CENK

Savunma Güvenlik Strateji Dergisi / Journal of Defense Security Strategy

ISSN: 3108-3781

CENK, Haziran 2026 / June 2026, s. 31-46

Dünyayı Saran Gizli Ağ: Denizaltı Fiber Optik Teknolojisi ve Dijital Jeopolitik

The Hidden Network Enveloping the World: Submarine Fiber Optic Technology and Digital Geopolitics

Kübra ÖZDEN
Lisans Öğrencisi, Kocaeli Üniversitesi Siyasal Bilgiler Fakültesi
ozdenkubra46@gmail.com
ORCID: https://orcid.org/0009-0003-3864-9163
DOI: 10.5281/zenodo.21076133

Makale Bilgisi | Article Information
Makale Türü/Article Type: Araştırma Makalesi / Research Article
Geliş Tarihi/Date Received: 07 Nisan / April 07
Kabul Tarihi/Date Accepted: 25 Haziran / June 25
Yayın Tarihi/Date Published: 30 Haziran / Haziran 30
Yayın Sezonu/Pub Date Season: 30 Haziran / Haziran 30

Atıf / Citation: Özden, K. (2026). Dünyayı saran gizli ağ: denizaltı fiber optik teknolojisi ve dijital jeopolitik. *CENK Savunma Güvenlik Strateji Dergisi, 2*(1), 31-46.
10.5281/zenodo.21076133

Etik Beyanı: Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan olunur (Kübra Özden).
Ethical Statement: It is declared that scientific and ethical principles have been followed while carrying out and writing this study and that all the sources used have been properly cited (Kubra Ozden).
Çıkar Çatışması: Çıkar çatışması beyan edilmemiştir.
Conflicts of Interest: The author has no conflict of interest to declare.
Finansman: Bu araştırmayı desteklemek için dış fon kullanılmamıştır.
Grant Support: No external funding was used to support this research.
İntihal: Bu makale, ithenticate yazılımınca taranmıştır. İntihal tespit edilmemiştir.
Plagiarism: This article has been scanned by ithenticate. No plagiarism detected.
Web: https://cenkjournal.com/index.php/pub| mailto: editor@cenkjournal.com

Copyright © Kübra ÖZDEN
CC BY 4.0

Abstract

In the digital era, security paradigms are rapidly evolving from physical domains toward cyber and data infrastructures. At the center of this transformation are submarine fiber-optic cables, which carry approximately 99% of global communications and data traffic. These cables are not merely technical communication lines; they have become strategic components of states' intelligence capabilities, power projection, and geopolitical influence. Over the past decade, the Mediterranean basin has witnessed a new geopolitical architecture shaped by energy and digital infrastructure projects. Through initiatives such as the Blue-Raman cable and the EuroAsia Interconnector, Israel has become a significant hub in regional digital networks, gaining not only communication advantages but also new opportunities for signals intelligence. Turkey occupies a central position in one of the region's most critical digital corridors, serving as a natural transit route for Asia–Europe data flows with simultaneous access to the Mediterranean, Aegean, and Black Seas. Maritime jurisdiction agreements with neighboring states have expanded Türkiye's maritime authority and its influence over energy and fiber-optic cable routes. NATO, the European Commission, and the Joint Research Centre classify Türkiye's maritime zones as high-value areas for digital infrastructure security. Nevertheless, initiatives such as the EastMed Gas Forum and cable projects excluding Türkiye seek to redirect regional data traffic through alternative routes as part of an infrastructure-based containment strategy, forming a multilayered order aimed at constraining Türkiye's cybersecurity role and intelligence capabilities. As of 2026, escalating conflicts and the targeting of critical infrastructures have transformed these systems into emerging security vulnerabilities for states.

Keywords: Submarine Fiber-optic cables, Digital infrastructure, Mediterranean geopolitics, Signal intelligence, Data corridor governance.

Öz

Dijital çağın güvenlik anlayışı, fiziksel sahadan siber altyapı ve veri altyapılarına doğru hızla evrilmektedir. Bu dönüşümün merkezinde ise küresel iletişim ve veri akışının yaklaşık %99'unu taşıyan deniz altı fiber optik kablolar yer almaktadır. Bu kablolar yalnızca teknik iletişim hatları değil; devletlerin istihbarat, güç projeksiyonu ve jeopolitik nüfuz araçlarının stratejik bileşenleri haline gelmiştir. Akdeniz havzasında özellikle son on yılda enerji ve dijital altyapı projeleri üzerinden yeni bir jeopolitik mimari oluşmuş; İsrail, Blue-Raman ve EuroAsia Interconnector gibi bölgesel projeler aracılığıyla, bölgesel ağlarda önemli bir kavşak noktası hâline gelmiştir. Bu hatların bir kısmının İsrail üzerinden geçmesi, ülkeye yalnızca iletişim avantajı sağlamamanın yanında pasif ve aktif sinyal istihbaratı açısından yeni fırsatlar doğurmaktadır. Türkiye ise hem Asya–Avrupa veri akışının doğal geçiş hattı hem de Akdeniz, Ege ve Karadeniz'e eş zamanlı erişimi sayesinde bölgenin en kritik dijital koridorlarından birinin merkezinde yer almaktadır. Bu kapsamda çevre ülkelerle imzaladığı deniz yetki alanı mutabakatları, deniz yetki kapasitesini genişletmiş; buna bağlı olarak enerji ve fiber optik kablo güzergâhları üzerindeki etkisini artırmıştır. NATO, Avrupa Komisyonu ve JRC raporları Türkiye'nin deniz yetki alanlarını dijital altyapı güvenliği bakımından yüksek stratejik değer olarak sınıflandırmaktadır. Buna karşın, EastMed Gas Forum gibi girişimler ve Türkiye'yi dışlayan bazı kablo ve enerji projeleri, "altyapı üzerinden çevreleme" stratejisiyle bölgesel veri trafiğinin Türkiye dışındaki rotalara yönlendirilmesini amaçlamaktadır. Bu durum hem Türkiye'nin siber güvenlik rolünü hem de istihbarat kapasitesini sınırlamaya yönelik çok katmanlı bir bölgesel düzeni işaret etmektedir. 2026 itibarıyla artan çatışmalar ve kritik altyapıların hedef hâline gelmesi, bu yapıları devletler için yeni birer güvenlik açığına dönüştürmüştür.

Anahtar Kelimeler: Denizaltı fiber-optik kablo, dijital altyapı güvenliği, Akdeniz jeopolitiği, Sinyal istihbaratı, Veri koridoru yönetimi.

Giriş

21. yüzyılda savaşların doğası değişmekte ve dönüşmektedir. Artık çatışmalar yalnızca konvansiyonel silahlarla değil; aynı zamanda dijital altyapılar, siber ağlar ve veri akışları üzerinden de şekillenmektedir. Bu yeni güvenlik ortamında, yalnızca bilgiye sahip olmak değil, bilgi akışını yönlendirebilme ve denetleyebilme kapasitesi ulusların stratejik üstünlüğünü belirleyen temel unsurlardan biri hâline gelmiştir. Bu çerçevede, söz konusu liderliği elinde bulunduran Google, Meta, Microsoft ve Amazon gibi devlet dışı ancak küresel ölçekte etkili teknoloji aktörleri, güç dengelerinde belirleyici bir konuma yükselmiştir.

Telgraftan günümüze uzanan süreçte evrilen bu hatlar, bugün yaklaşık 600 etkin kablo sistemi, 1,4 milyon kilometreyi aşan uzunluk ve 1.600'den fazla iniş istasyonu ile deniz altında geniş bir ağ oluşturmaktadır. Devasa ölçekte veri taşıyan bu fiber optik hatlar; internet, ticaret, finans,

bankacılık, ulaşım, sağlık ve iletişim gibi kritik sektörlerin tamamını kapsayan bir dijital omurga işlevi görmektedir. Bu alanlar her ne kadar birbirinden bağımsız sektörler olarak değerlendirilse de üretilen ve iletilen verilerin büyük bölümü aynı altyapı üzerinden aktarılmaktadır. Bu nedenle, söz konusu hatlara yönelik gerçekleştirilebilecek fiziksel sabotajlar veya ileri düzey siber saldırılar yalnızca iletişim ağlarını değil, tüm dijital ekosistemi sekteye uğratabilecek riskler barındırmaktadır. Dolayısıyla bu hatların yalnızca veri taşıyan altyapılar olarak değil, aynı zamanda potansiyel tehdit unsurları olarak da ele alınması gerekmektedir. Bu noktada, söz konusu altyapılara kimin sahip olduğu ve bu hatların ticari veri taşımacılığının ötesinde hangi stratejik işlevleri üstlenebileceği soruları, yeterince incelenmemiş kritik bir alan olarak öne çıkmaktadır.

Bu genel çerçeve içerisinde, İsrail'in son yıllarda Akdeniz çevresindeki dijital altyapı projelerinde giderek daha merkezi bir rol üstlenmesi dikkat çekmektedir. Özellikle Google tarafından hayata geçirilen ve geleneksel Mısır güzergâhını devre dışı bırakan Blue-Raman adlı uluslararası fiber optik kablo hattının bir bölümünün İsrail topraklarından geçmesi, ülkenin küresel veri trafiğinde önemli bir geçiş noktası olma iddiasını güçlendirmiştir. Proje kamuoyuna altyapı ve ticari veri taşımacılığı amacıyla sunulmuş olsa da bazı analizler, bu tür girişimlerin sinyal istihbaratı (SIGINT) ve veri gözetimi açısından stratejik bir potansiyel taşıdığına işaret etmektedir. İsrail'in askerî ve teknolojik kapasitesi dikkate alındığında, denizaltı kablo altyapılarının yalnızca iletişim amacıyla değil, aynı zamanda elektronik istihbarat faaliyetlerine imkân tanıyacak şekilde değerlendirilebilmesi ihtimali göz ardı edilmemelidir. Her ne kadar bu durum doğrudan teyit edilmiş bir olgu olmasa da bölgedeki veri trafiğinin kontrolü üzerinden oluşabilecek güç projeksiyonu kapasitesine dair önemli bir gösterge sunmaktadır.

Bu çalışma, uluslararası ilişkilerde "Kritik Altyapı Güvenliği" ve "Dijital Jeopolitik" yaklaşımlarını teorik zemin olarak benimsemektedir. Realist teori çerçevesinde, teknolojik altyapılar yalnızca ekonomik araçlar değil; devletlerin güç kapasitelerini artıran, rekabet alanlarını genişleten ve uluslararası sistemde konumlarını yeniden tanımlayan stratejik unsurlar olarak değerlendirilmektedir. Bu bağlamda, özellikle denizaltı fiber optik kabloların korunması ve bu hatlar üzerindeki veri akışının denetlenmesi, siber egemenlik ve bilgi kontrolü tartışmalarıyla doğrudan ilişkilidir. Nitekim söz konusu altyapılar, bölgesel aktörler açısından caydırıcılık üretme ve bilgi üstünlüğü sağlama kapasitesinin temel bileşenlerinden biri haline gelmiştir.

Bu teorik çerçeveden hareketle çalışma, denizaltı fiber optik kablo altyapılarının kontrolünün, bölgesel aktörlerin stratejik güç projeksiyonu ve istihbarat kapasitesi üzerindeki etkilerini incelemeyi amaçlamaktadır. Araştırma, özellikle İsrail ve Türkiye örnekleri üzerinden bu etkinin nasıl farklılaştığını ve Doğu Akdeniz'deki güç dengelerini nasıl yeniden şekillendirdiğini analiz etmektedir. Bu doğrultuda makale, dijital ekosistemin omurgasını oluşturan denizaltı fiber optik kabloların taşıdığı güvenlik risklerini tarihsel gelişim süreci içinde istihbarat perspektifiyle ele almakta; Akdeniz'de hız kazanan kablo projelerini ve bu projelerde İsrail'in oynadığı merkezi rolü stratejik bir bakış açısıyla değerlendirmeyi hedeflemektedir.

1. Denizaltı Kabloların Tarihçesi

Günümüzde gelişen elektronik teknolojilerle birlikte kitle iletişim araçlarının sayısı giderek artmakta, bu araçların işlev ve kullanım alanları da çeşitlenmektedir. Bu gelişmeler sayesinde, iletişim kurmak istediğimiz kişi ya da kurumlara anında ulaşabilmekteyiz. Oysa bundan yaklaşık iki asır önce, 19. yüzyılın başlarında durum oldukça farklıydı; iletişim olanakları sınırlıydı ve bilgi akışı günümüzle kıyaslanamayacak kadar yavaştı. Ülkeler arasındaki haberleşme yalnızca

gemilerle taşınan mektuplar aracılığıyla sağlanıyor, hava şartları ve deniz koşullarına bağlı olarak bu süreç hem yavaşlıyor hem de belirsizleşiyordu. Örneğin 1830'larda Avrupa'dan Hindistan'a gönderilen bir mektubun ulaşması neredeyse beş ila sekiz ay sürerken, yanıtın alınması ise yaklaşık iki yılı bulabiliyordu (Curtin, 1984).

Bu yavaş ve güvensiz iletişim biçimi, özellikle Sanayi Devrimi ile artan ticaret, diplomasi, askeri koordinasyon ve istihbarat ihtiyaçlarını karşılamakta yetersiz kalmaktaydı. Bu nedenle 19. yüzyılın başlarında elektrik ve manyetizma alanında gerçekleştirilen bilimsel çalışmalar, kıtalararası hızlı iletişimi mümkün kılacak telgraf teknolojisinin doğmasına zemin hazırladı.

1831 yılında Amerikalı fizikçi Joseph Henry, güçlü elektromıknatıslar üzerine yaptığı deneylerle elektromanyetik iletişimin teknik temelini attı. Henry, elektromıknatısla uzun mesafede sinyal iletilebileceğini gösterse de bu buluşu pratik bir iletişim sistemine dönüştürmedi. Bu adımı atan kişi, 1830'lu yıllarda New York Üniversitesi'nde profesör olan Samuel Morse oldu. Morse, elektrik akımıyla çalışan bir işaretleme sistemi geliştirdi ve günümüzde hâlâ kullanılan Mors Kodunu oluşturdu.

24 Mayıs 1844'te Washington'dan Baltimore'a gönderilen "What hath God wrought?" ("Tanrı neler yarattı?") mesajı, pratik telgraf iletişiminin başlangıcı olarak kabul edilmektedir. Bu hat, Kuzey Amerika'da kamu tarafından finanse edilen ilk telgraf hattı olma özelliğini taşımaktadır. Bu tarihten sonra telgraf hızla genişlemiş ve kıtalar arası haberleşmenin temelini oluşturan denizaltı kablolarının çekilmesine giden süreci başlatmıştır.

1.1. İlk Denizaltı Kablo Denemeleri

Denizaltı telgraf kablolarının döşenmesi fikri, kısa sürede telgraf teknolojisinin doğal bir uzantısı hâline geldi. 1850 yılına gelindiğinde, John Watkins Brett'in İngiliz Kanalı Denizaltı Telgraf Şirketi tarafından guetta-perka ile kaplanmış tek telli ilk uluslararası denizaltı kablosu Manş Denizi üzerinden döşendi. Dover ile Calais'i birbirine bağlayan bu kablo kısa ömürlü olsa da uluslararası telgraf ağının oluşumunda sembolik bir dönüm noktasıdır (Atlantic Cable, 2025). Bu girişim, dönemin teknolojik kapasitesi düşünüldüğünde hem cesur hem de yenilikçi bir adım olarak değerlendirilmektedir.

Döşenen bu hat, Manş Denizi'nin en dar bölgesi olan Dover'dan başlayarak, karşı kıyıda yer alan Fransız kenti Calais'e ulaşmaktaydı. Dolayısıyla kablo, iki yakayı birbirine bağlayan güzergâhı nedeniyle "Dover–Calais Kablosu" adıyla anılmıştır. Her ne kadar kablo yalnızca kısa bir süre çalışmış olsa da uluslararası telgraf ağının gelişiminde simgesel bir öneme sahip olmuş, ilerleyen yıllarda ortaya çıkan daha gelişmiş altyapı projelerine altyapı projelerine zemin hazırlayan bir girişim olmuştur.

1857 yılına gelindiğinde, Transatlantik kablonun hem fikrine hem de inşasına katkı sunan Frederick Newton Gisbourne bu projenin tanıtımını yaptı.

Denizaltı telgraf kablolarının döşenmesi fikri, telgraf teknolojisinin doğal bir uzantısı olarak 1850'lerde hızla gelişti. 1850 yılında John Watkins Brett'in İngiliz Kanalı Denizaltı Telgraf Şirketi tarafından doğal bir termoplastik (guetta-perka) ile kaplanmış tek telli ilk uluslararası denizaltı kablosu Manş Denizi üzerinden döşenerek Dover ile Calais'i birbirine bağladı; kısa ömürlü olsa da küresel telgraf ağının oluşumunda sembolik bir adım oldu. Bu dönemde Kanada'da mühendis Frederic Newton Gisborne, Newfoundland'ı Amerika Birleşik Devletleri'ne bağlayacak bir telgraf hattı tasarladı ve bu hattın Cabot Boğazı üzerinden denizaltı kablosuyla tamamlanması planlandı. Projenin tanıtımını yapan Gisborne'un New York'ta Cyrus West Field ile tanışması,

hattın Atlantik Okyanusu'nu aşacak şekilde genişletilmesinin önünü açtı ve böylece 19. yüzyılın en büyük mühendislik girişimlerinden biri olan "Transatlantik Telgraf Kablo Projesi" doğdu. Bu kapsamda 2 Haziran 1856'da Londra'dan hareket eden SS Propontis gemisi, Birleşik Krallık'tan Newfoundland'a giden ilk doğrudan seferini gerçekleştirerek Newfoundland'dan Cape Breton Adası'na ve Nova Scotia üzerinden Prens Edward Adası'na döşenecek kabloları taşıdı ve New York ile Newfoundland arasında kurulacak ilk doğrudan iletişim bağlantısının altyapısını oluşturdu (Chesnoy, 2015).

Gerçekleştirilen bu ilk denemeler her ne kadar teknik sorunlarla karşılaşsa ve kısa süre devre dışı bırakılsa da yıllar geçtikçe kablo yapıları geliştirilerek daha profesyonel ve çalışır hale getirildi. Örneğin, 1866 yılında daha dayanıklı kablolarla transatlantik denizaltı telgraf hattı kalıcı olarak kuruldu ve sorunsuz bir şekilde çalışır hale getirildi. Bu dönem boyunca sistemler düşük bant genişliği ve yüksek gecikme gibi sınırlarla karşılaştı, ancak iletişim devrimini başlattı (Chesnoy, 2015).

İkinci Dünya Savaşı sonrası gelişen elektronik teknolojisi, denizaltı haberleşmesini yeni bir boyuta taşıdı. Telgraf hatlarının yetersizliği üzerine, koaksiyel kablolar ve sinyal güçlendirici cihazlar (amplifikatör) sayesinde uluslararası telefon görüşmeleri çok daha kararlı hale geldi. 1956'da hizmete giren TAT-1, ilk transatlantik telefon kablosuydu ve sesli iletişimi küresel ölçekte mümkün kıldı. Ancak kapasite yine sınırlıydı ve analog yapının geliştirilme sınırları vardı (Chesnoy, 2015).

1.2. Fiber Optik Devrimin Başlangıcı: 1976-1995 Döneminde Denizaltı Telekomünikasyonun Dönüşümü

1976–1988 döneminde ise koaksiyel kablo teknolojisi TAT-6 ile belirli bir duraklama yaşamış, STC (NG 45 MHz) ve KDD (STM 140 MHz) gibi şirketler yeni sistemler geliştirmiştir. Bu yıllarda gelişmiş ülkelerde dijital anahtarlama ve bakır veya koaksiyel hatlar üzerinden dijital iletim sistemleri yaygınlaşmıştır. 1982'den itibaren fiber optik kablolar karasal ağlarda kullanılmaya başlanmış ve analog denizaltı koaksiyel sistemler ile dijital karasal kablolar veya mikrodalga sistemler (TMUX) arasında arayüz tesisleri geliştirilmiştir; ancak bunlar uzun vadeli bir çözüm sunamamıştır (Chesnoy, 2015).

Denizaltı telekomünikasyonunda bir sonraki adım için en uygun çözüm fiber cam olarak ortaya çıkmış ve ilk büyük hedef Atlantik Okyanusu'nu geçmek olmuştur. Optik fiberin temel araştırmaları 1966'da İngiltere'de yapılmış ve fiber camın koaksiyel kablolara kıyasla daha yüksek bilgi kapasitesi ve maliyet avantajı sağlayabileceği belirlenmiştir. Minyatür lazerler olmadan optik fiberin pratik kullanımı mümkün olmadığı; şans eseri yarı iletken lazerler optik fiberle aynı dönemde geliştirilmiş olması ve 1962'de Robert Hall, galyum arsenit tabanlı lazerlerin optik pencerelerde çalıştığını tespit etmesi yeni bir dönüm noktası olarak nitelendirilmiştir. 1977'de Londra kuzeyinde Hitchin–Stevenage hattı STL tarafından 4 km uzunluğunda kurulmuş ve 850 nm dalga boyunda 140 Mbit/s hızında çalışmıştır. Ardından dört büyük araştırma merkezi, 1300 nm dalga boyunda ikinci pencereye sahip tek modlu fiberleri kullanarak saçılımın (dispersion) azalması ve kayıpların düşmesini sağlamıştır. Bu dönemde lazer diyotları, fotodiyotlar ve batırılmış tekrarlandırıcılar için entegre devreler geliştirilmiş, kablo ve tekrarlandırıcı mekanikleri ile güç besleme ve elektromanyetik/nükleer darbelere karşı koruma sistemleri yeniden tasarlanmıştır (Chesnoy, 2015).

1988–1995 yılları arasında önemli fiber optik ağlar kurulmuş ve İngiltere'den Belçika, İrlanda, Fransa, Hollanda, Almanya ve Danimarka'ya denizaltı kabloları döşenmiştir. Fransa, İtalya ve

İspanya, adalara ulusal kablo hatları kurarken, Japonya kendi iç ağını geliştirmiştir. Yeni tedarikçiler (Pirelli, Siemens, STK, Ericsson) tekrarlandırıcı kullanmadan çalışan sistemler sunmuştur. TAT-8, 1988'de devreye alınmış ve fiber çift başına 7.680 kanal kapasitesi sunarak, tek bir ışık farklı yöne dağıtabilecek 'fiber çiftleri' üretme imkânı sağlamıştır. TPC-3 hattı ise 1989'da AT&T ve KDD tarafından inşa edilmiştir. Bu sistemler, farklı tedarikçiler tarafından üretilen segmentlerin birleştirilebileceğini ve daha yüksek (140Mbit/s) kapasite ile bu birimlerin kullanılabileceğini göstermiştir (Chesnoy, 2015).

Aynı dönemde AT&T, Florida–Venezuela hattını; STC, Hong Kong–Tayvan hattını; NEC ise Malezya iç hatlarını inşa etmiştir. Alcatel, Pirelli ile EMOS (İtalya–Yunanistan–Türkiye–İsrail) ve TASMAN (Avustralya–Yeni Zelanda) hatlarını 1990'da tamamlamıştır. TAT-8 fiberlerinin geliştirilmesi sırasında 1550 nm dalga boyunda çalışan ikinci optik pencere keşfedilmiş ve bu pencere, sistem kayıplarını azaltarak tekrarlandırıcı sayısını düşürmüş ve maliyet avantajı sağlamıştır. Bu teknoloji ile TAT-9 ve TPC-4 hatlarında fiber başına 560 Mbit/s kapasite sağlanmış, 1991–1995 arasında beş transatlantik denizaltı kablosu döşenmiştir (Chesnoy, 2015).

Transpasifik TPC-4 hattı, Guam'da PACRIM West ve Hawaii'de PACRIM East hatlarıyla bağlanarak Avustralya ve Yeni Zelanda'ya denizaltı bağlantısı sağlamıştır. 1994'te SEA-ME-WE-2 hattı dünya çevresini tamamlamış, CANTAT-3 ise (fiber çifti başına 2,5 Gbit/s kapasite) STC tarafından tasarlanan en son uzun mesafe yenilenmiş kablo teknolojisi olmuştur. 1994'te Amerika'da FCC, AT&T'yi parçalayarak yerel ağları "Baby Bell" olarak adlandırılan şirketlere vermiş ve uzun mesafe ile denizaltı kablo teknolojisinin yönetimini AT&T'de bırakmıştır. İngiltere'de ise rekabet kuralları değiştirilmiş ve British Telecom özelleştirilmiştir. Avrupa Birliği'nde telekomünikasyon liberalleşmiş, Dünya Ticaret Örgütü ile uluslararası düzenlemeler yürürlüğe girmiştir. Konsorsiyum modeli, büyük denizaltı kablo sistemlerinin yönetiminde bu yeni rekabet ortamına rağmen devam etmiştir (Chesnoy, 2015).

Bu dönemde üç özel kablo hattı kurulmuştur: PTAT-1 (1989), Transpasifik (NPC, 1991) ve FLAG (1995, TAT-12 sonrası). FLAG hattı, SEA-ME-WE-2'ye rekabet sunmuştur. Yeni ülkeler fiber optik teknolojiden yararlanmaya başlamış Hindistan, Orta Doğu, Çin, Rusya, Arjantin ve Uruguay gibi ülkeler küresel iletişim ağına entegre olmuştur. Bu hatlar fiber başına 565 Mbit/s kapasite sunmuştur (Chesnoy, 2015).

2. Fiber Optik Kablolar ve Etki Alanları

Denizaltı fiber optik kablolar, günümüzde yalnızca kıtalar arası bağlantı sağlamanın, internet ve iletişim altyapısı olmanın ötesine geçerek gelişmiş algılama ve izleme teknolojilerinin bir parçası haline gelmiştir. Özellikle Distributed Acoustic Sensing (DAS-Uzun Mesafe Akustik Algılayıcı) teknolojisinin olgunlaşmasıyla birlikte, mevcut optik fiber hatları büyük ölçekli, sürekli ve yüksek çözünürlüklü akustik sensör ağlarına dönüştürülebilmektedir.

DAS, optik fiber boyunca gönderilen lazer darbelerinin fiber içindeki saçılma sinyalini analiz ederek çalışır. Fiber kabloda oluşan titreşim, gerilme veya çevresel değişiklikler, geri saçılan ışığın fazında ölçülebilir değişikliklere neden olur. Böylece, su altındaki gemi trafiği, çevresel titreşimler, hatta kabloya yönelik olası müdahaleler gerçek zamanlı olarak tespit edilebilir (Williams et al., 2019).

Son yıllarda yapılan çalışmalar, DAS ile donatılmış denizaltı fiberlerinin gemi tespiti konusunda yüksek performans sunduğunu göstermektedir. Örneğin, Ramirez-Torres ve çalışma arkadaşları tarafından 2025 yılında gerçekleştirilen deneylerde, DAS tabanlı sistemlerin gemi algılama ve konumlandırma görevlerinde %90'ın üzerinde başarı elde ettiği raporlanmıştır. (Ramírez-Torres

et al., 2025). Bu sonuçlar, fiber kabloların deniz güvenliği, kıyı devriyesi ve altyapı koruma alanlarında etkin bir sensör görevi görebileceğini ortaya koymaktadır.

Denizaltı fiber optik kablolar yalnızca akustik algılama için değil, aynı zamanda kuantum iletişim teknolojileri açısından da önemli bir potansiyele sahiptir. Yapılan çeşitli deneylerde, mevcut telekom altyapısının kuantum anahtar dağıtımı (QKD) gibi uygulamalara uyum sağlayabildiği gösterilmiştir. Wengerowsky ve arkadaşları (2018), 96 km uzunluğundaki bir denizaltı telekom kablosu üzerinden kuantum dolanıklığı başarıyla aktarmış ve fotonların polarizasyon kararlılığının mesafe boyunca korunduğunu göstermiştir. Benzer bir çalışma 192 km'lik başka bir denizaltı hattında tekrarlanmış ve güvenilir dolanıklık dağıtımı elde edilmiştir (Wengerowsky et al., 2019). Bu bulgular, mevcut denizaltı fiber altyapısının uzun vadede kuantum-dirençli iletişim kanalları için güçlü bir aday olduğunu göstermektedir.

2.1. Denizaltı Kabloların Risk Faktörleri

Denizaltı kablolar, bahsedildiği üzere sadece veri taşımakla kalmayıp, enerji hattı oluşumundan, sefer güvenliğine kadar geniş bir alanda tüm dünyada hizmet vermektedir. Kablo teknolojisinin yapısı gereği iki nokta arasında bağlantı sağlanması gerektiğinden, bu noktalara ulaşım sağlanılması, teknik ekipmanların sevk edilmesi ve çalışma gerçekleştirilmesi oldukça maliyetli ve uzmanlık isteyen bir alan olarak ortaya çıkmakta, bununla birlikte bağlantı sağlanılan alanların iniş istasyonu olarak kurgulanması ve iletim hatlarının sonlandırılması, diğer hatlara eriştirilmesi gibi birçok işlemin yapılması ciddi bir iş gücü ihtiyacını ortaya koymaktadır.

Uluslararası sularda yürütülen bu çalışmalar başta doğa olayları olmak üzere, gemilerden bırakılan çapalara takılması, deniz korsanlarının terör eylemlerine maruz kalması ile ekipman ve/veya kablolarını tahribe uğratılması; bu neviden uzun koridorları haiz hatların gözetiminde ve denetiminde yaşanılan zorluklarla birlikte değerlendirildiğinde doğal sebeple ve/veya operasyonel amaçlarla sabotaj risklerini arttırmaktadır. Aynı zamanda kablo iniş istasyonlarının olası doğal afet durumları ile savaş ve terör olaylarında hedef olarak seçilerek imha edilmesi gerek kablonun tahribi gerek insan kaynağının kaybedilmesi gibi çeşitli risk faktörlerini barındırmaktadır.

Bu bakımdan veri iletiminin ve kablo teknolojisinin önemine atfen, güncel olarak Rusya – Ukrayna savaşında gün yüzüne çıkan haberleşme noktalarının tahrip edilmesi ve fiber-optik dron teknolojisinin savaş sahası ve savunma hattındaki etkinliği örnek olarak verilebilir. Her iki ülkenin kuvvetleri tarafından, fiber-optik kablolarını kesen veya yakan yarı-tam otonom savunma sistemleri üretilmesi; Türkiye'de ise bu konuda bazı savunma sanayii ar-ge projelerinin yürütülmesi, tehdit boyutunu somut olarak ortaya koymaktadır.

Öte yandan 2022'deki Rusya-Ukrayna geriliminden bu yana Baltık Denizi'nde bir dizi denizaltı kablosunun ve gaz boru hattının, şüpheli saldırılarda hasar gördüğü belirlenmiş, İsveçli yetkililerin Baltık Denizi'nin altından Letonya'ya uzanan bir kabloya zarar verdiğinden şüphelenilen bir gemiye el koyduğu ve ilk soruşturma sonuçlarının sabotaja işaret ettiğini belirtilmiştir. 2024 yılının şubat ayında Kızıldeniz'de birkaç iletişim kablosunun kesilmesiyle yaşanan diğer bir olayda Asya ve Avrupa arasındaki internet trafiği etkilenmiştir. Söz konusu kesintinin, Yemen hükümetinin İran destekli Husi hareketinin kabloları sabote edebileceği yönündeki uyarısından kısa bir süre sonra gerçekleştiği dikkat çekici olmakla birlikte Husiler bu kabloları hedef almadıklarını açıklamışlardır.

2.2. Denizaltı Fiber-optik Bağlantı Güncel Görünümü

Telgraf hatlarından, dünyayı gizlice saran bir kablo ağına dönüşen fiber-optik sistemler, günümüz itibariyle yaklaşık 600 aktif denizaltı kablo sistemi bulunmakta ve bunlara ek olarak 81 planlanan proje bulunmakta, toplamda yaklaşık 1.712 iniş istasyonu aktif veya yapım aşamasındadır (Telegeography, 2025).

1990-2010 yılları arasında fiber-optik kablo veri iletim kapasitesi 1-40 Terabit/s iken bu değer günümüzde toplam 1+ Petabit/s olarak ölçeklenebilmiştir. Ayrıca büyük ölçekli veri merkezi kurulum ihtiyaçları, yeşil enerji altyapılarının kurulması ile ulusal çapta iç bağlantı ve ilk bağlantı noktası oluşturma talepleri bölgesel açıdan denizaltı fiber-optik kablo yatırımlarının motivasyon kaynağı olarak ortaya çıkmaktadır (TeleGeography, 2025).

Tablo 1. Fiber-optik Kablo Bağlantılarının Kıtalara Göre Oransal ve Stratejik Dağılımları.

Bölge	Dağılım	Özellik	Anahtar Ülkeler
Asya-Pasifik	~%40	Yoğun nüfus, hızlı büyüme	Çin, Japonya, Hindistan, Güneydoğu Asya, Avustralya, Singapur
Avrupa	~%30	Akdeniz yoğunluğu, Baltık bağlantıları	İngiltere, Fransa, İtalya, Yunanistan, İspanya, Hollanda, İsveç
Kuzey Amerika	~%20	Yüksek kapasite ve Trans Atlantik-Pasifik bağlantıları	ABD (Doğu-Batı sahilleri), Kanada
Latin Amerika	~%5-7	Kıyı ülkelerde yoğunlaşma	Brezilya, Arjantin, Şili, Meksika, Karayipler
Afrika	~%3-5	Dijital erişim artışı	Güney Afrika, Kenya, Nijerya, Mısır, Fas
Orta Doğu	~%2-3	Avrupa-Asya köprüsü	Türkiye, Katar, BAE, Suudi Arabistan, İsrail

Kaynak: TeleGeography, ITU ve World Bank verilerine dayalı yazar derlemesi (2025).

3. Fiber Optik Ağların Akdeniz'deki Varlığı

Akdeniz, günümüzde küresel dijital iletişim ağının en yoğun ve stratejik bölgelerinden biri hâline gelmiştir. Avrupa, Asya ve Afrika arasındaki veri akışının büyük bir bölümü, bölge üzerinden geçen deniz altı fiber optik kablolar aracılığıyla gerçekleşmektedir. Uluslararası telekomünikasyon altyapısının yaklaşık %95'ten fazlasının deniz altı kablolarına dayanması (ENISA, 2022), Akdeniz'in bölgesel değil küresel ölçekte kritik bir iletişim koridoru olduğunu göstermektedir.

1980'lerin sonlarından itibaren koaksiyel sistemlerin yerini hızla fiber optik teknolojilerin almasıyla, Akdeniz'de çok katmanlı bir kablo ağı ortaya çıkmıştır. İtalya, Yunanistan, Türkiye, İsrail, Mısır ve Kıbrıs gibi ülkeler, farklı konsorsiyumlar aracılığıyla onlarca uluslararası kablo sisteminin ana güzergâhında yer almaktadır. Uluslararası Telekominasyon Birliği (ITU), bölgenin "yüksek kapasiteli veri taşıyan kıtalararası hatların doğal geçiş bölgesi" olduğunu vurgulamaktadır (ITU, 2019).

Bu kablolar yalnızca ticari telekomünikasyon açısından değil, devletlerin siyasi, ekonomik ve güvenlik stratejileri açısından da belirleyici bir role sahiptir. NATO ve Avrupa Birliği tarafından hazırlanan çeşitli raporlarda, denizaltı kablo hatlarının hem "kritik altyapı" hem de "jeostratejik varlık" olarak değerlendirildiği belirtilmektedir (CCDCOE, 2019). Kabloların iniş istasyonları, optik güçlendirme merkezleri ve yönlendirme altyapıları, siber ve fiziksel tehditlerin yoğunlaştığı noktalar olarak tanımlanmaktadır.

Akdeniz'deki kablo yoğunluğunun artmasının bir diğer nedeni ise geleneksel Mısır–Süveyş hattının aşırı yüklenmesi ve alternatif rotalara duyulan stratejik ihtiyaçtır. Bu çerçevede İtalya–Yunanistan–Türkiye, İsrail–Kıbrıs–Yunanistan, Tunus–İtalya ve Fransa–Cezayir gibi hatlar

bölgedeki veri akışının çeşitlendirilmesini sağlamaktadır. Avrupa Parlamentosu, özellikle son on yılda planlanan yeni fiber optik hatların "jeopolitik risklerden kaçınma ve alternatif istikamet yaratma stratejisi" kapsamında değerlendirildiğini belirtmektedir (European Parliament, 2024).

Dolayısıyla Akdeniz'deki fiber optik kablo varlığı, yalnızca teknik bir altyapı gelişimi olarak değil, aynı zamanda bölgedeki devletler arası rekabetin, ekonomik entegrasyonun ve istihbarat faaliyetlerinin altyapısal zeminini oluşturan çok katmanlı bir jeopolitik unsur olarak karşımıza çıktığı değerlendirilmektedir.

4. Fiber Optik Ağların İstihbarattaki Rolü

Dijital çağda denizaltı fiber optik kablolar, yalnızca iletişimin teknik altyapısı değil, aynı zamanda modern devletlerin güç projeksiyonu, istihbarat toplama ve jeopolitik nüfuz faaliyetlerinin merkez unsurlarından biri hâline gelmiştir. Günümüz küresel ekonomisinin ve devletlerarası iletişimin temel taşı olan bu kablolar, yüksek bant genişliği sayesinde sadece internet trafiğini değil; ticari sırları, diplomatik yazışmaları, finansal işlemleri ve askeri koordinasyonu da taşımaktadır (Sherman, 2021). Bu nedenle fiber optik kablolar, salt teknolojik bir varlık olmanın ötesine geçerek uluslararası ilişkilerde stratejik bir unsur olarak değerlendirilmektedir.

Saha araştırmaları, dünya veri trafiğinin %95'inden fazlasının deniz altı kabloları üzerinden aktığını ortaya koymaktadır (TeleGeography, 2024). Bu yüksek bağımlılık seviyesi, kabloları hem siber hem fiziksel açıdan kritik bir hedef hâline getirmekte ve istihbarat servisleri için önemli fırsatlar sunmaktadır. Kabloların sahiplik yapıları ve yönetim sistemleri de bu çerçevede stratejik bir rol oynar. Atlantic Council analizlerine göre, optik ağlarda kullanılan yeniden yapılandırılabilir optik ekleme-çıkarma sistemlerinin (ROADMs) uzaktan yönetilebilir olması, yetkisiz erişim, sinyal manipülasyonu ya da trafik yönlendirme gibi istismar edilebilir riskleri beraberinde getirmektedir (Maurer, 2021). Bu zafiyetler, gelişmiş siber operasyon kapasitesine sahip aktörlere pasif ve aktif istihbarat toplama imkânı sağlayabilir.

Denizaltı kablolarına yönelik istihbarat ilgisi yeni bir olgu değildir. Soğuk Savaş döneminde ABD Ulusal Güvenlik Ajansı'nın (NSA) yürüttüğü "Operation Ivy Bells" faaliyeti, Sovyet iletişim hatlarının gizlice dinlenmesiyle sonuçlanmış ve denizaltı altyapılarının istihbarat için ne kadar kritik olduğunu göstermiştir (Waterman, 2015). Günümüzde fiber optik teknolojisine geçiş, bu stratejinin yalnızca teknik açıdan evrim geçirdiğini fakat amacın değişmediğini ortaya koymaktadır.

Denizaltı kabloları üzerindeki istihbarat faaliyetlerinin önemli bir parçası ise karadaki kablo iniş istasyonlarıdır. Bu tesisler hem fiziksel saldırıya hem de siber müdahaleye açık olmaları nedeniyle en kırılgan noktalar arasında sayılmaktadır. UNIDIR raporları, birçok ülkede kablo iniş istasyonlarının potansiyel hedef olarak görüldüğünü ve aktif olarak gözetlendiğini ortaya koymaktadır (UNIDIR, 2023). Bu noktaların kontrolü, sinyal yakalama, trafik yönlendirme veya kesintiye uğratma gibi operasyonları mümkün kılabilir.

Devletlerin kablo altyapılarını yalnızca dinleme amacıyla değil, aynı zamanda veri rotalarını yeniden şekillendirme ve güvenli iletişim koridorları oluşturma amacıyla da kullandığı bilinmektedir. ISPI'nin analizlerine göre, büyük güçler kritik iletişim hatlarının kontrolünü elde ederek hem kendi veri güvenliğini artırmakta hem de rakip devletlerin trafiğini etkileme kapasitesi kazanmaktadır (ISPI, 2022). Bu durum, kabloların jeopolitik değerini daha da artırmaktadır.

NATO CCDCOE'nin raporu da denizaltı kablolarının artan jeopolitik gerilimler, casusluk riskleri ve sabotaj faaliyetleri nedeniyle giderek daha önemli bir çatışma alanı hâline geldiğini vurgular (NATO CCDCOE, 2019). Bu bağlamda, fiber optik kablolar yalnızca iletişim altyapısı değil, küresel güvenlik mimarisinin temel bileşenlerinden biri olarak değerlendirilmektedir.

5. Türkiye: Türkiye'nin Stratejik Konumu

Türkiye, Akdeniz havzasında eşine az rastlanır jeopolitik konumu sayesinde hem enerji hem ticaret hem de dijital iletişim hatları açısından stratejik bir merkez niteliği taşımaktadır. Karadeniz, Ege ve Doğu Akdeniz'e aynı anda erişimi, ülkenin deniz yetki alanlarını yalnızca ekonomik kazanımlar için değil, aynı zamanda istihbarat ve güvenlik faaliyetleri için de önemli hâle getirmektedir.

Türkiye'nin Doğu Akdeniz'de 2019 yılında Libya ile imzaladığı Deniz Yetki Alanlarının Sınırlandırılması Mutabakatı, bölgedeki deniz yetki alanlarını yeniden şekillendirmiş ve Türkiye'nin bu koridor üzerinden geçen potansiyel fiber optik hatlar üzerindeki stratejik etkisini artırmıştır. Avrupa Komisyonu, Doğu Akdeniz'deki deniz yetki alanı düzenlemelerinin bölgedeki enerji ve dijital iletişim hatlarının güvenliğiyle doğrudan bağlantılı olduğunu belirtmektedir (European Commission, 2020). Bu durum, deniz yetki alanı düzenlemelerinin yalnızca ekonomik değil, aynı zamanda güvenlik ve istihbarat boyutu olduğunu açıkça ortaya koymaktadır.

Uluslararası Deniz Hukuku çerçevesinde kıyı devletlerinin münhasır ekonomik bölge (MEB) ve kıta sahanlığı üzerinde kablo döşeme faaliyetlerine ilişkin düzenleme, izin ve güvenlik standartları belirleme yetkisi bulunmaktadır (Tanaka, 2015). Türkiye'nin Doğu Akdeniz'de yetki alanlarını genişletmesi, bu bölgelerde yürütülecek kablo faaliyetleri üzerinde daha güçlü bir düzenleyici ve gözetleyici kapasite oluşturmuştur. NATO'nun 2023 tarihli deniz güvenliği raporu Doğu Akdeniz'i "dijital altyapı açısından yüksek yoğunluklu risk bölgesi" olarak tanımlamakta ve bölgenin stratejik önemine işaret etmektedir (NATO, 2023).

Avrupa Birliği Ortak Araştırma Merkezi'nin (JRC) analizleri, Asya'dan Avrupa'ya yönelen dijital veri trafiğinin önemli bir bölümünün Türkiye çevresindeki deniz alanlarını geçtiğini ve Türkiye'yi bir "dijital koridor merkezi" haline getirdiğini ortaya koymaktadır (JRC, 2021). Antalya, Mersin, Hatay ve İstanbul gibi kablo iniş noktaları, Türkiye'nin veri güvenliği ve istihbarat kapasitesinin kritik unsurları olarak öne çıkmaktadır.

Eurispes'in değerlendirmesine göre ise Türkiye-Libya hattı, Mısır–Süveyş merkezli geleneksel kablo koridorlarına alternatif yeni güzergâhların oluşmasını sağlayabilir ve Türkiye'yi "yükselen bir dijital düzenleyici ve güvenlik aktörü" hâline getirebilir (Eurispes, 2021). Bu durum, Türkiye'nin kablo trafiğini yönlendirme, güvenlik standartlarını belirleme ve bölgesel veri akışını etkileme kapasitesini güçlendirmektedir.

NATO'nun Strategic Direction South Hub birimi, Türkiye'nin MEB ve kıta sahanlığı alanlarının dijital altyapı güvenliği açısından "jeopolitik kaldıraç" niteliği taşıdığını belirtmektedir (NATO SDS Hub, 2022). Bu değerlendirme, Türkiye'nin deniz yetki alanlarının modern istihbarat stratejileri açısından kritik bir değer taşıdığını ortaya koymaktadır.

Bu çerçevede Türkiye, son yıllarda geliştirdiği enerji ve dijital altyapı politikaları kapsamında yerli ve millî kapasitesini artırmaya ve dijital altyapı üzerindeki kontrolünü güçlendirmeye yönelik adımlar atmaktadır. Bu doğrultuda, 2000'li yılların başında sınırlı seviyede olan fiber optik altyapı uzunluğu, uygulanan politikalar ve yatırımlar sonucunda 2025 yılı itibarıyla yaklaşık 657 bin kilometreye ulaşmıştır (Cumhurbaşkanlığı, 2026). Söz konusu artış, yalnızca karasal altyapı

ile sınırlı kalmayıp, deniz altı iletişim hatlarının da sisteme dahil edilmesiyle daha bütüncül bir yapıya dönüşmüştür. Bu kapsamda Türkiye ile Kuzey Kıbrıs Türk Cumhuriyeti (KKTC) arasında kurulması planlanan deniz altı fiber optik hattı, iletişim altyapısının çeşitlendirilmesi ve kapasitenin artırılması çerçevesinde değerlendirilmektedir (Anadolu Ajansı, 2025).

Türkiye'nin Avrupa, Asya ve Orta Doğu arasında konumlanan jeostratejik yapısı, dijital veri akışları açısından bir geçiş ve bağlantı alanı oluşturmasına imkân tanımaktadır. Bu kapsamda geliştirilen altyapı projeleri, veri iletim kapasitesinin artırılması, ağ sürekliliğinin sağlanması ve farklı sistemlerin entegrasyonu açısından önem arz etmektedir. Bilgi Teknolojileri ve İletişim Kurumu'nun stratejik planlarında da fiber altyapının genişletilmesi, yerli üretimin desteklenmesi ve kritik altyapıların korunmasına yönelik hedefler öncelikli alanlar arasında yer almaktadır (BTK, 2023).

6. İsrail: İsrail'in Denizaltı Kablo Projeleri

İsrail, Doğu Akdeniz'de giderek yoğunlaşan jeostratejik rekabetin merkezinde yer alan ve özellikle dijital altyapı, enerji iletimi ve çok katmanlı güvenlik mimarileri açısından kritik projelerde aktif rol üstlenen bir aktör hâline gelmiştir. Bu konumlanış hem coğrafi avantajlarından hem de teknoloji-güvenlik ekseninde geliştirdiği kurumsal kapasiteden kaynaklanmaktadır. Özellikle denizaltı fiber optik kablo hatlarının yeniden şekillenmesi, İsrail'e ilk kez geniş ölçekli veri akışlarını yönlendirme, analiz etme ve kontrol edilebilir güzergâhlar üzerinden farklı bölgelere bağlanma imkânı tanımaktadır.

Bu bağlamda öne çıkan en kritik altyapılardan biri Blue-Raman fiber optik sistemidir. Google destekli bu ağ, iki ana bölümden oluşmaktadır: Akdeniz altından İtalya'dan İsrail'e uzanan "Blue" segmenti ve İsrail'den başlayarak Ürdün, Suudi Arabistan ve Umman'a yönelen "Raman" segmenti. Projenin en stratejik sonucu, geleneksel trans-Avrasya veri akışının Mısır üzerindeki yoğun bağımlılığını azaltması ve İsrail'e alternatif ve doğrudan bir dijital koridor oluşturmasıdır. Bu yapı; rotanın güvenliği, veri hacminin büyüklüğü ve ara bağlantı istasyonlarının konumları düşünüldüğünde, İsrail'e hem teknik hem istihbari anlamda benzersiz fırsatlar sunmaktadır. Özellikle "Unit 8200" gibi ileri sinyal istihbarat birimleri için, kabloya bağlı "landing station" noktalarının sağlayabileceği pasif dinleme imkânı sağlamakta ve metadata akışları ve şifrelenmemiş segmentler üzerinden trafik analizi yapılabilmesini mümkün kılmaktadır (Rid, 2020).

Benzer biçimde İsrail, EuroAsia Interconnector projesiyle hem Avrupa enerji şebekesine hem de dijital altyapılarına entegre olmayı amaçlamaktadır. İsrail–Güney Kıbrıs–Girit üzerinden Avrupa'ya uzanan bu hat, dünyanın en uzun ve en derin denizaltı güç iletim projelerinden biri olarak tanımlanmakta olup (European Commission, 2019), yalnızca elektrik iletimini değil aynı zamanda veri aktarımını mümkün kılan çift kullanımlı (dual-use) bir altyapı niteliği taşımaktadır. Bu durum İsrail'e hem enerji güvenliği hem de siber-istihbarat kapasitesi bakımından yeni bir derinlik kazandırmaktadır. Zira enerji iletim altyapılarında taşınan kontrol sinyalleri, yük yönetimi verileri ve SCADA iletişimi, modern siber güvenlik literatüründe yüksek değerli istihbarat unsurları olarak değerlendirilmektedir (Kello, 2017).

Doğu Akdeniz çevresinde şekillenen bir başka önemli girişim ise QuantumCable projesidir. Yunanistan, Kıbrıs, İsrail, Suudi Arabistan, Umman ve Hindistan arasında planlanan bu hat, yalnızca fiber optik kapasitesini artırmayı değil; aynı zamanda enerji, veri ve bulut merkezleri arasında yüksek hızda, düşük gecikmeli bir "çoklu altyapı koridoru" oluşturmayı hedeflemektedir. Proje, İsrail'in hem Avrupa enerji ağlarına eklemlenmesini güçlendirmekte hem

de Asya–Avrupa ekseninde veri akışında transit ülke olma konumunu pekiştirmektedir. Bu çerçevede Doğu Akdeniz, yalnızca bölgesel enerji denkleminde değil, küresel dijital rekabette de stratejik bir geçiş alanına dönüşmektedir.

Bu altyapı hamleleri, küresel jeopolitikte yeni bir rekabet ekseninin ortaya çıkmasıyla paralel ilerlemektedir: "IMEC: Hindistan–Orta Doğu–Avrupa Ekonomik Koridoru" 2023 yılı G20 Zirvesi'nde açıklanan bu girişim, Çin'in "Bir Kuşak, Bir Yol" projesine alternatif bir model olarak değerlendirilmektedir. Planlanan güzergâh Hindistan'dan başlayarak Birleşik Arap Emirlikleri, Suudi Arabistan, Ürdün ve İsrail üzerinden Avrupa'ya ulaşmaktadır. Bu hat; dijital altyapı, enerji nakil hatları, liman bağlantıları ve veri merkezleriyle çok katmanlı bir "yeni ticaret-teknoloji koridoru" yaratmayı hedeflemektedir. ABD yönetiminin projeye açık siyasi desteği (White House, 2023) ve özellikle İsrail'in Orta Doğu'daki normalleşme süreçleriyle eşzamanlı ilerlemesi, bu hattın jeopolitik önemini daha da artırmaktadır.

Tüm bu projeler bir arada değerlendirildiğinde, İsrail'in yalnızca bölgesel bir enerji veya iletişim aktörü olmanın ötesine geçerek, küresel veri akışının kritik bir bileşeni hâline geldiği görülmektedir. Ayrıca denizaltı kablolarının karaya çıktığı istasyonların siber ve fiziksel güvenliğinde yaşanan kırılganlıklar; saldırı, manipülasyon veya yönlendirme gibi tehditlerin varlığını artırmakta, böylece bu altyapıları stratejik hedef hâline getirmektedir. NATO'nun 2025 yılı başında duyurduğu ve denizaltı dronlarıyla desteklenen "Baltic Sentry" görev gücü, bu tür altyapıların artık kolektif savunma planlamasında öncelikli bir unsur olarak değerlendirildiğini göstermektedir (NATO, 2025).

Bu çerçevede İsrail'in dâhil olduğu projeler; yalnızca teknik kapasite inşası değil, aynı zamanda Doğu Akdeniz, Orta Doğu ve Hint Okyanusu ekseninde veri, enerji ve güvenlik hatlarının yeniden şekillendiği daha geniş bir jeopolitik dönüşümün parçası olarak anlam kazandığı değerlendirilmektedir.

7. Türkiye'yi Yalnızlaştırma Politikası: Infrastructural Containment

Doğu Akdeniz'de son on yılda şekillenen jeopolitik konfigürasyon, Türkiye'nin bölgesel kapasitesini ve deniz yetki alanlarındaki stratejik konumunu sınırlamaya yönelik çok katmanlı diplomatik ve teknik girişimleri içerdiği gözlemlenmektedir. Bölgedeki yeni enerji ve dijital altyapı projeleri, alternatif ittifak ağlarının oluşturulmasıyla eş zamanlı yürütülerek Türkiye'nin kıta sahanlığı, münhasır ekonomik bölge (MEB) ve deniz ulaştırma koridorları üzerindeki etkinliğini azaltmaya yönelik stratejik bir etki doğurmuştur (Cumhurbaşkanlığı İletişim Başkanlığı, 2020). 2025 yılının yaz aylarında İsrail ile Yunanistan arasına döşenecek yeni bir fiber optik kablo güzergahını belirlemek üzere kiralanan araştırma gemisi MEB politikaları doğrultusunda Türkiye tarafından engellenmiş ve dört gün sürecek diplomatik bir süreç yaşanması (Middle East Forum, 2025), stratejik ve politik etkinliğin göstergesi olarak kabul edilmektedir.

EastMed Gas Forum gibi inisiyatifler ve buna bağlı hat projeleri, Türkiye'nin dışlanmasıyla kurgulanan enerji iş birliklerinin örneklerinden olup; benzer şekilde bazı elektrik ve fiber optik hat projelerinde Türkiye'yi bypass eden güzergâh tercihleri gözlenmektedir (Global Energy Monitor, 2024; Istituto Affari Internazionali [IAI], 2018). EuroAsia Interconnector ve benzeri projeler teknik gerekçeler taşısa da aynı zamanda jeopolitik tercihlerin yansıması olarak da okunabilmektedir (European Parliament, 2021).

Bunun sonucunda denizaltı fiber optik hatların rotalarının yeniden kurgulanmasıyla Türkiye kıyılarına uğramayan yeni hatlar devreye girebilmekte; bu durum hem Türkiye'nin bölgesel siber

güvenlik rolünü zayıflatmakta hem de veri trafiği üzerindeki analiz ve denetim kapasitesini sınırlamaktadır. Özel sektörün ve bazı devlet aktörlerinin yönlendirdiği yeni veri koridoru tercihleri, bölgesel dijital mimaride Türkiye'nin etkisini azaltmaya yönelik bir stratejik görünüm ortaya koymaktadır (TeleGeography, 2024; Europen Commission, Joint Research Centre [JRC], 2021).

Diplomatik ve askerî gelişmeler de bu altyapı eğilimleri ile örtüşmektedir. Bölgede artan askerî varlıklar, savunma iş birlikleri ve üs yatırımları, Türkiye'nin güvenlik mimarisindeki konumunu etkilemekte; bu dinamikler bölgesel bloklaşmayı güçlendirmektedir (RAND Corporation, 2020–2021; Atlantic Council, 2020–2021). Bu bağlamda, "altyapı üzerinden çevreleme" (infrastructural containment) yaklaşımı, teknik ve diplomatik araçların birlikte kullanıldığı bir stratejik model olarak değerlendirilmelidir.

Türkiye açısından ise mesele yalnızca coğrafi bir ulaşım koridoru olmanın ötesindedir: ülke, doğu ile batı arasındaki veri ve enerji akışlarında merkezi bir konuma potansiyel olarak sahiptir. Bu potansiyel, transit ülke avantajını genişletme imkânı sunarken aynı zamanda önemli güvenlik, regülasyon ve uluslararası iş birliği gerektirir. Türkiye'nin bu süreçlere dâhil edilmesi, bölgesel istikrar, veri güvenliği ve enerji arz güvenliği açısından önemli bir belirleyici olacaktır (Tagliapietra, 2020; Centre for European Policy Studies [CEPS], 2021; TeleGeography, 2024).

Son günlerde yapay zekâ sistemlerinin yaygınlaşması ile ortaya çıkan veri merkezi ihtiyacı ve bu veri merkezlerinin çeşitli coğrafyalarda konuşlandırılması bağlamında Türkiye'nin jeopolitik önemi bir kez daha gündeme gelmiş, 2029 yılına kadar en az üç ağ kümesinden oluşan bir bulut bölgesi geliştirmek için Google tarafından yatırım anlaşmaları imzalanmıştır. Öte yandan yerli-ulusal kapasite artışı ve kesintisiz iletişim adına TÜRKSAT tarafından 2027 yılında devreye alınması beklenen veri merkezi inşaatının temelleri atılmıştır.

Sonuç

Denizaltı fiber optik kablolar, günümüzün en görünmez ama en kritik stratejik altyapıları arasında yer almaktadır. Bu altyapıya hâkim olmak, yalnızca hızlı iletişim sağlamak değil; veri akışını yönlendirme, trafiği analiz etme ve gerektiğinde müdahale edebilme kapasitesi elde etmek anlamına gelmektedir. Akdeniz'deki dijital ve enerji projelerinin yön değiştirmesi, bölgesel güç dengelerini yeniden şekillendiren önemli bir unsur hâline gelmiştir.

İsrail'in son yıllarda hızla artan dijital altyapı projelerindeki rolü, ülkeyi Akdeniz çevresinde yükselen bir veri merkezi hâline getirirken; Türkiye'nin bu süreçlerin dışında bırakılmasına yönelik bazı girişimler, bölgesel rekabetin teknik altyapı üzerinden yürütüldüğünü göstermektedir. Türkiye, coğrafi konumu, geniş deniz yetki alanları ve artan dijital koridor potansiyeliyle, bölgenin en güvenli, en kısa ve en ekonomik veri ve enerji geçiş güzergâhını temsil etmektedir. Bu nedenle Türkiye'nin bölgesel dijital mimaride aktif ve belirleyici bir aktör hâline gelmesi, ulusal güvenlik, siber savunma, veri egemenliği ve bölgesel istikrar açısından stratejik bir zorunluluk olarak ortaya çıkmaktadır.

Bu çalışma, geçmişten bugüne gelişen ve fiber optik teknolojisine dönüşen deniz altı iletişim altyapılarının yalnızca veri taşıma işlevine sahip olmadığını göstermektedir. Söz konusu hatlar, bölge devletleri için potansiyel bir zafiyet unsuru oluştururken; altyapıya sahip şirketler ve aktörler açısından stratejik bir avantaj sağlamaktadır. Ayrıca, bu hatlar aracılığıyla sinyal dinleme ve istihbarat faaliyetlerinin yürütülebileceği ve kablo iniş istasyonlarının stratejik öneme sahip olduğu vurgulanmaktadır. Dolayısıyla, denizaltı fiber optik altyapılar, sadece iletişim ağları

olarak değil; aynı zamanda bölgesel güç projeksiyonu ve istihbarat kapasitesinin kritik bir aracı olarak değerlendirilmelidir.

Bu çalışma, literatürdeki mevcut jeopolitik analizlerden farklı olarak, fiber optik teknolojilerdeki teknik gelişmeleri (örneğin DAS sistemleri) doğrudan uluslararası güvenlik ve istihbarat doktrinleriyle ilişkilendirerek özgün bir katkı sunmaktadır. Elde edilen bulgular, Doğu Akdeniz'deki rekabetin yalnızca hidrokarbon kaynakları üzerinden değil, aynı zamanda veri güzergahları üzerinden de şekillendiğini açık biçimde ortaya koymaktadır. Bu bağlamda, gelecekte yapılacak çalışmaların, denizaltı fiber optik kablo güvenliğinin uluslararası hukuk, özellikle deniz hukuku çerçevesindeki boşluklarını ve yapay zekâ destekli veri analizinin bu altyapılar üzerindeki etkisini daha kapsamlı şekilde incelemesi gerekmektedir.

Kaynakça

Anadolu Ajansı. (2024). *Türkiye'deki fiber ağ dünyanın çevresini 16 kez dolaşacak uzunluğa erişti*. https://www.aa.com.tr/tr/bilim-teknoloji/turkiyedeki-fiber-ag-dunyanin-cevresini-16-kez-dolasacak-uzunluga-eristi/3797867

Anadolu Ajansı. (2024). *Türkiye'nin fiber altyapı uzunluğu bu yıl 600 bin kilometreye çıkarılacak*. https://www.aa.com.tr/tr/bilim-teknoloji/turkiyenin-fiber-altyapi-uzunlugu-bu-yil-600-bin-kilometreye-cikarilacak/3106880

Anadolu Ajansı. (2025, December 31). *Türkiye ile KKTC arasındaki fiber optik protokolü Resmî Gazete'de yayımlandı*. https://www.aa.com.tr/tr/ekonomi/turkiye-ile-kktc-arasindaki-fiber-optik-protokolu-resmi-gazetede-yayimlandi/3786620

BBC. (2025, September 11). *Sweden seizes ship after suspected Baltic Sea cable sabotage*. https://www.bbc.com/news/articles/cqx9g5wwp89o

BBC Türkçe. (2025, November 18). *Microsoft cloud services disrupted by Red Sea cable cuts*. https://www.bbc.com/news/articles/c3rvx470yg8o

Bilgi Teknolojileri ve İletişim Kurumu. (2023). *2023–2025 stratejik planı*. https://www.btk.gov.tr

CCDCOE. (2019). *Strategic importance of, and dependence on, undersea cables*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf

Chesnoy, J., & Antona, J.-C. (2025). *Undersea fiber communication systems* (3rd ed.). Academic Press.

CNBC. (2025). *Underwater cables are a vital piece of the AI buildout*. https://www.cnbc.com/2025/11/08/big-tech-ai-underwater-cables.html

Csernatoni, R. (2022). *The geopolitics of submarine cables: The infrastructure of the digital age*. ISPI Policy Brief. https://www.ispionline.it/en/publication/geopolitics-submarine-cables-infrastructure-digital-age-35516

Cumhurbaşkanlığı İletişim Başkanlığı. (2020). *Türkiye'nin Doğu Akdeniz stratejisi*. https://kulakver.iletisim.gov.tr/tr/kitap/turkiyenin-dogu-akdenizi-stratejisi

ENISA. (2022). *Subsea cables: What is at stake?*https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf

European Commission. (2019). *Euro-Asia submarine electricity interconnection cable (EuroAsia Interconnector)*. https://international-partnerships.ec.europa.eu/policies/global-gateway/euro-asia-submarine-electricity-interconnection-cable_en

European Commission. (2020). *Eastern Mediterranean security and infrastructure mapping report*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0299

European Parliament. (2024). *Security threats to undersea communications cables and infrastructure*. SEDE Committee Report. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Fridbertsson, N. T. (2023, October 7). *Protecting critical maritime infrastructure: The role of technology* (032 STC 23 E Rev. 2 Fin). NATO Parliamentary Assembly, Science and Technology Committee. https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc

International Telecommunication Union. (2019). *Measuring digital development: Facts and figures 2019*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

Joint Research Centre. (2021). *Digital pathways between Europe and Asia*. Publications Office of the European Union.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

L'Eurispes. (2025, September 22). *Mediterraneo allargato, epicentro del nuovo disordine globale*. https://www.leurispes.it/mediterraneo-allargato-epicentro-del-nuovo-disordine-globale/

Middle East Forum. (2025, November 20). *The Eastern Mediterranean has become Europe's digital fault line*. https://www.meforum.org/mef-observer/the-eastern-mediterranean-has-become-europes-digital-fault-line

NATO. (2023). *Maritime strategy and critical undersea infrastructure security*. https://www.nato-pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Robit Teknoloji. (2025). *URKUT: Fiber FPV bariyer*. https://www.robit.com.tr/project/urkut-fiber-fpv-bariyer

Runde, D. F., Murphy, E. L., & Bryja, T. (2024). *Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition*. Center for Strategic and International Studies. https://features.csis.org/safeguarding-subsea-cables/

Sandroni, C., & Tonini, G. (2025). *NATO and critical infrastructures: Regasification plants in the Mediterranean*. NATO Defense College Foundation. https://www.natofoundation.org/food/nato-and-critical-infrastructures-regasification-plants-in-the-mediterranean/

Sherman, J. (2021). *Cyber defense across the ocean floor: The geopolitics of submarine cable security*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/

Tanaka, Y. (2015). *The international law of the sea*. Cambridge University Press.

The Misgav Institute for National Security and Zionist Strategy. (2025, June). *The India–Middle East–Europe (IMEC) economic corridor*. https://www.misgavins.org/wp-content/uploads/2025/06/%D7%A1%D7%95%D7%A4%D7%99.-%D7%97%D7%95%D7%91%D7%A8%D7%AA-IMEC-1-1-1.pdf

Türkiye Cumhuriyeti Cumhurbaşkanlığı. (2026). *5G teknolojisi Türkiye'nin önünde yepyeni bir sayfa açacak*. https://www.tccb.gov.tr/haberler/410/164468/-5g-teknolojisi-turkiye-nin-onunde-yepyeni-bir-sayfa-acacak

UNIDIR. (2023). *Wading murky waters: Subsea communications cables and responsible state behaviour*. https://unidir.org/publication/wading-murky-waters-subsea-communications-cables-and-responsible-state-behaviour/

Williams, E. F., Fernández-Ruiz, M. R., Magalhaes, R., Vanthillo, R., Zhan, Z., González-Herráez, M., & Martins, H. F. (2019). Distributed sensing of microseisms and teleseisms with submarine dark fibers. *Nature Communications, 10*(1), Article 5778. https://doi.org/10.1038/s41467-019-13262-7