Mirko Farina, "The Costs and Perils of Weaponizing Consumer Technologies (the 2024 Pager and Walkie-Talkie Explosions in Lebanon and Syria)", *IEEE Technology and Society Magazine*, 2024.
52 Alexa Pytlak, Jessica Siebens, ve Sahil Lad, "Old Tactics, New Targets: Unraveling Lebanon's Pager Attacks", *Stimson Center*, 25 Eylül 2024, https://www.stimson.org/2024/old-tactics-new-targets, erişim 24.10.2024.
53 Age.
54 Age.
55 Age.
56 Chuan Sheng, Wanlun Ma, Qing-Long Han, Wei Zhou, Xiaogang Zhu ve Sheng Wen, "Pager Explosion: Cybersecurity Insights and Afterthoughts", *IEEE/CAA Journal of Automatica Sinica*, 11:12, 2024, s. 2359-2362.

Söz konusu çağrı cihazı saldırıları, hibrit savaş ve siber güvenlik literatüründe giderek daha fazla önem kazanan bazı temel temaları da ön plana çıkarmaktadır. Örneğin, Hoffman tarafından kavramsallaştırılan hibrit tehditler, devletlerin ve devlet dışı aktörlerin konvansiyonel ve düzensiz taktikleri, terörizmi ve suç faaliyetlerini senkronize bir şekilde kullanarak belirsizlik yaratma ve geleneksel askerî üstünlüğü aşındırma çabalarını ifade eder.[57] Lübnan'daki olay, Hoffman'ın teorik çerçevesinin pratik bir yansıması olarak okunabilir. Benzer şekilde Nye, siber gücün (*cyber power*) uluslararası politikadaki rolüne ilişkin analizleri, siber saldırıların sadece teknik bir sorun olmanın ötesinde, devletlerin güç projeksiyonu, caydırıcılık ve diplomatik ilişkilerinde nasıl bir araç haline geldiğini ortaya koymaktadır.[58] Çağrı cihazı saldırıları, siber yeteneklerin istihbarat operasyonları ve kinetik etkilerle birleştirilerek stratejik hedeflere ulaşmada nasıl kullanılabileceğine dair çarpıcı bir örnektir. Ayrıca Rid'in, siber savaşın büyük ölçüde casusluk, sabotaj ve yıkıcılık (*subversion*) faaliyetlerinin sofistike birer versiyonu olduğu yönündeki argümanları da bu bağlamda önemlidir.[59] Lübnan vakası, Rid'in işaret ettiği gibi, doğrudan bir "*savaş*" eylemi olmasa da sofistike bir sabotaj ve istihbarat operasyonu olarak değerlendirilebilir ve bu tür eylemlerin uluslararası güvenlik üzerindeki etkileri göz ardı edilemez.

Saldırıların etkisinin günlerce kamuoyunda tartışıldığı süreçte, sosyal medya platformlarında ve geleneksel medya kanallarında görüş bildiren siber güvenlik, elektronik/sinyal/RF ve istihbarat alanlarındaki uzmanlar arasında genel bir görüş birliği oluşmuştur. Bu değerlendirmelere göre, söz konusu saldırılar bir istihbarat operasyonu çerçevesinde planlanmış, tedarik zincirindeki zafiyetleri hedef almış ve hem siber hem de elektronik yöntemlerden yararlanılmıştır. Gerçekte ise bu saldırı, farklı uzmanlık alanlarının kesişiminde yer alan disiplinler arası bir yaklaşımla kurgulanmış olup bu yönüyle alternatif yorumlara açık bir analiz çerçevesi sunmaktadır. Bu açıdan saldırının farklı bir yoruma dönük analizi şu satırlarda ifade edilmektedir:[60]

> *"Hizbullah'ın tedarik zincirlerinin kırılganlığını hafife alırken yaptığı yaygın hata, geleneksel en iyi uygulamaların yeterli olduğuna inanmasıdır. Ancak, düşmanların TTP'leri sürekli olarak gelişiyor ve bu gelişmeye ayak uyduramazsak, geride kalma riskimiz var. Tehdit Bilgili Savunma yaklaşımı, savunmalarımızı gerçek ve ortaya çıkan tehditlere uyarlama ihtiyacını vurgulayarak buna bir yanıt olarak ortaya çıkıyor. MITRE ATT&CK gibi araçlar, kötü niyetli grupların kullandığı taktiklere ilişkin değerli içgörüler sundukları için bu süreçte önemlidir".*

3. Yöntem

Bu çalışmada, nitel araştırma yöntemleri çerçevesinde yapılandırılmış bir vaka çalışması yaklaşımı benimsenmiş ve "Tasarım Bilimsel Araştırma Yöntemi" çerçevesinde yapılandırılmıştır. Vaka çalışması, belirli bir kişi, grup, olay, kurum veya duruma derinlemesine ve detaylı bir şekilde odaklanan bir araştırma yöntemidir. Genellikle, bir olayın veya durumun "neden" ve "nasıl" meydana geldiğini anlamak için kullanılır.[61] Tasarım Bilimsel Araştırma Yöntemi, bir problemi çözmek veya mevcut bir durumu iyileştirmek için yeni bir yapı (model, yöntem, algoritma ve sistem) tasarlamayı ve gerekçelendirmeyi

57 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies*, 2007.
58 Joseph S. Nye, *Cyber Power*, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.
59 Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence", *Foreign Affairs*, 92:6, 2013, s. 77-87.
60 Lima, "Israeli Pager Attack: Cybersecurity Lessons".
61 Robert K. Yin, *Case Study Research: Design and Methods*, 5, Thousand Oaks, CA, Sage, 2009.

amaçlayan bir araştırma yaklaşımıdır.[62] Bu kapsamda Eylül 2024'te Hizbullah'a yönelik gerçekleştirilen çağrı cihazı saldırısına ilişkin kamuya açık araştırma raporları, istihbarat analizleri, medya içerikleri ve teknik forumlardaki uzman yorumları sistematik olarak incelenmiş, bu içeriklerden elde edilen veriler, saldırının yapısını ve kullanılan teknikleri ortaya koymak üzere analiz edilmiştir. Mevcut MITRE ATT&CK matrisinin teknik ve taktik boyutları incelenmiş, saldırının tespit ve analizinde yetersiz kalan alanlar tespit edilmiştir. Bu bağlamda, mevcut çerçeveye entegre edilebilecek iki yeni teknik model önerilmiştir. Bu öneriler, RF sinyallerine dayalı saldırıların da tehdit istihbaratı matrisine dahil edilmesini sağlayarak, dijital ve analog tehditleri bir arada ele alan bütüncül bir modelin temellerini oluşturmaktadır.

4. Mevcut Çerçeve ve Önerilen Model

MITRE ATT&CK, bilgileri güncel tutabilmek için topluluktan gelen ve sahada gözlemlenen olayları içeren girdilere büyük ölçüde bağımlıdır.[63] Bireyler ve kuruluşlar, MITRE ATT&CK bilgi tabanını geliştirmek amacıyla sürekli olarak çeşitli tehdit istihbaratı verileri ve bilgileri paylaşmaktadır. Bu paylaşımlar sayesinde siber güvenlik profesyonelleri, elde edilen verileri tehdit profilleri, taktikler ve teknikler gibi bileşenler halinde bilgi tabanına entegre ederek, bilgi birikiminin zenginleşmesine katkı sağlamaktadır.[64] Literatürde de bu zenginleşmeye katkı sağlayan çalışmalar yer almaktadır. Jo ve arkadaşları, gemi siber güvenliği alanında yürütülen 15 önemli çalışmayı MITRE ATT&CK çerçevesini kullanarak incelemiştir.[65] Yapılan bu analizler sonucunda, modern gemilerde dikkate alınması gereken ortak güvenlik tedbirleri tespit edilmiş ve bu bulgulara dayanarak gemi ortamına özgü yeni bir güvenlik önlemleri matrisi sunulmuştur. Kanj Bonhard ve arkadaşları, kurumsal e-posta dolandırıcılığı tehdit aktörlerinin kullandığı TTP'leri MITRE ATT&CK çerçevesi kapsamında haritalandırarak 10 taktik, 34 teknik ve 46 alt-teknik belirlemiş ve özellikle posta kutusu manipülasyonu ile savunma atlatma konularındaki eksiklikleri gidermek amacıyla 5 yeni alt-teknik önermişlerdir.[66] Ahn ve arkadaşları, bir kurumun siber saldırı veya güvenlik ihlali sonrasında hızla toparlanabilme yeteneği olan siber dayanıklılığını arttırmak amacıyla Sıfır Güven (*Zero Trust* - ZT) güvenlik modelini ile MITRE ATT&CK matrisinin birleştirilmesini önermektedir.[67] Pell ve arkadaşları, 5G ağları için MITRE ATT&CK çerçevesini genişletme konusundaki yaklaşımını sundukları çalışmalarında 5G'nin bulut tabanlı mimariye geçişinin geleneksel bulut tehditlerini de beraberinde getirdiğine inanarak tüm taktikleri korumuş, ancak 5G mimarisine özgü tehditleri bir uzantı olarak tanımlayarak standart protokolun kötüye kullanımını bir teknik olarak işlemişlerdir.[68] Söz konusu MITRE ATT&CK çerçevesindeki son yıllardaki gelişmeleri dikkate alarak gerçekleşen saldırılara karşı matris üzerinde alınabilecek mevcut tedbirler değerlendirilmiş, akabinde henüz bu saldırıya karşı

62 Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger ve Samir Chatterjee, "A Design Science Research Methodology for Information Systems Research", *Journal of Management Information Systems,* 24:3, 2007, s. 45-77.
63 Strom, Applebaum, Miller, Nickels, Pennington ve Thomas, "MITRE ATT&CK: Design and Philosophy".
64 B. Al-Sada, A. Sadighian, ve G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database*", IEEE Access,* 12, 2023, s. 1217-1234.
65 Yonghyun Jo, Oongjae Choi, Jiwoon You,Youngkyun Cha ve Dong Hoon Lee, "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework", *Sensors*, 22:5, 2022, s. 1860.
66 Sebastien Kanj Bonhard, Pau Garcia Villalta, Oriol Rosés ve Josep Pegueroles, "A Review of Tactics, Techniques, and Procedures (TTPs) of MITRE Framework for Business Email Compromise (BEC) Attacks", *IEEE Access*, 2025, s. 50761-50776.
67 Gwanghyun Ahn, Jisoo Jang, Seho Choi ve Dongkyoo Shin, "Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model with the MITRE ATT&CK Matrix", *IEEE Access*, 12, 2024, s. 89291-89309.
68 Robert Pell, Sotiris Moschoyiannis, Emmanouil Panaousis ve Ryan Heartfield, "Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK", arXiv preprint arXiv:2108.11206, 2021, https://arxiv.org/abs/2108.11206.

mevcut olmayan tedbir olarak eklenmesi önerilen teknik model açıklanmıştır. Genişletilmiş MITRE matrisine ait görsel çalışmanın sonunda ek olarak sunulmuştur.

4.1. Mevcut ATT&CK Çerçeve Matrisi

Mevcut durumda CTI yaklaşımını belirten ve güncelleyen çözüm olarak MITRE ATT&CK çerçevesi, siber güvenlik düzleminde genel kabul görmektedir. MITRE ATT&CK içerisinde yer alan teknik, taktik ve prosedürler (TTP) dışında atak yüzeyine göre matrisler "*Enterprise*" (Kurumsal Bilgi Teknolojileri [BT] Organizayonu), "*Mobile*" (Mobil Taşınabilir Cihazlar) ve "*ICS*" (Industrial Control Systems – Endüstriyel Kontrol Sistemleri, EKS) olarak çeşitli saldırı düzlemi ("*domain*"ler) şeklinde ayarlanmıştır. Şekil 1'de "*Enterprise*" (Kurumsal BT Organizasyonu) için ATT&CK Matrisi[69] bulunmaktadır:

Şekil 1. *Enterprise* (Kurumsal BT Organizasyonu) ATT&CK Çerçevesi[70]

APT grupları ister devlet destekli ister finansal motivasyonla bir araya gelmiş olsunlar, özel saldırı yöntemleri ve kendilerine özgü tehdit örüntülerini içeren teknik, taktik ve prosedürleri, yani TTP olarak ifade edilen saldırı davranışlarına sahiptirler. MITRE ATT&CK çerçevesi içinde TTP terimi, bir siber saldırganın kullandığı taktik, teknik ve prosedürler aşağıdaki gibi detaylandırılabilir:

- **Taktik:** Saldırganın nihai hedefi (örneğin, ayrıcalık yükseltme).
- **Teknik:** Bu hedefe ulaşmak için kullanılan yöntem (örneğin, kimlik bilgisi dökümü).
- **Prosedür:** Belirli bir saldırgan grubunun veya zararlı yazılımın, o tekniği nasıl uyguladığı (örneğin, Mimikatz aracıyla LSASS işlemini dump etmek).

Örnek olarak bir APT grubunun hedef aldığı bir kuruma sızmak için aşağıdaki MITRE ATT&CK çerçevesine göre izlediği TTP zinciri senaryo olarak aşağıdaki gibi ele alınabilir:

69 MITRE, *MITRE Enterprise Matrix*, https://attack.mitre.org/matrices/enterprise/, erişim 20.01.2025.
70 Nissim Pariente, "The Machine Identity Attack Surface - MITRE ATT&CK Framework Redefined", *Token Security*, 30 Nisan 2024, https://www.token.security/blog/the-machine-identity-attack-surface---mitre-attack-framework-redefined, erişim 20.01.2025.

Tablo 1. Bir APT Grubunun İzleyebileceği Örnek Bir TTP Zinciri Senaryosu

Taktik:	İlk Erişim (Initial Access)
Teknik:	Hedef Odaklı Oltalama Eklentisi (Spearphishing Attachment | T1566.001)
Prosedür:	Hedef çalışana özel hazırlanmış bir e-posta ve Word belgesi ile zararlı makro gönderilir.
Taktik:	Çalıştırma (Execution)
Teknik:	Kötücül Makro Yazılım (Malicious Macro | T1059.005)
Prosedür:	Kullanıcı belgeyi açınca makro, PowerShell komutu çalıştırır.
Taktik:	Kimlik Bilgisi Erişimi (Credential Access)
Teknik:	İşletim Sistemi Kimlik Bilgisi Sızdırma (OS Credential Dumping | T1003)
Prosedür:	Mimikatz aracı ile hafızadan kullanıcı şifreleri çekilir.
Taktik:	Yanal Hareket (Lateral Movement)
Teknik:	Uzak Erişim Servisleri (Remote Services – SMB/WinRM | T1021)
Prosedür:	Ele geçirilen şifre ile diğer makinelerde oturum açılır.
Taktik:	Veri Sızdırma (Exfiltration)
Teknik:	HTTPS Veri Sızdırma (Exfiltration Over HTTPS | T1041)
Prosedür:	Toplanan belgeler saldırganın kontrolündeki sunucuya HTTPS ile gönderilir.

APT saldırı gruplarının izlediği TTP örüntülerini anlamak adına, örnek bir vaka olarak APT29 saldırı grubu tarafından gerçekleştirilen "SolarWinds Saldırısı" izlerine bakılabilir. APT29, Rus istihbaratıyla bağlantılı bir tehdit aktörüdür. 2020'de SolarWinds Orion yazılımına zararlı kod yerleştirerek birçok Amerikan kurumunu etkileyen sofistike bir tedarik zinciri saldırısı gerçekleştirdi. Bu saldırı davranışına dair TTP dizilimi,[71] tehdit aktörünün yazılım tedarik zinciri zafiyetinden yararlanarak zararlı SUNBURST arka kapısını meşru bir güncelleme aracılığıyla dağıtımını içermektedir. Yasal SolarWinds imzası taşıyan bu zararlı kod, "Signed Binary Proxy Execution" tekniğiyle çalıştırılmış ve "Scheduled Task" kullanılarak sistemde kalıcılık sağlanmıştır. "Obfuscation" yöntemleriyle analizden kaçırılan zararlı yazılım, HTTPS protokolü üzerinden "Komuta ve Kontrol" (C2) iletişimi kurarak kurban sistemde keşif faaliyetleri gerçekleştirmiştir. Elde edilen kimlik bilgileriyle "Pass the Token" tekniği kullanılarak yatay hareket yapılmış; nihayetinde "Exchange" ve "O365" hesapları üzerinden hassas e-posta verileri toplanarak dışarı sızdırılmıştır. Sonuç olarak sofistike saldırı operasyonlarıyla ün kazanmış bu tür APT gruplarının davranış ve karakterini resmeden TTP diziliminde; "Taktik" ile hedef odaklı adım, "Teknik" ile kullanılan yöntem, "Prosedür" ile saldırganın bu tekniği nasıl uyguladığı tanımlanmaktadır.

18-19 Eylül'deki çağrı ve telsiz cihazları saldırılarının kamuoyuna yansıdığı şekliyle ele alındığında, en dikkat çeken husus, tedarik zinciri istismarı veya zafiyeti olacaktır. Bu

71 TTP dizilimindeki taktik ve prosedürler Türkçe olarak ifade edilse de siber ve bilişim kavramlarının çeviri karşılıkları nedeniyle TTP içerisindeki teknikleri içeren aşamalar orijinal İngilizce haliyle bırakılmıştır. Bknz. Sudhakar Ramakrishna, "New Findings from our Investigation of SUNBURST.", *SolarWinds Blog*, 11 Ocak 2021, https://www.solarwinds.com/blog/new-findings-from-our-investigation-of-sunburst, erişim 06.05.2025.

noktada, mevcut atak matrisi incelendiğinde bu yönde bir teknik bulunduğu görülmektedir. Öncelikle "İlk Erişim" (Initial Access) taktiği altında, "Tedarik Zinciri İhlali" altında yer alan "Donanım Tedarik Zinciri İhlali" alt tekniği (T1195.03) mevcut matriste yer alan bir yöntem olarak bulunmaktadır. Ancak bu teknik ve alt tekniğin saldırıları için geçerli platformların "Linux", "Windows" ve "MacOS" olduğuna dikkat edilmelidir. Bu açıdan gerçekleşen saldırılarla ilgili uygulanacak bir tedbir olarak geçerli olamayacağı değerlendirilmektedir.

Benzer isimde teknik ve alt teknik "*Mobile*" (Mobil cihaz) matrisi alanında da bulunmaktadır. Ancak aynı şekilde platformların sadece yukarıda bahsi geçen üç işletim sisteminde geçerli olduğuna dikkat edilmelidir. Bu noktada diğer bir matris olan "ICS" (EKS) alanında da "Tedarik Zinciri İhlali" tekniği (T0862) yer almaktadır. Bu teknik altında alt teknik bulunmamaktadır. Ayrıca herhangi bir platformu işaret eden gösterge de mevcut değildir. Bu nedenle, çağrı cihazı saldırısı özelinde, "ICS" (EKS) matrisi daha ilintili ve geçerli olabileceği göze çarpmaktadır. Bu yüzden ilgili kısmın atak matrisi olan "ICS" alanında ifade edilen "Tedarik Zinciri İhlali" şu şekilde açıklanmaktadır:[72]

> *"Cihazlar, yazılımlar ve teslimat mekanizmalarının son kullanıcıya ulaşmadan önce manipüle edilmesi yoluyla sistem güvenliğini tehlikeye atan bir siber saldırı türüdür. Bu tür ihlaller (zafiyetler), geliştirme araç ve ortamlarının yanı sıra yazılım dağıtım mekanizmalarını hedef alabilir ve meşru yazılım yamalarının değiştirilmesini içerebilir. Özellikle kontrol sistemleri gibi BT (bilgi teknolojileri) ve OT (operasyonel teknoloji) ağlarının bir arada bulunduğu ortamlarda, bir BT bileşenindeki zafiyet OT ortamına sızma fırsatları yaratabilir. Ayrıca, sahte cihazların küresel tedarik zincirine dahil edilmesi, güvenlik standartlarını karşılamayan ve düşük kaliteli malzemelerle üretilen ürünlerin varlık sahipleri ve operatörler için ciddi güvenlik ve operasyonel riskler oluşturmasına neden olabilir".*

Yukarıdaki açıklamaya istinaden, bu teknik ve alt tekniğin tedbir olarak yeterli gelmeyeceği, yetenekli saldırgan bir rakibin her çeşit zafiyeti tarayarak bulacağı herhangi bir açıklığı istismar edebileceği vakıadır. Bu açıdan atak matrisindeki diğer teknik ve alt tekniklere genel stratejik ve taktik operasyonel bakışla yaklaşmak faydalı olacaktır. Bu yüzden, teknikleri de kapsayan taktiklerin siber ölüm zincirindeki adımların hepsini içerdiğinden emin olacak şekilde görüntülemek gerekecektir. Aşağıda atak matrisinde her bir saldırı düzlemi (*domain*) için taktik ve kategorileri yer almaktadır:

Tablo 2. Karşılaştırmalı Taktik-Saldırı Düzlemi Atak Matrisi[73]

Taktik \ Domain	***Enterprise*** **(Kurumsal Bilgi Teknolojileri)**	***Mobile*** **(Taşınabilir Cihaz)**	***ICS*** **(Endüstriyel Kontrol Sistemleri)**
Gözetleme	Var	Yok	Yok
Kaynak Geliştirme	Var	Yok	Yok
İlk Erişim	Var	Var	Var
Çalıştırma	Var	Var	Var
Kalıcılık	Var	Var	Var
Yetki Yükseltme	Var	Var	Var

72 MITRE, "T0862: Remote Access Software", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T0862/, erişim 21.01.2025.

73 MITRE, "MITRE ATT&CK Tactics", https://attack.mitre.org/tactics/, erişim 22.01.2025.

Savunma Atlatma	Var	Var	Var
Kimlik Erişimi	Var	Var	Yok
Keşif	Var	Var	Var
Yatay Hareket	Var	Var	Var
Toplama	Var	Var	Var
Komuta ve Kontrol	Var	Var	Var
Veri Sızdırma	Var	Var	Yok
Tepki İşlevini Kısıtlamak	Yok	Yok	Var
Süreç Kontrolünü Bozmak	Yok	Yok	Var
Etki	Var	Var	Var
Ağ Etkileri	Yok	Var	Yok
Uzak Servis Etkileri	Yok	Var	Yok

Çağrı ve telsiz cihazları saldırısı özelinde, söz konusu saldırının yukarıda da belirtildiği gibi en kritik aşaması tedarik zinciri ihlali/zafiyeti olsa da planlayıcı hasım aktörün bu operasyonun başarı şansını tek başına tedarik zinciriyle denemeyeceği göz önüne alınmalıdır. Bu bağlamda atak matrisini daha detaylı ele alarak çalışmanın başında bahsi geçen diğer disiplinlerle benzerlik ve yakınlık kurgulanmalıdır. Benzer şekilde, siber güvenlik disiplini açısından atak matrisi içerisinde yer alan muhtemel ve potansiyel diğer teknik ve taktikleri ele almak araştırmanın sonuçlarını destekleyecektir. Bir önceki paragrafta "İlk Erişim" taktiği gibi "Kaynak Geliştirme" (*Resource Development*) taktiği de saldırıya ilişkin ipuçları verebilecek teknik ve alt teknikleri içermektedir. "Kaynak Geliştirme" taktiği altında yer alan "Altyapı Edinmek" (*Acquire Infrastructure*) tekniği (T1583) de yine benzer bir önlem olarak ifade edilmektedir:[74]

> *"Saldırganlar hedefleme sırasında kullanılabilecek altyapıyı satın alabilir, kiralayabilir veya elde edebilir. Muhasım operasyonları barındırmak ve düzenlemek için çok çeşitli altyapılar mevcuttur. Altyapı çözümleri arasında fiziksel veya bulut sunucuları, etki alanları ve üçüncü taraf web hizmetleri bulunur. Bazı altyapı sağlayıcıları, altyapı edinimini sınırlı veya ücretsiz olarak sağlayan ücretsiz deneme süreleri sunar. Bu altyapı çözümlerinin kullanımı, rakiplerin operasyonları sahneye koymalarına, başlatmalarına ve yürütmelerine olanak tanır. Uygulamaya bağlı olarak, rakipler fiziksel olarak kendilerine bağlanmayı zorlaştıran altyapılar kullanabilir ve ayrıca hızla sağlanabilen, değiştirilebilen ve kapatılabilen altyapıları kullanabilir".*

Saldırılar kapsamında ilintili olabilecek ve yine "İlk Erişim" taktiği altında tedarik zinciri ihlali tekniğinden sonra yer alan "Güvenilir İlişki" (*Trusted Relationship*) tekniği (T1199) de platform olarak dar kapsamlı olmasına rağmen tanım olarak benzer bir önermeyi desteklemektedir:[75]

> *"Saldırganlar, hedeflenen kurbanlara erişimi olan kuruluşları ihlal edebilir veya başka şekillerde bunlardan yararlanabilir. Güvenilir üçüncü taraf ilişkisi aracılığıyla erişim, korunmayan veya bir ağa erişim elde etmenin standart mekanizmalarından daha az incelemeye tabi tutulan mevcut bir*

74 MITRE, "T1583: Acquire Infrastructure", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1583/, erişim 22.01.2025.

75 MITRE, "T1199: Trusted Relationship", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1199/, erişim 23.01.2025.

bağlantıyı kötüye kullanır. Kuruluşlar genellikle dahili sistemleri ve bulut tabanlı ortamları yönetmelerine olanak sağlamak için ikinci veya üçüncü taraf harici sağlayıcılara yükseltilmiş erişim izni verir. Bu ilişkilere örnek olarak BT hizmetleri yüklenicileri, yönetilen güvenlik sağlayıcıları, altyapı yüklenicileri verilebilir. Üçüncü taraf sağlayıcının erişimi, bakımı yapılan altyapıyla sınırlı olacak şekilde tasarlanmış olabilir, ancak kuruluşun geri kalanıyla aynı ağda bulunabilir. Bu nedenle, diğer tarafın dahili ağ sistemlerine erişim için kullandığı "Geçerli Hesaplar" tehlikeye atılabilir ve kullanılabilir".

Yukarıdaki yaklaşımla devam edildiğinde; "İlk Erişim" taktiği altında "Donanım İlaveleri" (*Hardware Additions*) tekniği (T1200) de benzer şekilde tanım ve açıklama olarak vakadaki istismarın kök nedenine yakın olsa bile sadece "Linux", "Windows" ve "MacOS" platformlar için geçerli olması nedeniyle tam anlamıyla örtüşen bir tedbir olmadığı görülmektedir. Yine aynı durumda diğer benzer teknikler; "Trafik Sinyalleşmesi" (*Traffic Signaling*) tekniği (T1205), "Yapay Kodları Saklama" (*Hide Artifacts*) tekniği (T1564), "Zayıf Şifreleme" (*Weaken Encryption*) tekniği (T1600) ve "Ağ Dinleme" (*Network Sniffing*) tekniği (T1040) bu bağlamda, çağrı cihazları saldırısının arka planındaki mantığa yaklaşmakla birlikte tam anlamıyla teknik detaylar örtüşmediği için böyle sofistike bir saldırıyı önleyebilecek bir tedbir olarak uyarlanması, bu çalışma kapsamında değerlendirilmemektedir. Bu sebeple, çağrı cihazı saldırısının kendine özgü yaklaşımı göz önüne alındığında, tehdit aktörlerine karşı atak matrisinde tedbir sağlayabilecek ilintili taktik kategorisine eklenecek yeni bir teknik model önerilmektedir.

4.2. Önerilen Model (TTP & Matris Kategorisi)

Bu çalışma, çağrı cihazı saldırılarını nihai hedef olarak değil, EH, SIGINT ve siber uzay arasında gelişen hibrit tehditlerin erken bir örneği olarak değerlendirmektedir. Önerilen teknik model, bu tür saldırılarda kullanılan taktik, teknik ve prosedürlerin (TTP) yalnızca çağrı cihazlarına değil, benzer sinyal tabanlı sistemlere yönelik genişletilebilirliğini amaçlamaktadır. Bu kapsamda önerilen teknik model, yalnızca çağrı cihazı gibi tekil sistemlere değil; elektromanyetik spektrumda çalışan, düşük bant genişliğine ve yüksek parazit hassasiyetine sahip tüm sistemlere uygulanabilecek şekilde genişletilebilir. Bu yönüyle model, hibrit tehditler karşısında spektrum tabanlı tehdit tespitine yönelik CTI altyapılarına yeni bir matris katkısı sunmayı amaçlamaktadır. Bu bağlamda önerilen model, sinyal istismarı tabanlı saldırıların tespiti için mevcut MITRE ATT&CK çerçevesine SIGINT ve EH bileşenlerinin entegrasyonuna yönelik kavramsal bir açılım sağlamaktadır. Model, dar örneklemlerden yola çıkarak daha kapsayıcı CTI mimarilerine zemin hazırlamayı hedeflemektedir.

Bu hususlardan yola çıkarak saldırıların kendine özgü yapısı nedeniyle içerisinde yer alan EH, RF ve SIGINT kabiliyetleriyle atak matrisi içerisine yeni bir model olarak uygun bir teknik önerisi getirilmektedir. Diğer bir ifadeyle, mevcut CTI yaklaşımı ve MITRE ATT&CK çerçevesinde bu analizlere istinaden EH ve RF sinyalleriyle ilişkili saldırı izlerini tespit edebilecek kabiliyetlere haiz bir teknik önerilmektedir. Örneğin, RF sinyallerinin manipülasyonu, iletişim cihazlarının hedef alınması veya EH tekniklerinin uygulandığı durumlar, matris içinde kapsamlı bir teknik kategoriye dönüşmektedir. Dolayısıyla atak matris altında bilinen saldırıların tespiti ve müdahalesine yönelik mevcut teknikleri tekrar etmek yerine, dijital ve fiziksel ortamların kesişim kümesinde gerçekleşen hibrit tehditlere dair yeni bir perspektif geliştirilmektedir. Özellikle çağrı ve telsiz cihazlarına yönelik saldırılardan yola çıkarak, bu olaylar örnek olay formatında değerlendirilmiş ve siber-fiziksel alanlarda faaliyet gösteren hasım aktörlerin kullandığı taktiklerin modellenmesi hedeflenmiştir.

Bu bağlamda, klasik MITRE ATT&CK matrisinin kapsamadığı EH, RF ve SIGINT unsurları dikkate alınarak yeni bir teknik kategori önerilmektedir. Özellikle iletişim altyapılarının manipülasyonu, RF sinyallerinin yönlendirilmesi veya bozulması, EH teknikleri ile iletişimin engellenmesi gibi eylemler, geleneksel CTI araçlarının dışında kalan, ancak artan oranda karşılaşılan bir tehdit sınıfını oluşturmaktadır. Üstelik bu çalışma, çağrı cihazları gibi örnek olaylardan ilhamla, gelecekte farklı platformları da hedef alabilecek benzer tehditlere karşı genişletilebilir bir model sunmaktadır. Model önerisi, yalnızca çağrı cihazı kategorisiyle sınırlı olmayıp, benzer RF tabanlı veya radyo link sistemlerine yönelik tehditlerin de modellenmesine olanak tanıyacak biçimde geniş bir yelpazede düşünülmüştür. RF jammer cihazları, spektrum analizörleri, yazılım tanımlı radyo (SDR) sistemleri gibi hem donanım hem yazılım tabanlı unsurlar, bu tür saldırıların teknik ayak izlerini oluşturmakta ve siber-fiziksel saldırıların dijital CTI platformlarına entegrasyonu için yeni araçlara ihtiyaç duyulmaktadır.

Bu çerçevede önerilen teknik model, EH/RF izlerinin dijital tehdit istihbarat sistemlerinde yapılandırılmış biçimde izlenmesini sağlayacak yazılım araçları, teknik göstergeler ve ilişkilendirme mekanizmalarının geliştirilmesini önermektedir. Böylece tehdit istihbaratı yalnızca ağ trafiği veya zararlı yazılımlar üzerinden değil, sinyal tabanlı manipülasyon teknikleri üzerinden de zenginleşecektir. Araştırmanın odaklandığı çağrı cihazları saldırısı örneği, bu kapsayıcı modelin somut bir çıkış noktası olarak değerlendirilmelidir. Sonuç olarak bu çalışma kapsamında yürütülen araştırma, çağrı cihazları özelinde gelişse de RF spektrum temelinde yer alan tüm sistem ve altyapılar dahil edilebilir durumdadır. Bu noktada hedef alınabilecek sistemlere yönelik ilk aşamada önlem olarak yeni teknik model önerisi aşağıdaki gibidir:

Tablo 3. RF Spektrumu ve Sinyalleri için Yeni Teknik Model Önerisi

Teknik:	"T1569.xx – Spectrum-Based Signal Injection"
Taktik:	"Execution" (Çalıştırma)
Teknik Adı: "Spectrum-Based Signal Injection" (Spektrum Tabanlı Sinyal Enjeksiyonu)	
Tanım:	Saldırganlar, belirli RF spektrumlarını hedef alarak telsiz, çağrı cihazı veya diğer sinyal tabanlı haberleşme sistemlerine sahte mesajlar enjekte edebilir. Bu teknik, sinyal manipülasyonu yoluyla bilgi akışını bozmak, yanlış yönlendirme yapmak veya kriz anlarında karar destek sistemlerini yanıltmak amacıyla kullanılabilir. Özellikle acil servisler, endüstriyel kontrol sistemleri ve askerî birimlerde kritik operasyonel sonuçlar doğurabilir.

Böyle bir saldırı yüzeyinde hedefe ulaşan saldırganlar aksiyon alırken *"*sahte acil tıbbi çağrılar oluşturarak sağlık sistemlerinde kriz yaratabilir" veya "kritik altyapıyı yöneten teknisyenleri yanlış yönlendirerek operasyonları aksatabilir" veyahut da "acil durum servislerini sahte tehditlerle yanlış yönlendirerek gerçek tehditleri gizleyebilir". Bu yönde bir saldırının tedbirleri olarak birtakım iyileştirme (*mitigation*) önerileri aşağıda listelenmektedir:

- **Şifreleme Kullanımı:** Modern çağrı cihazı sistemlerinde uçtan uca şifreleme uygulanmalıdır.
- **Sayısal İmza:** Mesaj bütünlüğünü korumak için sayısal imza kullanılmalıdır.
- **RF Anomali Algılama:** Radyo trafiğini analiz eden sistemler sahte mesajları tespit etmektedir.

- **Çok Faktörlü Doğrulama:** Kritik mesajlar için ikinci bir doğrulama gerekmektedir.

Bu teknik için iyileştirme önerilerinin hayata geçirilmesi, sadece teknik bir çabanın ötesinde, kapsamlı politika ve stratejik düzenlemeler gerektirmektedir. Örneğin, "Şifreleme Kullanımı" ve "Sayısal İmza" gibi önlemlerin yaygınlaştırılması, kritik iletişim altyapılarında kullanılacak cihazlar için ulusal düzeyde asgari güvenlik standartlarının belirlenmesini ve bu standartlara uyumun denetlenmesini sağlayacak yasal ve kurumsal çerçevelerin oluşturulmasını zorunlu kılmaktadır. Telekomünikasyon düzenleme kurumları, ulusal siber güvenlik merkezleri ve ilgili bakanlıkların koordinasyonu, bu politikaların etkin bir şekilde uygulanmasında kritik rol oynamaktadır.[76] "RF Anomali Algılama" sistemlerinin geliştirilmesi ve entegrasyonu, ulusal sinyal istihbaratı ve elektronik harp kapasitelerinin sivil ve kritik altyapıların korunmasına yönelik olarak da planlanmasını gerektirmektedir. Bu tür yetenekler, bir ülkenin teknolojik bağımsızlığını ve bilgi üstünlüğünü pekiştirerek ulusal gücün bir unsuru haline gelir. Ayrıca, "Çok Faktörlü Doğrulama" gibi önlemlerin benimsenmesi, sadece teknik bir güvenlik katmanı eklemekle kalmaz, aynı zamanda kullanıcıların güvenlik bilincini arttırarak olası sosyal mühendislik saldırılarına karşı psikolojik bir direnç de oluşturur.[77] Bu tür bütüncül yaklaşımlar, devletlerin hibrit tehditlere karşı caydırıcılığını güçlendirip kriz anlarında iletişim sistemlerine olan güvenin sarsılmasını engelleyerek toplumsal paniğin de önüne geçebilir.

Teknik model önerisinin atak matrisi içinde "Çalıştırma" (*Execution*) taktiği altında eklenmesi uygun görünmektedir. Hem aktif saldırılarda (operasyon manipülasyonu) hem de kaos yaratmak için (bilgi harbi ve dezenformasyon) kullanılabilecek bir saldırı vektörü olarak ele alınmalıdır. Hizbullah'a karşı Mossad tarafından gerçekleşen saldırılar, siber atak yüzeyi dijital ortamlardan ziyade analog varsayılan çağrı ve telsiz cihazlarına yönelik olduğu için, Elektronik Harp, RF ve SIGINT gibi yetenek ve kapasitelerini öne çıkaracak teknik model önerisi kurgulanmıştır. Bu açıdan, Hizbullah hedeflerine yönelik saldırılar, aynı zamanda bir istihbarat operasyonu olarak kabul edilse de sürecin teknoloji ayağında, EH, SIGINT ve RF manipülasyonunu içeren bu tür hibrit saldırılara ilişkin aşağıdaki gibi bir teknik model önerisi önerilmektedir:

Tablo 4. RF Sinyal ve Çağrı/Telsiz Haberleşme Özelinde Teknik Model Önerisi

Teknik:	"T1602.xx – RF Message Injection & Manipulation"
Taktik:	"Impact" (Etki)
Teknik Adı: "RF Message Injection & Manipulation" (RF Mesaj Enjeksiyonu ve Manipülasyonu)	
Tanım:	Saldırganlar, eski tip çağrı cihazları, telsiz haberleşmesi (VHF/UHF), ve diğer RF tabanlı analog-dijital sistemleri hedef alarak sahte mesajlar gönderebilir, EH ve SIGINT kabiliyetleriyle mevcut mesajları değiştirebilir veya iletişimi kesintiye uğratabilir.

SIGINT ve EH yetenekleriyle desteklenerek özellikle askerî gruplar, istihbarat servisleri ve devlet destekli aktörler tarafından tetiklenebilecek bu saldırı türü, mevcut dijital altyapı yerine analog veya hibrit ortamlarda gerçekleştirir. Önerilen bu teknik modelin adımları ise şu şekilde sürdürülür:

76 Serkan Gündoğdu, "Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM)", *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33:3, 2023, s. 1325-1337.

77 Scott D. Applegate, "Social Engineering: Hacking the Wetware!", *Information Security Journal: A Global Perspective*, 18:1, 2009, s. 40-46.

- **RF Sinyal Toplama:** Hedef telsiz/çağrı cihazı frekansları belirlenir.
- **Protokol Analizi:** Kullanılan haberleşme protokolleri incelenir.
- **Mesaj Enjeksiyonu:** Sahte mesajlar oluşturularak operasyonel yanlış yönlendirme yapılır.
- **Karıştırma ve Şifre Kırma:** Analog veya zayıf şifrelemeye sahip haberleşmeler engellenir veya deşifre edilir.
- **Psikolojik Operasyonlar ve Aldatma:** Yanlış bilgiler yayarak düşmanın karar mekanizmaları etkilenir.

Önerilen teknik modelin saldırı adımlarını inceleyerek buna yönelik çeşitli iyileştirme önerileri ihtiyaç vardır. Bu yüzden MITRE ATT&CK çerçevesi dahilinde üç farklı saldırı düzlemi olan matris içerisinde iyileştirme (*mitigation*) olarak geçen bu seçeneklere dair çalışma kapsamında aşağıdaki gibi bir tablo ilave edilmiştir:

Tablo 5. Önerilen Teknik Model için İyileştirme Seçenekleri

ID	İyileştirme Adı	Açıklama
M1030/0930 – *Network Segmentation* (Ağ Segmentasyonu)	Şifreli ve Güvenli Haberleşme Protokolleri	RF tabanlı sistemlerde AES-256 veya ECC şifreleme ve kimlik doğrulama kullanarak sahte mesajların enjekte edilmesi önlenir.
M1031 – *Network Intrusion Prevention* (Ağ Saldırısı Önleme)	RF Sinyal Filtreleme ve Anomali Algılama	SDR-tabanlı izleme sistemleri ile anormal RF sinyalleri tespit edilir ve sahte mesaj girişimleri engellenir.
M1037 – *Filter Network Traffic* (Ağ Trafiği Filtreleme)	Frekans Atlamalı Spektrum Yayılımı (FHSS) ve LFM Kullanımı	Düşman RF sinyal analizine karşı FHSS/LFM gibi tekniklerle haberleşme güvence altına alınır.
M1038/0938 – *Execution Prevention* (Çalıştırma Önleme)	Çok Katmanlı Doğrulama Mekanizmaları	Gelen RF mesajlarını ikinci bir kanal (şifreli uygulamalar, sesli doğrulama) ile kontrol ederek sahte mesaj enjeksiyonları engellenir.
M1029 – *Remote Data Storage* (Uzak Veri Depolama)	Sinyal İstihbaratı ve Olay Müdahale Ekipleri	EH ve SIGINT ekipleri entegre edilerek düşman RF operasyonları izlenir ve proaktif müdahale edilir.

Bu saldırı tekniği, RF tabanlı analog veya modern hibrit haberleşme sistemlerine yönelik ciddi bir tehdit oluşturduğundan, önerilen iyileştirme stratejileri (Tablo 5) çok katmanlı bir yaklaşımla ele alınmaktadır. Bu stratejiler, sadece teknik önlemleri ve operasyonel prosedürleri değil, aynı zamanda politika yapım süreçlerini, kurumsal yapılanmaları ve ulusal güvenlik anlayışlarını da kapsamaktadır. Böylece MITRE ATT&CK matrisi, sadece teknik bir referans olmaktan çıkarak hibrit tehditlere karşı bütüncül ve disiplinler arası bir strateji geliştirme aracı haline gelebilir.

Ağ Segmentasyonu iyileştirme adımı, teknik düzeyde şifreleme standartlarının benimsenmesini önermekle birlikte, politika düzeyinde bu standartların kritik sektörlerde zorunlu hale getirilmesi, ilgili yasal düzenlemelerin yapılması ve uyum denetim mekanizmalarının kurulmasını gerektirmektedir. Bu, ulusal bir politika kararıdır ve telekomünikasyon otoriteleri ile siber güvenlik kurumlarının eşgüdümünü zorunlu kılmaktadır.

Ağ saldırısı önleme, ağ trafiği filtreleme ve çalıştırma önleme adımları politika yapım süreçleri açısından, gerekli teknolojilerin geliştirilmesi ve yaygınlaştırılması için Ar-Ge faaliyetlerini, spektrum yönetimi politikalarının güvenlik odaklı güncellenmesini ve bu sistemlerin ulusal

erken uyarı ve müdahale merkezlerine entegrasyonunu gerektirmektedir. Bu tür yetenekler, ülkenin elektromanyetik spektrum üzerindeki egemenliğini pekiştirmekle kalmayıp hasım aktörlerin RF tabanlı saldırılarına karşı caydırıcılık oluşturarak ulusal güvenliğe doğrudan katkı sağlayacaktır. Psikolojik olarak, bu tür görünür etkin savunma sistemlerinde, kamuoyunun devletin koruma kapasitesine olan güvenini arttıracağı beklenebilir.

Uzak Veri Depolama (M1029) başlığı altında önerilen EH ve SIGINT ekiplerinin entegrasyonu, doğrudan bir ulusal güvenlik ve istihbarat politikası meselesi konumundadır. Bu tür entegre ekiplerin oluşturulması, farklı kurumlar (askerî, sivil istihbarat, siber güvenlik merkezleri ve kolluk kuvveti) arasında etkin bir iş birliği ve bilgi paylaşım mekanizmasının kurulmasını gerektirmektedir. Kurumsal olarak, bu ekiplerin yetki ve sorumluluklarının net bir şekilde tanımlanması, yasal altyapılarının güçlendirilmesi ve sürekli tatbikatlarla operasyonel yeteneklerinin geliştirilmesi elzemdir. Bu tür bir yapılanma, düşman RF operasyonlarının proaktif bir şekilde izlenmesi ve bunlara hızlı müdahale edilmesi sayesinde, potansiyel bir krizin büyümeden engellenmesine veya etkilerinin minimize edilmesine olanak tanıyacaktır.

5. Tartışma ve Güvenlik Analizi

Bu bölüm, çalışmanın konusunda ifade edilen mevcut matris ve önerilen modele ilişkin güvenlik analizi ve tartışma kısımlarını içermektedir.

5.1. Tartışma

İsrail'in bu operasyonu, MITRE ATT&CK çerçevesinde yer almayan ancak elektromanyetik spektrum temelli tehditlerin, tedarik zinciri manipülasyonu ile birleştiğinde, siber güvenlik modellerine nasıl entegre edilmesi gerektiğine dair önemli ipuçları sunmaktadır. İlk aşamada, İsrail'in Hizbullah'a yönelik yürüttüğü saldırılar, eş zamanlı patlamalarla iki dalga halinde gerçekleştirilmiş ve ilk gün "çağrı" cihazlarını, ikinci gün ise "el telsizi" cihazlarını hedef almıştır. Bu saldırılar, Hizbullah içinde operasyonel bütünlüğü bozmak ve karar alma süreçlerini sekteye uğratmak amacı taşımaktadır. İsrail'in bu saldırılarda yalnızca fiziksel hedeflere değil, aynı zamanda psikolojik ve operasyonel etkiler yaratmaya odaklandığı belirtilmektedir. Özellikle bu saldırıların zamanlaması ve hedef seçimleri, dijital harp ile geleneksel askerî operasyonların hibrit bir stratejiyle nasıl bütünleştirildiğini göstermektedir. İlk iki gün süren dijital harp sonrası Tel Aviv'in doğrudan askerî müdahaleye geçmesi, operasyonel süreçlerin çok katmanlı planlandığını ortaya koymaktadır.[78]

Söz konusu yukarıdaki ifadelere dayanarak araştırma kapsamında dijital harp sahasında EH ve SIGINT imkanlarının siber istihbarat ve CTI kabiliyetleriyle ele alınarak hibrit ve disiplinler arası yaklaşımla kurgulanabileceği potansiyelini göstermektedir. Çünkü İsrail'in bu operasyonu gerçekleştirme biçimi, insan istihbaratı ile siber, sinyal ve elektronik istihbaratın entegre edildiği, yüksek hassasiyetle yürütülen bir planlamayı işaret etmektedir. Özellikle Hizbullah'ın haberleşme cihazlarına yönelik gerçekleştirilen saldırıların, tedarik zincirine sızma yoluyla mümkün hale geldiği vurgulanmaktadır. İsrail'in, hedeflenen cihazların tedarik sürecine önceden müdahale ederek, cihazlara patlayıcı veya zararlı yazılım yerleştirdiği ve bu sayede hedefe doğrudan zarar vermeden önce haberleşme altyapısını çökerttiği belirtilmektedir. Bu durum, tedarik zinciri saldırılarının modern askerî stratejilerde nasıl kritik bir unsur haline geldiğini ve elektronik harp ile siber güvenlik arasındaki sınırların giderek bulanıklaştığını göstermektedir. Bu operasyon hem askerî hem

78 Merve Seren, "İsrail'in Yeni İstihbarat Operasyonu: Pager ve Walkie-Talkie saldırıları", *Fikir Turu*, 24 Eylül 2024, https://fikirturu.com/jeo-politika/israilin-yeni-istihbarat-operasyonu/, erişim 25.09.2024.

de istihbarat doktrinlerinde yeni bir paradigma oluşturmuştur ve tedarik zinciri güvenliğinin, ulusal güvenlik stratejilerinde öncelikli bir unsur olması gerektiğine dikkat çekmiştir.[79]

Bu çalışmanın temel araştırma sorularından birisi olan "MITRE ATT&CK çerçevesi, elektromanyetik spektrum ve tedarik zinciri güvenliği boyutları eklenerek nasıl genişletilebilir?" ifadesine yanıt ararken, ATT&CK matrisinin mevcut sınırları ile analog ve fiziksel sistemleri yeterince kapsayamayan yapısı ortaya çıkmaktadır. Özellikle elektromanyetik spektrum temelli saldırılar ve donanım tedarik zincirine yönelik tehditler, mevcut çerçevede bütünsel olarak temsil edilmemektedir. İsrail'in Lübnan'da gerçekleştirdiği sinyal tabanlı saldırı operasyonu bu boşluğa dikkat çekmekte ve yeni bir modelleme ihtiyacını gündeme getirmektedir.

MITRE ATT&CK çerçevesi, esas olarak yazılım ve ağ katmanlarında çalışan dijital saldırı tekniklerini modellemekte başarılıdır. Ancak elektromanyetik spektrum üzerinden gerçekleştirilen saldırılar, özellikle RF tabanlı iletişim cihazlarını hedef aldığında, bu çerçevede kendisine karşılık bulamamaktadır. "Spectrum-Based Signal Injection" tekniğiyle önerilen yeni modelleme, özellikle çağrı cihazları gibi analog sistemlerin güvenlik boyutunu MITRE terminolojisi içine entegre etmeyi hedeflemektedir. İsrail'in saldırısı örneğinde olduğu gibi, analog haberleşme protokollerini hedefleyen düşük frekanslı enjeksiyonlar, dijital ağ güvenliği araçlarıyla tespit edilememekte, buna karşılık taktik ve operasyonel seviyede yüksek etkiler yaratmaktadır. Bu durum, elektromanyetik spektrumun saldırı yüzeyi olarak modellenmesi gerektiğini ve bu alanın MITRE içinde ayrı bir kategori olarak ele alınmasını zorunlu kılmaktadır.

Gerçekleşen saldırıların en başından itibaren dillendirilen tedarik zinciri zafiyeti ve istismarı siber istihbarat disiplininde ve MITRE çerçevesinde halihazırda kendisine yer bulmaktadır. Ancak mevcut MITRE çerçevesinde yer alan teknikler üç farklı saldırı düzlemi (*domain*) için de dijital tabanlı cihazlar için uygulanabilir yöntemleri içermektedir. Lakin gerçekleşen çağrı cihazı saldırılarının RF sinyalleri işleyecek analog tabanlı veya analog-dijital dönüştürücü modülleri içeren cihazlara yönelik olduğu bir vakıadır. Hizbullah'ın basit tasarıma sahip çağrı cihazlarını kullanması, modern gözetim sistemlerinden kaçınma amacı taşırken, bu durum aynı zamanda cihazların güvenlik açıklarının kurcalanmasına karşı savunmasız hale gelmesine de neden olmuştur. Modern şifreleme veya kurcalamaya karşı koruma mekanizmalarından yoksun olan bu cihazlar, kolayca modifiye edilebilecek bir zafiyet yaratmıştır. İsrail'in bu güvenlik açığını istismar ettiği ve Hizbullah'ın lojistik ekipleri tarafından fark edilmeyecek şekilde çağrı cihazlarına patlayıcı maddeler yerleştirdiği değerlendirilmektedir. Bu sürecin, paravan bir şirket aracılığıyla gerçekleştirilen kontrollü bir üretim ve teslimat mekanizması üzerinden yürütüldüğü, ardından senkronize bir patlatma ile operasyonun tamamlandığı düşünülmektedir. Bu durum, düşük teknolojili cihazların basit yapılarının dahi istihbarat operasyonlarında nasıl stratejik bir avantaja dönüştürülebileceğini göstermektedir.[80]

ATT&CK matrisinde tedarik zinciri saldırılarına ilişkin belirli teknikler bulunsa da bunlar daha çok yazılım güncellemeleri ve lojistik manipülasyonlar çerçevesinde sınırlı kalmaktadır. Oysa modern siber-fiziksel saldırılar, donanım bileşenlerinin üretiminden yerleşik anten yapılarına kadar geniş bir yelpazeyi hedef almaktadır. İsrail'in saldırısında kullanılan sinyal enjeksiyonu tekniği, yalnızca mesaj içeriklerini değil, mesajların alındığı

79 Age.

80 Salih Bıçakçı, "Lübnan'da Patlayan Çağrı Cihazları: Elektronik Harp, Siber Sabotaj ve Kötülüğün Sıradanlığı", *Fikir Turu*, 23 Eylül 2024, https://fikirturu.com/jeo-politika/lubnanda-patlayan-cagri-cihazlari/, erişim 24.09.2024.

cihazın fiziksel kabiliyetlerini de manipüle etmiştir. Bu durum, ATT&CK çerçevesinin donanım güvenliğine ilişkin daha derinlemesine alt tekniklerle genişletilmesi gerektiğini göstermektedir. Zira Lübnan'daki operasyon kapsamında çağrı cihazlarının eşzamanlı patlaması, RF sinyalleri ve donanım yazılımı manipülasyonuna dayalı karmaşık bir mühendislik çalışması ile açıklanabilir. Çağrı cihazlarının basit tasarımı ve sınırlı işlem kapasitesi, modern güvenlik protokollerinden yoksun olmaları nedeniyle, RF sinyalleriyle uzaktan tetiklenmeye veya ürün yazılımına yönelik bir sabotaja açık hale gelmiştir. Olası senaryolardan biri, cihazlara güç yönetim sistemlerini etkileyen özel bir RF sinyali gönderilmesi ve elektrik akımında bir dalgalanma yaratılarak patlamaların başlatılmasıdır. Diğer olasılık ise, cihazların belirli bir RF frekansına ayarlanarak merkezi bir "patlatma" komutunu algılayacak şekilde tasarlanmış olmasıdır. Ayrıca, cihazların ürün yazılımına önceden yerleştirilen bir arka kapı sayesinde, belirli bir sinyal veya zaman gecikmeli komutla patlamaların tetiklenmesi mümkün olabilir. Bu durumda, senkronizasyonun sağlanması için cihazlara küçük zamanlayıcıların entegre edilmesi ve bu zamanlayıcıların RF sinyalleri ile tetiklenmesi muhtemeldir. Bu operasyon, istihbarat örgütlerinin düşük teknolojili cihazlara yönelik hassas mühendislik ve karmaşık siber/elektronik manipülasyon tekniklerini başarıyla birleştirdiğini gösteren bir planlama örneği olarak literatüre geçmiştir.[81]

Bu bağlamda geliştirilen "T1569.xx – *Spectrum-Based Signal Injection*" ve "T1602.xx – *RF Message Injection & Manipulation*" teknik model önerileri, teknik düzeyde hem elektromanyetik hem donanım hem de taktiksel bütünlük açısından hibrit bir saldırı modelini temsil etmektedir. Bu öneri, halihazırda "Çalıştırma" (*Execution*) taktiği altında yer alan benzer tekniklerle kavramsal bir akrabalık taşımakta ancak donanımsal sinyal manipülasyonlarını kapsayan yeni bir katman tanımlamaktadır. Böylece, ATT&CK çerçevesi genişletilerek, analog/dijital hibrit savaş alanlarına daha duyarlı hale getirilebilir. Tüm bu bulgular, araştırma sorusunun ortaya koyduğu boşluğun somut örneklerle desteklendiğini göstermektedir. MITRE ATT&CK çerçevesi, elektromanyetik spektrumun ve donanım temelli saldırıların dikkate alınmadığı sürece, hibrit savaş ve istihbarat operasyonlarının gerçekliğini modellemekte yetersiz kalmaktadır. Bu nedenle, elektromanyetik spektrum tabanlı saldırılar ve fiziksel cihaz manipülasyonları, çerçevenin genişletilmesi gereken temel alanlar olarak önerilmekte ve "Spektrum Tabanlı Sinyal Enjeksiyonu" ve "RF Mesaj Enjeksiyonu ve Manipülasyonu" bu genişlemenin bir ön modeli olarak sunulmaktadır.

5.2. Güvenlik Analizi

Bu çalışmada analiz edilen olaylar, hibrit tehditlerin operasyonel güvenliğe yönelik çok yönlü riskler barındırdığını ortaya koymaktadır. EH, SIGINT ve RF teknikleri ile siber saldırılar arasında giderek belirsizleşen çizgiler, geleneksel güvenlik önlemlerinin yeterliliğini sorgulatmaktadır. Özellikle, RF tabanlı sinyallerin ve iletişim altyapılarının manipülasyonu gibi tehditler, siber tehdit istihbaratı çerçevesinde ele alınması gereken yeni bir kategoriye veya matris içerisinde uygun taktik altında bir tekniğe işaret etmektedir. Dünya genelinde hükümetleri ve kuruluşları siber güvenlik çerçevelerini yeniden değerlendirmeye sevk eden[82] ve analiz edilen çağrı cihazı saldırıları olayı, hibrit tehditlerin sadece teknik bir zafiyetten ibaret olmayıp aynı zamanda operasyonel güvenliğe, toplumsal psikolojiye ve uluslararası ilişkilere yönelik çok yönlü riskler barındırdığını çarpıcı bir şekilde ortaya koymaktadır. Özellikle, RF tabanlı sinyal tehditleri, CTI ve genel güvenlik analizleri çerçevesinde

81 Age.

82 Pantha Protim Sarker, Upoma Das, Nitin Varshney, Shang Shi, Akshay Kulkarni, Farimah Farahmandi ve Mark Tehranipoor, "When Everyday Devices Become Weapons: A Closer Look at the Pager and Walkie-Talkie Attacks", arXiv preprint arXiv:2501.17405, 2025.

ele alınması gereken, ancak mevcut yaklaşımların tam olarak kapsayamadığı yeni risk kategorileri oluşturmaktadır. Bu durum, güvenlik analizlerinin sadece teknik zafiyetlere değil, aynı zamanda bu zafiyetlerin istismar edilme biçimlerinin ardındaki stratejik niyetlere, sosyopolitik bağlamlara ve potansiyel toplumsal etkilere de odaklanması gerektiğini göstermektedir.

MITRE ATT&CK çerçevesini görselleştiren atak matrisi üzerinde RF ve EH tabanlı saldırıları siber tehditlerle ilişkilendirmek zorlayıcı ve anlaşılmaz olabilir. Matristeki taktik ve tekniklerin kapsamıyla söz konusu alanların doğası uyuşmayabilir. Örneğin, iletişim cihazlarının bozulması veya ele geçirilmesi gibi RF manipülasyon teknikleri, "Komuta ve Kontrol" veya "İlk Erişim" aşamalarında daha önce tanımlanmamış saldırı vektörleri olarak incelenmektedir. Bu tür bir genişletme, özellikle siber tehdit istihbaratıyla ve atak matrisiyle somutlaştırılan kategorilerin yapısını kullanışsız hale getirebilir. Sonuç olarak, hibrit saldırıların karakteristiğini yansıtan RF ve EH tabanlı bileşenlerin, tehdit istihbaratı analizinde ayrı bir odak noktası haline getirilmesi hem siber hem de fiziksel güvenlik mekanizmalarının iyileştirilmesine olanak tanıyacak şekilde ele alınmıştır. Ancak sinyal istihbaratı ile EH veya RF yöntemleri, mevcut atak matrisinin işleyişini sekteye uğratmayacak şekilde kurgulanmıştır.

Önerilen teknik modelin ve iyileştirme stratejilerinin bir diğer önemli kırılganlığı, çağrı cihazı saldırılarında görüldüğü gibi, iyi kurgulanmış ve devlet destekli sofistike istihbarat operasyonlarına karşı tam bir koruma sağlayamama ihtimalidir. Bir devletin, elindeki geniş imkân ve kabiliyetler (insan istihbaratı, teknik istihbarat, diplomatik ve ekonomik araçlar) sayesinde, mevcut savunma mekanizmalarını aşabilecek özgün ve çok katmanlı bir hibrit saldırı operasyonu planlaması her zaman mümkündür. Böyle bir durumda, MITRE ATT&CK matrisine eklenecek yeni teknikler dahi yetersiz kalabilir. Bu, siber güvenliğin ve genel olarak ulusal güvenliğin sadece teknik tedbirlerle sağlanamayacağını, aynı zamanda güçlü bir karşı-istihbarat kapasitesi, stratejik öngörü, uluslararası iş birlikleri ve toplumsal direnç gibi unsurları da gerektirdiğini göstermektedir. Bu bağlamda, güvenlik analizleri, sadece bilinen tehdit vektörlerine değil, aynı zamanda potansiyel "bilinmeyen bilinmeyenlere" karşı da esneklik ve adaptasyon yeteneği geliştirmeye odaklanmalıdır.

Hizbullah'a yönelik çağrı cihazı operasyonu, istihbarat, sabotaj ve düşük yoğunluklu savaş stratejileri açısından önemli bir dönüm noktası olarak değerlendirilmektedir. Bu operasyon, siber çatışma, elektronik harp ve fiziksel savaşın giderek daha fazla iç içe geçtiğini ve modern istihbarat operasyonlarının artık dijital ve fiziksel alanların birleşimini kapsadığını ortaya koymaktadır. Yapay zekâ ve diğer gelişen teknolojilerin bu tür saldırılara açık olduğu düşünüldüğünde, gelecekte daha karmaşık ve sofistike operasyonların gerçekleşmesi olası görünmektedir.[83] Bu durum, teknolojinin yıkıcı potansiyelinin sınırlandırılması meselesini gündeme getirmektedir. Bu sınırlamanın sadece teknik önlemlerle değil, aynı zamanda uluslararası düzeyde kabul görmüş etik normlar, ortak ahlaki kabuller ve uluslararası hukuk çerçeveleri ile mümkün olabileceği düşünülmektedir.[84] Ancak savaşın değişen doğası günümüzde teknolojik yenilikler ve siyasi gelişmeler tarafından şekillenmektedir. Bu durum, hükümetlerin ve bireylerin savaş sırasındaki eylemlerini değerlendirmek için uluslararası hukuk ve haklı savaş doktrini etkisinde kullanılan geleneksel standartlara karmaşık meydan

83 Izabela Marszałek-Kotzur, "Ethical Perspective of the Development and Use of Modern Military Technologies", *Scientific Papers of Silesian University of Technology Organization & Management*, 165, 2022.
84 Luciano Floridi, *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, 2010.

okumalar sunmaktadır.[85] Esnek yapısından dolayı bir güç dengesizliğinin varlığında hukukun güçlüden yana tavır aldığı bir dünyada,[86] normların ve hukuk kurallarının oluşturulması, benimsenmesi ve etkin bir şekilde uygulanması, devletlerin egemenlik anlayışları, ulusal güvenlik çıkarları ve teknolojik rekabet gibi faktörler nedeniyle karmaşık bir politik süreçtir. Zira bazı ağır suçlarda devletlerin kendi sınırları dışındaki olayları yargılamasına olanak tanıyan, devlet egemenliğini sınırlayan bir yetki olan evrensel yargı yetkisinde dahi, hangi suçların kapsama girdiği ve yargılama yetkisinin nasıl paylaşıldığı uzun sürelerdir tartışılagelen bir konudur.[87]

Cenevre Sözleşmesi, saldırıların yalnızca askerî unsurlara yöneltilmesini, sivil hedefleri ise hariç tutmasını zorunlu kılmaktadır. Ölümcül otonom silahların etik ilkelerle programlanarak savaşta insan müdahalesinin yerini alması ve tutarlı yetenekleri sayesinde, etik savaş yürütmede daha ileri keşifler yapılana dek insan faktörünün çatışmalardan çıkartılması gerektiği belirtilmektedir.[88] Ancak otonom olarak gerçekleştirildiği değerlendirilen çağrı cihazı operasyonu da çağrı cihazlarının savaşçı olmayan kişilere ve olaya karışmamış sivillere, hatta patlamadan hemen önce cihazları yanlışlıkla almış olabilecek çocuklara da dağıtılmış olabileceği, çağrı cihazının patladığı an itibarıyla kimin taşıdığının bilinmediği ve belki de bilinemeyeceği iddia edilerek saldırının hukukiliği yönünde eleştirilere konu olmuştur.[89]

Bu sebeple bu tür tehditlere karşı ulusal güvenlik politikaları için üretilecek stratejik ve politik çıkarımlar hem teknolojik hem de hukuki ve yönetsel değişkenleri içermelidir. Siyaset, politikayı (devletin amaç ve hedeflerini) üretir. Strateji ise bu politikayı, askerî unsurlarla ilişkilendirir ve politikanın arzu edilen hedeflerine ulaşılmasını sağlayacak askerî kuvvetleri ve görevlerini belirler. Operasyonel ve taktik seviyeler ise strateji tarafından belirlenen somut görevleri icra eder.[90] Özellikle uluslararası tehditlerin oluşmasını beklemek tehlike arz eden bir stratejidir.[91] Bu bağlamda yeni tehditler ve güvenlik açıklarının tespiti amacıyla, tehdit algılama mekanizmaları etkin bir şekilde kullanılmalı ve tahkim edilmelidir. Bu kapsamda, ihlal veya saldırı bulma ve yanıt verme ekiplerinin kapasiteleri arttırılarak, proaktif bir güvenlik duruşu sağlanmalıdır. Mevcut cihazların elektromanyetik dayanıklılığını arttıracak modifikasyonların yanı sıra bu direnci barındıran cihazların temini de uygun olmakla birlikte[92] bu tür kritik teknolojileri yerli imkanlarla geliştirmek ve üretmek bir tercih değil, mutlak bir zorunluluk haline gelmiştir.[93]

85 Scott D. Sagan, "Ethics, Technology & War", *Daedalus*, 145:4, 2016, s. 611.

86 Burak Güneş, "Egemenlik ve İnsancıl Müdahale: Çelişkili Bir Kuram Olarak Uluslararası Hukuk", *Güvenlik Bilimleri Dergisi*, 10:1, 2021, s. 31-58.

87 Merve Ş. Akdemir, "Egemenlik ve Evrensel Yargı Yetkisi İlişkisinin Uluslararası Ceza Hukuku Boyutu", *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 8:2, 2022, s. 261275.

88 Steven Umbrello, Phil Torres ve Angelo F. De Bellis, "The Future of War: Could Lethal Autonomous Weapons Make Conflict More Ethical?", *AI & Society*, 35:1, 2020, s. 273-282.

89 Amichai Cohen ve Yuval Shany, "Well, it Depends: Explosive Pagers Attack Revisited", *Articles of War*, 11 Ekim 2024, https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/, erişim 24.09.2024; Fabio Massacci, "Exploding Pagers and the Birth of State Cyberterrorism", *IEEE Security & Privacy*, 23:1, 2025, ss. 4-6

90 Murat Caliskan, "Hybrid Warfare and Strategic Theory", *Horizon Insights*, 6, 2019.

91 Cahit Karakuş, "Kritik Alt Yapılara Siber Saldırı", *Yüksek Lisans Tezi*, İstanbul Kültür Üniversitesi, 2013.

92 Shobendra S. Mahat, "Vulnerabilities of the Communication System to an Electromagnetic (EM) Attack, Threat Assessment and Mitigation", *The Shivapuri Journal*, 26:1, 2025, s. 134-144.

93 Halil Ibrahim Sincar ve Bestami Bodruk "Turkish Minister Underscores Need for National Technology after Pager Explosions in Lebanon", *Anadolu Ajansı (AA)*, 18 Eylül 2024, https://www.aa.com.tr/en/turkiye/turkish-minister-underscores-need-for-national-technology-after-pager-explosions-in-lebanon/3334019, erişim 29.05.2025.

Sonuç

Bu çalışma, siber güvenlikte hibrit savaş konseptine yönelik stratejik bir bakış açısı sunarak, elektronik harp ve siber tehditlerin bir arada nasıl ele alınabileceğini analiz etmiştir. Tedarik zinciri saldırılarının karmaşıklığı ve etkileri incelenmiş; MITRE ATT&CK çerçevesine dayalı olarak bu tür saldırıların izlerinin daha kapsamlı bir şekilde tespit edilmesine yönelik bir model yaklaşımı önerilmiştir. Çalışma, tehdit istihbaratının geleneksel sınırlarını genişleterek, RF ve EH tekniklerini kapsayan bir model geliştirmiştir.

Bu çalışma kapsamında önerilen teknik model, yalnızca mevcut saldırıların izlenmesi ve belgelenmesi için değil, aynı zamanda gelecekteki tehditlerin daha iyi öngörülmesi ve önlenmesi için yeni metodolojilerin benimsenmesini teşvik etmektedir. Hibrit tehditlerin doğasına uygun olarak genişletilmiş bir MITRE ATT&CK matrisi, saldırı yüzeylerinin daha detaylı analizine ve daha etkin savunma stratejilerinin oluşturulmasına olanak tanıyacaktır. Sonuç olarak, RF ve EH tabanlı saldırılarla ilgili kategorilerin entegre edilmesi, dijital ve fiziksel güvenlik arasında köprü kurarak daha kapsamlı bir tehdit analizi çerçevesi sunmaktadır. Bu tür yenilikçi yaklaşımlar, siber ve elektronik harp alanındaki güvenlik politikalarının yeniden şekillendirilmesini ve daha proaktif tehdit avcılığı yöntemlerinin geliştirilmesini sağlayacaktır. Gelecekte yapılacak çalışmalar, önerilen modelin pratik uygulamalarını ve gerçek dünya senaryolarında sağlayabileceği etkileri daha detaylı şekilde ele almalıdır.

Çağrı cihazı saldırısı, hibrit tehdit ortamında siber ve kinetik operasyonlar arasındaki sınırların bulanıklaştığını net şekilde ortaya koymuştur. Bu durum, düşük maliyetli analog cihazların bile tedarik zinciri güvenliğini tehdit edebileceğini kanıtlamıştır. Tedarik zincirinin dijital ve fiziksel bileşenlerinin bütünleşik zafiyetleri hem BT hem de OT katmanlarında saldırı yüzeyini genişletmektedir. Sahte cihazlar, donanımsal arka kapılar ve yazılım manipülasyonları, operasyonel güvenliği doğrudan etkileyecek biçimde silahlandırılabilmektedir. Sonuç olarak, hibrit tehditlere karşı güvenlik analizlerinin sadece teknik düzeyde değil, aynı zamanda düzenleyici ve sistemik düzeyde de ele alınması gereklidir. Siber savaş, geleneksel çatışma doktrinlerinin dijitalleştirilmiş bir uzantısı hâline gelmiş; bu nedenle siber tehdit analizleri, fiziksel çatışma bağlamlarıyla entegre edilmelidir.

Yazarların Katkı Oranı

Yazarlar araştırmaya eşit oranda katkıda bulunmuştur.

Çıkar Çatışması

Araştırmanın yazarları olarak herhangi bir çıkar çatışma beyanımız bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Bu çalışmanın hazırlanması sırasında yazarlar, yalnızca metnin okunabilirliğini arttırmak, dil bilgisel hataları düzeltmek ve akışı iyileştirmek amacıyla ChatGPT-4 aracından yararlanmıştır. Bu ve benzeri teknolojiler içerik üretmek, bilimsel çıkarımlar yapmak ve bilimsel önerilerde bulunmak için kullanılmamıştır. Yapay zekâ destekli araçların kullanımı yazarların denetimi ve kontrolü altında gerçekleştirilmiş ve ortaya çıkan metin yazarlar tarafından dikkatlice gözden geçirilip düzenlenmiştir. Yapay zekâ sistemlerinin zaman zaman eksik, hatalı veya ön yargılı içerik üretebileceği göz önünde bulundurularak, çalışmanın tüm içeriğine ve doğruluğuna ilişkin nihai sorumluluk yazarlara aittir.

KAYNAKÇA

Basılı Eserler

AHN Gwanghyun, JANG Jisoo, CHOI Seho ve SHIN Dongkyoo (2024). "Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model with the MITRE ATT&CK Matrix", *IEEE Access*, 12, 89291–89309.

AKDEMİR Merve Ş. (2022). "Egemenlik ve Evrensel Yargı Yetkisi İlişkisinin Uluslararası Ceza Hukuku Boyutu", *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 8:2, 261-275.

AL-KHAWAJA Ali ve SADKHAN Sattar B. (2021). "Intelligence and Electronic Warfare: Challenges and Future Trends", *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, IEEE, 118-123.

AL-SADA, Bader, SADIGHIAN, Alireza ve OLIGERI, Gabriele (2023). "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database", *IEEE Access*, 12, 1217–1234.

APPLEGATE Scott D. (2009). "Social engineering: Hacking the wetware!", *Information Security Journal: A Global Perspective*, 18:1, 40-46.

BACK Tobias B. (2025). "Weaponising 'apparently harmless portable objects': emerging categorisations of trust and risk in post 'pager attacks' Lebanon", *Small Wars & Insurgencies*, 36:6, 1025-1048.

BELLABY Ross W. (2016). "Justifying Cyber-Intelligence?", *Journal of Military Ethics*, 15:4, 299–319.

BORUM Randy, FELKER John, KERN Sean, DENNESEN Kristen ve FEYES Tonya (2015). "Strategic Cyber Intelligence", *Information & Computer Security*, 23:3, 317–332.

BRATKO Artem, ZAHARCHUK Denys ve ZOLKA Valentyn (2021). "Hybrid Warfare–A Threat to the National Security of the State", *Revista de Estudios en Seguridad Internacional*, 7:1, 147–160.

CALISKAN Murat (2019). "Hybrid warfare and strategic theory", *Horizon Insights*, 6.

CHRISTIANSON David L. (2019). "Signals intelligence", Geral W. Hopple ve Bruce W. Watson (ed.), *The Military Intelligence Community*, New York, Routledge, 39-54.

COHEN Amichai ve SHANY Yuval (2024). "Well, it depends: Explosive pagers attack revisited", *Articles of War*, https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/, erişim 24.09.2024.

FLORIDI Luciano (2010). *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press.

GHERNOUTI-HÉLIE Solange (2010). "A national strategy for an effective cybersecurity approach and culture", *2010 International Conference on Availability, Reliability and Security*, IEEE, 370-373.

GILL Peter (2012). "Intelligence, Threat, Risk and the Challenge of Oversight", *Intelligence and National Security*, 27:2, 206-222.

GÜNDOĞDU Serkan (2023). "Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM)", *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33:3, 1325-1337.

GÜNEŞ Burak (2021). "Egemenlik ve İnsancıl Müdahale: Çelişkili Bir Kuram Olarak Uluslararası Hukuk", *Güvenlik Bilimleri Dergisi*, 10:1, 31-58.

HAMMI Badis, ZEADALLY Sherali ve NEBHEN Jamel (2023). "Security threats, countermeasures, and challenges of digital supply chains", *ACM Computing Surveys*, 55:14s, 1-40.

HOFFMAN Frank G. (2007). "Conflict in the 21st century: The rise of hybrid wars", *Arlington: Potomac Institute for Policy Studies.*

JO Yonghyun, CHOI Oongjae, YOU Jiwoon, CHA Youngkyun ve LEE Dong H., (2022). "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework", *Sensors*, 22:5, 1860.

KANJ BONHARD S., VILLALTA Pau G., ROSES Oriol, PEGUEROLES Josep (2025). "A Review of Tactics, Techniques, and Procedures (TTPs) of MITRE Framework for Business Email Compromise (BEC) Attacks", *IEEE Access*.

KARAKUŞ Cahit (2013). Kritik Alt Yapılara Siber Saldırı, *Yüksek Lisans Tezi*, İstanbul Kültür Üniversitesi.

LASICA Daniel T. (2009). "Strategic implications of hybrid war: A theory of victory", School of Advanced Military Studies, United States Army Command and General Staff College.

LAVAZZA Andrea ve FARINA Mirko (2024). "The Costs and Perils of Weaponizing Consumer Technologies (The 2024 Pager and Walkie-Talkie Explosions in Lebanon and Syria)", *IEEE Technology and Society Magazine*.

LIAROPOULOS Andrew (2011). "War and Ethics in Cyberspace", *Leading Issues in Information Warfare and Security Research*, 1:121.

MAHAT Shobendra S. (2025). "Vulnerabilities of the Communication System to an Electromagnetic (EM) Attack, Threat Assessment and Mitigation", *The Shivapuri Journal*, 26:1, 134-144.

MARSHALL Kimball P. (1999). "Has Technology Introduced New Ethical Problems?", J*ournal of Business Ethics*, 19, 81-90.

MARSZAŁEK-KOTZUR Izabela (2022). "Ethical Perspective of the Development and Use of Modern Military Technologies", *Scientific Papers of Silesian University of Technology, Organization & Management/Zeszyty Naukowe Politechniki Slaskiej, Seria Organizacji i Zarzadzanie*, 165.

MASSACCI Fabio (2025). "Exploding Pagers and the Birth of State Cyberterrorism", *IEEE Security & Privacy*, 23:01, 4-6.

NAIK Nitin, JENKINS Paul, GRACE Paul ve SONG Jingping (2022). "Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model", *2022 IEEE International Symposium on Systems Engineering (ISSE)*, IEEE, 1–7.

NYE Joseph S. (2010). *Cyber Power*, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

PEFFERS Ken, TUUNANEN Tuure, ROTHENBERGER Marcus A. ve CHATTERJEE Samir (2007). "A Design Science Research Methodology for Information Systems Research", *Journal of Management Information Systems*, 24:3, 45–77.

PELL Robert, MOSCHOYIANNIS Sotiris, PANAOUSIS Emmanouil ve HEARTFIELD Ryan (2021). "Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK", arXiv preprint arXiv:2108.11206, https://arxiv.org/abs/2108.11206.

REICHBORN-KJENNERUD Erik ve CULLEN Patrick (2022). "What is hybrid warfare?", *Norwegian Institute for International Affairs (NUPI).*

RID Thomas (2013). "Cyberwar and peace: Hacking can reduce real-world violence", *Foreign Affairs*, 92:6, 77-87.

SAGAN Scott D. (2016). "Ethics, technology & war", *Daedalus*, 145:4, 6-11.

SARKER Pantha Protim, DAS Upoma, VARSHNEY Nitin, SHI Shang, KULKARNI Akshay, FARAHMANDI Farimah ve TEHRANIPOOR Mark (2025). "When Everyday Devices Become Weapons: A Closer Look at the Pager and Walkie-talkie Attacks", arXiv preprint arXiv:2501.17405.

SCHLEHER D. Curtis (1999). *Electronic Warfare in the Information Age*, Norwood, MA: Artech House, Inc., 1999.

SCOTT Len (2019). "Secret Intelligence, Covert Action and Clandestine Diplomacy", Christopher Andrew, Richard J. Aldrich ve Wesley K. Wark (ed.), *Secret Intelligence*, London, Routledge, 526–544.

SHENG Chuan, MA Wanlun, HAN Qing-Long, ZHOU Wei, ZHU Xiaogang ve WEN Sheng (2024). "Pager Explosion: Cybersecurity Insights and Afterthoughts", I*EEE/CAA Journal of Automatica Sinica*, 11:12, 2359-2362.

SKRODELIS Heinrihs K. ve ROMANOVS Andrejs (2021). "Cyber-Physical Risk Security Framework Development in Digital Supply Chains", *62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, IEEE, 1–5.

STROM Blake E., APPLEBAUM Andy, MILLER Doug P., NICKELS Kathryn C., PENNINGTON Adam G. ve THOMAS Cody B. (2018). "MITRE ATT&CK: Design and Philosophy", *Technical Report*, McLean, VA: The MITRE Corporation.

SUN Nan, DING Ming, JIANG Jiaojiao, XU Weikang, MO Xiaxing, TAI Yonghang ve ZHANG Jun (2023). "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", *IEEE Communications Surveys & Tutorials*, 25:3, 1748-1774.

SVETOKA Sanda (2016). "Social media as a tool of hybrid warfare", *NATO Strategic Communications Centre of Excellence.*

UMBRELLO Steven, TORRES Phil ve DE BELLIS Angelo F. (2020). "The future of war: Could lethal autonomous weapons make conflict more ethical?", *Ai & Society*, 35:1, 273-282.

URBINI Ignacio M. G., VENOSA Paula, BAZÂN Patricia ve DEL RIO Nicolâs (2022). "Distributed Cybersecurity Strategy, applying the Intelligence Operations Theory", *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, 1-6.

WARNER Michael (2019). "A matter of trust: Covert action reconsidered", *Studies in Intelligence*, 63:4, 33–41.

İnternet Kaynakları

ARSLAN İkbal Muhammet (2024). "BM: Lübnan ve Suriye'de Eş Zamanlı Çağrı Cihazı Patlamaları Şok Edici", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/tr/dunya/bm-lubnan-ve-suriyede-es-zamanli-cagri-cihazi-patlamalari-sok-edici/3333807, erişim 07.01.2025.

BIÇAKÇI Salih (2024). "Lübnan'da Patlayan Çağrı Cihazları: Elektronik Harp, Siber Sabotaj ve Kötülüğün Sıradanlığı", *Fikir Turu*, https://fikirturu.com/jeo-politika/lubnanda-patlayan-cagri-cihazlari/, erişim 24.09.2024.

Ekonomi ve Dış Politika Araştırma Merkezi (2016). "Nükleer Tesislerin Siber Güvenliğine Giriş", *EDAM*, https://edam.org.tr/siber-politikalar-ve-dijital-demokrasi/nukleer-tesislerin-siber-guvenligine-giris, erişim 01.02.2025.

GEBEILY Maya, PEARSON James ve GAUTHIER-VILLARS David (2025). "How Israel's bulky pager fooled Hezbollah", *Reuters*, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/, erişim 17.10.2024.

IEEE Spectrum (2024). "The Real Story of Stuxnet", https://spectrum.ieee.org/the-real-story-of-stuxnet, erişim 01.02.2025.

ISB Staff Reporter (2024). "Hezbollah Pager Attack: A Wake-up Call to Tech Manufacturers to Secure their Supply Chains?", *Information Security Buzz*, https://informationsecuritybuzz.com/hezbollah-pager-attack-a-wake-up-call/, erişim 20.10.2024.

LACY Mark (2024). "Lebanon Pager Attacks: The Weaponisation of Everything has Begun", *The Conversation*, https://theconversation.com/lebanon-pager-attacks-the-weaponisation-of-everything-has-begun-239423, erişim 23.10.2024.

LIMA Marcelo (2024). "Israeli Pager Attack: Cybersecurity Lessons", *LinkedIn*, https://www.linkedin.com/pulse/israeli-pager-attack-cybersecurity-lessons-security-marcelo-kcjxf, erişim 21.10.2024.

LINKEDIN,https://www.linkedin.com/search/results/all/?keywords=%23pagerexplosion&origin=HASH_TAG_FROM_FEED&sid=Q3u, erişim 20.09.2024.

MEDIUM, https://medium.com/search?q=%23pagerexplosion, erişim 20.09.2024.

MITRE, "MITRE ATT&CK Groups", https://attack.mitre.org/groups/, erişim 5.01.2025.

MITRE, "MITRE Enterprise Matrix", https://attack.mitre.org/matrices/enterprise/, erişim 20.01.2025.

MITRE, "T0862: Remote Access Software", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T0862/, erişim 21.01.2025.

MITRE, "MITRE ATT&CK Tactics", https://attack.mitre.org/tactics/, erişim 22.01.2025.

MITRE, "T1583: Acquire Infrastructure", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1583/, erişim 22.01.2025.

MITRE, "T1199: Trusted Relationship", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1199/, erişim 23.01.2025.

NIST, "Tactics, Techniques, and Procedures", *National Institute of Standards and Technology*, https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures, erişim 22.04.2025.

PARIENTE Nissim (2024). "The Machine Identity Attack Surface – MITRE ATT&CK Framework Redefined", *Token Security*, https://www.token.security/blog/the-machine-identity-attack-surface---mitre-attack-framework-redefined, erişim 20.01.2025.

PICUS Security (2024). "What is Advanced Persistent Threat (APT)?", *Picus Security*, https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt, erişim 05.05. 2025.

PYTLAK Allison, SIEBENS Siebens ve LAD Shreya (2024). "Old Tactics, New Targets: Unraveling Lebanon's Pager Attacks", *Stimson Center*, https://www.stimson.org/2024/old-tactics-new-targets, erişim 24.10.2024.

RAMAKRISHNA Sudhakar (2021). "New Findings from Our Investigation of SUNBURST", *SolarWinds Blog*, https://www.solarwinds.com/blog/new-findings-from-our-investigation-of-sunburst, erişim 06.05.2025.

REDDIT (2024). "Israel planted explosives in 5,000 Hezbollah pagers, say sources", https://www.reddit.com/r/geopolitics/comments/1fjnx3y/israel_planted_explosives_in_5000_hezbollah/, erişim 19.09.2024.

SEREN Merve (2024). "İsrail'in Yeni İstihbarat Operasyonu: Pager ve Walkie-Talkie saldırıları", *Fikir Turu*, https://fikirturu.com/jeo-politika/israilin-yeni-istihbarat-operasyonu/, erişim 25.09.2024.

SİNCAR Halil İbrahim, BODRUK Bestami (2024). "Turkish Minister Underscores Need for National Technology after Pager Explosions in Lebanon", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/en/turkiye/turkish-minister-underscores-need-for-national-technology-after-pager-explosions-in-lebanon/3334019, erişim 29.05.2025.

SINGH Inder (2024). "New Paradigm in Cyber Warfare: Strategic Pager Attack on Hezbollah", *Medium*, https://inderbarara.medium.com/new-paradigm-in-cyber-warfare-strategic-pager-attack-on-hezbollah-d100247bd9ec, erişim 22.10.2024.

STAHL Lesley (2025) " Israel's spy agency, Mossad, spent years orchestrating Hezbollah walkie-talkie, pager plots", *CBS News*, https://www.cbsnews.com/news/israeli-mossad-pager-walkie-talkie-hezbollah-plot-60-minutes/, erişim 06.01.2025.

STAHL Lesley (2025). "Former Mossad Agents Detail Explosive Pagers, Hezbollah Terrorists Plot – 60 Minutes Transcript", *CBS News*, https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/, erişim 09.06.2025.

TWITTER (X). https://x.com/hashtag/pagerexplosions?src=hashtag_click, erişim 19.09.2024.

EKLER:

1. Genişletilmiş MITRE Matrisi: