T E S P A M

Türkiye Enerji Stratejileri ve Politikaları Araştırma Merkezi

KRİTİK ENERJİ ALTYAPISI GÜVENLİĞİNDE

PARADİGMA DEĞİŞİMİ

Savaşın, İklimin ve Su Altının Yeni Cephesi Olarak Enerji Sistemleri:

Vaka Analizleri, Koruma Mimarisi, Küresel Risk İndeksi ve Türkiye

STRATEJİK ARAŞTIRMA RAPORU

Eylül 2026 · Ankara

Hazırlayan

TESPAM Kızıl Elma Enstitüsü

Oğuzhan Akyener yönetiminde, TESPAM bünyesinde hazırlanmıştır

Bu rapor, TESPAM Kızıl Elma Enstitüsü tarafından kamu ve özel sektör karar alıcılarına yönelik olarak hazırlanmıştır.

İÇİNDEKİLER

YÖNETİCİ ÖZETİ

Rusya Devlet Başkanı Vladimir Putin, 2026 yazında kamuoyuna yaptığı değerlendirmelerde, ülkesinin kritik altyapısına ve özellikle enerji tesislerine yönelik saldırıların akaryakıt arzında sorun yarattığını açıkça kabul etti. Aynı konuşmalarda, bu tesislerin güvenilir biçimde korunmasının artık öncelikli bir görev olduğunu ve insansız hava aracı ile füze saldırılarının püskürtülmesinde görev alan bütün kurumların eşgüdüm içinde çalışması gerektiğini vurguladı. Dünyanın en büyük enerji ihracatçılarından birinin devlet başkanının, kendi rafineri ağının korunamadığını kabul etmesi, sıradan bir savaş haberi değildir. Bu ifade, 1970'lerden bu yana enerji güvenliği literatürünün üzerine kurulduğu temel varsayımlardan birinin — üretici devletin kendi topraklarındaki enerji altyapısını koruyabileceği varsayımının — ampirik olarak çöktüğünün itirafıdır.

Bu rapor, söz konusu çöküşün anatomisini çıkarmakta, benzer kırılmanın Suudi Arabistan, İran, Körfez ülkeleri, Ukrayna, Baltık havzası ve Doğu Akdeniz örneklerinde nasıl tekrarlandığını incelemekte, altyapı türlerine göre ayrıştırılmış bir koruma mimarisi önermekte, özgün bir **Kritik Enerji Altyapısı Güvenlik İndeksi (TESPAM-KEAGİ)** geliştirmekte ve bulguları Türkiye'nin varlık envanteri üzerinden politika önerilerine dönüştürmektedir.

Temel Bulgular

1. **Maliyet asimetrisi, caydırıcılığı tersine çevirdi.** Birkaç on bin dolarlık menzili genişletilmiş bir insansız hava aracı, milyar dolarlık bir atmosferik distilasyon ünitesini aylarca devre dışı bırakabilmektedir. Uluslararası Enerji Ajansı verilerine göre 2026 yılının ilk sekiz ayında Rusya'da ortalama her üç günde bir rafineri başarıyla vurulmuş; Haziran 2026'da Rus rafineri işlem hacmi yirmi yılın en düşük seviyesine gerilemiştir. Savunan taraf, saldıran tarafa kıyasla her engellemede yüz ila bin kat daha fazla harcamak zorundadır. Bu oran sürdürülebilir değildir.
2. **Coğrafi derinlik artık koruma sağlamıyor.** Ukrayna'nın 2026 boyunca ulaştığı menzil, Sibirya'daki Omsk rafinerisine kadar uzanmıştır. Ağustos 2026 sonu itibarıyla Rusya'nın büyük rafinerilerinden yalnızca beşi hiç vurulmamış durumdaydı ve bunların tümü Ukrayna sınırından 3.500 ila 6.500 kilometre uzaklıktaki Doğu Sibirya ve Uzak Doğu'da yer almaktaydı. Benzer biçimde Suudi Arabistan'ın Doğu-Batı Boru Hattı, Eylül 2026'da Irak topraklarından kalkan insansız hava araçlarıyla Riyad ve Medine bölgelerinde vurulmuştur.
3. **Tek bir varlık artık küresel piyasayı hareket ettiriyor.** Hürmüz Boğazı'nın 2026 savaşı boyunca fiilen kapanmasının ardından Suudi Arabistan, günde yaklaşık beş milyon varili Doğu-Batı hattı üzerinden Yanbu'ya yönlendirmişti. Bu hattın 10-11 Eylül 2026 saldırılarının ardından kapatılması, Brent fiyatını kısa sürede 110 dolar bandına taşımıştır. Yedek güzergâh, birincil güzergâh kadar kırılgan hale gelmiştir.
4. **Devlet dışı aktörler devlet ölçeğinde etki üretiyor.** Husilerin Kızıldeniz kıyı şeridi ve Mayyun (Perim) adası üzerindeki kontrolü, Bab-el Mendeb üzerinden yapılan tahliyeyi de tehdit altına sokmuş; böylece Suudi Arabistan'ın hem doğu hem batı çıkışları eşzamanlı olarak baskılanmıştır. Bu, 2019 Abkaik-Hureys saldırısından farklı olarak, tek atımlık bir şok değil, sürdürülen bir kuşatma niteliğindedir.
5. **Siber katman, fiziksel saldırının hazırlık aşaması haline geldi.** Aralık 2025'te Polonya'nın enerji sektöründe yenilenebilir üretim tesisleri ve bir kojenerasyon santralinin internete açık uç cihazlar üzerinden ele geçirilerek uzaktan terminal birimlerinin silici (wiper) yazılımla tahrip edilmesi, siber saldırının artık veri hırsızlığı değil donanım imhası anlamına geldiğini göstermiştir. Sektör analistleri, 2026 itibarıyla küresel enerji ve kamu hizmetleri altyapısının üçte birinden fazlasında sessiz erişim, veri toplama ve operasyonel haritalama biçiminde önceden konumlanma faaliyeti bulunduğunu değerlendirmektedir.

6. **Deniz altı sistemler hukuki bir boşlukta savunmasız kalmaktadır.** Ekim 2023'ten 2025 sonuna kadar yalnızca Baltık havzasında en az on bir deniz altı kablosu hasar görmüş veya kesilmiştir. Küresel ölçekte bir kablo arızasının ortalama onarım süresi kırk gün civarındadır. Çapa sürükleme yöntemi, kasıt ile ihmal arasındaki ayrımı ispat edilemez kıldığı için klasik caydırıcılık mekanizmalarını işlevsiz bırakmaktadır.
7. **Onarım kapasitesi, yeni savunma hattıdır.** Rusya örneğinde asıl belirleyici olan, tek bir saldırının verdiği hasar değil, ardışık dalgaların onarım döngüsünden daha hızlı gelmesidir. Yüksek gerilim güç transformatörlerinde teslim süresi iki ila dört yıla ulaşmışken, bir rafineri distilasyon kolonunun özel alaşımlı iç aksamı için bekleme süresi aylarla ölçülmektedir. Stok tutmayan bir enerji sistemi, savunulamaz bir enerji sistemidir.
8. **İklim değişikliği, failsiz bir saldırı kampanyası gibi davranmaya başlamıştır.** 2026 yazında Tuna Nehri'ndeki rekor düşük su seviyesi, Macaristan'ın elektrik üretiminin yarısını karşılayan Paks Nükleer Santrali'ni kapasitesinin onda birine indirmiş, Romanya'nın tek nükleer tesisi Cernavodă'yı ordunun müdahale girişimlerine rağmen tamamen durdurmuş; aynı dönemde Avrupa'nın hidroelektrik üretimi on yılın en düşük seviyesine gerilemiştir. Kasıtlı bir failin bulunmaması, sonucun eşzamanlılık ve tekrarlanma bakımından bir saldırı kampanyasından ayırt edilemez olmasını değiştirmemektedir.

Türkiye Açısından Ana Sonuç

Türkiye, bu raporda geliştirilen indekste 100 üzerinden **66** puanla "yüksek-orta" risk bandında konumlanmaktadır. Bu puan, ülkenin kendi topraklarında yaşanan bir çatışmadan değil, üç ayrı kırılganlık kümesinin üst üste binmesinden kaynaklanmaktadır: birincisi, transit ülke konumunun Türkiye'yi başkalarının savaşlarının hedef kümesine dâhil etmesi; ikincisi, enerji arzında yüksek ithalat bağımlılığı ile birlikte giriş noktalarının sayıca sınırlı olması; üçüncüsü ise elektrik sisteminin Avrupa şebekesiyle senkron çalışmasına rağmen fiilen sınırlı ithalat-ihracat kapasitesine sahip, ada benzeri bir davranış sergilemesidir. TürkAkım ve Mavi Akım'ı besleyen Russkaya kompresör istasyonuna 2025 ve 2026 boyunca tekrarlanan insansız hava aracı saldırıları, Türkiye'nin arz güvenliğinin artık yalnızca kendi sınırları içindeki tedbirlerle sağlanamayacağını göstermiştir.

Rapor, Türkiye için kısa, orta ve uzun vadeye yayılan yirmi bir maddelik bir politika seti önermektedir. Bunların merkezinde, kritik enerji altyapısını tanımlayan ve koruma yükümlülüklerini operatörler ile devlet arasında paylaştıran müstakil bir çerçeve mevzuatın kabulü; Ceyhan, Aliağa, İzmit ve Kıyıköy gibi yoğunlaşma noktalarında katmanlı insansız hava aracı savunmasının kurulması; ulusal bir kritik yedek parça stok rejiminin oluşturulması; ve denizaltı boru hattı, enterkonektör ile veri kablolarının izlenmesi için Deniz Kuvvetleri, BOTAŞ, TEİAŞ ve özel operatörleri kapsayan ortak bir deniz tabanı farkındalık merkezinin kurulması yer almaktadır.

1. GİRİŞ: BİR İTİRAFIN ANATOMİSİ

1.1. Putin'in Sözleri ve Sözlerin Ötesi

Siyasal liderlerin açıklamaları, çoğu zaman söyledikleri kadar söylemek zorunda kaldıkları için de anlamlıdır. Haziran 2026'da Rus devlet televizyonuna konuşan Vladimir Putin, kritik altyapıya ve özellikle enerji tesislerine yönelik saldırıların ülkedeki üretim tesislerinde sorunlara yol açtığını, o an itibarıyla belirli bir arz açığı bulunduğunu, ancak durumun kritik olmadığını ifade etti. Aynı değerlendirmede, bakım çalışmalarının hızlandırılması, gerekli ithalat hacminin sağlanması ve tesislerin güvenilir biçimde korunması gerektiğini sıraladı. Birkaç hafta sonra Moskova'da enerji şirketleri yöneticileriyle yaptığı toplantıda ise altyapı tesislerine yönelik saldırıların etkisinin asgariye indirilmesi gerektiğini söyledi.

Bu cümlelerin diplomatik dili, altındaki gerçeği tam olarak örtemiyor. Dünyanın en büyük hidrokarbon ihracatçılarından biri, kendi toprakları üzerindeki rafineri ağını koruyamadığını kabul etmekte; yakıt ithalatını gündeme almakta; ve yaklaşık yirmi bölgede akaryakıt satışına kısıtlama getirmek zorunda kalmaktadır. Enerji ihraç eden bir devletin, kendi iç pazarında benzin tayınlamasına gitmesi, enerji güvenliği literatüründe yerleşik olan üretici-tüketici kırılganlık hiyerarşisini tersine çevirmektedir.

Rakamlar, söylemin arkasındaki gerçekliği daha açık biçimde ortaya koyuyor. Uluslararası Enerji Ajansı'nın Eylül 2026 tarihli değerlendirmesine göre, Rusya'nın otuz iki büyük rafinerisi ve günlük yaklaşık 6,5 milyon varillik kurulu işleme kapasitesi bulunmaktadır; bu haliyle ülke tarihsel olarak Amerika Birleşik Devletleri ve Çin'in ardından dünyanın üçüncü büyük rafine ürün üreticisidir. Ancak Haziran 2026'da rafineri işlem hacmi günlük 3,8 milyon varile inmiş, bu seviye yirmi yılı aşkın sürenin en düşüğü olmuş ve bir önceki yıla göre yaklaşık yüzde otuzluk bir daralmaya işaret etmiştir. Benzin üretimi yüzde yirmi, dizel üretimi ise yaklaşık yüzde otuz azalmış, hükümet iç piyasayı korumak için ihracat kısıtlamalarına gitmiştir.

Eylül 2026'ya gelindiğinde tablo daha da ağırlaşmıştır. Rusya'nın altı büyük dizel üreticisi rafinerisinden yarısı ya tamamen durmuş ya da nominal kapasitesinin dörtte biri seviyesine inmiştir. Kirişi tesisi tamamen devre dışı kalmış, Volgograd ve NORSİ yaklaşık çeyrek kapasiteyle çalışır hale gelmiş, Taneco ise yeni bir saldırının hedefi olmuştur. Leningrad bölgesinde akaryakıt istasyonlarında miktar sınırlaması uygulanmaya başlanmıştır.

1.2. Raporun Sorusu ve Katkı İddiası

Bu rapor, tekil bir çatışmanın muhasebesini yapmayı değil, o çatışmanın açığa çıkardığı yapısal dönüşümü kavramsallaştırmayı amaçlamaktadır. Merkezî soru şudur: Kritik enerji altyapısının korunmasına ilişkin yerleşik varsayımlar hangi noktalarda geçersizleşmiştir ve bu geçersizleşme, devletler ile operatörler için hangi yeni yükümlülükleri doğurmaktadır?

Soruya yanıt ararken rapor dört düzeyde ilerlemektedir. İkinci bölüm, enerji güvenliği kavramının kuramsal seyrini izleyerek "altyapı güvenliği" boyutunun neden ayrı bir analiz kategorisi haline geldiğini tartışmaktadır. Üçüncü bölüm, Rusya, Ukrayna, Suudi Arabistan, İran, Körfez ülkeleri, Baltık havzası ve Latin Amerika örneklerinden oluşan karşılaştırmalı bir vaka külliyatı sunmaktadır. Dördüncü ve beşinci bölümler, paradigma değişimini on kırılma başlığı altında sistematize etmekte ve altyapı türlerine göre ayrıştırılmış bir koruma mimarisi önermektedir. Altıncı ve yedinci bölümler siber tehditler ile deniz altı sistemleri ayrı ayrı derinleştirmektedir. Sekizinci bölüm, bölge ve varlık türü bazında özgün bir risk indeksi geliştirmekte; dokuzuncu bölüm bulguları Türkiye'ye uyarlamaktadır.

Raporun özgün katkısı üç noktada toplanmaktadır. Birincisi, enerji altyapısı güvenliğini tek bir tehdit vektörü (terör, siber veya askerî) üzerinden değil, vektörlerin bileşimi üzerinden ele alan bütünleşik bir

çerçeve önermesidir. İkincisi, koruma önerilerini genel ilkeler düzeyinde bırakmayıp altyapı türüne göre farklılaştırmasıdır; bir rafineri ile bir denizaltı enterkonektörünün kırılganlık profilleri arasındaki fark, koruma yatırımının dağılımını doğrudan belirlemektedir. Üçüncüsü ise, niteliksel değerlendirmeleri karşılaştırılabilir bir skorlama sistemine dönüştüren TESPAM-KEAGİ indeksidir.

1.3. Yöntem ve Sınırlar

Rapor, nitel vaka analizi ile çok ölçütlü karar analizi tekniklerini birleştiren karma bir yöntem izlemektedir. Vaka seçiminde, 2019-2026 arasında enerji altyapısının doğrudan hedef alındığı, kamuya açık kaynaklarla doğrulanabilen ve piyasa etkisi ölçülebilen olaylar esas alınmıştır. İndeks bileşenlerinin ağırlıklandırılmasında uzman değerlendirmesi kullanılmış; her bileşen için kullanılan göstergeler sekizinci bölümde açıkça tanımlanmıştır.

Yöntemin üç sınırı baştan kabul edilmelidir. Birincisi, aktif çatışma bölgelerinde hasar tespiti doğası gereği belirsizdir; taraflar hem abartma hem de gizleme yönünde güdülere sahiptir. Uydu görüntüleri ve termal anomali verileri bu belirsizliği azaltmakta, ancak ortadan kaldırmamaktadır. İkincisi, siber olaylarda raporlanmama eğilimi yüksektir; kamuya yansıyan vakalar buzdağının görünen kısmıdır. Üçüncüsü, indeks skorları mutlak olasılık tahminleri değil, göreli konumlandırma araçlarıdır; amaç, kaynak tahsisinde önceliklendirmeye yardımcı olmaktır.

2. KAVRAMSAL ÇERÇEVE: ENERJİ GÜVENLİĞİNDEN ALTYAPI GÜVENLİĞİNE

2.1. Kavramın Tarihsel Seyri

Modern enerji güvenliği kavramı, Birinci Dünya Savaşı öncesinde Winston Churchill'in Kraliyet Donanması'nı kömürden petrole geçirme kararıyla birlikte doğdu. O tarihte güvenlik, esas olarak arz kaynağının çeşitlendirilmesi anlamına geliyordu. 1973 petrol ambargosu, kavramı devlet politikası düzeyine taşıdı ve Uluslararası Enerji Ajansı ile stratejik petrol rezervi sistemini doğurdu. Bu dönemde enerji güvenliği, temel olarak bir arz kesintisi riskine karşı sigortalanma problemiydi.

1990'lar ve 2000'ler, kavramı genişletti. Asya Pasifik Enerji Araştırma Merkezi tarafından formüle edilen ve literatürde yaygın kabul gören dört boyutlu çerçeve — bulunabilirlik, erişilebilirlik, karşılanabilirlik ve kabul edilebilirlik — enerji güvenliğini jeolojik, jeopolitik, ekonomik ve çevresel eksenlerde tanımladı. Cherp ve Jewell'in çalışmaları, kavramı hayati enerji sistemlerinin kırılganlıklarından korunması olarak yeniden formüle ederek, analizi kaynak eksenli olmaktan çıkarıp sistem eksenli hale getirdi.

Bu literatürün tamamında örtük bir varsayım bulunmaktaydı: Altyapının kendisi verili ve büyük ölçüde güvenliydi. Riskin kaynağı, kaynağa erişim (ambargo, siyasi kesinti), fiyat (piyasa şoku) veya teknik yetersizlikti. Tesislerin fiziksel bütünlüğü, uluslararası hukuk, karşılıklı caydırıcılık ve pratik erişilemezlik tarafından korunuyordu. Enerji tesislerine yönelik saldırılar istisna niteliğindeydi ve çoğunlukla iç çatışma bağlamında, sınırlı ölçekte gerçekleşiyordu: Kolombiya'da Caño Limón-Coveñas hattına yönelik onlarca yıllık sabotaj kampanyası, Nijer Deltası'nda boru hattı kaçakçılığı ve tahribatı, Irak'ta Kerkük-Yumurtalık hattının kesintiye uğratılması bu kategoride değerlendirilebilir.

2.2. Beşinci Boyut: Savunulabilirlik

2026 itibarıyla ortaya çıkan tablo, dört boyutlu çerçeveye beşinci bir boyutun eklenmesini zorunlu kılmaktadır: **savunulabilirlik (defensibility)**. Bu boyut, bir enerji sisteminin kasıtlı ve tekrarlanan saldırılar karşısında işlevini sürdürebilme kapasitesini ifade eder ve dört alt bileşeni bulunur:

- **Fiziksel dayanıklılık:** Tesisin, belirli büyüklükteki bir kinetik etkiye karşı yapısal direnci; kritik ekipmanın korunaklı konumlandırılması; yedeklilik seviyesi.
- **Tespit ve müdahale:** Yaklaşan tehdidin yeterli erken uyarı süresiyle algılanması ve etkisiz hâle getirilmesi kapasitesi.
- **Onarım hızı:** Hasar sonrası işlevi yeniden tesis etme süresi; kritik yedek parça stoku; nitelikli personel ve mühendislik kapasitesi.
- **Sistemik ikame edilebilirlik:** Varlık devre dışı kaldığında, işlevinin başka bir varlık, güzergâh veya kaynak tarafından ne ölçüde ve ne hızda üstlenilebileceği.

Savunulabilirlik boyutu, geleneksel enerji güvenliği ölçütleriyle ters yönde hareket edebilir. Ölçek ekonomisi, birim maliyeti düşürmek için üretimi az sayıda büyük tesiste yoğunlaştırır; bu, karşılanabilirlik açısından olumlu, savunulabilirlik açısından olumsuzdur. Benzer biçimde, dijitalleşme ve uzaktan izleme operasyonel verimliliği artırırken saldırı yüzeyini genişletir. Bu gerilim, teknik bir optimizasyon sorunu değil, açık biçimde siyasal bir tercih meselesidir ve bu raporun ileriki bölümlerinde defalarca karşımıza çıkacaktır.

2.3. Caydırıcılık Kuramının Enerji Altyapısına Uygulanamazlığı

Soğuk Savaş dönemi caydırıcılık kuramı üç önkoşula dayanır: saldırganın kimliğinin belirlenebilmesi (atfedilebilirlik), misillemenin inandırıcı olması (kabiliyet) ve misillemenin maliyetinin saldırının getirisini

aşması (orantı). Enerji altyapısına yönelik çağdaş saldırılar, bu üç önkoşulun her birini ayrı ayrı zayıflatmaktadır.

Atfedilebilirlik sorunu en belirgin olanıdır. Eylül 2026'da Suudi Arabistan'ın Doğu-Batı hattına yönelik saldırılarda hiçbir grup sorumluluk üstlenmemiş; Amerikan yönetimi Irak'taki İran destekli grupları işaret etmiş, İran Dışişleri Bakanlığı bu suçlamayı kesin biçimde reddetmiştir. Benzer biçimde Baltık'taki kablo kesintilerinde çapa sürükleme yöntemi, kasıt ile denizcilik ihmali arasındaki hukuki ayrımı ispat edilemez kılmaktadır. Bir fiilin kime ait olduğu kanıtlanamıyorsa, misillemenin meşruiyeti de kurulamaz.

Orantı sorunu daha derindir. Bir devletin, kendi rafinerisini vuran tarafa karşı misilleme yapabilmesi için hedef olarak kullanabileceği eşdeğer bir varlık gerekir. Ukrayna gibi rafineri kapasitesi savaş öncesinde zaten büyük ölçüde tahrip edilmiş bir ülkeye karşı, rafineri hedefli misilleme anlamlı bir maliyet yaratmaz. Asimetrik envanter, karşılıklı caydırıcılığı tek yönlü hâle getirir.

2.4. Hibrit Savaş ve Gri Bölge Ekseni

Enerji altyapısına yönelik saldırıların önemli bir bölümü, savaş ile barış arasındaki gri bölgede gerçekleşmektedir. Bu alanın tanımlayıcı özelliği, fiilin Birleşmiş Milletler Antlaşması'nın 51. maddesi anlamında silahlı saldırı eşiğine bilinçli olarak yaklaşmaması ancak stratejik etki üretmesidir. Nord Stream boru hatlarının Eylül 2022'de tahrip edilmesi, Balticconnector doğal gaz hattı ile ona paralel iletişim kablolarının Ekim 2023'te hasar görmesi, Estlink 2 elektrik enterkonektörünün Aralık 2024'te kesilmesi bu kategorinin tipik örnekleridir.

Gri bölge faaliyetlerinin enerji altyapısını tercih etmesinin nedeni tesadüfi değildir. Bu varlıklar, üç özelliği bir arada taşır: stratejik etkileri yüksektir, ekonomik maliyetleri ölçülebilirdir ve sivil-askerî ayrımı belirsizdir. Bir elektrik enterkonektörünün kesilmesi, doğrudan can kaybına yol açmadığı için askerî yanıtı meşrulaştırmaz; ancak hedef ülkenin arz maliyetini ve siyasi manevra alanını daraltır. Bu, düşük maliyetli baskı aracı olarak son derece verimli bir tercihtir.

2.5. Türkiye Literatüründen Bir Çıkış Noktası

Enerji güvenliğinin sayısallaştırılabilir, karşılaştırılabilir bir çerçeveye oturtulması ihtiyacı, Türkiye literatüründe de bir karşılığa sahiptir. Akyener, enerji güvenliği tanımlarının çoğunlukla yazarların kendi mesleki disiplinini merkeze alan, birbirini tekrar eden bir örüntü izlediğini tespit ederek, makro düzey analiz, enerji türlerine göre süreç analizi, dolaylı etmen analizi ve proje bazlı analizden oluşan dört basamaklı, matematiksel temelli bir enerji güvenliği modeli önermiş; bu modeli örnek uygulama olarak Türkiye'ye uyarlamıştır (Akyener, t.y.). Söz konusu çalışma, yazarın kendi ifadesiyle, ithalatçı veya ihracatçı ayrımı gözetmeksizin bütün ülke ve bölgelere uygulanabilecek, uluslararası literatürde ilk bütünsel enerji güvenliği modeli olma iddiasını taşımaktadır.

Bu raporda geliştirilen TESPAM-KEAGİ indeksi, doğrudan bir devamı olmasa da, aynı yöntemsel sezgiyi paylaşmaktadır: enerji güvenliğinin nitel bir kanaat meselesi olarak bırakılmaması, bileşenlerine ayrıştırılıp ağırlıklandırılarak karşılaştırılabilir bir puana dönüştürülmesi gerektiği kanaati. Aradaki fark, odak noktasındadır. Akyener'in modeli enerji güvenliğinin bütününü — kaynak çeşitliliğinden ekonomik erişilebilirliğe kadar — kapsayacak biçimde tasarlanmışken, KEAGİ kasıtlı olarak dar bir kesite, ikinci bölümde tanımlanan savunulabilirlik boyutuna odaklanmakta ve bu boyutu bölge ile altyapı türü düzeyinde ayrıştırmaktadır. İki çalışma, enerji güvenliğinin farklı katmanlarında benzer bir sayısallaştırma mantığının işletilebileceğini göstermesi bakımından birbirini tamamlamaktadır.

3. AMPİRİK ZEMİN: KARŞILAŞTIRMALI VAKA ANALİZLERİ

3.1. Rusya: Sürdürülen Rafineri Kampanyası (2022-2026)

Rusya vakası, enerji altyapısına yönelik modern saldırı kampanyalarının en kapsamlı ve en uzun soluklu örneğidir. Ukrayna, 2022'deki tam ölçekli işgalin ardından Rus petrol altyapısını hedef almaya başlamış; ancak kampanyanın ölçeği, menzili ve etkinliği 2025-2026 döneminde niteliksel bir sıçrama yaşamıştır.

Kampanyanın stratejik mantığı üç katmanlıdır. Birinci katman, savaş finansmanının daraltılmasıdır: rafine ürün ihracatı, Rus bütçesinin önemli bir kalemidir. İkinci katman, askerî lojistiğin baskılanmasıdır; dizel, hem sivil ekonominin hem de cephe ikmalinin ortak yakıtıdır. Üçüncü katman ise toplumsal algı üzerinde baskı kurmaktır; benzin istasyonlarındaki kuyruklar, cephedeki gelişmelerden çok daha görünür bir savaş maliyeti üretir.

Uygulamadaki dönüşüm, üç teknik gelişmeye dayanmaktadır. Birincisi menzildir: 7 Temmuz 2026'da Gazprom Neft'in günlük 450 bin varil kapasiteli Omsk rafinerisinin vurulması, kampanyanın Sibirya derinliklerine ulaştığını göstermiştir. İkincisi doygunluk taktiğidir: tek bir tesise çoklu insansız hava aracı dalgaları gönderilerek koruyucu ağlar ve nokta hava savunması aşılmaktadır. Üçüncüsü hedefleme hassasiyetidir; saldırılar, tesisin herhangi bir noktasına değil, atmosferik distilasyon üniteleri gibi darboğaz ekipmanlara yönelmektedir. Rosneft'e ait Sizran rafinerisinde günlük 17.100 ton kapasiteli ve tesisin toplam kapasitesinin yaklaşık yüzde yetmiş birini oluşturan ana distilasyon ünitesinin hasar görmesi, onarımın en az bir ay süreceği değerlendirmesine yol açmıştır.

Tablo 3.1. Rusya Rafineri Kampanyasının Sayısal Görünümü (2026)

Gösterge	Savaş Öncesi / Referans	2026 Durumu	Değişim
Büyük rafineri sayısı	32	32 (5'i hiç vurulmamış)	—
Kurulu işleme kapasitesi	~6,5 milyon v/g	~6,5 milyon v/g (nominal)	—
Fiili işleme hacmi	~5,4 milyon v/g	3,8 milyon v/g (Haziran)	−%30
Benzin üretimi	Referans (2025)	2025 seviyesinin altında	−%20
Dizel üretimi	Referans (2025)	2025 seviyesinin altında	−%30 (yaklaşık)
Başarılı saldırı sıklığı	Seyrek	Ortalama 3 günde bir	—
Yurt içi benzin karşılama oranı	%100+	~%70 (yaz, ithalatsız)	−%30
UEA öngörüsü (2026-27 ort.)	—	~4,0 milyon v/g	Düşük taban

Kaynak: Uluslararası Enerji Ajansı değerlendirmeleri (Eylül 2026), Reuters piyasa analizleri ve kamuya açık sektör raporlarından TESPAM derlemesi. "v/g": varil/gün.

Kampanyanın en öğretici yönü, Rusya'nın aldığı karşı tedbirlerin sınırlılığıdır. Koruyucu metal ağlar, hendekler ve nokta hava savunma sistemleri, tekil saldırılara karşı etkili olmakta, ancak çoklu dalgalar karşısında doygunluğa ulaşmaktadır. Devlet, bakım sürelerini kısaltmış, planlı bakımları ertelemiş, orta ve küçük ölçekli işletmeleri üretime dâhil etmiş ve yakıt kalite standartlarını gevşetmiştir. Bu tedbirlerin tamamı, sistemi kısa vadede ayakta tutarken orta vadeli güvenilirlik riskini artırmaktadır: ertelenmiş bakım, gelecekteki arıza olasılığını yükseltir.

Coğrafi dağılım da kritiktir. Ağustos 2026 sonu itibarıyla hiç vurulmamış beş büyük rafinerinin tamamının Doğu Sibirya ve Uzak Doğu'da, Ukrayna sınırından 3.500 ila 6.500 kilometre uzaklıkta bulunması, coğrafi derinliğin hâlâ bir koruma sağladığını; ancak bu korumanın eşiğinin sürekli yükseldiğini göstermektedir. Menzil teknolojisindeki her ilerleme, bu güvenli bölgeyi daraltmaktadır.

3.2. Ukrayna: Şebeke Savaşının Laboratuvarı

Madalyonun diğer yüzünde, Rusya'nın Ukrayna elektrik sistemine yönelik kampanyası yer almaktadır. Putin, 2026 yazındaki açıklamalarında Rus ordusuna Ukrayna'nın enerji altyapısına yönelik yoğun saldırılar düzenleme talimatı verdiğini açıkça ifade etmiş ve bunu karşılıklılık çerçevesinde gerekçelendirmiştir.

Ukrayna vakası, elektrik sistemlerinin petrol sistemlerinden farklı bir kırılganlık profiline sahip olduğunu göstermektedir. Petrol zincirinde stok tutulabilir ve kesinti tamponlanabilirken, elektrik sisteminde üretim ile tüketim eşzamanlı olmak zorundadır. Bu nedenle elektrik altyapısına yönelik saldırıların etkisi anında hissedilir. Ayrıca sistem, yüksek gerilim güç transformatörleri gibi az sayıda, yüksek maliyetli ve uzun tedarik süreli bileşenlere bağımlıdır. Bir transformatörün tahrip edilmesi, aylar hatta yıllar süren bir yeniden tedarik süreci anlamına gelir.

Ukrayna'nın geliştirdiği yanıt stratejisi, savunma literatürüne kalıcı bir katkı sunmaktadır. Bu strateji dört unsura dayanmaktadır: kritik trafo merkezlerinin beton koruma yapılarıyla çevrelenmesi; dağıtık kojenerasyon ve küçük ölçekli üretim birimleriyle merkezî üretime olan bağımlılığın azaltılması; komşu ülkelerle senkron bağlantı üzerinden acil ithalat kapasitesinin artırılması; ve planlı kesinti programlarıyla talebin yönetilerek sistem çöküşünün önlenmesi. Bu modelin, benzer tehdide maruz kalabilecek diğer ülkeler açısından doğrudan aktarılabilir bir değeri vardır.

Vakanın bir diğer boyutu, siber ve kinetik saldırıların eşgüdümlü kullanımıdır. Ukrayna elektrik şebekesi, 2015 ve 2016'da dünyada bilinen ilk siber kaynaklı elektrik kesintilerine sahne olmuştu. 2015'teki olayda kötücül yazılım, dağıtım şirketlerinin denetleyici kontrol sistemlerine sızarak kesicilerin uzaktan açılmasını sağlamış; 2016'daki ikinci olayda ise endüstriyel protokolleri doğrudan hedefleyen özel bir zararlı yazılım kullanılmıştır. Bu iki olay, siber saldırıların fiziksel dünyada ölçülebilir sonuçlar üretebileceğini kanıtlayan dönüm noktalarıdır.

3.3. Suudi Arabistan: Abkaik'ten Petroline'a

3.3.1. Abkaik-Hureys (Eylül 2019): Tek Atımlık Şok

14 Eylül 2019'da Suudi Aramco'nun Abkaik işleme tesisi ve Hureys sahasına yönelik insansız hava aracı ve seyir füzesi saldırısı, modern enerji altyapısı güvenliği tartışmasının başlangıç noktasıdır. Abkaik, dünyanın en büyük petrol istikrar kazandırma (stabilization) tesisiydi ve saldırı, Suudi üretiminin yaklaşık yarısını, yani küresel arzın yüzde beşe yakınını geçici olarak devre dışı bıraktı. Brent fiyatı, tek işlem gününde kaydedilen en sert yükselişlerden birini yaşadı.

Abkaik olayının dört dersi vardı. Birincisi, dünyanın en pahalı hava savunma sistemlerine sahip bir ülkenin, alçak irtifadan ve beklenmedik bir azimuttan gelen küçük hava araçlarına karşı savunmasız kalabileceğiydi. İkincisi, saldırının hedef seçiminde gösterdiği mühendislik bilgisiydi: küresel küreler (spheroids) ve istikrar kuleleri gibi darboğaz ekipmanlar isabetle vurulmuştu. Üçüncüsü, Suudi Arabistan'ın olağanüstü onarım kapasitesiydi; üretim, beklentilerin çok üzerinde bir hızla yeniden tesis edildi. Dördüncüsü ise, sorumluluğun Husiler tarafından üstlenilmesine rağmen saldırının menşeine ilişkin belirsizliğin sürmesiydi.

3.3.2. Doğu-Batı Boru Hattı (Eylül 2026): Yedek Güzergâhın Çöküşü

2026 vakası, 2019'dan niteliksel olarak farklıdır. Şubat 2026'da başlayan savaş boyunca Hürmüz Boğazı'nın büyük ölçüde kapanmasının ardından Suudi Arabistan, normalde Körfez üzerinden sevk edilen günde yaklaşık beş milyon varili, 1.200 kilometre uzunluğundaki Doğu-Batı Ham Petrol Boru Hattı (Petroline) üzerinden Kızıldeniz'deki Yanbu limanına yönlendirmişti. Aramco üst yönetimi, bu hattın arz kesintisinin hafifletilmesinde acil stok salımlarından daha büyük rol oynadığını ifade etmişti.

10 Eylül 2026 sabahı, Irak topraklarından kalkan insansız hava araçları, hattın Riyad ve Medine bölgelerinden geçen kesimlerini hedef aldı. Pompa istasyonlarında yangınlar çıktı, yaralanmalar meydana geldi ve Suudi Enerji Bakanlığı 11 Eylül'de hattı ihtiyaten kapattığını açıkladı. Uydu görüntüleri, Medine'nin güneydoğusundaki el-Mesbaa yakınlarındaki bir pompa istasyonunda geniş çaplı yangın hasarını doğruladı; Sentinel-3 görüntülerinde yaklaşık yüz kilometre uzunluğunda bir duman izi tespit edildi. Brent fiyatı kısa sürede 110 dolar seviyesine yükseldi ve mayıs ayından bu yana ilk kez yüz doların üzerinde kapandı.

Bu vakanın stratejik anlamı, hedef seçimindeki incelikte yatmaktadır. Saldırı, üretim sahalarını değil, yedek tahliye güzergâhını hedef almıştır. Birincil çıkışı (Hürmüz) zaten kapatılmış bir ülkenin ikincil çıkışının da devre dışı bırakılması, klasik anlamda "çeşitlendirme" stratejisinin sınırlarını göstermektedir. Üstelik Husilerin Yemen'in Kızıldeniz kıyı şeridi ve Mayyun adası üzerindeki kontrolü, Bab-el Mendeb üzerinden yapılacak tahliyeyi de riskli hale getirmiştir. Çeşitlendirme, ancak alternatif güzergâhların bağımsız risk profillerine sahip olması durumunda koruma sağlar; aynı aktör tarafından eşzamanlı olarak tehdit edilebilen güzergâhlar, gerçek anlamda çeşitlendirme oluşturmaz.

3.4. İran: Enerji Altyapısının Askerî Hedefe Dönüşmesi

İran vakası, enerji altyapısının doğrudan askerî kampanya hedefi haline gelmesinin en açık örneğidir. Haziran 2025'teki çatışmada Güney Pars sahasının 14. fazına ait kara tesisleri ile Buşehr'deki Fecr-i Cem gaz işleme tesisi insansız hava araçlarıyla vurulmuş; Tahran'ın Şahran ve Rey bölgelerindeki akaryakıt depoları yangınlara sahne olmuştu. İran ise misilleme olarak Hayfa rafinerisini hedef almış, bu da İsrail'in enerji altyapısına yönelik ilk doğrudan saldırı olarak kayıtlara geçmişti.

Şubat 2026'da başlayan daha geniş ölçekli savaşta, enerji altyapısı kampanyanın merkezine yerleşti. 7 Mart 2026'da Tahran ve Karac'daki yakıt depolama tesisleri ve enerji kompleksleri vuruldu; Tahran rafinerisinin yanı sıra Ağdasiye, Şahran ve Karac depoları sistematik biçimde hedef alındı. 18 Mart 2026'da ise dünyanın en büyük doğal gaz sahası olan Güney Pars ile Aselluye rafinerisine yönelik saldırı gerçekleştirildi. Bu saldırı, İran'ın toplam gaz üretiminin yaklaşık yüzde on ikisini etkiledi, iki rafineride üretimi durdurdu ve İran'ın Irak'a gaz sevkiyatını kesmesine yol açtı.

Güney Pars vakası, jeolojik ortaklığın yarattığı özgün bir risk kategorisini gündeme getirmektedir. Saha, İran ile Katar arasında paylaşılmaktadır; Katar tarafında Kuzey Kubbe (North Dome) olarak adlandırılır. Ortak rezervuarlara yapılan saldırılar, hedef alınmayan tarafın üretimini de dolaylı biçimde riske atabilir; basınç yönetimi, rezervuar bütünlüğü ve çevresel etkiler sınır tanımaz. Bu, ortak saha işletmeciliğinin jeopolitik risk profiline eklenmesi gereken yeni bir boyuttur.

İran vakasının bir diğer boyutu, enerji altyapısına yönelik saldırıların insani ve çevresel sonuçlarıdır. İran Çevre Örgütü yetkilileri, akaryakıt depolarının sistematik biçimde imha edilmesini çevre kırımı olarak nitelendirmiş; Şahran bölgesinde işlenmemiş petrolün sokaklara aktığı bildirilmiştir. Enerji altyapısı saldırılarının hukuki statüsü, uluslararası insancıl hukuk açısından tartışmalıdır: bu tesisler çoğunlukla çift kullanımlı (dual-use) varlıklardır ve hem askerî hem sivil işlev görürler. Orantılılık ilkesinin bu tür hedeflere uygulanması, çağdaş savaş hukukunun çözülmemiş sorunlarından biridir.

3.5. Körfez: Zincirleme Mücbir Sebep İlanları

2026 savaşının belki de en çarpıcı boyutu, çatışmanın taraf olmayan ülkelerin enerji altyapısına yayılmasıdır. İran'ın misilleme stratejisi, Körfez İşbirliği Konseyi ülkelerinin enerji tesislerini, limanlarını ve sanayi bölgelerini kapsayacak biçimde genişlemiştir.

Tablo 3.2. 2026 Savaşında Hasar Gören Başlıca Körfez Enerji Varlıkları

Ülke	Tesis	Kapasite / Nitelik	Etki
Suudi Arabistan	Ras Tanura	550 bin v/g ham işleme	Geçici durdurma, yeniden devrede
Suudi Arabistan	Satorp (Cubeyl)	460 bin v/g rafineri	Üniteler durduruldu (7-8 Nisan)
Suudi Arabistan	Riyad rafinerisi	120 bin v/g	İhracata doğrudan etki
Suudi Arabistan	Samref (Yanbu)	Ortak mülkiyet rafinerisi	İHA isabeti
Suudi Arabistan	Doğu-Batı hattı	1.200 km, ~5 mn v/g akış	Kapatma (11 Eylül)
Katar	Ras Laffan	LNG kompleksi	Yangınlar, geniş hasar; mücbir sebep
Bahreyn	Bapco (El-Maameer)	400 bin v/g tek rafineri	Yangın; grup çapında mücbir sebep
Bahreyn	GPIC petrokimya	Gübre/metanol	Ünitelerde yangın (5 Nisan)
Kuveyt	Mina el-Ahmedi	Rafineri	Tekrarlanan saldırı, ünite durdurma
Kuveyt	Mina Abdullah	Rafineri	Yangın (19 Mart)
BAE	Habşan	Gaz işleme	Düşen enkaz hasarı; yeniden devrede
BAE	Fucayre Limanı	Bunker/ihraç terminali	Balistik füze saldırısı
Umman	Mina el-Fahal	Ham petrol ihraç terminali	İhtiyaten kapatma, 12 Mart'ta açılış
Umman	Selale	Terminal	Askıya alma, sonra yeniden devrede

Kaynak: Bloomberg, Reuters, ACLED Orta Doğu değerlendirmeleri ve şirket açıklamalarından TESPAM derlemesi (Mart-Eylül 2026). Liste, kamuya yansıyan olaylarla sınırlıdır ve kapsamlı değildir.

ACLED verilerine göre savaşın başlangıcından itibaren İran'ın misilleme saldırıları hiçbir Körfez ülkesini dışarıda bırakmamış; Amerikan tesisleri, enerji altyapısı, limanlar, havalimanları ve yerleşim alanlarını kapsayan altı yüz altmışı aşkın olay kaydedilmiş, en az kırk bir kişi hayatını kaybetmiştir. Birleşik Arap Emirlikleri en yoğun hedef alınan ülke olurken, Kuveyt en fazla can kaybının yaşandığı ülke olmuştur. Tahran ile yakın diplomatik kanalları koruyan Umman ise en az hedef alınan ülke olarak öne çıkmıştır.

Körfez vakası, üç yapısal dersi ortaya koymaktadır. Birincisi, enerji altyapısının coğrafi yoğunlaşmasının sistemik risk ürettiğidir: Bahreyn gibi tek rafineriye sahip ülkelerde, o tesise yönelik tek bir isabet ülke çapında mücbir sebep ilanına yol açabilmektedir. İkincisi, mücbir sebep ilanlarının zincirleme etkisidir; Katar, Kuveyt ve Bahreyn'in ardışık ilanları, uzun vadeli tedarik sözleşmelerinin güvenilirliğine dair küresel bir soru işareti doğurmuştur. Üçüncüsü ise sigortalanabilirlik krizidir: savaş riski primlerinin fırlaması, altyapı yatırımlarının finansal fizibilitesini doğrudan etkilemektedir.

3.6. Hürmüz ve Bab-el Mendeb: Boğazların Silahlandırılması

2026 savaşı, deniz geçiş noktalarının enerji güvenliğindeki merkezî rolünü yeniden hatırlatmıştır. Hürmüz Boğazı, dünya petrol ticaretinin yüzde yirmisinden fazlasının geçtiği dar bir su yoludur ve hem İran hem Umman karasularını kapsar. İran, savaş boyunca gemileri geleneksel seyir hatları yerine kendi karasularına yönlendirmeye çalışmış, talimatlara uymayan gemilere saldırmıştır.

Kriz, kesintili bir seyir izlemiştir. 7 Nisan 2026'da iki haftalık bir ateşkes üzerinde uzlaşılmış, ancak metin üzerinde mutabakat sağlanamamıştır. 13 Nisan'da Islamabad görüşmelerinin başarısızlığının ardından İran limanlarına ve bu limanlara giden gemilere yönelik bir abluka başlatılmış; bu abluka boyunca yüz kırkı aşkın gemi yönlendirilmiş, dokuz gemi etkisiz hâle getirilmiştir. Haziran 2026'da imzalanan mutabakat muhtırası kısa bir normalleşme umudu yaratmış, ancak Temmuz 2026'da İran kuvvetlerinin talimatlara uymayan ticari gemilere yönelik saldırılarıyla çatışma yeniden alevlenmiştir.

Fiyat hareketleri, boğaz risklerinin piyasaya yansıma biçimini göstermektedir. Savaşın başlangıcında Brent yüzde on ila on üç yükselerek 80-82 dolar bandına çıkmış, ateşkes beklentileriyle Mayıs 2026'da sert bir

düşüş yaşamış, Haziran ortasında 78 dolara kadar gerilemiş, ancak Ağustos'ta İran'ın yeni talepleriyle yeniden 84 dolar seviyesine tırmanmıştır. Eylül'deki Doğu-Batı hattı saldırısı ise fiyatı 108-110 dolar bandına taşımıştır. Bu dalgalanma profili, enerji piyasalarının artık arz-talep dengesinden çok altyapı bütünlüğü haberlerine tepki verdiğini göstermektedir.

Bab-el Mendeb cephesinde ise Husilerin Yemen'in Kızıldeniz kıyı şeridinde ve Mayyun adasında kontrol sağlaması, Süveyş üzerinden yapılan ticaretin güvenliğini yapısal olarak sorgulanır hâle getirmiştir. Hürmüz ve Bab-el Mendeb'in eşzamanlı baskı altında olması, Doğu-Batı hattının kapanmasıyla birleştiğinde, küresel ticaretin yaklaşık yüzde otuz dokuzunda ve sevkiyatların yüzde otuz birinde aksama yaratmıştır. Bu, modern enerji piyasaları tarihinde eşi görülmemiş bir eşzamanlı kesinti bileşimidir.

3.7. Baltık ve Kuzey Denizi: Deniz Tabanındaki Sessiz Cephe

Avrupa'nın kuzey denizleri, kinetik olmayan ancak stratejik etkisi yüksek bir saldırı biçiminin sahnesi hâline gelmiştir. Eylül 2022'de Nord Stream boru hatlarının tahrip edilmesi, bu dönemin başlangıç noktasıdır. Ekim 2023'te Finlandiya ile Estonya arasındaki Balticconnector doğal gaz boru hattının ve ona paralel iletişim kablolarının bir Çin bayraklı geminin çapasını deniz tabanında sürüklemesi sonucu hasar görmesi, yöntemin prototipini oluşturmuştur.

Kasım 2024'te iki iletişim kablosunun birbirine yakın zaman ve mekânda kesilmesi, Aralık 2024'te Estlink 2 elektrik enterkonektörünün dört telekomünikasyon hattıyla birlikte hasar görmesi ve Finlandiya'nın Rus petrolü taşıyan bir tankere el koyması, olayların bir örüntüye dönüştüğünü gösterdi. Ekim 2023 ile 2025 sonu arasında yalnızca Baltık havzasında en az on bir deniz altı kablosunun hasar gördüğü veya kesildiği tespit edilmiştir. 31 Aralık 2025'te Finlandiya özel kuvvetlerinin Fitburg adlı bir kargo gemisine çıkması, serinin en son halkalarından biri olmuştur.

Yanıt mekanizmaları da bu süreçte şekillenmiştir. NATO, Ocak 2025'te Baltic Sentry operasyonunu başlatmış; Birleşik Krallık öncülüğünde Nordic Warden girişimi devreye girmiştir. Avrupa Komisyonu, 5 Şubat 2026'da 347 milyon euroluk bir deniz altı altyapı girişimi ile bir Kablo Güvenliği Araç Kutusu açıklamıştır. Paketin içinde, Baltık için yirmi milyon euroluk bir hızlı onarım pilot projesi yer almakta; bölgesel limanlarda modüler onarım ekipmanının önceden konumlandırılması hedeflenmektedir. Ancak ekipmanın konuşlandırılması için hâlâ özel donanımlı gemiler gerekmektedir ve küresel ölçekte bir kablo arızasının medyan onarım süresi kırk gün civarındadır.

Tehdidin niteliği de derinleşmektedir. 2026 baharında Svalbard takımadaları yakınlarındaki Arktik sularda, müttefik donanmalarının Rus denizaltılarının kabloları parmak izi bırakmadan devre dışı bırakmaya yönelik bir sistemle talim yaptığını tespit etmesi, faaliyetin fırsatçı sabotajdan planlı kabiliyet geliştirmeye evrildiğini göstermektedir. Denizcilik istihbaratı şirketlerinin verileri, Rusya bağlantılı gemilerin deniz tabanı altyapısı üzerinde olağandışı seyir örüntüleri sergilediğini ortaya koymaktadır.

3.8. Siber Cephe: Polonya Olayından CyberAv3ngers'a

Aralık 2025'te Polonya enerji sektöründe gerçekleşen olay, siber tehdidin ulaştığı olgunluk seviyesini göstermektedir. CERT Polska'nın Ocak 2026'da yayımladığı ve Amerikan Siber Güvenlik ve Altyapı Güvenliği Ajansı'nın Şubat 2026'da duyurduğu rapora göre, saldırgan yenilenebilir enerji santrallerini, bir kombine ısı-güç santralini ve bir imalat şirketini hedef almış; internete açık uç cihazlar üzerinden ilk erişimi sağlamış; ardından silici yazılım yerleştirerek uzaktan terminal birimlerine fiziksel zarar vermiştir.

Bu olayın ayırt edici özelliği, saldırının amacının veri değil donanım olmasıdır. Silici yazılımların endüstriyel kontrol ortamlarında kullanılması, siber saldırının artık geri döndürülebilir bir kesinti değil, kalıcı ekipman kaybı anlamına gelebileceğini göstermektedir.

Nisan 2026'dan itibaren ise CyberAv3ngers olarak bilinen İran bağlantılı tehdit grubu, programlanabilir mantık denetleyicilerini hedef almaya başlamıştır. Bazı olaylarda grup, proje dosyalarını veya denetleyici yapılandırmalarını değiştirmiş; operatörlere insan-makine arayüzlerinde ve denetleyici kontrol sistemlerinde sunulan bilgiyi manipüle etmiştir. Bu son unsur özellikle tehlikelidir: operatörün gördüğü veriye güvenemediği bir sistemde, güvenli işletim kararı verilemez.

Sektörel istatistikler tablonun genişliğini göstermektedir. Verizon'ın 2026 veri ihlali araştırmasının kamu hizmetleri kesiti, altı yüz otuz sekiz olay ve beş yüz doksan yedi doğrulanmış veri ifşası kaydetmiş; sistem sızması, temel web uygulaması saldırıları ve sosyal mühendislik, kamu hizmeti ihlallerinin yüzde doksan dördünü oluşturmuştur. Endüstriyel siber güvenlik değerlendirmeleri, operasyonel teknoloji cihazlarının yaklaşık yüzde on ikisinin bilinen istismar edilebilir zafiyetler taşıdığını, yüzde yedisinin ise fidye yazılımı kampanyalarıyla ilişkilendirildiğini ortaya koymaktadır.

3.9. İklim Değişikliği Kaynaklı Üretim Güvenliği Krizi: 2026 Avrupa Yazı

Bu rapora kadar ele alınan vakaların ortak paydası, bir failin varlığıdır: bir devlet, bir vekil aktör, bir sabotajcı. Ancak 2026 yazında Avrupa'nın yaşadığı üretim krizi, enerji altyapısı güvenliğinin failsiz de bozulabileceğini göstermiştir. İklim değişikliğinin ürettiği aşırı sıcaklık ve kuraklık, kıtanın enerji sistemine, kasıtlı bir saldırı kampanyasıyla aynı imzayı taşıyan bir baskı uygulamıştır: eşzamanlı, coğrafi olarak dağınık ve tekrarlayan kapasite kayıpları.

Tuna Nehri boyunca su seviyeleri, ağustos başında mevsim normallerinin belirgin biçimde altına geriledi. Nehrin soğutma suyu sağladığı Macaristan'ın tek nükleer tesisi olan Paks Nükleer Güç Santrali — ülke elektrik üretiminin yaklaşık yüzde kırkını karşılamaktadır — su seviyesindeki düşüş nedeniyle reaktörlerini birer birer devre dışı bırakmak zorunda kaldı; iki bin megavatlık kurulu kapasite ağustos başında iki yüz kırk megavata, yani onda birinin altına indi. Başbakan Péter Magyar, tesisin dört reaktörünün tamamen kapatıldığını açıklayarak vatandaşlardan akşam saatlerinde tüketimi sınırlamalarını istedi; kapatma sürecinin birkaç hafta süreceği öngörülüyordu.

Komşu Romanya'da da tablo ağır seyretti. Ülkenin nükleer üretiminin merkezi olan Cernavodă Nükleer Güç Santrali'nin iki reaktörü, Tuna'daki su seviyesinin düşmesi üzerine devre dışı kaldı. Aynı dönemde Romanya, Tuna havzasında nehir akışını artırabilmek için yatak içindeki bir kaya kütlesini patlayıcıyla parçalama yoluna gitti — sivil bir su yönetimi tedbirinin, ancak bir savaş ekonomisinde görülebilecek türden bir mühendislik müdahalesine dönüştüğü bir andı. Su krizinin sanayiye yansıması da gecikmedi: ülkedeki iki otomobil fabrikası, üretimlerini 19 Ağustos'a kadar durdurduklarını açıkladı.

Kriz nükleer santrallerle sınırlı kalmadı. Enerji düşünce kuruluşu Ember'in derlediği verilere göre, Avrupa'da haziran ve temmuz aylarında sıcaklıklar birçok bölgede kırk dereceyi aştı; bu durum klima kullanımını ve elektrik talebini belirgin biçimde yükseltirken, kuraklık bazı üretim kaynaklarını aynı anda kısıtlayarak kıtanın elektrik sistemindeki kırılganlıkları açığa çıkardı. İtalya'da Po Nehri'ndeki düşük su seviyeleri termik santral kapasitesinin yaklaşık üçte birini etkilerken, Polonya'da nehir seviyelerindeki gerileme yaklaşık 1,3 gigavatlık kömür kapasitesinin devre dışı kalmasına yol açtı; İngiltere'de beş doğal gaz santralinin üretim kaybı 2,5 gigavatlık kapasiteyi devre dışı bıraktı. Kuraklık, hidroelektrik santrallerdeki üretimde de ciddi düşüşe yol açtı. Isınan nehirler yalnızca güç santrallerini değil bizzat nehir taşımacılığını da zorlamakta; bu da kuraklığın üretimi kısıtlamanın ötesinde, üretime girdi taşıyan lojistiği de aksatabildiğini göstermektedir.

Talep tarafında ise ısı, sistemi ters yönden sıkıştırmaktadır. Sigorta şirketi Allianz'ın hesaplamasına göre, sıcaklık otuz ile otuz beş derece aralığındayken her ilave derece elektrik talebini yaklaşık yüzde 1,2 artırmaktadır. Sonuç, arzın daraldığı tam da talebin soğutma yükü nedeniyle zirve yaptığı bir kıskaçtır. Güneş enerjisi üretiminin sıcak günlerde artması gündüz saatlerinde bir miktar tampon sağlasa da, panel verimi

hücre sıcaklığı yükseldikçe düşer; dolayısıyla üretim, tam da talebin en yüksek olduğu öğle sıcağında beklenenin altında kalabilir ve arz sıkışıklığı güneşin battığı, sıcaklığın ve talebin hâlâ yüksek olduğu akşam saatlerine kayabilir. Reuters'ın ekonomistlerin değerlendirmelerini derlediği bir analize göre, 2026 yazındaki sıcak hava, kuraklık ve yangınların Avrupa ekonomisine verdiği zarar, tarım, turizm, enerji ve ulaştırmadaki ilk verilerle birlikte şimdiden yüz milyarlarca euro ile ölçülmektedir.

Bu krizin raporun çerçevesi açısından taşıdığı anlam, ikinci bölümde tanımlanan savunulabilirlik boyutunun fiziksel dayanıklılık alt bileşenine geri döner: bir tesisin belirli bir kinetik etkiye karşı direnci kadar, çalışması için varsaydığı çevresel koşulların (soğutma suyu debisi, sıcaklık aralığı) ne ölçüde güvenceye alındığı da o tesisin savunulabilirliğinin parçasıdır. Soğuk Savaş döneminde tasarlanan nükleer ve termik santraller, on yıllık ortalamaların çok altına inen nehir debilerini varsaymamıştır; tasarımcıları ve işletmecileri, Macaristan başbakanının ifadesiyle, böylesi bir durumu "hiç ihtimal vermemiştir". İklim değişikliği, bu varsayımı sistematik olarak geçersiz kılmakta ve tek seferlik bir anomaliyi değil, tekrarlanan bir mevsimsel örüntüyü ortaya çıkarmaktadır. Bu bakımdan iklim kaynaklı üretim riski, raporun geri kalanında ele alınan kasıtlı saldırılarla aynı politika kutusuna girmektedir: her ikisi de önceden öngörülüp yatırım kararlarına yansıtılması gereken, tekrar eden bir tehdittir; farklı olan yalnızca failin varlığı ya da yokluğudur.

3.10. Karşılaştırmalı Değerlendirme

Tablo 3.3. Vaka Analizlerinin Karşılaştırmalı Matrisi

Vaka	Baskın Vektör	Hedef Mantığı	Etki Süresi	Atfedilebilirlik
Rusya rafinerileri (2022-26)	Uzun menzilli İHA	Ekonomik yıpratma + lojistik	Aylar-yıllar (kümülatif)	Yüksek (açık)
Ukrayna şebekesi (2022-26)	Füze + İHA	Toplumsal direnç kırma	Mevsimlik, tekrarlı	Yüksek (açık)
Abkaik (2019)	İHA + seyir füzesi	Piyasa şoku + prestij	Haftalar	Düşük (tartışmalı)
Petroline (2026)	Sınır ötesi İHA	Yedek güzergâhın imhası	Belirsiz	Çok düşük
Güney Pars (2026)	Hava harekâtı	Üretim kapasitesi imhası	Aylar	Yüksek (açık)
Körfez tesisleri (2026)	Füze + İHA	Misilleme + baskı	Değişken	Orta
Baltık kabloları (2023-26)	Çapa sürükleme	Gri bölge baskısı	40 gün (medyan)	Çok düşük
Nord Stream (2022)	Su altı patlayıcı	Kalıcı güzergâh imhası	Kalıcı	Çözülmemiş
Polonya OT (2025)	Siber (silici)	Donanım imhası	Haftalar-aylar	Düşük
Ukrayna şebekesi (2015-16)	Siber (ICS)	Kavram kanıtlama	Saatler	Orta
Avrupa 2026 yaz kuraklığı	İklim (sıcaklık/kuraklık)	Fail yok — doğal süreç	Haftalar, mevsimlik	Yok

Kaynak: TESPAM analizi. "Atfedilebilirlik", saldırının failinin uluslararası hukuk standartlarında ispatlanabilirlik derecesini ifade etmektedir.

Matris, üç eğilimi görünür kılmaktadır. Birincisi, atfedilebilirliğin düştüğü vakalarda saldırıların tekrarlanma sıklığı artmaktadır; ispat edilemezlik, fiilen bir güvenli alan yaratmaktadır. İkincisi, siber vektörlerin etki süresi geleneksel olarak kısa kabul edilirken, silici yazılımların devreye girmesiyle bu süre kinetik saldırılara yaklaşmaktadır. Üçüncüsü, en yıkıcı sonuçların tek büyük saldırılardan değil, onarım döngüsünden daha hızlı tekrarlanan orta ölçekli saldırılardan doğduğudur. Rusya vakasında belirleyici olan, herhangi bir tekil isabetin büyüklüğü değil, kampanyanın ritmidir.

4. PARADİGMA DEĞİŞİMİNİN ANATOMİSİ: ON KIRILMA

Önceki bölümde sunulan vakalar, birbirinden bağımsız olaylar dizisi değil, ortak bir yapısal dönüşümün farklı tezahürleridir. Bu bölüm, söz konusu dönüşümü on kırılma başlığı altında sistematize etmektedir. Her kırılma, enerji altyapısı güvenliğine ilişkin yerleşik bir varsayımın geçersizleşmesine karşılık gelmektedir.

4.1. Birinci Kırılma: Maliyet Asimetrisinin Tersine Dönmesi

Klasik savunma ekonomisinde, saldırı genellikle savunmadan pahalıdır; bu, istikrarın temel dayanaklarından biridir. Enerji altyapısı bağlamında bu denklem tersine dönmüştür. Menzili genişletilmiş, ticari bileşenlerden üretilmiş bir insansız hava aracının maliyeti on binlerce dolar mertebesindeyken, onu engelleyecek bir hava savunma füzesinin maliyeti yüz binlerce doları bulabilmekte; koruduğu tesisin yeniden inşa maliyeti ise yüz milyonlarca dolara ulaşabilmektedir.

Bu asimetri, savunma tarafını yapısal olarak sürdürülemez bir konuma yerleştirmektedir. Savunan taraf, tüm varlıklarını her an korumak zorundadır; saldıran taraf, tek bir zayıf noktayı tek bir anda bulmak yeterlidir. Bu, güvenlik literatüründe uzun süredir bilinen savunma-saldırı asimetrisinin enerji altyapısındaki en keskin görünümüdür. Sonuç, korumanın maliyet-etkin olabilmesi için mutlak engellemeden vazgeçilip zarar sınırlama ve hızlı onarım stratejilerine yönelinmesidir.

4.2. İkinci Kırılma: Menzilin Demokratikleşmesi

Yirminci yüzyılda derinlemesine hedef vurma kabiliyeti, az sayıda devletin tekelindeydi. Bugün bu kabiliyet, hem orta ölçekli devletler hem de devlet dışı aktörler için erişilebilir hâle gelmiştir. Ukrayna'nın Sibirya'daki Omsk rafinerisine ulaşması, Husilerin Yemen'den Suudi Arabistan'ın iç bölgelerini vurması ve Irak'tan kalkan araçların Medine yakınlarındaki pompa istasyonlarını hedef alması, bu demokratikleşmenin somut göstergeleridir.

Menzilin yaygınlaşmasının stratejik sonucu, "güvenli arka bölge" kavramının erimesidir. Enerji altyapısı yatırımlarında tesis yer seçimi, tarihsel olarak jeoloji, lojistik ve pazar yakınlığı ölçütlerine göre yapılmıştır; tehdit coğrafyası ancak sınır bölgelerinde bir kriter olmuştur. Bugün, tehdit menzili haritası, yatırım fizibilitesinin zorunlu bir girdisi hâline gelmiştir.

4.3. Üçüncü Kırılma: Onarım Döngüsünün Yeni Savaş Alanı Olması

Enerji altyapısı kampanyalarının etkinliğini belirleyen değişken, tekil saldırıların şiddeti değil, saldırı sıklığının onarım hızını aşıp aşmadığıdır. Rusya örneğinde, üç günde bir başarılı isabet frekansı, onarım ekiplerinin ve tedarik zincirinin kapasitesini aşmıştır. Bir tesis onarılırken bir diğeri vurulmakta; onarılan tesis yeniden hedef alınmaktadır. Saratov rafinerisinin 8 Eylül'de durdurulması, 10-11 Eylül'de üretime dönmeye hazırlanırken yeniden vurulması, bu ritmin tipik örneğidir.

Bu durum, savunma yatırımının ağırlık merkezini değiştirmektedir. Perimetre güvenliğine ayrılan her ilave birimin marjinal faydası azalırken, kritik yedek parça stokuna, modüler onarım kapasitesine ve mobil mühendislik ekiplerine ayrılan kaynağın marjinal faydası artmaktadır. Yüksek gerilim güç transformatörlerinde teslim süresinin iki ila dört yıla ulaştığı bir ortamda, stratejik trafo stoku tutmak artık bir lüks değil, bir zorunluluktur.

4.4. Dördüncü Kırılma: Darboğaz Ekipman Hedeflemesi

Saldırganlar, tesis düzeyinde değil ekipman düzeyinde düşünmeye başlamıştır. Bir rafinerinin atmosferik distilasyon ünitesi, bir gaz işleme tesisinin amin ünitesi, bir LNG tesisinin soğutma kompresörü, bir iletim

sisteminin otomatik trafosu — bunlar, tesisin tamamını temsil eden tekil noktalardır. Bu ekipmanlar genellikle özel tasarım, uzun tedarik süreli ve sınırlı sayıda üretici tarafından imal edilen kalemlerdir.

Bu eğilim, koruma stratejisinde "kritiklik haritalaması" disiplinini zorunlu kılmaktadır. Her tesis için, devre dışı kalması hâlinde tesisin işlevini en uzun süre durduracak bileşenlerin belirlenmesi, bu bileşenlerin fiziksel koruma önceliğine alınması ve yedeklerinin stoklanması gerekmektedir. Türkiye dâhil pek çok ülkede bu tür bir sistematik haritalamanın, kurumlar arası paylaşılan bir formatta mevcut olmadığı değerlendirilmektedir.

4.5. Beşinci Kırılma: Atfedilebilirliğin Erimesi

Sorumluluğun ispat edilememesi, saldırganlar için düşük maliyetli bir hareket alanı yaratmaktadır. Baltık'taki çapa sürükleme olaylarında olduğu gibi, fiilin kasıtlı mı yoksa ihmalden mi kaynaklandığının hukuken belirlenememesi, hem misillemeyi hem de tazminat mekanizmalarını devre dışı bırakmaktadır. Eylül 2026'daki Doğu-Batı hattı saldırısında hiçbir grubun sorumluluk üstlenmemesi, aynı stratejinin kara hedeflerine uyarlandığını göstermektedir.

Atfedilebilirlik krizinin yapısal çözümü, adlî teknik kapasitenin uluslararasılaştırılmasıdır: olay yerinde delil toplama standartlarının belirlenmesi, uydu ve deniz tabanı sensör verilerinin ortak havuzlarda toplanması ve bağımsız teknik soruşturma mekanizmalarının kurulması. Bu, kısa vadede gerçekleşmesi güç bir hedeftir; ancak alternatifi, ispat edilemez saldırıların kalıcı bir norm haline gelmesidir.

4.6. Altıncı Kırılma: Devlet Dışı Aktörlerin Devlet Ölçeğinde Etki Üretmesi

Husilerin Kızıldeniz kıyı şeridi ve Mayyun adası üzerinde kontrol sağlayarak küresel enerji ticaretinin önemli bir güzergâhını tehdit edebilir hale gelmesi, devlet dışı aktörlerin ulaştığı stratejik ağırlığı göstermektedir. Bu aktörler, klasik devlet kapasitesine sahip olmamakla birlikte, doğru coğrafi konum ve orta menzilli silah sistemleriyle küresel piyasaları etkileyebilmektedir.

Bu durum, enerji güvenliği diplomasisinin muhataplarını çoğaltmaktadır. Devletlerarası anlaşmalar ve caydırıcılık mimarileri, tanımı gereği devlet muhataplara yöneliktir. Kontrol ettiği coğrafya üzerinden kaldıraç üreten ancak uluslararası hukuki yükümlülük altına girmeyen aktörler karşısında, mevcut araç seti yetersiz kalmaktadır.

4.7. Yedinci Kırılma: Siber ve Kinetik Vektörlerin Birleşmesi

Siber saldırılar, artık bağımsız bir tehdit kategorisi olmaktan çıkıp kinetik harekâtın hazırlık ve çarpan bileşeni hâline gelmektedir. Önceden konumlanma faaliyetleri, kriz anında devreye girecek erişimlerin barış döneminde oluşturulmasını ifade eder. Sektör değerlendirmeleri, 2026 itibarıyla küresel enerji ve kamu hizmetleri altyapısının üçte birinden fazlasında bu tür sessiz erişim, veri toplama ve operasyonel haritalama faaliyetinin gerçekleştiğini öne sürmektedir.

Birleşik vektörün en tehlikeli senaryosu, kinetik saldırı anında savunma ve müdahale sistemlerinin siber yolla devre dışı bırakılmasıdır: yangın söndürme sistemlerinin kilitlenmesi, acil kapatma valflerinin engellenmesi veya operatör arayüzlerindeki bilgilerin manipüle edilmesi. Bu senaryo teorik değildir; CyberAv3ngers vakasında operatörlere sunulan bilginin değiştirilmesi, tam olarak bu kabiliyetin kanıtıdır.

4.8. Sekizinci Kırılma: Sigortalanabilirlik ve Finansman Krizi

Enerji altyapısı yatırımları, uzun geri ödeme süreli ve yüksek borçlanma oranlı projelerdir. Savaş riski primlerinin fırlaması ve bazı bölgelerde savaş riski teminatının fiilen bulunamaz hale gelmesi, projelerin

finansal kapanışını doğrudan etkilemektedir. Mücbir sebep ilanlarının zincirleme biçimde yayılması, uzun vadeli alım sözleşmelerinin güvenilirliğine ilişkin bir belirsizlik primi doğurmuştur.

Bu kırılmanın ikinci dereceden etkisi, yatırımın coğrafi yeniden dağılımıdır. Risk primi yüksek bölgelerde yeni kapasite yatırımı ertelenirken, göreli olarak güvenli kabul edilen bölgelerde yoğunlaşma artmaktadır. Uzun vadede bu, arz kaynaklarının çeşitliliğini azaltarak paradoksal biçimde sistemik kırılganlığı yükseltebilir.

4.9. Dokuzuncu Kırılma: Enerji Dönüşümünün Yeni Saldırı Yüzeyi

Yenilenebilir enerjiye ve dağıtık üretime geçiş, enerji güvenliği açısından iki yönlü bir etki üretmektedir. Olumlu yönde, güneş ve rüzgâr kaynakları boğazlardan geçirilemez, tankerle taşınamaz ve üçüncü bir ülke tarafından kesilemez; bu, jeopolitik riske karşı güçlü bir korunma sağlar. Olumsuz yönde ise, binlerce dağıtık varlığın uzaktan izlenmesi ve kontrol edilmesi zorunluluğu, saldırı yüzeyini niceliksel olarak büyütmektedir.

Polonya olayında hedef alınan tesisler arasında yenilenebilir enerji santrallerinin bulunması tesadüf değildir. Dağıtık varlıklar, genellikle merkezî santrallere kıyasla daha zayıf fiziksel güvenlik, daha standart ve dolayısıyla daha kolay istismar edilebilir kontrol ekipmanı ve daha az olgun siber güvenlik yönetişimine sahiptir. Aynı marka ve modeldeki binlerce inverterin ortak bir zafiyet taşıması, tek bir istismarın sistem çapında etki üretmesine imkân verir.

4.10. Onuncu Kırılma: Sivil-Askerî Ayrımının Bulanıklaşması

Enerji altyapısının büyük bölümü, tanımı gereği çift kullanımlıdır. Bir rafineri hem sivil ulaşımı hem askerî lojistiği besler; bir iletim hattı hem hastaneleri hem komuta merkezlerini besler. Bu durum, uluslararası insancıl hukukun ayrım ve orantılılık ilkelerinin uygulanmasını güçleştirmektedir.

Tartışmanın pratik sonucu, enerji tesislerinin hukuki koruma statüsünün zayıflamasıdır. İran Çevre Örgütü yetkililerinin akaryakıt depolarının sistematik imhasını çevre kırımı olarak nitelendirmesi, bu tartışmanın çevresel boyutunu da gündeme getirmektedir. Enerji altyapısına yönelik saldırıların insani ve ekolojik maliyetlerinin muhasebesi, çağdaş savaş hukukunun henüz cevap üretmediği bir alandır ve bu boşluk, saldırganlar açısından fiilî bir serbestlik alanına dönüşmektedir.

4.11. On Birinci Kırılma: İklimin Üretim Güvenliğine Dönüşmesi

Üçüncü bölümde ele alınan 2026 Avrupa yazı, bu raporun kapsamına failsiz bir tehdit kategorisini eklemektedir. Geleneksel olarak iklim değişikliği, enerji planlamasında uzun vadeli bir verimlilik ve yatırım sorunu olarak konumlandırılmıştır: karbon fiyatlaması, varlıkların atıl kalma riski, altyapının onlarca yıllık ufukta yeniden şekillenmesi. 2026 yazı, bu çerçevenin eksik olduğunu göstermiştir. Sıcaklık ve kuraklık, artık yılda birkaç haftaya sıkışan, öngörülebilir ancak şiddeti giderek artan bir operasyonel güvenlik olayı olarak enerji sistemine girmektedir; Paks ve Cernavodă'da olduğu gibi santral kapatma kararına, nehir taşımacılığında olduğu gibi lojistik aksamaya, Avrupa hidroelektrik üretiminde olduğu gibi mevsimlik düşük rekorlarına yol açmaktadır.

Bu kırılmanın raporun geri kalanıyla kesiştiği nokta, risk yönetiminin ayrık kutularda yürütülmesinin artık savunulamaz olmasıdır. Bir enerji şirketi, fiziksel güvenlik bütçesini kinetik ve siber tehditlere, sürdürülebilirlik bütçesini iklim uyumuna ayırıyorsa, iki bütçenin kesiştiği alan — bir nükleer santralin soğutma suyu güvencesi, bir hidroelektrik santralin üretim garanti kapasitesi — boşlukta kalır. Savunulabilirliğin fiziksel dayanıklılık bileşeni, artık yalnızca "bu tesis bir İHA saldırısına dayanır mı" sorusunu değil, "bu tesis tasarım varsayımlarının çok ötesindeki bir soğutma suyu veya girdi kesintisine dayanır mı" sorusunu da kapsamalıdır.

Tablo 4.1. Eski ve Yeni Paradigmanın Karşılaştırılması

Boyut	Geleneksel Paradigma (öncesi)	Yeni Paradigma (2019 sonrası)
Temel risk	Arz kesintisi, fiyat şoku, ambargo	Fiziksel imha, kalıcı kapasite kaybı
Tehdit aktörü	Devlet (siyasi karar), yerel terör örgütü	Devlet + vekil aktör + siber aktör + belirsiz fail
Coğrafi kapsam	Sınır bölgeleri, çatışma alanları	Ülke derinliği dâhil tüm varlık ağı
Koruma yaklaşımı	Perimetre güvenliği, güvenlik personeli	Katmanlı savunma + dayanıklılık + hızlı onarım
Başarı ölçütü	Saldırının engellenmesi	Kesinti süresinin ve yayılımının sınırlanması
Kritik varlık	Üretim sahası, ana boru hattı	Darboğaz ekipman, kontrol sistemi, yedek güzergâh
Stok mantığı	Ham madde ve ürün stoku	Ürün stoku + kritik yedek parça stoku
Kurumsal sahiplik	İşletmeci şirket + kolluk	Şirket + silahlı kuvvetler + siber otorite + düzenleyici
Zaman ufku	Olay bazlı, kriz yönetimi	Sürekli kampanya, kalıcı hazırlık
Sigorta	Standart varlık ve kâr kaybı teminatı	Savaş riski primi, teminat bulunamaması
İklim riski	Uzun vadeli verimlilik/yatırım sorunu	Tekrarlayan, mevsimlik operasyonel güvenlik riski

5. ALTYAPI TÜRLERİNE GÖRE TEHDİT VE KORUMA MİMARİSİ

Enerji altyapısı, homojen bir kategori değildir. Bir rafineri ile bir deniz altı enterkonektörü, bir LNG terminali ile bir yeraltı gaz deposu arasında tehdit maruziyeti, kırılganlık yapısı ve onarım süresi açısından derin farklar bulunmaktadır. Koruma yatırımlarının verimli dağıtılabilmesi için bu farkların sistematik olarak tanımlanması gerekmektedir. Bu bölüm, on ayrı altyapı kategorisi için tehdit profilini ve önerilen koruma mimarisini ayrı ayrı ele almaktadır.

5.1. Rafineriler ve Petrokimya Tesisleri

Rafineriler, 2022 sonrası dönemin en çok hedef alınan enerji varlık kategorisidir. Bunun üç nedeni vardır. Birincisi, geniş alana yayılmış, kamuflajı imkânsız ve uydu görüntülerinden kolayca haritalanabilen tesislerdir. İkincisi, yüksek yanıcı madde yoğunluğu nedeniyle görece küçük bir isabet dahi zincirleme yangınlara yol açabilir. Üçüncüsü, ürün çıktıları hem sivil ekonominin hem askerî lojistiğin ortak girdisidir; bu da onları stratejik olarak yüksek değerli kılar.

Kritik bileşenler, tesis alanının tamamına eşit dağılmamıştır. Atmosferik ve vakum distilasyon üniteleri, hidrokraker ve katalitik kraker reaktörleri, yüksek basınçlı fırınlar, ana ürün pompaları ve kontrol odaları, tesisin işlevini tek başına durdurabilecek düğüm noktalarıdır. Sizran rafinerisinde tek bir distilasyon ünitesinin tesis kapasitesinin yaklaşık yüzde yetmiş birini oluşturması, bu yoğunlaşmanın somut bir örneğidir.

Tablo 5.1. Rafineri ve Petrokimya Tesisleri: Tehdit-Önlem Matrisi

Tehdit Vektörü	Kırılganlık Noktası	Önerilen Önlem
Uzun menzilli İHA	Distilasyon kolonları, fırınlar, kontrol odası	Katmanlı İHA savunması (radar + RF karıştırma + kısa menzilli silah), pasif koruyucu ağ ve blast duvar
Balistik/seyir füzesi	Tüm tesis alanı	Erken uyarı entegrasyonu, personel sığınakları, kritik ekipmanda gömülü/korunaklı tasarım
Sabotaj / iç tehdit	Vana sahaları, acil kapatma sistemleri	Personel güvenlik taraması, erişim ayrımı, kritik komutlarda çift onay
Siber (OT)	DCS/SCADA, emniyetli kapatma sistemleri (SIS)	SIS'in DCS'ten fiziksel ayrımı, tek yönlü veri geçidi (data diode), IEC 62443 uyumu
Tedarik zinciri	Özel alaşım kolon iç aksamı, kompresör	Kritik yedek parça stoku, ikinci kaynak tedarikçi sözleşmeleri
İkincil yangın/patlama	Tank çiftliği yakınlığı, boru köprüleri	Tank arası mesafe revizyonu, köpüklü söndürme kapasitesi, yangın duvarları
Zincirleme kapasite kaybı	Tek ülkede yoğunlaşma	Ürün ithalat altyapısı ve alternatif tedarik sözleşmelerinin önceden hazırlanması

Rafineri korumasında ölçek ekonomisi ile dayanıklılık arasındaki gerilim en keskin biçimde ortaya çıkar. Az sayıda büyük tesis, birim maliyeti düşürür ancak riski yoğunlaştırır. Enerji güvenliği perspektifinden bakıldığında, toplam kapasitenin belirli bir eşiğin üzerinde tek bir tesiste toplanmaması, düzenleyici bir kriter hâline getirilmelidir. Bahreyn'in tek rafinerisinin vurulmasının ülke çapında mücbir sebep ilanına yol açması, bu kriterin gerekçesini somutlaştırmaktadır.

5.2. Kara Boru Hatları ve Pompa/Kompresör İstasyonları

Boru hatları, uzunlukları nedeniyle bütün hat boyunca korunması imkânsız varlıklardır. Ancak bu durum, hattın tamamının eşit ölçüde kırılgan olduğu anlamına gelmez. Hattın kendisi, delinmesi hâlinde görece hızlı onarılabilen bir çelik borudur; asıl kritik varlıklar, pompa ve kompresör istasyonlarıdır. Bu istasyonlar, uzun tedarik süreli türbin ve kompresör setleri, elektrik altyapısı ve kontrol sistemleri barındırır.

Suudi Doğu-Batı hattı vakası bu ayrımı net biçimde göstermiştir: saldırılar hattın kendisini değil, pompa istasyonlarını hedef almış; uydu görüntüleri el-Mesbaa yakınlarındaki bir istasyonda geniş çaplı yangın hasarını göstermiştir. Benzer biçimde TürkAkım ve Mavi Akım'a yönelik insansız hava aracı saldırı girişimleri, boru hattının kendisini değil, Krasnodar'daki Russkaya kompresör istasyonunu hedef almıştır — zira İHA'lar doğaları gereği deniz tabanındaki bir hedefi vuramaz. Aynı hatların Karadeniz tabanındaki su altı kesimine yönelik, dalgıç ve patlayıcı temelli ayrı ve daha az bilinen bir tehdit katmanı ise yedinci bölümde ele alınmaktadır.

Tablo 5.2. Boru Hatları ve İstasyonlar: Tehdit-Önlem Matrisi

Tehdit Vektörü	Kırılganlık Noktası	Önerilen Önlem
İHA saldırısı	Pompa/kompresör istasyonları, ölçüm istasyonları	İstasyon bazlı nokta hava savunması, kritik ekipmanda korunaklı muhafaza
Sabotaj / patlayıcı	Vana istasyonları, nehir geçişleri, açıkta kalan kesimler	Fiber optik dağıtık algılama (DAS), İHA devriyesi, hızlı müdahale ekipleri
Yasadışı bağlantı/hırsızlık	Kırsal ve denetimsiz kesimler	Basınç anomalisi analitiği, uydu/termal izleme, yerel toplum işbirliği
Siber (OT)	SCADA, uzaktan terminal birimleri (RTU)	RTU envanteri ve yama disiplini, internete açık cihazların kapatılması, ağ segmentasyonu
Doğal tehlike	Heyelan, deprem fay geçişleri, sel yatakları	Jeoteknik izleme, kaya tahkimatı, esnek bağlantı elemanları
Transit ülke riski	Sınır ötesi kesimler, üçüncü ülke istasyonları	İkili güvenlik protokolleri, ortak izleme merkezleri, alternatif güzergâh hazırlığı
Elektrik besleme kesintisi	İstasyonların şebeke bağımlılığı	Yerinde yedek üretim (jeneratör/gaz türbini), yakıt stoku

5.3. Deniz Altı Sistemler: Boru Hatları, Enterkonektörler ve Veri Kabloları

Deniz altı altyapıları, bu raporda ele alınan kategoriler arasında en yüksek kırılganlık-en düşük görünürlük bileşimine sahip olanlardır. Yedinci bölüm bu kategoriyi ayrıntılı biçimde ele almaktadır; burada temel tehdit-önlem çerçevesi sunulmaktadır.

Dört alt kategori ayırt edilmelidir. Denizaltı doğal gaz ve ham petrol boru hatları (Nord Stream, TürkAkım, Mavi Akım, Balticconnector), yüksek kapasiteli ve yüksek etkili varlıklardır; onarımları özel gemiler ve aylar gerektirir. Su altı üretim kuyu başları, ıslak ağaçlar (subsea tree) ve manifoldlar ise deniz tabanındaki üretim sahalarını yüzeye bağlayan, açık deniz platformu bulunmayan modern derin su geliştirmelerinin bel kemiğidir; bir sahanın onlarca kuyusu, tek bir manifold ve tek bir ana boru hattı üzerinden toplanabilmekte, bu da manifoldu sahanın tamamı için bir darboğaz hâline getirmektedir. Elektrik enterkonektörleri (Estlink, Great Sea Interconnector gibi HVDC bağlantıları), sistem dengesi açısından kritiktir ve dönüştürücü istasyonları kara tarafında ilave kırılganlık yaratır. Veri kabloları ise doğrudan enerji taşımaz, ancak enerji sistemlerinin uzaktan kontrolü ve piyasa işlemleri bu altyapıya bağımlıdır.

Bu dört kategorinin tamamını birleştiren ortak payda, inşa maliyeti ile imha maliyeti arasındaki orandır. Bir denizaltı boru hattı veya HVDC enterkonektörü, özel döşeme gemileri, aylar süren deniz operasyonları ve yüz milyonlarca ila milyarlarca dolarlık mühendislik yatırımıyla inşa edilir; buna karşılık aynı hattı kalıcı olarak devre dışı bırakmak için gereken araç — bir patlayıcı yükü, sürüklenen bir çapa, ticari ölçekli bir su altı aracı — çoğu zaman inşa maliyetinin binde biri mertebesindedir. Bu oran, dördüncü bölümde tanımlanan birinci kırılmanın (maliyet asimetrisinin tersine dönmesi) deniz tabanındaki en keskin görünümüdür; çünkü kara üzerindeki bir tesisin aksine, deniz tabanındaki bir hat sürekli gözetlenemez ve saldırganın erişimini fiilen engelleyecek bir fiziksel bariyer neredeyse hiçbir zaman yoktur.

Tablo 5.3. Deniz Altı Sistemler: Tehdit-Önlem Matrisi

Tehdit Vektörü	Kırılganlık Noktası	Önerilen Önlem
Çapa sürükleme	Sığ su kesimleri, yoğun trafik koridorları	Gömme derinliğinin artırılması, koruma kanalı, AIS anomali izleme, sürüklenen çapa erken uyarısı
Su altı patlayıcı / İSA	Derin su kesimleri, kesişme noktaları	Deniz tabanı sensör ağı, otonom su altı araçlarıyla periyodik denetim
Su altı drone / özel kuvvet	Karaya çıkış noktaları, vana odaları	Karaya çıkış tesislerinde askerî seviyede koruma, sualtı bariyer ve sonar
Dönüştürücü istasyon saldırısı	HVDC konvertör istasyonları (kara)	Kara tesislerinin kritik altyapı statüsüne alınması, yedek transformatör ve valf grubu
Onarım kapasitesi darboğazı	Sınırlı sayıda kablo gemisi	Bölgesel onarım gemisi paylaşım anlaşmaları, modüler ekipmanın limanlarda önceden konumlandırılması
Atfedilemezlik	Hukuki boşluk (UNCLOS)	Uluslararası ortak soruşturma protokolü, kıyı devleti yetkilerinin genişletilmesi
Kuyu başı / manifold hasarı	Tek noktadan toplanan çoklu kuyu üretimi	Manifold yedekliliği, kuyu başı acil kapatma valfleri, üretim sahasının çoklu manifolde bölünmesi

5.4. LNG Zinciri: Sıvılaştırma, Taşıma ve Gazlaştırma

LNG zinciri, enerji sistemleri arasında en yüksek sermaye yoğunluğuna ve en uzun yeniden inşa süresine sahip olan halkadır. Bir sıvılaştırma treni, mühendislik-tedarik-inşaat döngüsü dâhil beş yılı aşan sürelerde devreye alınır. Katar'ın Ras Laffan tesislerinin İran füzeleriyle vurulması ve çıkan yangınların ilgili gaz-sıvı dönüşüm tesisi dâhil geniş hasara yol açması, QatarEnergy'nin bazı uzun vadeli tedarik sözleşmelerinde mücbir sebep ilan etmesine neden olmuştur.

Zincirin her halkasının farklı bir kırılganlık profili vardır. Sıvılaştırma tesisleri sabit, büyük ve yüksek değerli hedeflerdir. LNG tankerleri hareketli olmakla birlikte darboğaz geçişlerinde savunmasızdır; Hürmüz kapandığında Katar'ın ihracatı için pratik bir alternatif güzergâh bulunmamaktadır. Gazlaştırma terminalleri ve yüzer depolama-gazlaştırma üniteleri (FSRU) ise ithalatçı ülkeler açısından kritik giriş kapılarıdır ve çoğunlukla nüfus yoğun kıyı bölgelerinde konumlanmıştır.

Tablo 5.4. LNG Zinciri: Tehdit-Önlem Matrisi

Halka	Başlıca Tehdit	Önerilen Önlem
Sıvılaştırma treni	Füze/İHA, yangın yayılımı	Tren arası ayrım mesafesi, bağımsız acil kapatma, kritik kompresör yedekliliği
İhraç terminali / iskele	Deniz kaynaklı saldırı, mayın	Liman yaklaşma kontrolü, sualtı algılama, tahliye planı
LNG tankeri	Boğaz geçişi, füze/İHA, mayın	Konvoy refakati, rota çeşitlendirme, savaş riski sigortası havuzu
FSRU / gazlaştırma	Kıyı saldırısı, sabotaj, siber	Demirleme noktası güvenliği, ikinci bağlantı noktası hazırlığı, OT ayrımı
Şebeke bağlantısı	Tek giriş noktası bağımlılığı	Çoklu giriş noktası, ters akış kabiliyeti, yeraltı depolamayla entegrasyon

5.5. Elektrik İletim Sistemi ve Trafo Merkezleri

Elektrik iletim sistemi, eşzamanlılık zorunluluğu nedeniyle en az tolerans payına sahip enerji altyapısıdır. Ukrayna deneyimi, sistemin kırılganlığının üretim tesislerinden çok iletim düğümlerinde yoğunlaştığını göstermiştir. Yüksek gerilim güç transformatörleri, bu düğümlerin kalbidir: her biri yüzlerce ton ağırlığında, özel tasarımlı, sınırlı sayıda üretici tarafından imal edilen ve teslim süresi yıllarla ölçülen ekipmanlardır.

İletim sistemine yönelik saldırıların ikinci dereceden etkileri, birinci dereceden etkilerinden daha yıkıcı olabilir. Elektrik kesintisi, su pompalama, doğal gaz basınç yönetimi, akaryakıt istasyonlarının çalışması, telekomünikasyon ve veri merkezleri üzerinden yayılır. Rinaldi ve arkadaşlarının altyapı karşılıklı

bağımlılıkları üzerine geliştirdiği kavramsal çerçeve, bu yayılımın fiziksel, siber, coğrafi ve mantıksal olmak üzere dört kanaldan gerçekleştiğini ortaya koymuştur.

Tablo 5.5. Elektrik İletim Sistemi: Tehdit-Önlem Matrisi

Tehdit Vektörü	Kırılganlık Noktası	Önerilen Önlem
İHA/füze	Trafo merkezleri, otomatik transformatörler	Beton koruma yapıları, dağınık yerleşim, kritik merkezlerde nokta savunma
Silahlı saldırı (ateşli silah)	Açıkta duran transformatör radyatörleri	Balistik perde, görüş hattı engelleme, hızlı sızıntı kapatma kiti
Siber (ICS)	Koruma röleleri, SCADA, uzaktan kesici kumandası	Rölelerde yerel kilit, uzaktan komutta çift doğrulama, ağ segmentasyonu
Yedek parça darboğazı	Yüksek gerilim güç transformatörleri	Ulusal stratejik trafo stoku, standartlaştırılmış mobil trafo filosu
Kaskad çöküş	Sistem kararlılığı, frekans kontrolü	Ada modunda çalışma (islanding) senaryoları, kara başlatma (black start) tatbikatı
Personel/uzmanlık	Sınırlı sayıda nitelikli ekip	Bölgesel müdahale ekipleri, komşu operatörlerle karşılıklı yardım anlaşmaları

5.6. Nükleer Santraller

Nükleer santraller, düşük olasılık-çok yüksek sonuç kategorisinin en belirgin örneğidir. Çatışma bölgelerinde bulunan santraller, doğrudan hedef alınmasalar bile dış elektrik besleme hatlarının kesilmesi veya soğutma suyu temininin aksaması yoluyla ciddi risk altına girebilirler. Zaporijya örneği, bir santralin bizzat vurulmadan da güvenlik açısından kritik duruma gelebileceğini göstermiştir. 2026 yazında Macaristan'daki Paks ve Romanya'daki Cernavodă santrallerinin yaşadığı kapasite kaybı, aynı sonucun bir düşmana hiç ihtiyaç duymadan, yalnızca bir nehrin debisiyle de üretilebildiğini göstermiştir; soğutma suyu temini, bu bakımdan dış elektrik beslemesiyle aynı kategoride bir bağımlılık olarak ele alınmalıdır.

Nükleer tesislerde koruma mimarisinin farkı, kaza sonrası etkinin geri döndürülemezliğidir. Bu nedenle öncelik, tesis işlevinin sürdürülmesinden çok güvenlik fonksiyonlarının her koşulda korunmasına verilmelidir: dış besleme kaybında yedek jeneratör ve yakıt stoku, soğutma suyu alternatifleri, kullanılmış yakıt havuzlarının korunması ve Uluslararası Atom Enerjisi Ajansı ile sürekli bilgi paylaşımı. Ayrıca nükleer tesislerin siber güvenliği, fiziksel güvenlikten ayrı bir rejime tabi tutulmalı ve dijital kontrol sistemlerinde tek yönlü veri geçişi standart hâline getirilmelidir.

5.7. Yenilenebilir ve Dağıtık Enerji Varlıkları

Rüzgâr ve güneş santralleri, batarya depolama sistemleri ve dağıtık kojenerasyon birimleri, enerji dönüşümünün taşıyıcıları olmakla birlikte kendine özgü bir kırılganlık profili taşımaktadır. Bu varlıklar coğrafi olarak dağınık olduğundan tek bir fiziksel saldırıyla tümüyle devre dışı bırakılmaları güçtür; bu, dayanıklılık açısından güçlü bir avantajdır. Ancak aynı dağınıklık, fiziksel güvenlik harcamalarının varlık başına düşmesine ve uzaktan yönetim bağımlılığının artmasına yol açar.

Asıl risk, tekdüzelikten kaynaklanmaktadır. Binlerce inverterin, rüzgâr türbini kontrol ünitesinin veya batarya yönetim sisteminin aynı üreticiye, aynı yazılım sürümüne ve aynı bulut yönetim platformuna bağlı olması, tek bir zafiyetin sistem çapında eşzamanlı etki üretmesine imkân tanır. Bir sektör çalışması, Birleşik Krallık'ta batarya depolama varlıklarının 2031'e kadar büyük bir siber saldırıya uğrama olasılığını yüzde doksan iki seviyesinde değerlendirmiştir. Bu tür öngörüler kesin tahminler olarak değil, yoğunlaşma riskinin göstergeleri olarak okunmalıdır.

Koruma mimarisi üç eksende kurulmalıdır. Birincisi, tedarikçi çeşitliliğinin düzenleyici bir kriter hâline getirilmesidir; belirli bir kurulu gücün üzerinde tek bir üreticinin kontrol ekipmanına bağımlılık sınırlandırılmalıdır. İkincisi, şebeke bağlantı yönetmeliklerine siber güvenlik şartlarının dâhil edilmesidir. Üçüncüsü, iletişim kaybı senaryolarında varlıkların güvenli varsayılan duruma geçmesini sağlayan yerel otonomi tasarımıdır; uzaktan kontrol kesildiğinde sistemin kontrolsüz davranmaması esastır.

5.8. Depolama Altyapıları

Depolama, dayanıklılığın temel aracı olmakla birlikte kendisi de bir hedeftir. İran'da Şahran, Ağdasiye, Rey ve Karac depolarının sistematik olarak hedef alınması, akaryakıt depolarının yüksek görünürlükleri ve yangın yayılım potansiyelleri nedeniyle tercih edilen hedefler olduğunu göstermiştir.

Yeraltı doğal gaz depolama tesisleri, yer üstü tank çiftliklerine kıyasla çok daha savunulabilir varlıklardır. Rezervuarın kendisi fiziksel saldırıya pratikte kapalıdır; kırılganlık, kuyu başları, yüzey işleme tesisleri ve kompresör istasyonlarında yoğunlaşır. Bu asimetri, depolama portföyünde yeraltı kapasitesinin payının artırılmasını, salt piyasa gerekçeleriyle değil güvenlik gerekçesiyle de savunulabilir kılmaktadır.

Stratejik stok politikası açısından üç ilke öne çıkmaktadır: stokun coğrafi dağıtımı (tek bir bölgede yoğunlaşmaması), stokun fiziksel korunaklılığı (mümkün olduğunca yeraltı veya gömülü tank), ve stok çekiş kapasitesinin kriz senaryolarında test edilmesi. Stokun varlığı, ona erişim altyapısı da korunmadıkça anlam ifade etmez.

5.9. Limanlar, Terminaller ve Deniz Taşımacılığı

Enerji ticaretinin büyük bölümü deniz yoluyla gerçekleştiğinden, limanlar ve terminaller sistemin darboğazlarıdır. 2026 savaşında Bahreyn'de Halife bin Selman Limanı'nda operasyonların askıya alınması, Fucayre Limanı'nın balistik füzeyle hedef alınması ve Umman'da Mina el-Fahal ile Selale terminallerinin geçici kapatılması, bu kategorinin maruziyetini göstermektedir. Bahreyn açıklarında bir tankerin isabet alması ve Selman sanayi bölgesinde bir geminin üzerine düşen enkazın can kaybına yol açması, riskin gemilere de uzandığını ortaya koymuştur.

Terminal güvenliğinde dört katman önerilmektedir: deniz tarafı yaklaşma kontrolü ve sualtı algılama; iskele ve yükleme kolu bölgesinin korunması; tank çiftliği ile terminal arasındaki bağlantı hatlarının yedeklenmesi; ve gemi trafiği yönetim sistemlerinin siber güvenliği. Ayrıca liman operasyonlarında elektrik ve veri bağımlılığı yüksek olduğundan, terminal içi bağımsız enerji ve iletişim kapasitesi bulundurulmalıdır.

5.10. Kesişen Katman: Operasyonel Teknoloji ve Kontrol Sistemleri

Yukarıda sayılan bütün kategoriler, ortak bir katman üzerinde çalışmaktadır: endüstriyel kontrol ve otomasyon sistemleri. Bu katman, kendi başına bir altyapı türü olmamakla birlikte, tüm türleri birbirine bağlayan ve dolayısıyla tek bir saldırıyla çoklu etki üretilmesine imkân tanıyan bir ortak paydadır. Altıncı bölüm bu katmanı ayrıntılı olarak ele almaktadır.

Tablo 5.6. Altyapı Türlerinin Karşılaştırmalı Kırılganlık Profili

Altyapı Türü	Hedef Görünürlüğü	Onarım Süresi	İkame Edilebilirlik	Yayılım Etkisi
Rafineri	Çok yüksek	Aylar	Düşük (ithalatla kısmî)	Yüksek
Pompa/kompresör istasyonu	Yüksek	Haftalar-aylar	Düşük	Çok yüksek
Denizaltı boru hattı	Düşük	Aylar	Çok düşük	Yüksek
HVDC enterkonektör	Düşük	Haftalar-aylar	Orta	Yüksek
Veri kablosu	Çok düşük	~40 gün (medyan)	Orta	Orta

Altyapı Türü	Hedef Görünürlüğü	Onarım Süresi	İkame Edilebilirlik	Yayılım Etkisi
LNG sıvılaştırma	Çok yüksek	Aylar-yıllar	Çok düşük	Çok yüksek
FSRU / gazlaştırma	Yüksek	Haftalar	Orta	Yüksek
Trafo merkezi (EHV)	Yüksek	Aylar-yıllar (trafo)	Düşük	Çok yüksek
Nükleer santral	Çok yüksek	Yıllar	Çok düşük	Çok yüksek
Hidroelektrik santral / baraj	Orta	Yapısal hasarda yıllar; kuraklıkta mevsimlik	Düşük-orta	Yüksek
Dağıtık YEK + batarya	Düşük (tekil)	Günler-haftalar	Yüksek	Düşük-orta
Yer üstü akaryakıt deposu	Çok yüksek	Haftalar-aylar	Orta	Orta
Yeraltı gaz deposu	Orta	Haftalar	Düşük	Yüksek
İhraç terminali / liman	Yüksek	Haftalar	Orta	Çok yüksek
OT/SCADA katmanı	Görünmez	Günler-haftalar	Yüksek (yedekli ise)	Çok yüksek

6. SİBER TEHDİTLER: GÖRÜNMEYEN CEPHENİN MİMARİSİ

6.1. Tehdit Manzarasının Dönüşümü

Enerji sektörüne yönelik siber tehditler, son on yılda üç kuşak geçirmiştir. Birinci kuşak, bilgi teknolojisi ağlarını hedef alan veri hırsızlığı ve casusluk faaliyetleridir. İkinci kuşak, fidye yazılımlarıyla iş süreçlerinin kilitlenmesidir; 2021'deki Colonial Pipeline olayı, bilgi teknolojisi ağına yapılan bir saldırının, operasyonel teknoloji ağı doğrudan etkilenmese bile faturalandırma ve lojistik kaygılarıyla boru hattının durdurulmasına yol açabileceğini göstermiştir. Üçüncü kuşak ise operasyonel teknoloji ortamlarını doğrudan hedef alan, fiziksel etki üretmeyi amaçlayan saldırılardır.

Üçüncü kuşağın tanımlayıcı örnekleri, Ukrayna'daki 2015 ve 2016 şebeke saldırıları, endüstriyel emniyet sistemlerini hedef alan zararlı yazılımlar ve 2025 sonunda Polonya'da uzaktan terminal birimlerini fiziksel olarak tahrip eden silici yazılım kampanyasıdır. Bu kuşakta amaç, bilgiye erişmek veya hizmeti geçici olarak kesmek değil, donanımı kullanılamaz hâle getirmektir.

6.2. Yapısal Kırılganlıklar

Endüstriyel kontrol sistemlerinin kırılganlığı, kötü yönetimden çok tasarım mirasından kaynaklanmaktadır. Bu sistemler, izole ortamlarda çalışacakları varsayımıyla, güvenilirlik ve gerçek zamanlı yanıt öncelikleriyle tasarlanmıştır. Kimlik doğrulama, şifreleme ve bütünlük kontrolü, çoğu endüstriyel protokolün tasarım gündeminde yoktu.

- **Ömür uyumsuzluğu:** Endüstriyel donanımın ekonomik ömrü yirmi ila otuz yıl iken, bilgi güvenliği teknolojilerinin ömrü üç ila beş yıldır. Bu uyumsuzluk, sahada sürekli olarak güncel olmayan bileşen bulunmasını yapısal hâle getirir.
- **Yama uygulanamazlığı:** Üretimin durdurulamaması, güvenlik yamalarının aylarca hatta yıllarca uygulanamamasına yol açar. Bakım pencereleri kısıtlıdır ve yama sonrası doğrulama testleri maliyetlidir.
- **İnternete açık varlıklar:** Uzaktan izleme ihtiyacı, programlanabilir mantık denetleyicilerinin ve uzaktan terminal birimlerinin doğrudan internete açılmasına yol açmaktadır. CyberAv3ngers kampanyasının temel giriş yolu tam olarak budur.
- **Tedarik zinciri ve servis sağlayıcı erişimi:** Bakım sözleşmeleri kapsamında üretici ve servis sağlayıcılara verilen uzaktan erişim hakları, çoğu zaman operatörün görünürlüğü dışında kalmaktadır. Amerikan yetkili makamları, Temmuz 2026'da bu riske özel olarak dikkat çekmiş ve operatörlerin servis sağlayıcılarıyla doğrudan iletişim kurmasını önermiştir.
- **Bilgi-operasyon teknolojisi yakınsaması:** Verimlilik amacıyla kurulan bulut tabanlı analitik ve uzaktan yönetim bağlantıları, iki ağ arasındaki geleneksel ayrımı aşındırmaktadır.

6.3. Önceden Konumlanma ve Yapay Zekâ Boyutu

Çağdaş tehdit manzarasının en endişe verici unsuru, saldırının kendisi değil hazırlığıdır. Önceden konumlanma, kriz anında kullanılmak üzere barış döneminde erişim sağlanması ve bu erişimin sessizce sürdürülmesi anlamına gelir. Sektör değerlendirmeleri, 2026 itibarıyla küresel enerji ve kamu hizmetleri altyapısının üçte birinden fazlasında bu tür faaliyetin gerçekleşmiş olabileceğini öne sürmektedir. Bu tespit, doğrulanması güç olmakla birlikte, savunma planlamasının "sızıntı olmuş varsayımı" üzerine kurulması gerektiğini göstermektedir.

Yapay zekâ, denklemin her iki tarafını da değiştirmektedir. Saldırı tarafında keşif faaliyetlerinin ölçeklenmesini, zafiyet analizinin hızlanmasını ve sosyal mühendislik içeriğinin niteliğinin artmasını

sağlamaktadır. Savunma tarafında ise anomali tespiti, davranışsal analiz ve olay müdahalesinin otomasyonunda kullanılmaktadır. Kritik denge, tepki süresi üzerindedir: saldırı otomasyonu savunma otomasyonundan hızlı ilerlerse, insan operatörün karar döngüsü devre dışı kalır.

6.4. Savunma Mimarisi: Katmanlı ve Önceliklendirilmiş Yaklaşım

Enerji sektöründe siber savunma, bilgi teknolojisi dünyasından ödünç alınan yaklaşımların doğrudan uygulanmasıyla kurulamaz. Önceliklerin sırası farklıdır: bilgi teknolojisinde gizlilik-bütünlük-erişilebilirlik sıralaması geçerliyken, operasyonel teknolojide emniyet-erişilebilirlik-bütünlük-gizlilik sıralaması esastır. Bu farklılık, mimarinin tamamını şekillendirmelidir.

Tablo 6.1. Enerji Sektörü İçin Katmanlı Siber Savunma Mimarisi

Katman	Temel Tedbir	Referans Çerçeve
Yönetişim	Kritik varlık envanteri, risk sahipliğinin tanımlanması, yönetim kurulu seviyesinde raporlama	ISO 27001, NIS2, CER Direktifi
Mimari ayrım	Purdue modeline uygun bölgelendirme, DMZ, tek yönlü veri geçidi (data diode)	IEC 62443-3-3, NIST SP 800-82
Varlık görünürlüğü	Pasif ağ izleme, OT varlık envanteri, protokol seviyesinde derin paket incelemesi	IEC 62443-2-1
Erişim yönetimi	Ayrıcalıklı erişim yönetimi, çok faktörlü doğrulama, servis sağlayıcı erişiminin zaman sınırlı olması	Sıfır güven (zero trust) ilkeleri
Emniyet fonksiyonu ayrımı	SIS sistemlerinin DCS'ten fiziksel ve mantıksal ayrımı, yerel kilit mekanizmaları	IEC 61511
Tedarik zinciri	Yazılım malzeme listesi (SBOM), üretici güvenlik taahhütleri, donanım kökeni denetimi	Tasarımdan güvenli (secure by design)
Tespit ve müdahale	OT'ye özgü olay müdahale planı, 7/24 izleme, ulusal siber olay merkeziyle entegrasyon	Ulusal SOME/USOM yapısı
Dayanıklılık	Yedeklerin çevrimdışı saklanması, manuel işletim prosedürleri, kara başlatma tatbikatları	İş sürekliliği standartları
Tatbikat ve doğrulama	Kırmızı takım çalışmaları, masa başı senaryolar, sektörel ortak tatbikatlar	Sürekli iyileştirme döngüsü

6.5. Düzenleyici Çerçevenin Rolü

Avrupa Birliği'nde NIS2 Direktifi ve Kritik Varlıkların Dayanıklılığı Direktifi (CER), enerji operatörlerine bağlayıcı güvenlik yükümlülükleri getirmiştir. Bu düzenlemelerin ayırt edici özelliği, yönetim organlarını kişisel olarak sorumlu tutması ve olay bildirimini zorunlu kılmasıdır. Endüstriyel kontrol sistemleri için IEC 62443 standart ailesi ve Amerikan NIST SP 800-82 rehberi, denetlenebilir bir teknik taban sunmaktadır.

Düzenleyici yaklaşımın etkili olabilmesi için üç koşul gerekmektedir. Birincisi, uyumun belge düzeyinde değil saha düzeyinde denetlenmesidir; bir politika dokümanının varlığı, bir ağ segmentasyonunun varlığıyla aynı şey değildir. İkincisi, olay bildiriminin cezalandırıcı değil öğretici bir çerçevede yapılandırılmasıdır; aksi hâlde raporlama eksik kalır. Üçüncüsü, küçük ve orta ölçekli operatörler için uyum maliyetinin desteklenmesidir; dağıtık enerji varlıklarının çoğu, kurumsal siber güvenlik kapasitesine sahip olmayan işletmeler tarafından işletilmektedir.

7. DENİZ ALTI SİSTEMLER: HUKUKUN ULAŞAMADIĞI CEPHE

7.1. Stratejik Önem ve Yapısal Kırılganlık

Deniz tabanındaki altyapı, modern enerji ve iletişim sistemlerinin görünmeyen omurgasıdır. Denizaltı doğal gaz ve ham petrol boru hatları kıtalar arası tedariki, yüksek gerilim doğru akım enterkonektörleri bölgesel elektrik entegrasyonunu, veri kabloları ise küresel iletişimin ezici çoğunluğunu taşımaktadır. Bu varlıkların ortak özelliği, aşırı derecede uzun, izlenmesi güç ve fiziksel olarak korunması pratikte imkânsız olmalarıdır.

Kırılganlık üç yapısal etkenden kaynaklanmaktadır. Birincisi, korumasızlıktır: bir kablo veya boru hattı, deniz tabanında çıplak veya sığ gömülü olarak, herhangi bir fiziksel bariyer olmaksızın durmaktadır. İkincisi, izlenememesidir; binlerce kilometrelik güzergâhın sürekli gözetimi, mevcut teknolojilerle ekonomik olarak mümkün değildir. Üçüncüsü ise onarım darboğazıdır: dünya genelinde kablo onarımı yapabilen özel gemilerin sayısı sınırlıdır ve bir arızanın medyan onarım süresi kırk gün civarındadır. Hava koşulları, erişim kısıtları veya eşzamanlı olaylar bu süreyi uzatabilmektedir.

Bu üç etkenin üzerine, dördüncü ve belki de en belirleyici olanı eklenmelidir: inşa ile imha arasındaki maliyet makası. Bir denizaltı boru hattı veya yüksek gerilim doğru akım kablosu, özel döşeme gemileri, uzman mühendislik ekipleri ve aylar süren deniz operasyonlarıyla, yüz milyonlarca ila milyarlarca dolarlık bir yatırımla inşa edilir. Aynı hattı kalıcı olarak kullanılamaz hâle getirmek için gereken araç ise bundan kıyaslanamayacak ölçüde ucuzdur. Bu makas, sekizinci bölümde geliştirilen KEAGİ-T indeksinde denizaltı boru hatlarının ve HVDC enterkonektörlerinin neden en yüksek risk skorları arasında yer aldığını da açıklamaktadır.

7.2. Varlık Envanteri: Boru Hatları, Kuyu Başları ve Bağlantı Üniteleri

Deniz tabanı altyapısı, tek bir varlık türü değil, birbirine bağlı bir ekipman zinciridir. Zincirin görünür ucu ana boru hattıdır; ancak zincirin geri kalanı çoğu zaman kamuoyunun ve hatta genel güvenlik planlamasının dikkatinden kaçmaktadır.

- **Ana taşıma hatları (trunk lines):** Sahayı veya üretici ülkeyi tüketim noktasına bağlayan büyük çaplı boru hatlarıdır — Nord Stream, TürkAkım, Mavi Akım, Balticconnector bu kategoridedir. Yüksek kapasiteli ve tek noktadan çok miktarda akışı taşıdıkları için en yüksek stratejik değere sahiptirler.
- **Su altı kuyu başları ve ıslak ağaçlar (subsea trees):** Açık deniz platformu bulunmayan derin su sahalarında, her üretim kuyusunun deniz tabanında bulunan ve akışı, basıncı ve acil kapatmayı kontrol eden vana topluluğudur. Görünürlükleri çok düşüktür; bir sahada onlarca kuyu başı bulunabilir ve her biri, isabet alması hâlinde o kuyunun üretimini durdurabilecek bir tekil nokta oluşturur.
- **Manifoldlar ve toplama hatları:** Birden fazla kuyu başının üretimini tek bir hatta topladığı ünitelerdir. Bir manifoldun hasar görmesi, ona bağlı bütün kuyuların üretimini aynı anda durdurabilir; bu nedenle manifold, sahanın tamamı için orantısız bir kırılganlık merkezidir.
- **Umbilical hatlar:** Kuyu başlarına elektrik, hidrolik güç, kontrol sinyali ve kimyasal enjeksiyon taşıyan çok damarlı kablo-hortum demetleridir. Fiziksel olarak ince ve kırılgan olmalarına karşın, kesilmeleri hâlinde bağlı oldukları kuyu başının uzaktan kontrolünü tamamen ortadan kaldırırlar.
- **PLET/PLEM bağlantı üniteleri:** Boru hattı uçlarının deniz tabanında sonlandığı ve gelecekteki bağlantılara imkân tanıyan yapılardır; sistemin genişleme ve bakım esnekliğini sağlarken, aynı zamanda hattın en erişilebilir noktalarından birini oluştururlar.

Bu envanterin pratik sonucu, koruma önceliğinin yalnızca ana hatta değil, zincirin en zayıf ve en az korunan halkasına — çoğunlukla manifold veya kuyu başına — yönlendirilmesi gerektiğidir. Bir saldırganın ana hattı

vurmak için kat etmesi gereken mesafe ile bir kuyu başını vurmak için kat etmesi gereken mesafe birbirinden farklı olabilir; sahanın tamamının güvenliği, en kolay erişilebilir düğümün güvenliği kadardır.

7.3. Saldırı Yöntemleri: Çapa Sürükleme, Patlayıcı ve Su Altı Aracı Operasyonları

Deniz tabanı altyapısına yönelik saldırılar iki farklı imza taşımaktadır. Birinci imza, düşük yoğunluklu ve inkâr edilebilir yöntemdir: uluslararası sularda seyreden ticari bir gemi, çapasını deniz tabanında sürükleyerek kabloya veya boru hattına zarar verir; fiilin kasıtlı olduğunu ispatlamak hukuken son derece güçtür; onarım ise haftalar sürer. Ekim 2023 ile 2025 sonu arasında bu yöntemle Baltık havzasında en az on bir kablonun hasar gördüğü değerlendirilmektedir. Yöntemin çekiciliği, maliyetinin düşüklüğünde ve inkâr edilebilirliğinin yüksekliğindedir: denizcilikte çapa kaybı ve sürüklenmesi bilinen bir kaza türü olduğu için, her olay teknik olarak kaza açıklamasıyla savunulabilir. Yaptırım rejimlerini dolanmak için kullanılan, bayrak ve sigorta yapıları belirsiz gölge filo gemileri bu belirsizliği derinleştirmektedir; Finlandiya'nın Aralık 2024'te el koyduğu tankerin bu kategoride değerlendirilmesi, olayların tesadüfi olmadığı yönündeki kanaati güçlendirmiştir.

İkinci imza ise çok daha yüksek yoğunluklu ve doğrudan kinetiktir: bir dalgıç ekibi veya su altı aracı tarafından yerleştirilen şekilli patlayıcı yükü. Bu yöntem inkâr edilebilirlik sunmaz — patlama izleri kaza açıklamasıyla bağdaştırılamaz — ancak buna karşılık saniyeler içinde, tamiri aylar sürecek bir hasar üretir. İki yöntem arasındaki seçim, saldırganın gizlilik ile kesinlik arasında yaptığı bir tercihi yansıtmaktadır: çapa sürükleme daha yavaş ve daha az kesin ama inkâr edilebilir bir sonuç verirken, patlayıcı operasyonu daha hızlı ve daha kesin ama açıkça saldırı olarak okunan bir sonuç verir. Bir sonraki alt bölüm, bu iki yöntemin de aynı coğrafyada, birbirine bağlı olaylar zincirinde nasıl bir arada kullanıldığını incelemektedir.

7.4. Vaka: Kuzey Akım'dan TürkAkım'a Uzanan Hat

26 Eylül 2022'de Bornholm adası açıklarında, Baltık Denizi'nin tabanında dört ayrı patlama meydana geldi. Patlamalar, Rusya'dan Almanya'ya gaz taşıyan Kuzey Akım 1 ve Kuzey Akım 2 boru hatlarının üç ayrı noktasını tahrip etti. İnşası on milyar avroyu aşan ve Gazprom'un yanı sıra Almanya (E.ON, Wintershall), Hollanda (Gasunie) ve Fransa (Engie) menşeli hissedarları da bulunan bu ikiz hat sistemi günlerce doğal gaz sızdırdı; sızıntının oluşturduğu gaz kabarcıkları, deniz yüzeyinde geniş çaplı kaynayan alanlar hâlinde uydu ve hava görüntülerine yansıdı. Danimarka, İsveç ve Almanya makamlarının ayrı ayrı yürüttüğü soruşturmalar, olayın kasıtlı sabotaj olduğunu ve borularda patlayıcı izlerine rastlandığını doğruladı; ancak İsveç ve Danimarka soruşturmaları, uluslararası sularda yetki yetersizliği gerekçesiyle fail tespit edilmeden Şubat 2024'te kapatıldı.

Sabotajın icra biçimi, bu raporun merkezî tezini — inşa ile imha arasındaki maliyet makasını — en çarpıcı biçimde örneklemektedir. On milyar avroyu aşan bir altyapıyı kalıcı olarak devre dışı bırakan operasyon, gazetecilik araştırmalarına göre altı kişilik bir mürettebatın kiraladığı küçük bir yelkenli tekne ve yaklaşık üç yüz bin dolarlık bir bütçeyle icra edilmiştir. Rostock'tan kiralanan "Andromeda" adlı teknede bir kaptan, dalgıçlar ve destek personeli yer almış; ekip, boru hatlarının üzerinde patlayıcı yerleştirmiş ve haftalar içinde limana dönmüştür. Aradaki oran — yüz milyonda birin altında bir operasyon maliyetiyle milyarlarca avroluk bir altyapının kalıcı olarak devre dışı bırakılması — bu raporun beşinci bölümünde tartışılan maliyet asimetrisinin somut, doğrulanmış bir vakasıdır.

Olayın failine dair somut bir gelişme, neredeyse üç yıl sonra, sabotajla doğrudan bağlantısı olmayan bir ülkenin istihbarat çalışması sayesinde geldi. Almanya Federal Başsavcılığı, Kuzey Akım sabotajının baş şüphelisi olarak eski bir Ukraynalı asker hakkında savaş suçu kapsamında iddianame hazırladı. "Kaptan" kod adıyla anılan şüpheli, 21 Ağustos 2025'te İtalya'da yakalandı ve 27 Kasım 2025'te Almanya'ya iade edildi; ancak gerçek kimliği uzun süre çözülemedi. Kimliğin nihayet ortaya çıkarılması, Türk istihbarat ve emniyet

birimlerinin yaptığı biyometrik incelemeyle mümkün oldu — bu da Kuzey Akım dosyasını, ilk bakışta uzak görünen bir bağlantıyla Türkiye'nin gündemine taşıdı.

Bağlantı, kimlik tespitinden ibaret kalmadı. Soruşturma dosyasına göre aynı şüphelinin ekibi, Romanya'dan kiraladığı bir yelkenli tekneyle Karadeniz'deki TürkAkım boru hattını da hedef alan sabotaj girişimlerinde bulunmuş, ancak bu girişimler başarısızlıkla sonuçlanmıştır. Bu, Nord Stream ile TürkAkım'ı aynı operasyonel zihniyetin, hatta aynı bireyin hedefleri olarak birbirine bağlayan, kamuya yansımış nadir vakalardan biridir: bir denizaltı boru hattına yönelik sabotaj kapasitesinin, tek bir olayla sınırlı kalmadığı, farklı denizlerde, farklı hatlara karşı tekrarlanabilir bir yetenek olarak var olduğu görülmüştür.

TürkAkım ve Mavi Akım, bu tekil girişimin ötesinde, 2025-2026 döneminde sistematik bir baskı altında kaldı. Ocak 2025'te Rusya Savunma Bakanlığı, Ukrayna'nın TürkAkım'ı besleyen Rusya tarafındaki Russkaya kompresör istasyonuna insansız hava aracıyla saldırı girişiminde bulunduğunu, hava savunma sistemlerinin bu girişimi etkisiz hâle getirdiğini açıkladı. 24 Şubat 2026'da Putin, FSB kurul toplantısında yaptığı konuşmada, "Karadeniz'in dibindeki gaz sistemlerimizde olası bir patlamaya ilişkin bilgiler alıyoruz" diyerek TürkAkım ve Mavi Akım'ın su altı kesimine yönelik bir sabotaj girişimine dair istihbarat edindiklerini kamuoyuyla paylaştı — bu kez hedef gösterilen, kıyıdaki kompresör istasyonu değil, boru hattının bizzat deniz tabanındaki kendisiydi. Birkaç hafta sonra Gazprom, son iki hafta içinde TürkAkım ve Mavi Akım'ı besleyen tesislere yönelik toplam on iki saldırı girişimi tespit edildiğini açıkladı. Nisan başında Rusya'nın Ankara Büyükelçiliği, Russkaya istasyonunun bu kez üç insansız hava aracıyla yeniden hedef alındığını, saldırının hava savunma sistemleri ve mobil operasyon gruplarının ortak müdahalesiyle püskürtüldüğünü ve tesise zarar verilmediğini duyurdu.

Bu vakalar zincirinin Türkiye açısından taşıdığı anlam açıktır. TürkAkım'ın Karadeniz'deki su altı kesimi, ne üretim ne tüketim ucu Türk toprağında olan, ancak arızası doğrudan Türkiye'nin gaz arzını etkileyecek bir varlıktır; hattın güvenliği, dokuzuncu bölümde ayrıntılı ele alınacağı gibi, Türkiye'nin doğrudan kontrol yetkisinin sınırlı olduğu bir coğrafyada, üçüncü tarafların istihbarat ve karşı-sabotaj kapasitesine de bağımlıdır. Kuznietsov vakasında olduğu gibi, tehdidin nihai olarak etkisiz kılınması bazen saldırıya uğrayan ülkenin değil, üçüncü bir ülkenin (bu örnekte Türkiye'nin) istihbarat kapasitesi sayesinde gerçekleşmiştir; bu da deniz tabanı güvenliğinin neden ulusal değil bölgesel bir işbirliği çerçevesinde ele alınması gerektiğinin somut bir kanıtıdır.

7.5. Hukuki Boşluk

Birleşmiş Milletler Deniz Hukuku Sözleşmesi, deniz altı kablolarının kasten veya ihmalen zarar görmesini suç olarak tanımlamakta ve taraf devletlere kendi bayraklarını taşıyan gemiler ile vatandaşları hakkında cezai düzenleme yapma yükümlülüğü getirmektedir. Ancak bu hükümler üç noktada yetersiz kalmaktadır.

- **Yargı yetkisi:** Münhasır ekonomik bölgede veya açık denizde meydana gelen olaylarda, yetki esas olarak bayrak devletindedir. Bayrak devleti işbirliği yapmıyorsa, kıyı devletinin elinde etkili bir araç kalmamaktadır.
- **Durdurma ve ziyaret yetkisi:** Yabancı bayraklı bir gemiyi uluslararası sularda durdurma ve gemiye çıkma yetkisi son derece sınırlıdır. NATO Baltic Sentry operasyonu kapsamında yapılan değerlendirmeler, bu hukuki sınırın operasyonun en önemli kısıtlarından biri olduğuna işaret etmektedir.
- **İspat standardı:** Kasıt unsurunun ispatı, çoğu olayda mümkün olmamaktadır. Kasıtlı zarar ile denizcilik ihmali arasındaki ayrım, adli soruşturmaların çoğunda belirsiz kalmaktadır.

Bu boşluk karşısında iki yaklaşım tartışılmaktadır. Birincisi, mevcut sözleşme hükümlerinin kıyı devleti lehine daha geniş yorumlanması ve kritik altyapı koruma bölgelerinin tanımlanmasıdır. İkincisi, kablolara

ve boru hatlarına yönelik saldırıların ayrı bir uluslararası rejim altında düzenlenmesidir. Her iki yaklaşım da, geniş bir devlet koalisyonu gerektirdiği için kısa vadede sonuç vermesi güç seçeneklerdir.

7.6. Yanıt Mimarisi

Kurumsal yanıtlar, 2024 sonrası dönemde hızlanmıştır. NATO, Ocak 2025'te Baltic Sentry operasyonunu başlatmış; fırkateynler, deniz karakol uçakları ve insansız deniz araçları bölgeye konuşlandırılmıştır. Birleşik Krallık öncülüğünde yürütülen Nordic Warden girişimi, şüpheli gemilerin izlenmesine odaklanmaktadır. Avrupa Komisyonu'nun Şubat 2026'da açıkladığı 347 milyon euroluk paket ve Kablo Güvenliği Araç Kutusu, yatırım ile koordinasyon mekanizmalarını birleştirmektedir.

Operasyonel etkinlik açısından belirleyici olan dört yetenek öne çıkmaktadır:

1. **Deniz tabanı durumsal farkındalığı:** Sabit sensör ağları, dağıtık akustik algılama teknolojileri ve otonom su altı araçlarıyla güzergâh boyunca sürekli veya periyodik izleme.
2. **Yüzey trafiği analitiği:** Otomatik tanımlama sistemi verilerinin makine öğrenmesiyle analiz edilerek olağandışı seyir örüntülerinin (yavaşlama, dolaşma, güzergâh üzerinde durma) gerçek zamanlı tespiti.
3. **Hızlı onarım kapasitesi:** Modüler onarım ekipmanının bölgesel limanlarda önceden konumlandırılması ve onarım gemisi kapasitesinin bölgesel paylaşım anlaşmalarıyla güvence altına alınması.
4. **Yedeklilik tasarımı:** Kritik bağlantılarda tek kablo bağımlılığının ortadan kaldırılması; coğrafi olarak ayrık güzergâhlarda ikinci ve üçüncü hatların planlanması.

Bu yeteneklerin hiçbiri tek başına yeterli değildir. Caydırıcılık, izleme kapasitesi ile hukuki müdahale yetkisinin birlikte mevcut olmasına bağlıdır; izleyip müdahale edemeyen bir sistem, yalnızca olayları belgelemiş olur.

7.7. Doğu Akdeniz: Maliyet Asimetrisi ve Yatırım Güvenliği

Baltık'ta geliştirilen yanıt mimarisinin Doğu Akdeniz'e doğrudan aktarılması sınırlıdır. Bölgedeki deniz yetki alanlarına ilişkin uyuşmazlıklar, ortak izleme ve müdahale mekanizmalarının kurulmasını siyasal olarak güçleştirmektedir; Baltık'ta NATO üyeliğinin sağladığı ortak hukuki ve operasyonel zemin, Doğu Akdeniz'de bulunmamaktadır. Buna ek olarak bölgedeki altyapı yoğunluğu hızla artmaktadır: mevcut ve planlanan doğal gaz hatları, elektrik enterkonektör projeleri ve veri kabloları aynı dar koridorlarda kesişmekte, bu da tek bir olayın çoklu sistem etkisi üretme olasılığını yükseltmektedir. Bölgedeki derin su koşulları ise onarım operasyonlarını teknik olarak daha güç ve daha pahalı kılmaktadır.

Bu tabloya yedinci bölümün merkezî bulgusu olan maliyet asimetrisi eklendiğinde, Doğu Akdeniz'deki yatırım güvenliği sorunu farklı bir boyut kazanmaktadır. Bölgedeki büyük ölçekli projeler — Yunanistan, Kıbrıs ve İsrail'i bağlayan Great Sea Interconnector'ın ilk aşaması yaklaşık iki milyar avroya, bölgedeki entegre doğal gaz sahası geliştirmeleri ve ihraç altyapısı ise toplamda kolaylıkla on milyar doları aşan bir sermayeye mal olmaktadır. Bu ölçekte bir yatırımı fiilen kullanılamaz hâle getirmek için gereken araç, ticari ölçekli bir çalışma sınıfı su altı aracı (ROV) veya benzer bir insansız su altı platformudur. Piyasadaki ROV'lar birkaç bin dolarlık gözlem sınıfı modellerden, en uç bilimsel derin deniz araçlarında onlarca milyon dolara kadar geniş bir yelpazeye yayılmaktadır; ancak bir boru hattı vanasını veya bağlantı ünitesini fiziksel olarak devre dışı bırakmaya yetecek iş sınıfı (work-class) bir aracın piyasa fiyatı, çoğunlukla birkaç yüz bin ile birkaç milyon dolar arasında kalmaktadır. On milyar dolarlık bir yatırımın, kendi maliyetinin binde biri ila on binde biri mertebesinde bir harcamayla etkisiz kılınabilmesi, klasik yatırım risk analizinin alışık olmadığı bir asimetridir.

Bu asimetrinin siyasi sonucu, ihtilaflı sınırlarda artık “oldu bittiye getirilmiş” bir yatırımın güvenli sayılamayacağıdır. Yirminci yüzyılın enerji jeopolitiğinde, bir devlet tartışmalı bir deniz alanında fiilî yatırım yaparak kendi lehine bir statüko yaratabilirdi; sondaj platformunun veya boru hattının varlığı, zamanla bir kabul edilmişlik kazanırdı. Su altı sabotaj kapasitesinin bu denli ucuzlaması, bu stratejiyi geçersiz kılmaktadır. Deniz yetki alanı anlaşmazlığı çözülmeden inşa edilen bir boru hattı veya enterkonektör, taraflardan biri için yalnızca siyasi değil, aynı zamanda fiziksel olarak da geri döndürülebilir bir yatırımdır; sınır anlaşmazlığının çözümsüz kaldığı bir hatta yapılacak tahribat, klasik anlamda bir savaş eylemi olarak dahi okunmayabilir, çünkü saldıran taraf kendi egemenlik iddiasını ihlal eden bir tesisi ortadan kaldırdığını öne sürebilir. Bu nedenle Doğu Akdeniz’de deniz yetki alanı müzakereleri tamamlanmadan yapılacak büyük ölçekli sabit yatırımlar, teknik ve ticari risklerin ötesinde, kalıcı bir güvenlik riski taşımaktadır.

8. TESPAM KRİTİK ENERJİ ALTYAPISI GÜVENLİK İNDEKSİ (KEAGİ)

8.1. İndeksin Amacı ve Sınırları

Enerji altyapısı güvenliğine ilişkin değerlendirmeler, çoğunlukla niteliksel ve karşılaştırılamaz biçimde üretilmektedir. Bir bölgenin "riskli" olduğunu söylemek, kaynak tahsisi kararı almak için yeterli bilgi sağlamaz. TESPAM Kritik Enerji Altyapısı Güvenlik İndeksi (KEAGİ), bu boşluğu doldurmak üzere geliştirilmiş, çok ölçütlü bir konumlandırma aracıdır.

İndeksin ne olduğu kadar ne olmadığının da açıkça belirtilmesi gerekir. KEAGİ, belirli bir dönemde belirli bir varlığın saldırıya uğrama olasılığını tahmin eden bir öngörü modeli değildir. Böyle bir model, düşman niyetine ilişkin gözlenemeyen değişkenlere bağımlı olacağı için yanıltıcı bir kesinlik duygusu üretirdi. İndeks, göreli bir konumlandırma sunar: hangi bölgenin veya varlık türünün, hangi bölgeye veya türe kıyasla daha yüksek yapısal risk taşıdığını gösterir. Kullanım amacı, koruma yatırımlarının ve politika dikkatinin önceliklendirilmesidir.

8.2. Metodoloji ve Bileşenler

İndeks, 0 ile 100 arasında bir bileşik skor üretmektedir; yüksek skor, yüksek risk anlamına gelir. Bölgesel indeks (KEAGİ-B) altı bileşen üzerine kuruludur. Her bileşen, kendi içinde 0-100 arasında puanlanmakta ve ağırlıklandırılmış toplamla bileşik skor elde edilmektedir.

Tablo 8.1. KEAGİ-B Bileşenleri, Ağırlıkları ve Göstergeleri

Bileşen	Ağırlık	Ölçtüğü Olgu	Başlıca Göstergeler
TY — Tehdit Yoğunluğu ve Aktör Kapasitesi	%25	Bölgede enerji altyapısını hedef alabilecek aktörlerin varlığı, menzili ve eylem sıklığı	Son 36 ayda kaydedilen saldırı sayısı; aktif çatışma varlığı; devlet dışı aktörlerin menzil kabiliyeti
Hİ — Hedef Değeri ve İkame Edilemezlik	%20	Bölgedeki varlıkların küresel/bölgesel arz içindeki ağırlığı ve yerine konulabilirliği	Bölgenin küresel arz payı; geçiş noktası niteliği; alternatif güzergâh varlığı
SZ — Savunma Zafiyeti	%15	Fiziksel ve siber koruma kapasitesinin yetersizlik derecesi (ters kodlanmış)	Hava savunma yoğunluğu; deniz gözetim kapasitesi; OT güvenlik olgunluğu
OZ — Onarım ve Yeniden Tesis Zafiyeti	%15	Hasar sonrası işlevin yeniden kazanılma süresindeki yetersizlik	Yedek parça stoku; mühendislik kapasitesi; yaptırım kaynaklı tedarik kısıtı
YZ — Yönetişim ve Mevzuat Zafiyeti	%10	Kritik altyapı korumasına ilişkin kurumsal ve hukuki çerçevenin olgunluk eksikliği	Müstakil mevzuat varlığı; kurumlar arası eşgüdüm; operatör yükümlülükleri; denetim
YE — Sistemik Yayılım Etkisi	%15	Bölgedeki bir kesintinin diğer sistemlere ve piyasalara yayılma derecesi	Sektörler arası bağımlılık; piyasa fiyat duyarlılığı; ikincil etkilenen ülke sayısı

Bileşen puanları, kamuya açık olay veri tabanları, uluslararası kuruluş raporları, sektörel teknik değerlendirmeler ve TESPAM uzman paneli tarafından yapılan yapılandırılmış değerlendirmeler esas alınarak belirlenmiştir. Ağırlıklandırma, bileşenlerin karar alıcı açısından eylem yaratma potansiyeline göre yapılmıştır: tehdit yoğunluğu en yüksek ağırlığı almakta, çünkü diğer bileşenlerin tamamı ancak gerçek bir tehdidin varlığında anlam kazanmaktadır.

Tablo 8.2. KEAGİ Risk Bantları

Bant	Skor Aralığı	Tanım	Politika Çıkarımı
Kritik	80-100	Altyapı fiilen çatışmanın hedefi durumunda	Acil koruma ve tahliye planlaması; yatırım kararlarının askıya alınması

Bant	Skor Aralığı	Tanım	Politika Çıkarımı
Yüksek	70-79	Saldırı gerçekleşmiş veya yüksek olasılıklı	Aktif koruma yatırımı; yedeklilik ve stok zorunluluğu
Yüksek-Orta	60-69	Yapısal maruziyet mevcut, tetikleyici konjonktürel	Senaryo planlaması; kritik varlık haritalaması; tatbikat
Orta	50-59	Sınırlı maruziyet, güçlü kurumsal kapasite	Standart uyum; periyodik gözden geçirme
Düşük-Orta	0-49	Düşük tehdit veya yüksek dayanıklılık	İzleme ve erken uyarı yeterli

8.3. Bölgesel Risk İndeksi (KEAGİ-B 2026)

Tablo 8.3. Bölgesel Kritik Enerji Altyapısı Güvenlik İndeksi, Eylül 2026

Sıra	Bölge	TY	Hİ	SZ	OZ	YZ	YE	KEAGİ	Bant
1	Basra Körfezi – Hürmüz	98	96	68	60	50	98	**83**	Kritik
2	Kızıldeniz – Bab-el Mendeb	92	85	78	75	70	88	**83**	Kritik
3	İran	90	85	80	85	70	78	**83**	Kritik
4	Avrupa Rusyası (rafineri kuşağı)	96	88	72	78	60	82	**82**	Kritik
5	Ukrayna	95	78	75	82	55	80	**80**	Kritik
6	Irak	82	68	88	85	90	70	**80**	Kritik
7	Karadeniz havzası	80	75	62	68	58	78	**72**	Yüksek
8	Libya ve Kuzey Afrika	75	58	85	82	88	55	**72**	Yüksek
9	Batı Afrika (Nijer Deltası)	72	52	82	78	85	48	**68**	Yüksek-Orta
10	Türkiye	68	78	55	58	60	72	**66**	Yüksek-Orta
11	Doğu Akdeniz	62	70	60	70	65	72	**66**	Yüksek-Orta
12	Baltık Denizi	78	62	52	65	40	68	**64**	Yüksek-Orta
13	Doğu Asya (Tayvan – G. Çin Denizi)	58	82	50	55	45	85	**64**	Yüksek-Orta
14	Latin Amerika	58	48	78	82	80	52	**64**	Yüksek-Orta
15	Kafkasya – Hazar	62	68	58	62	55	65	**62**	Yüksek-Orta
16	Güney ve Güneydoğu Asya	48	58	62	65	60	60	**58**	Orta
17	Kuzey Denizi – Norveç	58	78	42	48	30	72	**57**	Orta
18	Orta ve Batı Avrupa (kara)	52	62	45	52	35	70	**54**	Orta
19	Kuzey Amerika	45	60	42	45	32	68	**50**	Orta

Kaynak: TESPAM hesaplaması. Bileşen kısaltmaları için bkz. Tablo 8.1. Skorlar Eylül 2026 itibarıyla geçerli olup konjonktürel değişimlere duyarlıdır.

Tablonun en dikkat çekici bulgusu, ilk altı sıranın tamamının birbiriyle bağlantılı bir çatışma kümesine ait olmasıdır. Basra Körfezi, Kızıldeniz, İran ve Irak, 2026 savaşının doğrudan sahnesidir; Rusya ve Ukrayna ise ayrı bir çatışmanın taraflarıdır. İki çatışmanın eşzamanlılığı, küresel enerji sisteminin iki ayrı yerden aynı anda baskı altına alınması anlamına gelmektedir ve bu, 1970'lerden bu yana görülmemiş bir yoğunlaşmadır.

İkinci bulgu, yönetişim bileşeninin ayırt edici gücüdür. Irak ve Libya, tehdit yoğunluğu açısından bazı bölgelerin gerisinde olmalarına rağmen, kurumsal kapasite ve mevzuat zafiyeti nedeniyle üst sıralarda yer almaktadır. Buna karşılık Kuzey Denizi ve Batı Avrupa, hedef değeri yüksek olmasına rağmen güçlü kurumsal çerçeveleri sayesinde orta banda yerleşmektedir. Bu, korumanın yalnızca askerî değil, aynı zamanda idari bir kapasite meselesi olduğunun sayısal ifadesidir.

Üçüncü bulgu, Baltık Denizi'nin konumudur. Bölge, tehdit yoğunluğu açısından yüksek puan almakta, ancak güçlü yönetişim ve savunma kapasitesi nedeniyle bileşik skoru sınırlı kalmaktadır. Bu, gri bölge saldırılarının kurumsal dayanıklılıkla dengelenebileceğini göstermektedir. Aynı tehdit profilinin zayıf kurumsal kapasiteye sahip bir bölgede çok daha yüksek bir skor üreteceği açıktır.

8.4. Altyapı Türü Bazlı Risk İndeksi (KEAGİ-T 2026)

Bölgesel indeks, coğrafi önceliklendirme sağlar; ancak koruma yatırımının hangi varlık türüne yöneleceği sorusuna cevap vermez. Bu nedenle, altyapı türlerine özgü ikinci bir indeks geliştirilmiştir. KEAGİ-T, altı bileşen kullanmaktadır: maruziyet (%25), hedef cazibesi ve stratejik değer (%20), savunulabilirlik zafiyeti (%15), onarım süresi ve yedek parça darboğazı (%20), ikame edilemezlik (%10) ve sistemik yayılım (%10). Onarım bileşeninin ağırlığının bölgesel indekse kıyasla yükseltilmesi, dördüncü bölümde tartışılan "onarım döngüsünün savaş alanı olması" bulgusunun doğrudan yansımasıdır.

Tablo 8.4. Altyapı Türü Bazlı Güvenlik Risk İndeksi, Eylül 2026

Sıra	Altyapı Türü	Maruziyet	Hedef Cazibesi	Savunulabilirlik Zafiyeti	Onarım Darboğazı	İkame Edilemezlik	Yayılım	KEAGİ-T
1	Rafineri ve petrokimya	95	90	75	80	70	78	**84**
2	LNG sıvılaştırma tesisi	70	92	68	95	92	85	**83**
3	Pompa ve kompresör istasyonu	88	85	78	75	82	88	**83**
4	Yüksek gerilim trafo merkezi	72	82	72	92	80	92	**81**
5	Denizaltı boru hattı	68	80	90	85	88	82	**80**
6	İhraç terminali ve liman	82	88	70	62	75	90	**78**
7	HVDC enterkonektör	72	72	88	78	65	80	**76**
8	OT / SCADA kontrol katmanı	90	85	85	45	55	92	**76**
9	Deniz altı veri kablosu	85	62	92	70	55	72	**74**
10	Nükleer santral	35	95	55	95	95	95	**74**
11	Yer üstü akaryakıt deposu	88	72	82	55	50	62	**71**
12	Tanker ve deniz taşımacılığı	85	78	80	40	45	85	**70**
13	Açık deniz platformu	60	72	75	78	70	65	**70**
14	Yeraltı doğal gaz depolama	42	68	45	55	72	78	**57**
15	Dağıtık YEK ve batarya varlıkları	55	48	78	35	25	45	**49**

Kaynak: TESPAM hesaplaması. Nükleer santrallerin düşük maruziyet-çok yüksek sonuç profili, bileşik skorun tek başına yeterli olmadığı, bant analizinin de değerlendirilmesi gerektiğine örnek teşkil etmektedir.

Tablo, koruma yatırımı açısından üç önemli sonuç üretmektedir. Birincisi, ilk beş sıradaki varlıkların hiçbiri, klasik güvenlik anlayışının odaklandığı "sınır bölgesi tesisi" kategorisine girmemektedir; bunlar, ülke içinde, çoğunlukla sanayi bölgelerinde konumlanmış varlıklardır. İkincisi, LNG sıvılaştırma ve trafo merkezlerinin üst sıralarda yer almasının temel nedeni maruziyet değil, onarım darboğazıdır; bu, koruma bütçesinin bir kısmının stok ve tedarik zinciri güvencesine ayrılması gerektiğini göstermektedir. Üçüncüsü, dağıtık yenilenebilir varlıkların en düşük skoru alması, enerji dönüşümünün güvenlik açısından net bir kazanım

sunduğunu ortaya koymaktadır — ancak bu kazanım, siber yönetişim zafiyeti giderilmediği takdirde erozyona uğrayacaktır.

8.5. Bölge-Varlık Kesişim Matrisi: Sıcak Noktalar

İki indeksin kesişimi, kaynak tahsisinde en yüksek getiriyi sağlayacak noktaları görünür kılmaktadır. Aşağıdaki matris, seçilmiş bölgeler ile varlık türlerinin kesişiminde beklenen risk seviyesini göstermektedir.

Tablo 8.5. Bölge × Varlık Türü Risk Matrisi

Bölge	Rafineri	Boru hattı/istasyon	Deniz altı sistem	LNG	Trafo merkezi	Liman/terminal
Basra Körfezi – Hürmüz	Kritik	Yüksek	Yüksek	Kritik	Yüksek	Kritik
Kızıldeniz – Bab-el Mendeb	Yüksek	Kritik	Yüksek	Yüksek	Orta	Kritik
Avrupa Rusyası	Kritik	Kritik	Yüksek	Yüksek	Yüksek	Yüksek
Ukrayna	Yüksek	Yüksek	Orta	Orta	Kritik	Yüksek
İran	Kritik	Kritik	Orta	Kritik	Yüksek	Yüksek
Karadeniz havzası	Orta	Kritik	Yüksek	Orta	Orta	Yüksek
Doğu Akdeniz	Orta	Yüksek	Kritik	Yüksek	Orta	Yüksek
Baltık Denizi	Düşük	Orta	Kritik	Orta	Orta	Orta
Türkiye	Yüksek	Yüksek	Yüksek	Yüksek	Yüksek	Kritik
Doğu Asya	Düşük	Orta	Yüksek	Yüksek	Orta	Yüksek

8.6. En Yüksek Riskli Varlık ve Düğüm Noktaları

İndeksin operasyonel karşılığı, somut varlıklar düzeyinde önceliklendirmedir. Aşağıdaki liste, küresel enerji sisteminin bütünlüğü açısından en kritik ve aynı zamanda en maruz düğüm noktalarını sıralamaktadır. Sıralama, varlığın devre dışı kalması hâlinde küresel arz üzerinde yaratacağı etki ile mevcut tehdit maruziyetinin birleşiminden üretilmiştir.

Tablo 8.6. Küresel Öncelikli On Beş Kritik Düğüm (Eylül 2026)

#	Varlık / Düğüm	Ülke-Bölge	Kritiklik Gerekçesi
1	Hürmüz Boğazı geçişi	İran/Umman	Küresel petrol ticaretinin beşte biri; LNG için pratik alternatifsizlik
2	Doğu-Batı (Petroline) Boru Hattı	Suudi Arabistan	Hürmüz baypas kapasitesinin tamamına yakını; pompa istasyonları hedef alındı
3	Ras Laffan LNG kompleksi	Katar	Küresel LNG arzının büyük dilimi; yeniden inşa süresi yıllarla ölçülür
4	Abkaik işleme tesisi	Suudi Arabistan	Dünyanın en büyük ham petrol istikrar tesisi; 2019 emsali mevcut
5	Bab-el Mendeb geçişi	Yemen/Cibuti	Süveyş koridorunun güney kapısı; kıyı kontrolü el değiştirdi
6	Güney Pars / Kuzey Kubbe sahası	İran/Katar	Dünyanın en büyük gaz sahası; ortak rezervuar riski
7	Novorossiysk – Şeşharis terminali	Rusya	Karadeniz ham petrol ve ürün ihracının ana kapısı
8	Russkaya kompresör istasyonu	Rusya	TürkAkım ve Mavi Akım besleme noktası; tekrarlanan İHA girişimleri
9	Tengiz – Novorossiysk (CPC) hattı	Kazakistan/Rusya	Hazar üretiminin ana tahliye güzergâhı; pompa istasyonu saldırıları
10	Ceyhan terminal kompleksi	Türkiye	BTC ve Irak-Türkiye hatlarının ortak çıkışı; bölgesel güvenli liman işlevi
11	Kirişi rafinerisi	Rusya	Ülkenin en büyük dizel üreticilerinden; tamamen devre dışı

#	Varlık / Düğüm	Ülke-Bölge	Kritiklik Gerekçesi
12	Omsk rafinerisi	Rusya	Sibirya'daki en büyük tesis; menzil eşiğinin aşıldığının kanıtı
13	Baltık enterkonektör kümesi	Finlandiya/Estonya	Estlink hatları ve paralel veri kabloları; tekrarlanan kesintiler
14	Malakka Boğazı geçişi	Malezya/Endonezya	Asya'ya yönelik akışın ana darboğazı; henüz hedef alınmadı
15	Süveyş Kanalı ve SUMED hattı	Mısır	Kızıldeniz-Akdeniz bağlantısı; Bab-el Mendeb riskine bağımlı

Listenin ilk on sırasında yer alan varlıkların sekizi, doğrudan veya dolaylı olarak 2026 çatışmalarının etki alanındadır. Bu yoğunlaşma, küresel enerji sisteminin coğrafi risk dağılımının ne kadar dengesiz olduğunu göstermektedir. Malakka Boğazı gibi henüz hedef alınmamış düğümlerin listede yer alması ise, öngörücü planlamanın gerekliliğine işaret etmektedir: bir varlığın geçmişte hedef alınmamış olması, gelecekte alınmayacağı anlamına gelmemektedir.

9. TÜRKİYE: TRANSİT ÜLKENİN ÇİFT YÖNLÜ MARUZİYETİ

9.1. Yapısal Konum: Avantajın Maliyeti

Türkiye'nin enerji jeopolitiğindeki konumu, uzun süredir bir avantaj olarak tanımlanmıştır. Ülke, Rus gazını Avrupa'ya taşıyan TürkAkım ile Rusya'yı baypas eden Azerbaycan kaynaklı TANAP ve Bakü-Tiflis-Ceyhan hatlarını aynı anda barındıran tek ülkedir.

Bakü-Tiflis-Ceyhan Boru Hattı, yıllık elli milyon ton kapasitesiyle Hazar petrolünü Rusya ve İran dışındaki bir güzergâhtan küresel piyasalara ulaştırmakta; Irak-Türkiye Ham Petrol Boru Hattı, Kerkük çevresindeki üretimi Akdeniz'e taşımaktadır. Doğal gazda Mavi Akım yıllık on altı, TürkAkım ise iki hatla toplam otuz bir buçuk milyar metreküp kapasite sunmakta; Bakü-Tiflis-Erzurum hattı yaklaşık yirmi dört milyar metreküplük Güney Gaz Koridoru bağlantısını sağlamaktadır.

2026 krizi, bu konumun ikinci yüzünü görünür kılmıştır. Hürmüz kaynaklı kesintiler sonrasında Türkiye'nin çeşitlendirilmiş tedarik yapısı arz güvenliğini korumuş; Ceyhan, bölgesel ölçekte bir "güvenli liman" kimliği kazanmıştır. Ancak aynı dönemde TürkAkım ve Mavi Akım'ı besleyen Russkaya kompresör istasyonuna yönelik tekrarlanan insansız hava aracı saldırısı girişimleri, Türkiye'nin arz güvenliğinin kendi sınırları dışındaki bir tesisin korunabilmesine bağlı olduğunu göstermiştir. Rusya Savunma Bakanlığı, Mart 2026'da TürkAkım ve Mavi Akım'ı besleyen tesislere yönelik saldırı girişimlerini duyurmuş; Nisan başında yeni bir girişimi açıklamış; Gazprom, bu hatlara bağlı tesislerin iki hafta içinde on iki kez hedef alındığını bildirmiştir. Şubat 2026 sonunda ise üç sabit kanatlı insansız hava aracının Russkaya istasyonunun altyapısını hedef aldığı, saldırının Avrupa'ya gaz tedarikini durdurma amacı taşıdığı ifade edilmiştir.

Transit ülke konumunun stratejik bedeli budur: Türkiye, kendisi savaşan taraf olmasa dahi, başkalarının çatışmalarında hedef kümesinin bir parçası hâline gelmektedir. Bu durum, transit gelirlerinin sürdürülebilirliğini, tedarik güvenilirliğini ve ülkenin enerji merkezi iddiasını doğrudan etkilemektedir.

9.2. Türkiye'nin Maruziyet Profili: Üç Kırılganlık Kümesi

9.2.1. Transit ve Bağlantı Kırılganlığı

Türkiye'nin enerji altyapısı, ülke içinde başlayıp biten kapalı bir sistem değildir. Gaz arzı, komşu ülkelerdeki ve hatta ikinci derece komşulardaki tesislerin çalışmasına bağlıdır. Rus gazının Türkiye'ye ulaşması için Krasnodar'daki kompresör istasyonlarının çalışması; Azerbaycan gazının ulaşması için Gürcistan üzerindeki hat kesiminin güvenliği; Irak petrolünün Ceyhan'a akması için hattın Irak kesiminin işlemesi gerekmektedir. Bu bağımlılık zincirinin her halkası, Türkiye'nin doğrudan kontrol edemediği bir güvenlik ortamında bulunmaktadır.

9.2.2. Giriş Noktası Yoğunlaşması

Türkiye'nin enerji ithalat altyapısı, sayıca sınırlı giriş noktasında yoğunlaşmaktadır. Boru gazı için Kıyıköy, Durusu ve doğu sınırındaki giriş noktaları; LNG için Marmara Ereğlisi ve Aliağa terminalleri ile yüzer depolama-gazlaştırma üniteleri; ham petrol için Ceyhan, Dörtyol, Aliağa ve İzmit terminalleri temel kapılardır. Rafineri kapasitesinin de az sayıda büyük tesiste toplanması, aynı yoğunlaşma sorununu ürün tarafında tekrarlamaktadır.

Bu yoğunlaşma, ekonomik verimlilik açısından rasyoneldir; ancak KEAGİ çerçevesinde ikame edilemezlik puanını yükseltmektedir. Bahreyn örneğinde görüldüğü gibi, tek bir tesisteki kesinti ülke çapında etki üretebilmektedir. Türkiye'nin rafineri portföyünün Bahreyn'e kıyasla çok daha çeşitli olması önemli bir tampon sağlamakla birlikte, kritik terminal ve giriş noktalarındaki yoğunlaşma benzer bir risk taşımaktadır.

9.2.3. Elektrik Sisteminin Ada Benzeri Davranışı

Türkiye elektrik sistemi, Avrupa kıta şebekesiyle senkron paralel çalışmakla birlikte, ticari alışveriş kapasitesi sistem büyüklüğüne oranla sınırlıdır. Bu, bir kriz anında dışarıdan büyük ölçekli elektrik ithalatıyla açık kapatmanın pratik olmadığı anlamına gelir. Ukrayna'nın kriz döneminde komşu ülkelerden sağladığı acil ithalat kapasitesi, Türkiye ölçeğindeki bir sistem için aynı rahatlamayı sağlayamaz.

Sonuç olarak Türkiye, elektrik arz güvenliğini büyük ölçüde iç kaynaklarla ve iç dayanıklılıkla sağlamak durumundadır. Bu, yüksek gerilim iletim omurgasının ve kritik trafo merkezlerinin korunmasını, diğer ülkelere kıyasla daha yüksek bir öncelik hâline getirmektedir.

9.3. Türkiye Varlık Envanteri ve Risk Değerlendirmesi

Tablo 9.1. Türkiye ile İlişkili Kritik Enerji Varlıklarının Risk Skorları

Varlık / Sistem	Konum	Başlıca Tehdit Vektörü	Risk Skoru	Bant
Russkaya kompresör istasyonu (TürkAkım/Mavi Akım beslemesi)	Rusya (Krasnodar)	Uzun menzilli İHA	**88**	Kritik
Irak-Türkiye Ham Petrol Boru Hattı – Irak kesimi	Irak	Sabotaj, İHA, siyasi kesinti	**84**	Kritik
Basra/Hürmüz kaynaklı ham petrol ve LNG ithalat rotaları	Körfez – deniz	Boğaz kapanması, tanker saldırısı	**79**	Yüksek
Ceyhan terminal kompleksi (BTC + ITP + tank çiftliği)	Adana	İHA, sabotaj, siber	**76**	Yüksek
İstanbul ve Çanakkale Boğazları tanker trafiği	Marmara	Kaza, sabotaj, seyir güvenliği	**74**	Yüksek
Aliağa sanayi-rafineri-LNG kümesi	İzmir	Yoğunlaşma riski, siber, sabotaj	**72**	Yüksek
400 kV iletim omurgası ve kritik trafo merkezleri	Ülke geneli	Siber, sabotaj, trafo tedarik darboğazı	**70**	Yüksek
İzmit rafineri ve terminal kümesi	Kocaeli	Yoğunlaşma, deprem, siber	**70**	Yüksek
TürkAkım deniz altı kesimi ve Kıyıköy alım terminali	Karadeniz – Kırklareli	Deniz altı sabotaj, İHA	**68**	Yüksek-Orta
Bakü-Tiflis-Ceyhan hattı (Gürcistan ve Türkiye kesimleri)	Kafkasya – Anadolu	Sabotaj, bölgesel istikrarsızlık	**66**	Yüksek-Orta
Marmara Ereğlisi LNG ve FSRU'lar (Dörtyol, Saros)	Marmara – Akdeniz	Deniz kaynaklı saldırı, siber	**66**	Yüksek-Orta
TANAP hattı ve kompresör istasyonları	Doğu-Batı Anadolu	Sabotaj, İHA, siber	**64**	Yüksek-Orta
Doğu Akdeniz ve Karadeniz deniz altı veri/elektrik kabloları	Deniz	Çapa sürükleme, sabotaj	**62**	Yüksek-Orta
Akkuyu Nükleer Güç Santrali	Mersin	Dış besleme kaybı, siber, tedarik zinciri	**58**	Orta
Dağıtık GES/RES varlıkları ve inverter tedarik yoğunlaşması	Ülke geneli	Siber, tedarikçi tekdüzeliği	**56**	Orta
Silivri ve Tuz Gölü yeraltı doğal gaz depolama	Marmara – İç Anadolu	Yüzey tesisi saldırısı, siber	**52**	Orta

Kaynak: TESPAM hesaplaması, KEAGİ metodolojisi varlık düzeyine uyarlanarak. Skorlar, varlığın devre dışı kalması hâlinde Türkiye'nin enerji arz güvenliği üzerindeki etkisi ile mevcut tehdit maruziyetinin bileşimini ifade etmektedir.

Tablonun ilk iki sırasının Türkiye sınırları dışındaki varlıklardan oluşması, bu raporun Türkiye bölümündeki en önemli bulgusudur. Türkiye'nin enerji güvenliği açısından en yüksek riskli iki düğüm, Türk kamu otoritelerinin doğrudan koruma yetkisinin bulunmadığı topraklarda yer almaktadır. Bu durum, koruma

stratejisinin bir bölümünün diplomatik ve istihbari araçlarla, bir bölümünün ise ikame kapasite oluşturarak yürütülmesini zorunlu kılmaktadır.

9.4. Kurumsal Çerçeve: Mevcut Durum ve Boşluklar

Türkiye'de kritik altyapı korumasına ilişkin sorumluluk, çok sayıda kurum arasında dağılmış durumdadır. Boru hatları ve doğal gaz sisteminde BOTAŞ, elektrik iletiminde TEİAŞ, piyasa düzenlemesinde EPDK, siber olay müdahalesinde USOM ve sektörel SOME yapıları, fiziksel güvenlikte İçişleri Bakanlığı ve ilgili kolluk birimleri, hava savunmasında Milli Savunma Bakanlığı ve Türk Silahlı Kuvvetleri, deniz güvenliğinde Deniz Kuvvetleri ve Sahil Güvenlik Komutanlığı görev almaktadır. Enerji ve Tabii Kaynaklar Bakanlığı, sektörel koordinasyonu yürütmektedir.

Bu dağınıklık, kendi başına bir kusur değildir; hiçbir ülkede kritik altyapı koruması tek bir kurumun işi değildir. Sorun, dağınıklığın bir çerçeve mevzuatla bütünleştirilmemiş olmasıdır. Akademik literatürde uzun süredir dile getirilen tespit, Türkiye'de kritik altyapıyı tanımlayan, kategorilere ayıran, operatör yükümlülüklerini belirleyen ve denetim mekanizmasını kuran müstakil bir kanunun bulunmamasıdır. Tabii diğer taraftan artık tüm bakanlıkların Cumhurbaşkanlığı bünyesinde, olağanüstü durumlar karşısında koordinasyonu sağlamakla görevli ekipleri bulunmaktadır. Lakin ilgili model koordinasyon için yeterli değildir.

Diğer taraftan Avrupa Birliği'nde NIS2 ve CER direktiflerinin oluşturduğu bütünleşik çerçevenin Türkiye'deki karşılığı, parçalı düzenlemelerden oluşmaktadır.

Tablo 9.2. Kurumsal Kapasite Değerlendirmesi

Alan	Mevcut Durum	Başlıca Boşluk
Çerçeve mevzuat	Sektörel düzenlemeler mevcut	Kritik altyapıyı tanımlayan müstakil kanun yok
Varlık envanteri	Kurum bazında kısmî envanterler	Kurumlar arası paylaşılan, kritiklik derecelendirilmiş ortak envanter yok
Siber güvenlik	USOM/SOME yapısı kurulu, olgunlaşıyor	OT/ICS'ye özgü zorunlu standart ve saha denetimi sınırlı
İHA savunması	Askerî kapasite güçlü ve yerli	Sivil kritik tesislerde kalıcı konuşlu koruma sınırlı
Deniz tabanı farkındalığı	Askerî kapasite mevcut	Enerji altyapısına özgü sürekli izleme ve operatör entegrasyonu yok
Kritik yedek parça	Operatör bazında stoklar	Ulusal düzeyde koordine stratejik stok rejimi yok
Tatbikat kültürü	Sektörel tatbikatlar yapılıyor	Sektörler arası, çok aktörlü büyük ölçekli senaryo tatbikatı seyrek
Sigorta ve finansman	Ticari piyasaya bağımlı	Savaş riski için ulusal/bölgesel havuz mekanizması yok
Bilgi paylaşımı	Kamu-özel diyalog mevcut	Sektörel bilgi paylaşım ve analiz merkezi (ISAC) yapısı kurumsallaşmamış

9.5. Türkiye İçin Politika Önerileri

9.5.1. Kısa Vade (0-12 ay)

1. **Kritik enerji varlıkları ulusal envanterinin oluşturulması.** Tüm enerji altyapısı varlıkları, kritiklik derecesine göre üç kademede sınıflandırılmalı; her varlık için devre dışı kalma senaryosunda beklenen kesinti süresi ve ikame yolu belgelenmelidir. Envanter, ilgili kurumlar arasında güvenli bir platformda paylaşılmalıdır.

2. **Darboğaz ekipman haritalaması.** Her kritik tesis için, devre dışı kalması hâlinde tesis işlevini en uzun süre durduracak bileşenler tespit edilmeli; bu bileşenlerin fiziksel koruma önceliği ve yedek stok durumu ayrı bir kayıtta izlenmelidir.
3. **İnternete açık endüstriyel cihazların tespiti ve kapatılması.** Programlanabilir mantık denetleyicileri ve uzaktan terminal birimlerinin doğrudan internete açık olup olmadığı, sektör genelinde bir tarama kampanyasıyla tespit edilmeli ve bu erişimler derhal kapatılmalıdır. Bu, en düşük maliyetli ve en yüksek getirili tedbirdir.
4. **Servis sağlayıcı erişimlerinin envanterlenmesi.** Bakım sözleşmeleri kapsamında üretici ve servis sağlayıcılara verilen uzaktan erişim hakları kayıt altına alınmalı, zaman sınırlı hâle getirilmeli ve çok faktörlü doğrulamaya bağlanmalıdır.
5. **Ceyhan, Aliağa, İzmit ve Kıyıköy için öncelikli koruma planları.** Bu dört yoğunlaşma noktası için tesis bazlı, çok vektörlü koruma planları hazırlanmalı; hava, kara, deniz ve siber boyutlar tek bir planda birleştirilmelidir.
6. **Sektörler arası masa başı tatbikat.** Enerji, telekomünikasyon, su ve ulaştırma sektörlerini kapsayan, eşzamanlı çoklu kesinti senaryosuna dayalı bir tatbikat düzenlenmelidir.
7. **Transit hatlarda ikili güvenlik protokolleri.** Rusya, Azerbaycan, Gürcistan ve Irak ile mevcut ikili anlaşmalara, altyapı güvenliği bilgi paylaşımı ve erken uyarı hükümleri eklenmelidir.

9.5.2. Orta Vade (1-3 yıl)

1. **Kritik Altyapıların Korunması Çerçeve Kanunu'nun çıkarılması.** Kanun; kritik altyapı tanımını, sektörel kapsamı, operatör yükümlülüklerini, olay bildirim zorunluluğunu, denetim mekanizmasını ve yaptırım rejimini belirlemelidir. Avrupa Birliği'nin NIS2 ve CER direktifleriyle uyum, hem teknik kalite hem de ticari erişim açısından tercih edilmelidir.
2. **Ulusal kritik yedek parça stok rejimi.** Yüksek gerilim güç transformatörleri, boru hattı kompresör setleri, rafineri kritik ekipmanı ve HVDC valf grupları için ulusal düzeyde koordine edilen bir stratejik stok oluşturulmalıdır. Finansman, operatör katkısı ile devlet desteğinin birleştirildiği bir havuz modeliyle sağlanabilir.
3. **Mobil transformatör filosu.** Farklı gerilim kademelerinde, hızlı konuşlandırılabilir mobil transformatör ve şalt ekipmanı filosu kurulmalı; TEİAŞ bünyesinde bölgesel olarak konuşlandırılmalıdır.
4. **Kritik tesislerde kalıcı İHA savunma mimarisi.** Türkiye'nin yerli hava savunma ve elektronik harp kabiliyeti, sivil kritik enerji tesislerinin korunmasına uyarlanmalıdır. Radar, radyo frekansı tespit ve karıştırma ile kısa menzilli etkisiz hâle getirme katmanlarını birleştiren tesis bazlı sistemler, Ceyhan'dan başlayarak kademeli olarak kurulmalıdır.
5. **Deniz Tabanı Farkındalık Merkezi.** Deniz Kuvvetleri, Sahil Güvenlik, BOTAŞ, TEİAŞ, TPAO ve telekom operatörlerini kapsayan ortak bir merkez kurulmalı; denizaltı boru hatları, enterkonektörler ve veri kablolarının güzergâhları üzerinde sürekli izleme sağlanmalıdır. Otomatik tanımlama sistemi verilerinin anomali analizi ile dağıtık akustik algılama teknolojileri birleştirilmelidir.
6. **Enerji sektörü için OT güvenlik standardının zorunlu hâle getirilmesi.** IEC 62443 temelli, sektöre uyarlanmış bir zorunlu standart yayımlanmalı; uyum, belge düzeyinde değil saha denetimiyle doğrulanmalıdır. Küçük ve orta ölçekli üretim tesisleri için uyum desteği sağlanmalıdır.
7. **Enerji Sektörü Bilgi Paylaşım ve Analiz Merkezi (ISAC).** Kamu ve özel operatörler arasında tehdit istihbaratının gerçek zamanlı paylaşıldığı, cezalandırıcı olmayan bir yapı kurulmalıdır.
8. **Dağıtık varlıklarda tedarikçi çeşitliliği yükümlülüğü.** Şebeke bağlantı yönetmeliklerine, belirli bir kurulu gücün üzerinde tek bir üreticinin kontrol ekipmanına bağımlılığı sınırlayan hükümler eklenmeli; iletişim kaybı senaryolarında güvenli varsayılan davranış zorunlu kılınmalıdır.

9. **Ürün ithalat kapasitesinin acil senaryolara hazırlanması.** Rusya örneğinin gösterdiği üzere, rafineri kapasitesi kaybı hâlinde ürün ithalatı tek çıkış yoludur. Liman kabul kapasitesi, depolama ve dağıtım altyapısının bu senaryoya hazır olup olmadığı test edilmelidir.
10. **Savaş riski sigortası havuzu.** Bölgesel çatışma dönemlerinde ticari teminatın bulunamaması ihtimaline karşı, devlet destekli bir yeniden sigorta havuzu tasarlanmalıdır.

9.5.3. Uzun Vade (3-10 yıl)

1. **Giriş noktası çeşitlendirmesinin fiziksel olarak genişletilmesi.** Yeni LNG kabul kapasitesi ve ilave boru gazı giriş noktaları, salt ticari değil güvenlik gerekçeleriyle de planlanmalı; yeni kapasitenin coğrafi dağılımı, tehdit korelasyonu dikkate alınarak belirlenmelidir.
2. **Yeraltı doğal gaz depolama kapasitesinin artırılması.** Yeraltı depolamanın yer üstü tesislere kıyasla üstün savunulabilirlik profili, kapasite artırımını güvenlik politikası açısından da öncelikli kılmaktadır. Hedef, yıllık tüketimin daha yüksek bir oranını karşılayacak düzeye ulaşmak olmalıdır.
3. **Yenilenebilir ve nükleer payının artırılması.** Yerli ve yenilenebilir kaynaklar, boğazlardan geçirilemez ve üçüncü taraflarca kesilemez oldukları için jeopolitik riske karşı yapısal bir korunma sağlar. Enerji dönüşümü, iklim politikası olduğu kadar güvenlik politikasıdır.
4. **Elektrik sisteminde ada modunda çalışma kabiliyeti.** İletim sistemi, büyük ölçekli kesintilerde bölgesel adalara ayrılarak çalışabilecek biçimde tasarlanmalı; kara başlatma kapasitesi coğrafi olarak dağıtılmalı ve düzenli tatbikatlarla doğrulanmalıdır.
5. **Kritik ekipmanda yerli üretim kapasitesi.** Yüksek gerilim güç transformatörleri, boru hattı kompresörleri ve endüstriyel kontrol sistemlerinde yerli üretim ve bakım kabiliyeti, tedarik zinciri riskini azaltan yapısal bir yatırımdır.

10. SONUÇ

Bu raporun çıkış noktası, Vladimir Putin'in kendi ülkesinin enerji altyapısının korunamadığına ilişkin kabulüdür. O kabul, tekil bir savaşın tekil bir ayrıntısı değil, küresel bir yapısal dönüşümün en görünür işaretidir. Enerji altyapısı, yirminci yüzyıl boyunca korunması gereken ama fiilen büyük ölçüde korunan bir varlık kategorisidir. Yirmi birinci yüzyılın ilk çeyreğinin sonunda ise, çatışmanın hem aracı hem hedefi hâline gelmiş; savaşın en ekonomik, en etkili ve en az cezalandırılan cephesi olarak kurumsallaşmıştır.

Dönüşümün itici gücü, tek bir teknolojik yenilik değil, birkaç eğilimin kesişimidir. Uzun menzilli ve düşük maliyetli insansız sistemler, derinlemesine hedef vurma kabiliyetini yaygınlaştırmıştır. Dijitalleşme, saldırı yüzeyini genişletti ve fiziksel etki üreten siber saldırıları mümkün kılmıştır. Gri bölge doktrinleri, atfedilemez saldırıları stratejik bir araç hâline getirmiştir. Küresel tedarik zincirlerinin uzaması, hasar sonrası onarımı yavaşlatmıştır. Bu dört eğilim birleştiğinde, korumanın klasik biçimi — çevre güvenliği ve caydırıcılık — yetersiz kalmaktadır.

Yeni paradigmanın merkezinde, hedefin değişmesi vardır. Artık amaç, her saldırıyı engellemek değildir; bu, maliyet asimetrisi nedeniyle ulaşılamaz bir hedeftir. Amaç, saldırının etkisini sınırlamak, kesinti süresini kısaltmak ve sistemin yayılım etkisini kontrol altında tutmaktır. Bu, koruma yatırımının ağırlık merkezini perimetre güvenliğinden dayanıklılık altyapısına kaydırmayı gerektirir: kritik yedek parça stoku, modüler onarım kapasitesi, tedarikçi çeşitliliği, ada modunda çalışma kabiliyeti ve tatbikatla doğrulanmış kriz prosedürleri.

Raporun iki bulgusu, paradigma değişiminin failden bağımsız bir boyutu da olduğunu göstermektedir. Birincisi, 2026 Avrupa yazının açığa çıkardığı iklim kaynaklı üretim riskidir: Paks ve Cernavodă'nın soğutma suyu yetersizliği nedeniyle devre dışı kalması, hiçbir düşman aktör olmaksızın, kasıtlı bir saldırı kampanyasıyla aynı sonucu — eşzamanlı, tekrarlayan kapasite kaybı — üretmiştir. Bu, savunulabilirliğin artık yalnızca kinetik ve siber tehditlere karşı değil, tesisin tasarım varsayımlarını aşan iklimsel koşullara karşı da tanımlanması gerektiği anlamına geldiğini de ortaya koymaktadır. İkincisi, deniz tabanı altyapısında gözlemlenen maliyet makasıdır: Kuzey Akım'ın onarılamaz biçimde imha edilmesi, on milyar avroyu aşan bir yatırıma karşılık üç yüz bin dolarlık bir operasyonla mümkün olmuş; TürkAkım'ın su altı kesimine yönelik tekrarlanan girişimler ile Doğu Akdeniz'deki milyar dolarlık proje portföylerinin aynı türde bir araçla — ticari bir su altı aracıyla — tehdit altında olması, bu makasın istisna değil kural hâline geldiğini göstermektedir. İhtilaflı deniz alanlarında oldu bittiyle yatırım güvenliği yaratma stratejisi, bu makas karşısında geçerliliğini yitirmektedir.

Raporda geliştirilen indeks, bu yeni önceliklerin sayısal karşılığını sunmaktadır. Bölgesel sıralamanın ilk altı sırasının 2026'nın iki büyük çatışmasına ait olması, riskin coğrafi yoğunlaşmasını göstermektedir. Varlık türü sıralamasında rafinerilerin, LNG tesislerinin ve trafo merkezlerinin öne çıkması ise, kırılganlığın maruziyetten çok onarım süresinden kaynaklandığına işaret etmektedir. Bu iki bulgu birlikte okunduğunda, koruma politikasının iki eksende kurulması gerektiği anlaşılır: coğrafi olarak yoğunlaşan tehdide karşı erken uyarı ve aktif savunma, yapısal olarak yoğunlaşan kırılganlığa karşı stok ve yedeklilik.

Türkiye açısından tablo, hem uyarıcı hem de fırsat barındırıcıdır. Uyarıcıdır; çünkü ülkenin enerji güvenliği açısından en riskli iki düğümü kendi sınırları dışında bulunmaktadır ve transit ülke konumu, Türkiye'yi taraf olmadığı çatışmaların hedef kümesine dâhil etmektedir. Fırsat barındırıcıdır; çünkü bölgesindeki alternatiflerin kırılganlaştığı bir dönemde Ceyhan, Türkiye'nin liman ve boru hattı ağı ve ülkenin çeşitlendirilmiş tedarik yapısı, bölgesel bir güvenli liman kimliğini güçlendirmektedir. Bu kimliğin sürdürülebilirliği, doğrudan altyapı güvenliği kapasitesine bağlıdır: güvenli liman iddiası, ancak fiilen güvenli olunduğu sürece geçerlidir.

Son olarak, bu raporun kapsamı dışında kalan ancak kaçınılmaz olarak gündeme gelecek bir soru vardır. Enerji altyapısına yönelik saldırıların bir norm hâline gelmesi, uluslararası hukuk açısından kabul edilebilir midir? Bu tesislerin çift kullanımlı niteliği, onları meşru hedef hâline getirmeye yeterli midir? Sivil nüfusun ısınma, ulaşım ve sağlık hizmetlerine erişiminin kesilmesinin hukuki karşılığı nedir? Bu sorulara verilecek cevaplar, önümüzdeki on yılın güvenlik ortamını teknik tedbirlerden daha fazla belirleyecektir. Uluslararası toplumun bu alanda bir norm inşa edememesi hâlinde, enerji altyapısı, her çatışmanın varsayılan ilk hedefi olarak kalacaktır. Bugünkü eğilim, ne yazık ki bu yönü işaret etmektedir.

KAYNAKÇA

ACLED (2026). Middle East Overview: April 2026. Armed Conflict Location and Event Data Project.

adimhaber.com (2026). “Avrupa’da Etkili Olan Aşırı Sıcaklar, Enerji Üretimini de Vurdu.” 6 Ağustos 2026.

Akyener, O. (t.y.). Enerji Güvenliğinin Modellenmesi ve Türkiye Örneği. Yazarın kendi yayını, ISBN 6056581780.

Al Jazeera (2026). Doğu-Batı Boru Hattı, Hürmüz Boğazı ve Körfez enerji altyapısına ilişkin haber ve analizler, Mart-Eylül 2026.

Al Jazeera (2024). “Sweden Ends Nord Stream Probe Citing Lack of Jurisdiction.” 7 Şubat 2024.

Anadolu Ajansı ve Türk basını (2026). Türkiye’nin enerji arz güvenliği ve boru hattı altyapısına ilişkin haber ve analizler, Mart-Eylül 2026.

Atlantic Council (2025). How the Baltic Sea Nations Have Tackled Suspicious Cable Cuts. Issue Brief, Washington D.C.

BESA Center (2024). “The Great Sea Interconnector: Prospects for an Electrical Cable Connecting Greece, Cyprus, and Israel.” Begin-Sadat Center for Strategic Studies.

Bloomberg (2026). “List of Gulf Energy Infrastructure Damaged in Iran War.” Nisan 2026.

Bulletin of the Atomic Scientists (2026). “Seabed Zero: Baltic Sabotage and the Global Risks to Undersea Infrastructure.” Şubat 2026.

CBC News (2024). “How Did Divers Manage to Blow Up the Nord Stream Pipeline? We Went Down to the Spot to Find Out.” Ağustos 2024.

CERT Polska (2026). Energy Sector Incident Report. Varşova, 30 Ocak 2026.

Cherp, A. ve Jewell, J. (2014). “The Concept of Energy Security: Beyond the Four As.” Energy Policy, 75, 415-421.

CISA (2026). “Poland Energy Sector Cyber Incident Highlights OT and ICS Security Gaps.” Cybersecurity and Infrastructure Security Agency Alert, 10 Şubat 2026.

CISA / FBI (2026). “Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure.” Advisory AA26-097A (güncelleme: 22 Temmuz 2026).

CNBC (2026). Doğu-Batı Boru Hattı uydu görüntüleri ve petrol fiyatı analizleri, 11-14 Eylül 2026.

Congressional Research Service (2026). The Strait of Hormuz: Security Developments and Impacts on Oil, Gas, and Other Commodities. Rapor No. R45281, Washington D.C., Ağustos 2026.

Defense News (2026). “NATO Allies Foil Russian Subsea Cable Sabotage Plot.” 10 Eylül 2026.

denizmagazin.com (2012, güncel erişim 2026). “ROV (Remotely Operated Underwater Vehicle – Uzaktan Kumandalı Su Altı Aracı).”

ekonomim.net (2026). “Sıcaklar Avrupa’nın Elektrik Sistemindeki Kırılganlığı Ortaya Çıkardı.” Ağustos 2026, Ember verilerine atfen.

ekoturk.com (2026). “Gazprom Açıkladı: TürkAkım ve Mavi Akım’a 12 Saldırı Girişimi.” 11 Mart 2026.

Euronews (2026). “Second Ukrainian Arrested in Connection with Nord Stream Pipeline Explosions.” 19 Ağustos 2026.

Euronews (2026). “EU-Backed Electricity Link to Cyprus Stalls Amid Regional Tensions.” 19 Ağustos 2026.

European Commission (2026). EU Action Plan on Cable Security – Cable Security Toolbox. Brüksel, 5 Şubat 2026.

European Policy Centre (2025). Battle of the Baltic: Safeguarding Critical Undersea Infrastructure. Brüksel.

European Union (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2).

European Union (2022). Directive (EU) 2022/2557 on the resilience of critical entities (CER).

FDD (2026). “Saudi Arabia Closes Its East-West Pipeline After Attacks from Iraq.” Foundation for Defense of Democracies, 13 Eylül 2026.

Fox Business (2024). “A Drunken Evening, a Rented Yacht: The Real Story of the Nord Stream Pipeline Sabotage.” 17 Ağustos 2024.

IEA (2026). “Russian Refining Sector Struggles Amid Intensifying Ukrainian Attacks.” IEA Commentary, Paris, Eylül 2026.

IEA (2026). Oil Market Report, çeşitli sayılar. Paris: International Energy Agency.

IEC (2018-2024). IEC 62443 Series: Industrial Communication Networks – Network and System Security. Cenevre: International Electrotechnical Commission.

Kruyt, B., van Vuuren, D. P., de Vries, H. J. M. ve Groenenberg, H. (2009). “Indicators for Energy Security.” Energy Policy, 37(6), 2166-2181.

NATO (2025). Baltic Sentry: Enhancing the Protection of Critical Undersea Infrastructure. Brüksel.

nefes.com.tr (2025). “TürkAkım Boru Hattına Saldırı Girişimi.” 9 Nisan 2025.

NIST (2023). Guide to Operational Technology (OT) Security, Special Publication 800-82 Rev. 3. Gaithersburg: National Institute of Standards and Technology.

Özker, U. (2022). Türkiye’de Kritik Altyapı ve Siber Güvenlik. Ankara: KAS – EDAM Ortak Yayını.

Payne Institute for Public Policy (2026). Emergency Flaring Detected Along Saudi Arabia’s East-West Pipeline. Colorado School of Mines, Eylül 2026.

Perrow, C. (1984). Normal Accidents: Living with High-Risk Technologies. New York: Basic Books.

referansturk.com.tr (2026). “Putin’den Kritik Boru Hattı Uyarısı: Türkiye’ye Giden Hatlara Sabotaj İddiası.” 24 Şubat 2026.

Reuters (2026). Rus rafinerilerine yönelik saldırılar ve dizel üretimi analizleri, Eylül 2026.

Rinaldi, S. M., Peerenboom, J. P. ve Kelly, T. K. (2001). “Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies.” IEEE Control Systems Magazine, 21(6), 11-25.

Şahin, G. ve Eygün, M. E. (2024). “Hibrit Tehditler Kapsamında Türkiye’nin Kritik Altyapı Güvenliği: Petrol ve Doğalgaz Boru Hatları.” Uluslararası İlişkiler ve Politika Dergisi, 4(1), 1-16.

sde.org.tr (2026). “Aşırı Sıcaklar Avrupa’yı Kavuruyor: Fransa 3 Nükleer Santralini Kapattı, Macaristan’da Tuna Nehri’nin Suları Çekildi.” Ağustos 2026.

Suudi Arabistan Enerji Bakanlığı (2026). Doğu-Batı Boru Hattı’na yönelik saldırılara ilişkin basın açıklaması, 11 Eylül 2026.

TESPAM (2026). Enerji Güvenliği ve Jeopolitik Risk Değerlendirmeleri Serisi. Ankara: Türkiye Enerji Stratejileri ve Politikaları Araştırma Merkezi.

The Moscow Times (2026). “Kremlin Slams ‘Irresponsible’ Ukrainian Drone Attacks on TurkStream and Blue Stream Compressor Stations.” 19 Mart 2026.

theistanbulchronicle.com (2026). “Avrupa’nın Sıcak Hava Faturası: Milyarlarca Euro.” Ağustos 2026, Allianz ve Reuters değerlendirmelerine atfen.

Türkiye Gazetesi (2026). “Almanların İsmini Bile Bulamadığı Sabotajcıyı Türk İstihbaratı Çözdü! TürkAkım’ı Hedef Alan Kuznietsov Savaş Suçuyla Yargılanacak.” 2 Temmuz 2026.

Wikipedia (2026). “Nord Stream Pipelines Sabotage.” Erişim: Eylül 2026.

Wikipedia (2026). “Great Sea Interconnector.” Erişim: Eylül 2026.

Winzer, C. (2012). “Conceptualizing Energy Security.” Energy Policy, 46, 36-48.

Yergin, D. (2006). “Ensuring Energy Security.” Foreign Affairs, 85(2), 69-82.

Yetkin Report / Yetkin, M. (2025). “Ukrayna’nın TürkAkım’a Saldırı Girişimi: Ankara Ne Yapmalı?” 16 Ocak 2025.

Künye. Bu rapor, TESPAM Kızıl Elma Enstitüsü tarafından Eylül 2026’da Ankara’da hazırlanmıştır. Raporda yer alan indeks skorları ve karşılaştırmalı hesaplamalar TESPAM’ın özgün çalışmalarıdır ve kaynak gösterilerek kullanılabilir. Raporda yer alan değerlendirmeler, hazırlandığı tarih itibarıyla mevcut kamuya açık bilgilere dayanmaktadır.