Denizaltı Telekomünikasyon Kabloları ve Kritik Altyapı Güvenliği

Doç. Dr. S. Sezgin Mercan
Doç. Dr. Kıvılcım Romya Bilgin

Bugün birçok ülkeyi, bölgesel bütünleşmeyi ve uluslararası örgütü ilgilendiren önemli bir sorun alanını kritik altyapıların güvenliği ve sürdürülebilirliği oluşturmaktadır. Kritik altyapılar, toplumlar için büyük önem taşıyan ve arızalanmaları veya bozulmaları durumunda sürekli tedarik kıtlığına, kamu düzeninde, güvenlikte ve emniyette önemli aksamalara veya benzeri sonuçlara yol açacak kuruluşlar ve tesislerdir. Gıda (balıkçılık), su, enerji, sağlık, bilgi teknolojisi ve telekomünikasyon, ulaşım, medya, devlet yönetimi, finans gibi unsurlar kritik altyapının farklı sektörlerini oluşturmaktadır.[1] Bölgesel ve uluslararası düzeydeki çatışma ve savaşların kritik altyapılara verdikleri zararlar, çatışan tarafları ve ötesinde yakın çevrede yer alan, çatışma ve savaşın dolaylı ya da doğrudan tarafı olan ülkeleri, toplumları ve uluslararası örgütleri yakından etkilemektedir. Özellikle Batı ülkelerinde bu konuda 2000'li yıllarda başlayan iş birliği girişimleri ancak 2020'ler itibariyle kurumsal düzeye çıkabilmiştir. 2022 yılında AB ile NATO arasındaki iş birliği küresel seviyede varılan noktanın en önemli örneğidir.[2] Bu nedenle kritik altyapıların güvenliği, yalnızca teknik bir koruma veya bir iş birliği meselesi değil, uzun vadede bölgesel dayanışmayı ve uluslararası güvenlik mimarisinin işleyişini belirleyen stratejik bir yönetişim alanı olarak görülmelidir.

Bu stratejik çerçeve içinde, kritik altyapı tartışmasının dijital boyutunu en somut biçimde görünür kılan alanlardan biri denizaltı telekomünikasyon kablolarıdır. Denizaltı telekomünikasyon kabloları, günümüz dijital ekonomisinin ve kamu hizmetlerinin görünmez omurgasıdır. Kablo ekosistemi ölçek olarak büyüktür. 2025 yılı itibarıyla dünya genelinde 1,5 milyon kilometreyi aşan 600'ün üzerinde aktif denizaltı kablo sistemi olduğu belirtilmektedir.[3] Bu sistem, küresel IP/internet trafiğinin %99'dan fazlası denizaltı kabloları üzerinden taşınmaktadır.[4] Finansal işlemlerden bulut bilişime, hükümet iletişiminden platform ekonomisine kadar kritik hizmetlerin sürekliliği bu fiziksel altyapının güvenliğine bağlı hale gelmektedir. Bu nedenle kablo güvenliği yalnızca bir bağlantı meselesi değildir. Verinin erişilebilirliği, gizliliği ve bütünlüğü boyutlarıyla küresel veri güvenliği gündeminin önemli bir parçasıdır. AB'nin 2024 tarihli Tavsiyesi de denizaltı kablolarını uluslararası veri trafiği ve dijital egemenlik bağlamında stratejik bir unsur olarak ele alarak, risk değerlendirmesi ve dayanıklılık önlemlerinin sistematikleştirilmesini önermektedir.[5] Bu tablo, denizaltı kablolarını yalnızca ekonomik dolaşımın değil, aynı zamanda veri güvenliğinin sürekliliği açısından da değerli ve çok boyutlu tehditlere açık bir kritik altyapı kategorisine yerleştirmektedir. Dolayısıyla kablo güvenliği tartışması, somut vakalar üzerinden fiziksel

---

[1] What are Critical Infrastructures? https://www.bsi.bund.de/EN/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (Erişim: 31.12.2025); Christian Bueger, Tobias Liebetrau, "Critical maritime infrastructure protection: What's the trouble?" *Marine Policy*, 155, 2023, s.2.

[2] Annegret Bendiek, Mika Kerttunen, "Enhancing EU-NATO Cooperation in Preparedness and Critical Infrastructure Protection," *SWP Working Paper*, No.6, 2025, s.3.

[3] "Ekonominin geleceği denizaltı kablolarından geçiyor," https://immib.org.tr/tr/ekonominin-gelecegi-denizalti-kablolarindan-geciyor, (Erişim: 31.12.2025)

[4] OECD (PDF) – Enhancing the Resilience of Communication Networks (2025) https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/enhancing-the-resilience-of-communication-networks_a47d78a1/d6920477-en.pdf, (Erişim: 02.01.2026)

[5] European Commission – Recommendation on the security and resilience of submarine cable infrastructures https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures, (Erişim: 02.01.2026)

saldırı, siber risk, doğal afet veya terör gibi farklı risk türlerinin aynı anda nasıl kesiştiğini göstermeyi gerektirir.

Nitekim, fiziksel saldırılardan siber saldırılara, doğal afetlerden terörizme kadar uzanan geniş yelpazede irdelenebilecek olan kritik altyapıların güvenliği, en çok sağlık, finans, telekomünikasyon, ulaşım ve enerji sektörleri üzerinden açık vermektedir.[6] 2022'de Faroe Adaları'nı İskoçya ana karasına bağlayan SHEFA-2 deniz altı internet kablosunun iki ayrı olayda hasar görmesi ve Faroe Adaları'nın büyük bölümünde internet kesintilerine yol açması bir diğer örneği oluşturmuştur. Aynı dönemde Fransa'nın Marsilya kentini Lyon, Milano ve Barselona'ya bağlayan üç önemli deniz altı kablosu da kesilmiş ve bu durum küresel internet bağlantılarını etkilemiştir. Bunlar sabotaj sonucu olabileceği gibi, balıkçı teknelerinin kablolara zarar vermesi sonucu oluşabilen sorunlar olarak değerlendirilmiştir. Buradaki kritik husus, kısa sürede ve birden fazla kez bu gibi sorunların yaşanmış olmasıdır. Norveç'te daha önce Svalbard'daki iletişim ve bilimsel izleme kablolarının kesilmesi olaylarında, Rus balıkçı gemilerinin kablo güzergâhları üzerinde tekrar tekrar geçtiği tespit edilmişti. Nord Stream olaylarının ardından Norveç, Kuzey Denizi'ndeki petrol, gaz ve iletişim altyapılarının güvenliğini artırmış; deniz devriyeleri sıklaştırmış ve platformlar dronlarla izlenmeye başlanmıştır.[7] Bu örnekler, denizaltı kablolarının yalnızca Avrupa-Atlantik hattında değil, jeopolitik gerilimin yüksek olduğu Asya-Pasifik'te de benzer kırılganlıklar ürettiğini göstermektedir. Nitekim Tayvan vakası, kablo hasarının teknik bir arıza veya kaza ile kasıtlı bir eylem arasındaki esası oluşturan niyet ayrımının bulanıklaştığı bir örnektir. Tayvan'ın ana adasına uzanan iki denizaltı internet kablosu dijital dünyaya erişimde önemli kaynaklardır. 2023 yılında Tayvan Ulusal İletişim Komisyonu, adanın telekomünikasyon hizmetine atıfta bulunarak, iki Çin gemisi tarafından kabloların kesildiği iddiasını kamuoyuyla paylaşmıştı. Komisyon, bir Çin balıkçı gemisinin denizde yaklaşık 50 kilometre (31 mil) açıkta ilk kabloyu kestiğinden şüphelenildiğini belirtmişti. 8 Şubat'ta da bir Çin kargo gemisinin ikinci kabloyu kestiği iddiası basına yansımıştı. Tayvan hükümeti, bunun Çin tarafından yapılan kasıtlı bir eylem olduğunu söylemekten kaçınmış ve Çin gemilerinin sorumlu olduğuna dair doğrudan bir kanıt bulunmadığını açıklamıştı.[8] Netice itibarıyla, Tayvan örneği, denizaltı kablolarına yönelik olaylarda fail isnadının çoğu zaman tartışmalı kaldığını, bu nedenle kablo güvenliğinin sağlanmasında belirleyici olanın, niyet tartışmasına sıkışmadan sistemleri izleme, yedekleme ve hızlı onarım kapasitesini geliştirme üzerinden sistemlerin dayanıklılığını artırmak olduğunu göstermektedir.

Benzer biçimde, Avrupa'nın doğu sınırında yer alan Baltık Denizi de erken uyarı, koordinasyon ve onarım kapasitesinin test edildiği bir başka kritik sahneye dönüşmüştür. 2025 yılı itibariyle, Finlandiya-Estonya doğalgaz boru hattı, Estonya-Finlandiya elektrik kablosu ve İsveç ile Litvanya-Estonya-Letonya, Finlandiya ile Estonya-Almanya arasındaki sekiz veri kablosu Baltık Denizi'ndeki kargo gemisi veya petrol tankerlerinin demirlemesiyle kesintiye uğramış ve olayların kaza değil, kasıtlı olabileceği düşünülmüştür. Çünkü ilgili gemilerin Rus limanlarına gidip geldiği tespit edilmiştir.[9] Baltık Denizi'ndeki Estlink-2 elektrik kablosu ve bazı veri kablolarına zarar verildiği şüphesiyle Rusya ile bağlantılı olduğu belirtilen Eagle S adlı gemi, Fin polisince alıkoyulduktan sonra öne çıkan bir örnek

[6] A.g.e., s.4.
[7] Malte Humpert, "Fiber-optic Submarine Cable near Faroe and Shetland Islands Damaged; Mediterranean Cables also Cut," *High North News,*2022, https://www.highnorthnews.com/en/fiber-optic-submarine-cable-near-faroe-and-shetland-islands-damaged-mediterranean-cables-also-cut (Erişim: 31.12.2025)
[8] AP News, "Taiwan suspects Chinese ships cut islands' internet cables," https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70, (Erişim: 31.12.2026)
[9] A.g.e., s.5, 6.

olmuştur.[10] Bu gibi olaylara karşı gerek ulusal gerekse de uluslararası düzeyde önlem alınmasında geç kalınması ya da ön alıcı girişimlerin yapılamaması temel sorunlardandır. Bu sorunu aşmak için kamu sektörü, özel sektör, sivil-askeri bürokrasi ve sivil toplum arasında karşılıklı güven ve iş birliği zemininin oluşturulması temel bir ihtiyaçtır.[11] Bu nedenle Baltık örnekleri, etkili yaklaşımın, paydaşlar arasında standartlaştırılmış kriz prosedürleri ve hızlı onarım kapasitesi geliştirilmesiyle desteklenen kurumsallaşmış bir yönetişim rejimi kurmaktan geçtiğini göstermektedir.

Ne var ki Baltık ve Tayvan örneklerinin işaret ettiği kurumsal dayanıklılık ihtiyacı, deniz ortamında yalnızca kapasite eksiklerinden değil, aynı zamanda uluslararası hukukun yetki ve müdahale sınırlarından kaynaklanan yapısal kısıtlarla karşılaşmaktadır. Örneğin, deniz söz konusu olduğunda, kıyı devletlerinin münhasır ekonomik bölgelerinde diğer devletlerin faaliyetlerini engelleme yetkisi sınırlı kalmaktadır. Bir kıyı devleti, bu bölgelerde askeri faaliyetlere müdahale etme hakkına sahip değildir. Ancak, bazı devletler denizaltı altyapısını haritalandırma faaliyetlerini yürütmekte ve bu da diğer devletlerin güvenliğine yönelik tehdit oluşturmaktadır. Münhasır ekonomik bölgenin barışçıl amaçlarla kullanılmasını öngören uluslararası hukuk, casusluk faaliyetlerini genellikle yasaklamamaktadır. Bu durum ise denizaltı altyapısını haritalandırma gibi faaliyetlerin adeta meşru görülmesine yol açmaktadır. Eylemler düşmanca ve saldırgan bir nitelik taşıyorsa durum değişebilmektedir. Kıyı devletlerinin, münhasır ekonomik bölgedeki altyapılarına yönelik sabotaj faaliyetlerini engelleme hakkı vardır. Örneğin, boru hatları ve denizaltı kablolarına yönelik sabotaj, çevresel felakete yol açabilir. Bu durumda, kıyı devleti, şüpheli gemilere karşı önleyici tedbirler alabilmektedir. Kıyı devletleri, münhasır ekonomik bölgedeki bazı stratejik yapılar etrafında güvenlik bölgeleri oluşturabilmektedir. Bu bölgelerde, sabotaj ve terör eylemleri gibi tehditlere karşı önlemler alabilmektedir.[12] Dolayısıyla denizaltı kablolarının korunmasında hukukun çizdiği bu sınırlar, tam koruma yaklaşımını pratikte zayıflatmaktadır.

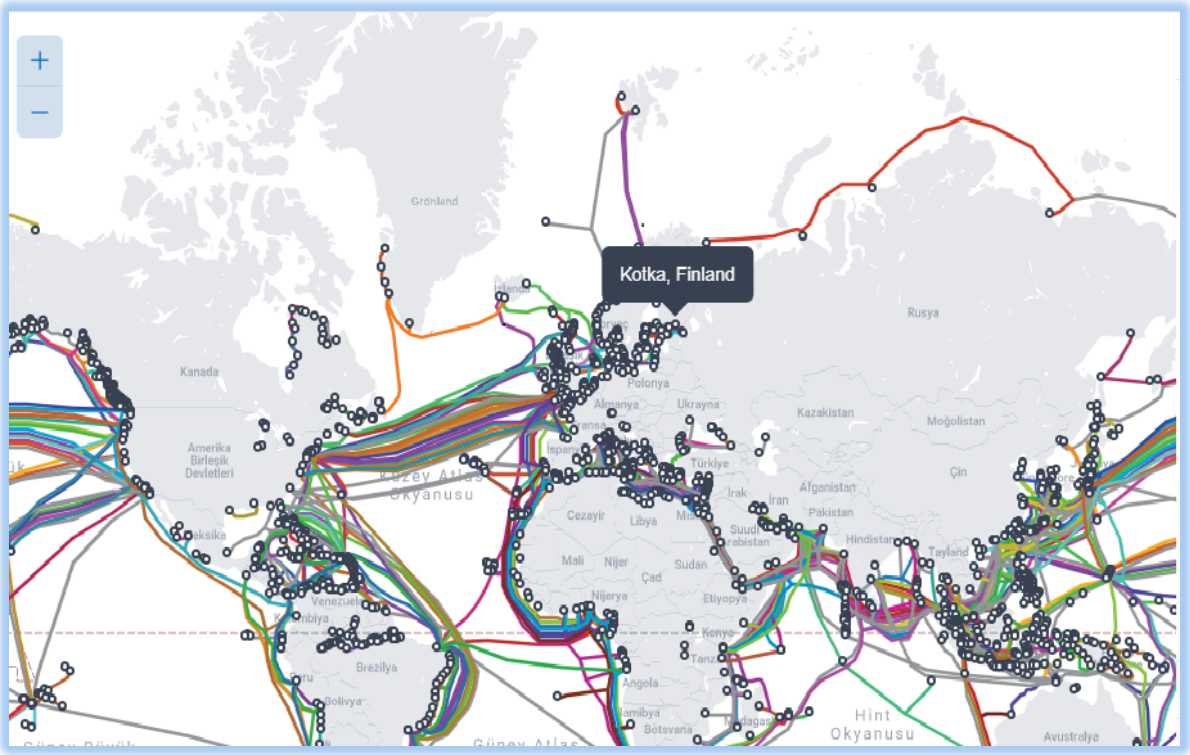
Kritik denizcilik altyapısının korunmasında bakım ve onarım boyutu genellikle ihmal edilmektedir. Halbuki güçlü onarım kapasitesi, altyapı arızalarının ve zincirleme etkilerinin sonuçlarını azaltmakta ve saldırıların etkisini de azaltmaktadır. Onarım kapasiteleri çoğunlukla özel sektöre aittir ve maliyet–fayda hesapları nedeniyle sınırlıdır. Bu nedenle devletler ile sektör arasında en iyi uygulamaların geliştirilmesi, deneyim paylaşımı ve bilgi alışverişi için yakın iş birliği gereklidir. Ayrıca, hükümetlerin, örneğin silahlı kuvvetler aracılığıyla, acil durumlarda onarım yapabilen çok amaçlı gemiler gibi tamamlayıcı onarım kapasiteleri sağlayıp sağlayamadıkları da irdelenmelidir. Birleşik Krallık Kraliyet Donanması'nın sualtı gözetimi için edindiği ve onarım görevlerinde de kullanılabilen gemisi buna örnektir.[13]

Dünyada oldukça geniş bir coğrafyaya yayılmış denizaltı kablo ağı bulunmasına karşın, bu ağlar zarar gördüğünde müdahale ve onarım kapasitesi hem sınırlı hem de yüksek maliyetlidir.[14] Dünya genelinde sadece 77 kablo döşeme gemisi olup, bunların sadece 22'si hat tamiri yapabilmektedir. Üstelik filonun büyük bölümü yaşlıdır ve gemilerin ortalama yaşı

---

[10] NPR, "Finland detains Russia-linked vessel over damaged undersea power cable in Baltic Sea," https://www.npr.org/2024/12/27/g-s1-40114/finland-russia-vessel-undersea-cables, (Erişim: 31.12.2025)
[11] A.g.e. s.10.
[12] Detaylı bilgi için bkz. Christian Schaller, "Critical Maritime Infrastructure and the Regime of the EEZ: A Blank Cheque for Saboteurs?" *European Journal of International Law,* 2024, https://www.ejiltalk.org/critical-maritime-infrastructure-and-the-regime-of-the-eez-a-blank-cheque-for-saboteurs/ (Erişim: 31.12.2025)
[13] Bueger, Liebetrau, s.6.
[14] Kablo haritası için bkz. https://www.submarinecablemap.com/

yaklaşık 30 yıldır.[15] Neticede, mevcut kapasite kısıtı ve filonun yaşlanması, denizaltı kablolarında dayanıklılığı artırmanın; kamu–özel iş birliğine dayalı, yedeklilik ve kriz protokollerini kurumsallaştıran ve etkin bir yönetişim mimarisiyle desteklenen somut bir kapasite gündemini zorunlu kıldığını göstermektedir.



Kaynak: https://www.submarinecablemap.com/

Sonuç olarak denizaltı telekomünikasyon kabloları, küresel veri akışı ve kritik kamu ila özel hizmetlerin sürekliliği açısından stratejik bir altyapı niteliği taşımaktadır. Ancak vakalar, bu altyapının hem tekrarlayan hasarlara açık olduğunu hem de olayların kaza mı kasıt mı olduğuna ilişkin değerlendirmenin çoğu zaman belirsiz kaldığını göstermektedir. Deniz ortamında hukukun ve operasyonel gerçekliğin çizdiği sınırlar, kabloların güvenliğine ilişkin müdahaleleri sınırlarken, politik önceliği sistemlerin izleme ve erken uyarı, paydaşlar arası koordinasyon, yedekleme ve özellikle hızlı bakım-onarım kapasitesinin güçlendirilmesi gibi uygulanabilir adımlara yöneltmektedir. Bu nedenle etkili bir strateji, tekil olayları tamamen önlemeye değil, kesinti ve hasar durumunda sistemin hızla toparlanmasını sağlayacak kurumsallaşmış bir dayanıklılık rejimi kurmaya dayanmalıdır.

[15] Ferdinand Gehringer, Matthias Hespe, "Lifelines under Threat," *International Reports*, Vol.41, Issue 1, 2025, s.21, 22.