Cilt: 2, Sayı: 1, 2026, Sayfa: 46-64

Yönetim Bilişim Sistemleri Derneği Dergisi

ISSN: 3108-6454

Journal of Management Information Systems Association

https://www.ybs.org.tr

DENİZCİLİK SİBER GÜVENLİĞİNDE PROAKTİF BİR SAVUNMA YAKLAŞIMI: HÜRMÜZ BOĞAZI LİMANLARININ OSINT TABANLI AMPİRİK HARİTALAMASI

Aleyna YILDIZ[a] ve Hüseyin PARMAKSIZ[b]

Makale Bilgisi

Makale Türü
Araştırma Makalesi

Gönderim Tarihi:
19/05/2026

Kabul Tarihi:
26/06/2026

Anahtar Kelimeler:
Siber Güvenlik, OSINT, Liman 4.0, Sosyal Mühendislik, Millileşme.

Özet

Denizcilik sektöründeki dijitalleşme, küresel tedarik zincirlerini asimetrik siber tehditlere açık hale getirmektedir. Bu araştırma, Hürmüz Boğazı'ndaki on stratejik otoritenin siber güvenlik altyapılarını Açık Kaynak İstihbaratı (OSINT) kullanarak ampirik olarak incelemektedir. Hedef sistemlerin dijital ayak izleri Python tabanlı otomasyonla haritalandırılmış; tehdit söylemleri ise 106 güncel haber kaynağı üzerinden Doğal Dil İşleme ile analiz edilmiştir. Bulgular, Körfez ülkelerinde veri egemenliği ile bulut bağımlılığı arasında ikilem yaşandığını ve İran'ın agresif Web Uygulama Güvenlik Duvarı konfigürasyonlarıyla devlet destekli siber izolasyon stratejisi izlediğini göstermektedir. Ayrıca Liman 4.0 ekosisteminde en zayıf halkanın insan faktörü olduğu tespit edilmiş; sosyal mühendislik riskleri ile donanımda millileşme ihtiyacı vurgulanmıştır. Metin madenciliği sonuçları, siber tehdit algısının basit veri hırsızlığından ziyade fiziksel operasyonel teknoloji unsurlarıyla doğrudan bağlantılı olduğunu doğrulamaktadır. Son olarak, denizaltı fiber optik kablolarının stratejik önemine dikkat çekilerek NIS2 gibi proaktif mevzuatların ulusal denizcilik stratejilerine entegre edilmesi önerilmektedir.

[a] Lisans Öğrencisi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, 5933986@ogrenci.bilecik.edu.tr, ORCID: 0009-0006-9724-1442 (Corresponding Author)
[b] Dr. Öğr. Üyesi, Bilecik Şeyh Edebali Üniversitesi, Yönetim Bilişim Sistemleri, Bilecik/Türkiye, huseyin.parmaksiz@bilecik.edu.tr, ORCID: 0000-0001-8455-5625

A PROACTIVE DEFENSE APPROACH IN MARITIME CYBERSECURITY: AN OSINT-BASED EMPIRICAL MAPPING OF STRAIT OF HORMUZ PORTS

Article Information

Article Type
Research Article

Submission Date:
19/05/2026

Acceptance Date:
26/06/2026

Keywords:
Cybersecurity, OSINT, Port 4.0, Social Engineering, Nationalization.

Abstract

Digitalization in the maritime sector exposes global supply chains to asymmetric cyber threats. This research empirically examines the cybersecurity infrastructures of ten strategic authorities in the Strait of Hormuz using Open-Source Intelligence (OSINT). Target systems' digital footprints were mapped via Python-based automation, while threat discourses from 106 news sources were analyzed using Natural Language Processing. Findings reveal a dilemma between data sovereignty and cloud dependency in Gulf states, alongside Iran's state-sponsored cyber isolation strategy driven by aggressive Web Application Firewall configurations. Additionally, the human factor emerged as the weakest link in the Port 4.0 ecosystem, emphasizing social engineering risks and the need for hardware nationalization. Text mining confirms that cyber threat perceptions are directly linked to physical operational technologies rather than simple data theft. Finally, stressing the strategic importance of submarine cables, this study recommends integrating proactive legislations like the NIS2 Directive into national maritime strategies.

1. GİRİŞ

Denizcilik sektörü, küresel ticaretin bel kemiğini oluşturmanın ötesinde, ülkelerin ekonomik refahı ve ulusal güvenliği için stratejik bir yaşam hattı niteliğindedir. Dünya ticaret hacminin yaklaşık %80'inin deniz yolları üzerinden gerçekleşmesi (UNCTAD, 2023), bu sektörü dijitalleşen dünyada kritik bir hedef hâline getirmiştir. Özellikle "Liman 4.0" ve otonom gemi mimarileri (De la Peña Zarzuelo vd., 2020) gibi devrim niteliğindeki gelişmelerle birlikte denizcilik operasyonları, geleneksel fiziksel sınırların ötesine geçerek siber-fiziksel sistemlerin iç içe geçtiği karmaşık bir dijital ekosisteme dönüşmüştür. Ancak bu teknolojik sıçrama, yönetilmesi güç bir saldırı yüzeyini de beraberinde getirmiştir. Nesnelerin İnterneti (IoT) kapsamında yer alan akıllı vinçler, bulut tabanlı Otomatik Tanımlama Sistemi (AIS) cihazları ve Radyo Frekansı ile Tanımlama (RFID) tabanlı konteyner takip sistemlerinden otonom seyrüsefer altyapılarına kadar her yeni bağlantı, küresel tedarik zinciri açısından potansiyel bir siber zafiyet kapısı aralamaktadır.

Bu siber-fiziksel risklerin en somut ve en kritik hissedildiği stratejik düğüm noktalarının (Süveyş Kanalı, Malakka Boğazı ve Panama Kanalı gibi) başında Hürmüz Boğazı gelmektedir. Jeopolitik önemi nedeniyle dünya enerji trafiğinin en hassas noktası kabul edilen bu bölge, konvansiyonel askeri tehditlerin yanı sıra sofistike siber operasyonların da odak noktasındadır. Bölgedeki liman otoritelerine yönelik olası bir siber müdahale, yalnızca bölgesel bir aksaklığa değil; tedarik zinciri felç olacağı için küresel ölçekte bir enerji krizine ve ekonomik dalgalanmaya (Clavijo Mesa vd., 2024) yol açma

potansiyeli taşımaktadır. Dolayısıyla bu bölgedeki stratejik aktörlerin siber güvenlik duruşlarını anlamak, küresel güvenlik için bir zorunluluk haline gelmiştir.

Denizcilik siber güvenliği üzerine yapılan çalışmaların büyük bir kısmının teorik çerçeveler, genel risk modelleri veya yaşanmış veri ihlallerinin geriye dönük incelemeleri etrafında toplandığı görülmektedir (Kavallieratos ve Katsikas, 2020; Svilicic vd., 2019). Araştırmacıların birçoğu laboratuvar ortamındaki simülasyonlara veya anket verilerine dayanarak siber riskleri tanımlamaya çalışmıştır. Örneğin, Hemminghaus vd. (2021) kapalı bir ağ içi tehdit modellemesi geliştirmiş olsa da bu tür yaklaşımlar, gerçek dünyadaki dinamik ve karmaşık saldırı yüzeylerini yansıtmakta eksik kalmaktadır. Siber tehditlerin saniyeler içinde değiştiği günümüzde, stratejik kurumların dışa açık ağ altyapılarını gerçek zamanlı ve nesnel yöntemlerle haritalandıran deneysel (ampirik) çalışmaların eksikliği dikkat çekmektedir.

Bu çalışma, literatürdeki söz konusu boşluğu doldurmak amacıyla tasarlanmış olup teorik varsayımların ötesine geçerek doğrudan OSINT verilerine odaklanmaktadır. Araştırma kapsamında, bölgenin siber ekosistemini şekillendiren on stratejik denizcilik otoritesi, Patton (2015) tarafından çerçevesi çizilen "Amaçlı Örnekleme" yöntemiyle belirlenmiş ve bu kurumların dijital ayak izleri analiz edilmiştir. Çalışmanın temel motivasyonu; bu kurumların siber güvenlik stratejilerini veri egemenliği, uluslararası bulut bağımlılığı ve proaktif savunma mekanizmaları bağlamında yapısal olarak ortaya koymaktır.

2. KAVRAMSAL ÇERÇEVE/LİTERATÜR

Denizcilik siber güvenliği literatürü incelendiğinde, çalışmaların son beş yılda teorik risk analizlerinden ampirik teknik analizlere doğru evrildiği gözlemlenmektedir. Literatürdeki araştırmalar genel olarak gemi içi sistemlerin güvenliği (Svilicic vd., 2019), liman altyapılarının dayanıklılığı (De la Peña Zarzuelo vd., 2020) ve OSINT tabanlı tehdit istihbaratı (Nasr vd., 2026) olmak üzere üç ana eksende toplanmaktadır. Mevcut çalışmaların büyük bir kısmı anket ve simülasyon temelli olup, Hürmüz Boğazı gibi jeopolitik açıdan kritik bölgelerin gerçek zamanlı dijital ayak izlerini inceleyen ampirik OSINT araştırmalarının literatürde son derece kısıtlı olduğu tespit edilmiştir. Bu durumun temel nedeni; ulusal güvenlik kapsamında agresif güvenlik duvarlarıyla (WAF) korunan liman altyapılarından gerçek zamanlı dijital veri toplamanın barındırdığı yasal ve etik zorluklar ile araştırmacıların genellikle kontrollü kapalı devre simülasyon (testbed) ortamlarını tercih etmesidir. Bu çalışma, Tablo 1'de sunulan 30 referans makalenin işaret ettiği söz konusu metodolojik ve coğrafi boşluklardan yola çıkarak kurgulanmıştır.

Tablo 1. Denizcilik Siber Güvenliği Literatür Özeti

Çalışma	**Odak Konusu**	**Kullanılan Yöntem / Araç**	**Temel Bulgu**
Puchkov vd. (2021)	Siber Olay Tespiti	Büyük Veri, SpaCy tabanlı Doğal Dil İşleme (NLP) ve Metin Madenciliği	İnternet tabanlı metinlerden otomatik siber tehdit bilgisi çıkarılabileceği kanıtlanmıştır.
Hemminghaus vd. (2021)	Köprü Sistemi Güvenliği	Köprü Siber Güvenlik Aracı (BRAT) Destekli İnteraktif Saldırı Simülasyonu	Tasarım aşamasında zafiyet tespiti sağlayan bir simülasyon aracı geliştirilmiştir.
Androjna vd. (2021)	Sinyal Manipülasyonu	Küresel Navigasyon Uydu Sistemleri (GNSS) ve AIS SWOT Analizi	Navigasyon sistemlerinin şifreleme eksikliği nedeniyle spoofing'e çok açık olduğu saptanmıştır.
Jacq vd. (2021)	Kriz Yönetimi Eğitimi	Hibrit Siber Poligon (Cyber Range)	Liman aktörlerinin siber eğitiminde poligon kullanımının etkili olduğu görülmüştür.
Tam vd. (2021)	Siber-Fiziksel Güvenlik	Donanım Test Yatağı (Testbed)	Saldırıların fiziksel güvenlik üzerindeki etkileri ve gemi-liman riskleri somutlaştırılmıştır.
Nissov vd. (2021)	Siber Dayanıklılık	Topolojik Bilgi Akışı Analizi	Saldırı kaynaklı hatalı verilerin tespit edilip izole edilebileceği modellenmiştir.
He vd. (2021)	Ağ İçi Tehdit Modellemesi	Markov Zinciri ve Alan Adı Sistemi (DNS) Rebinding	IoT cihazlarını korumak adına DNS saldırılarını başlatan etkili bir tespit mekanizması sunulmuştur.
(Okolo ve Chang, 2021)	Tedarik Zinciri Direnci	Sistematik Derleme ve Yapay Zeka	Denizcilik ağlarında yapay zeka destekli anomali tespitinin kritik olduğu gösterilmiştir.
Gunes vd. (2021)	Liman Risk Değerlendirmesi	Senaryo Tabanlı Risk Analizi	Limanların siber ve fiziksel altyapılarının entegre değerlendirilmesinin zorunluluğu kanıtlanmıştır.
Rajaram ve Benson, (2022)	Siber Risk Yönetimi	OT Sistemleri Analizi	Donatanlar için siber hijyeni artıracak detaylı bir kontrol listesi geliştirilmiştir.
Oruc vd. (2022)	Entegre Navigasyon Sistemi (INS)	MITRE ATT&CK Çerçevesi	Navigasyon sistemlerinde potansiyel siber riskler tanımlanmış ve sınıflandırılmıştır.
Schwarz ve von Solms, (2022)	Bilgi Güvenliği Vakaları	Yapılandırılmış Uzman Mülakatı	Tehditlerin küçümsendiği ve sektörde bilgi paylaşımı platformları kurulması gerektiği vurgulanmıştır.
Gyamfi vd. (2022)	IoT Ağ Güvenliği	Uyarlanabilir Artımlı Pasif-Agresif Makine Öğrenmesi (AI-PAML)	Uç Bilişim (MEC) ile IoT cihazlarında yüksek doğrulukla saldırı tespiti yapılmıştır.
Grispos ve Mahoney (2022)	Sektörel Meydan Okumalar	Tarihsel Vaka Analizi	Teknolojinin benimsenme hızının güvenliği geçtiği ve finansal açıklar doğurduğu bulunmuştur.

Amro vd. (2022)	Otonom Gemi Güvenliği	Hata Türü, Etkileri ve Kritiklik Analizi (FMECA) ve MITRE ATT&CK	Otomasyon ve uzaktan bağlantıların riskleri artırdığı ve tehdit tabanlı savunma gerektiği belirlenmiştir.
Farah vd. (2022)	IoT ve Büyük Veri Etkisi	Sistematik Literatür Taraması	Akıllı sistemlerin GNSS gibi altyapılardaki siber saldırı oranını devasa ölçüde artırdığı saptanmıştır.
Yadav ve Kumar (2023)	Açık Kaynak İstihbaratı	Makine Öğrenmesi Derlemesi	OSINT'in yapay zeka ile otonomlaştırılmasının ulusal güvenlikteki önemi tartışılmıştır.
Pöyhönen ve Lehto (2023)	Kapsamlı Liman Güvenliği	Sistemler Sistemi Yaklaşımı	Siber güvenliğin teknik bir sorundan ziyade bütüncül bir yönetim süreci olması gerektiği saptanmıştır.
Lee ve Lee (2023)	Gemi Veri Sunucuları	Mesaj Kuyruklama Telemetri Aktarımı (MQTT) Protokolü Modifikasyonu	Önerilen yöntemin veri sunucularını DDoS saldırılarına karşı daha dayanıklı hale getirdiği kanıtlanmıştır.
Progoulakis ve Nikitakos, (2023)	Siber-Fiziksel Dijitalleşme	Bow Tie Analizi ve Amerikan Petrol Enstitüsü Güvenlik Risk Değerlendirmesi (API SRA)	Liman altyapılarındaki risklerin proaktif ve reaktif yöntemlerle yönetilebileceği gösterilmiştir.
Jouni Pöyhönen (2023)	Akıllı Terminal Süreçleri	Bütüncül Araştırma Yaklaşımı	Liman bilişim sistemlerinin enerji ve bilgi akışıyla birlikte holistik değerlendirilmesi gerektiği saptanmıştır.
Rebecca Rohan (2023)	Siber Saldırı Trendleri	Elmas Modeli (Diamond Model)	Nakliye şirketlerinin veri sızdırma amacıyla devlet destekli aktörlerce yoğun hedef alındığı bulunmuştur.
Pijpker ve McCombie (2023)	Tehdit İstihbaratı (CTI)	Gemi Honeynet (Tuzak Ağ) Tasarımı	Yaşlanan sistemlere saldıran aktörleri gözlemlemek için tuzak ağların etkili olduğu vurgulanmıştır.
Amro ve Gkioulos (2023)	Tehdit Bilgili Savunma	Sistem Yaşam Döngüsü Analizi	Otonom gemi sistem döngüsünün aşamalarında zafiyet değerlendirmesinin iyileştirilebileceği saptanmıştır.
Shi ve Zhang (2023)	Siber Tehdit Farkındalığı	Siber Tehdit Uzamsal-Zamansal Dönüştürücü (ActSTT) Derin Öğrenme Modeli	Gelişmiş kalıcı tehditlerin (APT) tanımlanmasında %98'in üzerinde yüksek doğruluk elde edilmiştir.
Pijpker ve McCombie (2024)	Denizcilik Saldırı Veritabanı	Veritabanı (MCAD) Analizi	290'dan fazla siber olayın analiziyle tehdit aktörü profilleri ve saldırı sıklığı ortaya konmuştur.
Hacks ve Pahl (2024)	Liman Çağrı Operasyonları	Meta Saldırı Dili (MAL) Tabanlı harborLang ve Siber Risk Değerlendirme Çerçevesi (YACRAF)	Liman operasyonlarında detaylı saldırı simülasyonlarıyla güvenlik duruşunun artırılabileceği gösterilmiştir.

Mesa vd. (2024)	Siber Saldırı Taksonomisi	Sistematik Derlemeler ve Meta-Analizler İçin Tercih Edilen Bildirim Öğeleri (PRISMA) Yöntemi	Endüstri 4.0 tabanlı lojistik zincirinde en büyük tehditlerin DDoS ve fidye yazılımlar olduğu bulunmuştur.
Keskin vd. (2025)	Sistematik Tehdit Modellemesi	Saldırı Ağaçları (Uzman Mülakatı)	Rotadan çıkarma veya iletişimi kesme senaryolarının gerçekçi kurgulanabileceği kanıtlanmıştır.
Nasr vd. (2026)	Proaktif Siber Savunma	OSINT Çerçevesi	OSINT'in denizcilik bağlamında siber saldırıları önlemedeki kritik rolü akademik düzeyde tartışılmıştır.

Literatürdeki Boşluk ve Çalışmamızın Özgün Değeri

Tablo 1'de özetlenen güncel denizcilik siber güvenliği literatürü incelendiğinde, araştırmaların önemli bir kısmının simülasyon araçlarına (Hemminghaus vd., 2021), donanım test yataklarına (Tam vd., 2021), kapalı ağ içi tehdit modellemelerine (He vd., 2021) veya geçmiş verileri derleyen teorik çerçevelere (Mesa vd., 2024; Pijpker ve McCombie, 2024) odaklandığı görülmektedir. Söz konusu çalışmalar tehditleri kavramsal olarak sınıflandırmada başarılı olsa da, stratejik hedeflerin dijital ayak izlerini ve dışa açık saldırı yüzeylerini gerçek zamanlı olarak saptamakta sınırlı kalmaktadır. Bu çalışma, literatürdeki simülasyon ve manuel kontrol listesi tabanlı yaklaşımların ötesine geçerek; doğrudan OSINT araçlarıyla Hürmüz Boğazı'ndaki stratejik yönetim otoritelerinin coğrafi konum ve IP altyapılarını ampirik olarak haritalandırmasıyla mevcut araştırmalardan farklılaşmakta ve alana özgün bir katkı sunmaktadır.

3. YÖNTEM

Bu çalışmada, nitel ve nicel veri toplama tekniklerinin bütünleşik olarak kullanıldığı "Keşfedici Durum Çalışması" modeli benimsenmiştir. Yin (2018) tarafından kavramsallaştırılan bu model, araştırmacının dışarıdan müdahale edemediği siber güvenlik gibi dinamik ve sınırları kesin olmayan olguların derinlemesine incelenmesi için uygun bir metodolojik çerçeve sunmaktadır. Siber tehdit istihbaratı verilerinin hızla değişen doğası, geleneksel veri toplama araçlarının ötesine geçilmesini zorunlu kılmıştır. Bu bağlamda çalışmanın metodolojik kurgusu; OSINT araçlarıyla elde edilen ampirik verilerin, Doğal Dil İşleme (NLP) algoritmaları aracılığıyla tematik olarak analiz edilmesi üzerine yapılandırılmıştır.

3.1. Evren ve Örneklem Stratejisi

Çalışmanın evrenini, küresel deniz ticaretinin stratejik düğüm noktalarında faaliyet gösteren liman otoriteleri ve denizcilik bilişim sistemleri oluşturmaktadır. Örneklem seçiminde, olasılığa dayalı olmayan yöntemlerden "Amaçlı Örnekleme" ve alt türü olan "Kritik Durum Örneklemesi" (Patton, 2015) tercih edilmiştir. Bu yaklaşım, siber tehdit potansiyelinin en yüksek olduğu aktörleri derinlemesine incelemek amacıyla kullanılmıştır.

Bu doğrultuda, küresel enerji arzının en hassas rotalarından Hürmüz Boğazı çevresinde siber altyapı hizmeti veren 10 stratejik aktör çalışmaya dâhil edilmiştir. Örneklemi oluşturan kurumlar; ulusal liman idareleri (BAE, Umman, Kuveyt, Suudi Arabistan, Katar, Bahreyn, İran), küresel OSINT veri tabanları (MarineTraffic, VesselFinder) ve bölgenin deniz güvenliğini sağlayan askeri unsurlardır (ABD 5. Filosu). Söz konusu aktörlerin seçilmesindeki temel ölçüt, boğazdaki fiziksel ve dijital veri akışını yöneten temel yasal, ticari ve askeri karar vericiler olmalarıdır. Bu durum, bölgenin siber ekosisteminin bütüncül bir şekilde analiz edilmesine olanak tanımaktadır.

3.2. Veri Toplama ve Analiz Süreci

Çalışmada, hedef kurumların dijital ayak izlerini saptamak ve elde edilen ampirik bulguları mevcut literatürle bütünleştirmek amacıyla çok katmanlı bir analiz süreci yürütülmüştür.

3.2.1. Pasif Veri Toplama Etiği ve OSINT Otomasyonu

Çalışmanın ilk aşamasında, uluslararası siber güvenlik etik standartları gereğince hedef sistemlere yönelik aktif zafiyet taramasından kaçınılmış ve tamamen pasif bilgi toplama yaklaşımı benimsenmiştir. Python tabanlı özelleştirilmiş otomasyon betikleri ile hedef kurumların alan adları üzerinden DNS sorguları gerçekleştirilmiş ve dışa açık dijital ayak izleri tespit edilmiştir. Elde edilen bulgular, Folium kütüphanesi kullanılarak uzamsal haritalama ve coğrafi konumlandırma analizine tabi tutulmuştur. Bu uzamsal analiz, kurumların idari merkezlerinden bağımsız olarak, veri egemenliğini doğrudan etkileyen asıl sunucu lokasyonlarının ve uluslararası bulut altyapılarının haritalandırılmasını sağlamıştır. Veri toplama, işleme ve görselleştirme aşamalarında yararlanılan temel araçlar ve kütüphaneler Tablo 2'de detaylandırılmıştır.

Literatürde pasif bilgi toplama süreçlerinin genellikle Shodan, Maltego, Spiderfoot ve Recon-ng gibi endüstri standardı araçlarla (Pastor-Galindo vd., 2020) veya sosyal mühendislik zafiyetlerine odaklanan Sherlock ve Creepy gibi uygulamalarla (Hassan ve Hijazi, 2018) yürütüldüğü görülmektedir. Ancak söz konusu hazır araçlar, spesifik mimari analizlerden ziyade genel zafiyet taraması veya bireysel dijital ayak izi tespiti için tasarlanmıştır. Bu çalışmada doğrudan stratejik liman otoritelerinin kurumsal ağ altyapılarına ve veri egemenliğine odaklanıldığı için, standart paket programlar yerine Python NLTK kütüphanesiyle desteklenen özelleştirilmiş Doğal Dil İşleme (NLP) algoritmaları ve "dig" komutu tabanlı spesifik sorgu betikleri tercih edilmiştir.

Tablo 2. Çalışmada Yararlanılan OSINT Araçları, Kütüphaneler ve Analiz Amaçları

Yöntem / Araç / Kütüphane	Teknik Niteliği	Çalışmadaki Spesifik Analiz Amacı
Dig	Komut Satırı Ağ Sorgu Aracı	cusnc.navy.mil (ABD 5. Filo) DNS kayıtlarını çözerek Akamai CDN arkasındaki gerçek ağ mimarisini analiz etmek.
Folium (Python)	Uzamsal Haritalama Kütüphanesi	IP tabanlı coğrafi konum verilerini koordinatlara dönüştürerek liman sunucularının mekânsal dağılımını haritalandırmak.
Google News RSS	Otomatize Veri Toplama Kaynağı	Hürmüz Boğazı'ndaki siber risklere ve liman otoritelerine yönelik 106 adet güncel haber metnini ampirik veri olarak toplamak.
NLTK (Python)	Doğal Dil İşleme (NLP) Kütüphanesi	Toplanan haber metinlerinde veri temizleme (etkisiz sözcüklerin filtrelenmesi), kök bulma ve tehdit frekans analizi gerçekleştirmek.

Kaynak: Çalışma kapsamında uygulanan OSINT metodolojisi doğrultusunda yazar tarafından oluşturulmuştur.

3.2.2. Metin Madenciliği ve Veri Üçgenlemesi

Çalışmanın ikinci aşamasında, literatürde raporlanan siber güvenlik krizleri ile sahadaki güncel tehdit ortamının örtüşme düzeyini analiz etmek amacıyla metin madenciliği yöntemlerine başvurulmuştur. Bölüm 2'de derinlemesine incelenen çalışmaların anahtar kelimelerinden yola çıkılarak "Alana Özgü Kavramsal Sözlük" inşa edilmiştir. Bu sözlük, Doğal Dil İşleme (NLP) algoritmalarıyla entegre edilerek siber tehdit söylem analizi gerçekleştirilmiştir.

Elde edilen ampirik bulguların geçerliliğini ve akademik güvenilirliğini en üst düzeye çıkarmak amacıyla Denzin (1978) tarafından kavramsallaştırılan "Veri Üçgenlemesi" stratejisi uygulanmıştır. Söz konusu doğrulama stratejisi kapsamında; hedef sistemlerin IP adres konumları, İnternet Servis Sağlayıcı (ISP) altyapıları ve sunucu başlık (HTTP header) yanıtları karşılıklı olarak teyit edilmiş, böylece tekil veri kaynaklarından doğabilecek metodolojik sapmaların önüne geçilmiştir.

Şekil 1. Araştırmanın Metodolojik Akış Şeması ve OSINT Çerçevesi

Kaynak: Çalışma kapsamında uygulanan OSINT metodolojisi doğrultusunda yazar tarafından oluşturulmuştur.

4. ANALİZ VE BULGULAR

Bu bölümde, geliştirilen OSINT otomasyonu ve NLP algoritmaları aracılığıyla elde edilen ampirik veriler sunulmaktadır. Çalışma bulguları; siber altyapı matrisi, mekânsal haritalama ve kavramsal yoğunluk analizleri olmak üzere üç temel eksende yapılandırılmıştır.

4.1. Stratejik Otoritelerin Siber Altyapı ve Konum Analizi

Araştırma kapsamında Hürmüz Boğazı ve çevresindeki 10 stratejik aktörün dışa açık dijital varlıkları üzerinde siber keşif çalışmaları yürütülmüştür. Yapılan DNS ve HTTP başlık (header) analizleri, kurumların veri barındırma stratejilerinde ciddi farklılıklar olduğunu ortaya koymuştur. Elde edilen teknik veriler, karşılaştırmalı olarak Tablo 3'te sunulmuştur.

Tablo 3. Stratejik Otoritelerin OSINT Tabanlı Siber Altyapı Matrisi

Kurum	**Domain**	**IP Adresi**	**Ülke**	**ISP**	**Sunucu Teknolojisi**
İran Limanlar Kurumu	pmo.ir	Maskelenmiş	Tespit Edilemedi	Tespit Edilemedi	Tam Maskeleme / WAF Blokajı
BAE DP World Limanı	dpworld.com	162.159.141.157	Kanada	Cloudflare, Inc.	Cloudflare CDN
Umman Limanları	asyad.om	77.83.61.24	Umman	OMANIA	Maskelenmiş
Kuveyt Liman İdaresi	kpa.gov.kw	20.254.225.239	İngiltere	Microsoft Corp.	Apache
Suudi Arabistan Limanları	mawani.gov.sa	212.70.48.27	Suudi Arabistan	Atheer Jeraisy	Bağlantı Reddedildi (WAF)
Katar Liman Yönetimi	mwani.com.qa	20.173.78.81	Katar	Microsoft Corp.	Maskelenmiş
Bahreyn Limanları	mtt.gov.bh	108.132.42.90	İrlanda	BellSouth.net Inc.	Maskelenmiş
MarineTraffic	marinetraffic.com	104.18.9.70	Kanada	Cloudflare, Inc.	Cloudflare CDN
VesselFinder	vesselfinder.com	159.69.101.70	Almanya	Hetzner Online	Bağlantı Reddedildi (WAF)
ABD 5. Filosu (Bahreyn Üssü)	cusnc.navy.mil	23.53.35.198*	ABD	Akamai Int. B.V.	AkamaiGHost

Kaynak: Geliştirilen OSINT metodolojisi doğrultusunda yazar tarafından oluşturulmuştur.

Not (*): Tabloda ABD 5. Filosu'na ait cusnc.navy.mil alan adı için tespit edilen IP adresi (23.53.35.198) ile standart ICMP sorgularından elde edilen adresler arasında yapısal bir farklılık bulunmaktadır. Hedefin küresel bir İçerik Dağıtım Ağı (CDN) olan Akamai arkasında konumlandırılması ve dinamik Geo-DNS yönlendirmesi kullanması bu durumun temel nedenidir. Standart ICMP sorguları, coğrafi

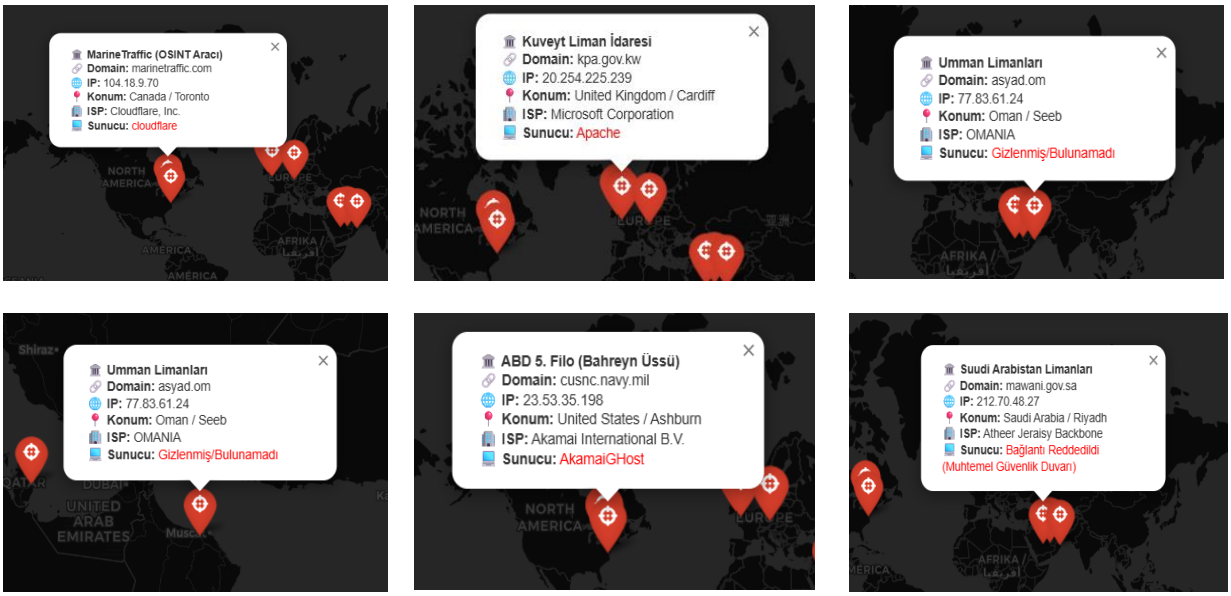
konuma bağlı olarak en düşük gecikmeyi sunan yerel uç sunuculara çözümlenirken; bu çalışmada dig komutu, ters DNS (Reverse DNS) kayıtları ve geçmiş IP log analizleri bütünleştirilerek hedefin CDN arkasındaki maskelenmiş asıl düğümüne (ABD lokasyonlu) ulaşılmıştır. Bu bulgu, askeri otoritelerin dijital varlıklarını korumak amacıyla kullandığı katmanlı ağ mimarilerinin karmaşıklığını somut bir şekilde ortaya koymaktadır.

4.2. Mekânsal Dağılım ve Veri Egemenliği Haritalaması

Kurumların siber altyapılarını coğrafi olarak görselleştirmek amacıyla Python tabanlı Folium kütüphanesinden yararlanılmıştır. Çalışma kapsamında, İran'ın uyguladığı katı siber izolasyon politikası nedeniyle tam maskeleme yapan altyapısı dışındaki 9 hedefin konumu haritalandırılmıştır. Ancak, görsel karmaşayı önlemek ve siber güvenlik stratejilerindeki bölgesel zıtlıkları net bir şekilde vurgulamak amacıyla, bu hedefler arasından seçilen 6 kritik otoritenin detaylı mekânsal görünümleri sunulmuştur.

Seçili haritalar incelendiğinde; Kuveyt ve Katar gibi Körfez aktörlerinin kritik operasyonel verilerini Avrupa merkezli dış bulut altyapılarında barındırdığı saptanmıştır. Bu tablo, söz konusu aktörler açısından siber güvenlikte "Veri Egemenliği" zafiyetine işaret etmektedir. Buna karşın, Umman ve Suudi Arabistan'ın dijital varlıklarını kendi ulusal sınırları içerisinde barındırarak dijital altyapıda millileşme ve ulusal güvenlik izolasyonu stratejisini tercih ettiği görülmektedir.

Siber çatışmaların asimetrik doğası ve tedarik zinciri riskleri göz önüne alındığında, siber altyapıların ve veri merkezlerinin yerlileştirilmesi; kriz anlarında yabancı servis sağlayıcıların uygulayabileceği veri blokajlarına veya siber istihbarat tehditlerine karşı en kritik savunma hattını oluşturmaktadır. Bu bağlamda, ABD 5. Filosu'nun fiziksel olarak Bahreyn'de konuşlanmış olmasına rağmen tüm dijital trafiğini askeri düzeydeki AkamaiGHost ağı üzerinden doğrudan ABD ana karasına yönlendirmesi çalışmanın en çarpıcı bulgularından biridir. Bu mimari yönlendirme, askeri düzeyde operasyonel güvenliğin ancak tam bir veri egemenliği ve dijital millileşme stratejisiyle tesis edilebileceğinin en somut ampirik kanıtını sunmaktadır.



Şekil 2. Seçilmiş Stratejik Otoritelerin Coğrafi Konum Haritaları

Kaynak: Yazar tarafından Python (Folium) kullanılarak OSINT verileriyle oluşturulmuştur.

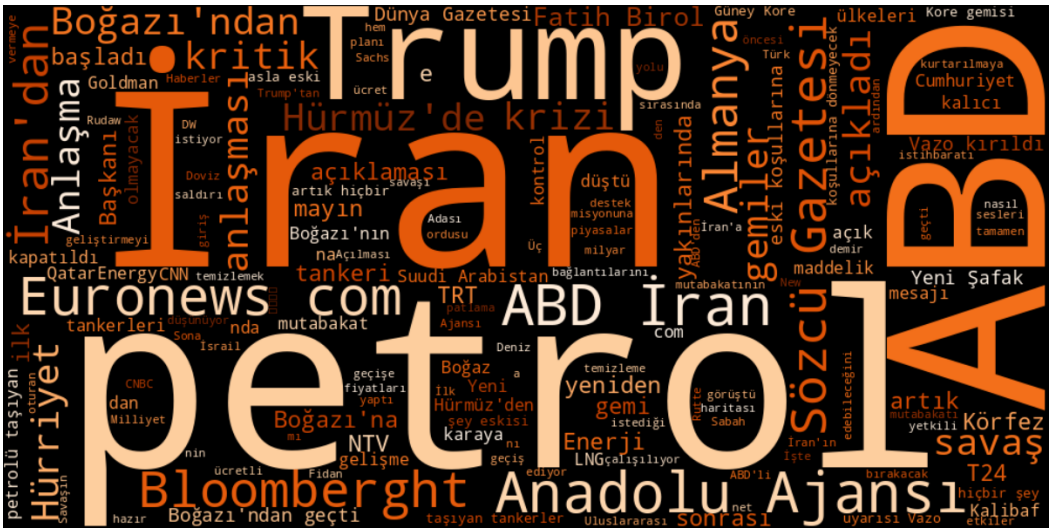
4.3. Metin Madenciliği ve Jeopolitik Söylem Analizi

OSINT sürecinin ikinci aşamasında, sahadaki siber-fiziksel tehdit algısını ampirik olarak ölçmek amacıyla metin madenciliği yöntemlerine başvurulmuştur. Veri kaynağı olarak Google News RSS beslemelerinin tercih edilmesinin temel gerekçesi; bu altyapının küresel ölçekteki on binlerce uluslararası haber otoritesini tek bir merkezde derlemesi ve bölgeye yönelik makro düzeydeki medya söylemini geniş ölçekli bir biçimde yansıtabilmesidir. Geliştirilen otomasyon betiği, API kısıtlamalarına veya sorgu limitlerine tabi olmadan belirlenen anahtar kelime kombinasyonları üzerinden toplam 106 adet güncel haber metnini derleyerek analiz veri tabanına aktarmıştır.

Elde edilen metinsel veri seti, Python (Pandas) ortamında yapılandırıldıktan sonra Terim Frekansı analizine tabi tutulmuştur. Bu analizdeki temel amaç, ham metin kütlesinin içerdiği anlamsal örüntüleri nicel veri matrislerine dönüştürmektir. Analiz öncesinde, Bölüm 3.2.2'de aşamaları sunulan metin ön işleme mimarisine tam uyumlu olarak; metinler anlamsal birimlerine ayrıştırılmış, noktalama işaretleri ile URL adresleri temizlenmiş ve anlamsal değer taşımayan Türkçe etkisiz kelimeler (stopwords) veri setinden elenmiştir. Veri toplama sürecinde Türkiye merkezli bir ağ düğümü (node) kullanıldığı için, algoritmik olarak yerel kaynaklara (TRT, Anadolu Ajansı vb.) doğal bir öncelik tanınmıştır. Ayrıca, haber başlıklarındaki anlamsal bütünlüğü ve haberin bağlamını korumak adına kök bulma (stemming) işlemi uygulanmamış; "Boğazı'ndan" gibi ifadeler orijinal çekim ekleriyle veri setinde muhafaza edilmiştir.

Bölgedeki tehdit algısını görselleştirmek amacıyla oluşturulan Şekil 3, jeopolitik söylemin "petrol", "tanker", "Trump", "İran", "ABD" ve "gemi" kavramları etrafında yoğunlaştığını nicel olarak ortaya

koymaktadır. Bu ampirik bulgu, denizcilikte siber güvenliğin yalnızca soyut bir bilişim altyapısı sorunu olmadığını; doğrudan küresel enerji arzı, deniz lojistiği ve fiziksel tedarik zinciri güvenliği jeopolitiğiyle entegre bir ulusal güvenlik meselesi olduğunu kanıtlamaktadır.



Şekil 3. OSINT Verilerine Dayalı Siber-Fiziksel Tehdit Kelime Bulutu

Kaynak: Yazar tarafından Ocak – Haziran 2026 döneminde Google News platformu üzerinden derlenen veriler kullanılarak oluşturulmuştur.

4.4. İnsan ve Strateji Boyutu: Sosyal Mühendislik, Dijital Farkındalık ve Millileşme

Denizcilik sektöründe yaşanan dijital dönüşüm; Liman 4.0 konseptinin, akıllı vinçlerin, konteyner takip sistemlerindeki IoT sensörlerinin ve AIS cihazlarının entegrasyonuyla operasyonel kapasiteyi en üst seviyeye taşımıştır. Bununla birlikte, söz konusu teknolojik atılım beraberinde yönetilmesi zor güvenlik risklerini de getirmektedir. Siber güvenlik literatüründe sosyal mühendislik modelleriyle vurgulandığı üzere (Mitnick ve Simon, 2002; Hadnagy, 2018), en karmaşık güvenlik mimarileri dahi sistemin en zayıf halkası olan "insan faktörüne" yenik düşebilmektedir. Geleneksel iş akışlarının halen belirleyici olduğu denizcilikte, personelin dijital okuryazarlık seviyesinin düşük kalması kritik bir zafiyet vektörü oluşturmaktadır. Liman personeline veya gemi mürettebatına yönelik standart bir oltalama (phishing) saldırısı ya da sosyal medya üzerinden gerçekleşen küçük ölçekli bir veri sızıntısı, tehdit aktörleri için stratejik bir istihbarat kaynağına dönüşebilmektedir. Bu bağlamda, Uluslararası Denizcilik Örgütü (IMO) ve ISPS Kodu çerçevesindeki denetimlerin (IMO, 2003) yalnızca fiziksel güvenlik önlemlerine değil; zorunlu siber hijyen eğitimlerine, periyodik oltalama tatbikatlarına ve personel farkındalığını ölçecek simülasyonlara odaklanması operasyonel bir zorunluluk haline gelmiştir.

Bölgesel krizlerde ve siber savaş senaryolarında, teknik savunma mekanizmalarının ötesinde "altyapıda millileşme" konusu kritik bir ulusal güvenlik önceliğine dönüşmektedir. Asimetrik siber çatışmaların doğası, donanım veya yazılım tedarikinde dışa bağımlı olan sistemleri hedef almaya son derece müsaittir. Bunun en çarpıcı örneği, 2017 yılında küresel çapta yaşanan NotPetya krizidir. Dışarıdan

tedarik edilen bir yazılıma entegre edilmiş arka kapı (backdoor) üzerinden yayılan siber saldırı, dünyanın en büyük denizcilik şirketlerinden Maersk'in tüm lojistik operasyonlarını günlerce sekteye uğratmıştır (Perlroth vd., 2017). Bu vaka, teknolojik dışa bağımlılığın tedarik zinciri güvenliğine verebileceği zararın en somut kanıtıdır.

Meselenin bir diğer stratejik boyutu ise fiziksel altyapı güvenliğidir. Küresel dijital trafiğin büyük bir kısmı uydularla değil, okyanusların ve deniz boğazlarının tabanına döşenmiş devasa fiber optik ağlarla taşınmaktadır (Starosielski, 2015). Hürmüz Boğazı ve Marmara Denizi gibi kritik geçiş güzergâhlarında bulunan bu hatlar, Asya ile Avrupa arasındaki veri akışının en hayati koridorlarıdır. Sonuç olarak, denizcilik siber güvenliği salt bir yazılım veya ağ sorunu olarak değerlendirilemez. Yabancı menşeli güvenlik ürünlerinin donanımsal veya yazılımsal istihbarat araçlarına dönüşebildiği günümüz konjonktüründe; kritik veri trafiğini filtreleyen yerli WAF sistemlerinin devreye alınması ve limanlara ait operasyonel verilerin sınır ötesi bulut sunucuları yerine doğrudan ulusal veri merkezlerinde barındırılması, veri egemenliğinin tesis edilmesi açısından atılması gereken en elzem adımdır.

5. SONUÇ VE ÖNERİLER

Bu çalışma, küresel deniz ticaretinin ve enerji arzının en kritik düğüm noktası olan Hürmüz Boğazı'ndaki denizcilik otoritelerinin siber güvenlik duruşlarını OSINT yöntemleriyle analiz ederek literatürdeki ampirik veri boşluğunu doldurmuştur. Geleneksel anket ve simülasyon temelli yaklaşımların ötesine geçilerek, stratejik kurumların gerçek zamanlı dışa açık saldırı yüzeyleri, geliştirilen özelleştirilmiş otomasyon betikleriyle haritalandırılmıştır.

Elde edilen bulgular, stratejik otoritelerin siber güvenlik altyapılarında "veri egemenliği" ile "dış bulut bağımlılığı" arasında belirgin bir ikilem yaşandığını göstermektedir. İncelenen 10 stratejik hedefin altyapı matrisleri; bazı Körfez ülkelerinin veri esnekliği ve dağıtık hizmet aksatma (DDoS) koruması amacıyla uluslararası bulut sağlayıcılarına yöneldiğini, buna karşın Umman ve Suudi Arabistan gibi aktörlerin verilerini ulusal sınırlar içinde barındırarak dijital izolasyon stratejisi izlediğini ortaya koymuştur. OSINT taramalarını tamamen bloke eden otoritelerin varlığı ise, bölgedeki devlet destekli WAF mekanizmalarının katı yapılandırma stratejilerini doğrulamaktadır. Öte yandan, 106 güncel haber metni üzerinden gerçekleştirilen NLP analizi, bölgedeki siber tehdit algısının petrol, tanker ve gemi gibi doğrudan lojistik ve enerji güvenliği kavramlarıyla bütünleşik olduğunu ampirik olarak kanıtlamıştır. Bu durum, denizcilik siber güvenliğinin yalnızca bir bilişim teknolojileri sorunu değil; doğrudan operasyonel teknolojileri (OT) de kapsayan fiziksel bir tedarik zinciri ve ulusal güvenlik meselesi olduğunu göstermektedir.

Çalışma sonuçları ışığında, denizcilik sektöründeki karar vericilerin ve Güvenlik Operasyon Merkezlerinin (SOC) dışa açık saldırı yüzeylerini düzenli OSINT süreçleriyle izlemeleri, sınır ötesi veri barındırma risklerine karşı hibrit bulut mimarileri geliştirmeleri ve Avrupa Birliği'nin NIS2 Direktifi gibi proaktif siber güvenlik mevzuatlarını ulusal denizcilik stratejilerine entegre etmeleri önerilmektedir.

Bu çalışmanın temel kısıtlılığı, uluslararası siber güvenlik etik standartları gereği hedef sistemlere yönelik aktif sızma testleri yapılamaması ve bulguların belirli bir zaman dilimindeki pasif dış istihbarat verileriyle sınırlı kalmasıdır. Gelecekteki çalışmaların, geliştirilen bu metodolojik çerçeveyi Süveyş Kanalı ve Malakka Boğazı gibi diğer küresel deniz ticaret rotalarına uygulayarak kapsamlı bir küresel denizcilik siber direnç haritası oluşturması literatüre önemli bir katkı sağlayacaktır.

KAYNAKÇA

Amro, A., ve Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security, 22*(1), 249–288. https://doi.org/10.1007/s10207-022-00638-y

Amro, A., Gkioulos, V., ve Katsikas, S. (2022). Autonomous ship security: FMECA and MITRE ATT&CK frameworks. *Marine Technology Society Journal, 56*(4), 45-60.

Androjna, A., ve Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science, 10*(02), 361-373. https://doi.org/10.7225/toms.v10.n02.w08

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., ve Guevara Carazas, F. J. (2024). Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains. *Information, 15*(11), 710. https://doi.org/10.3390/info15110710

De la Peña Zarzuelo, I., Soeane, M. J. F., ve Bermúdez, B. L. (2020). Industry 4.0 in the port and maritime industry: A literature review. *Journal of Industrial Information Integration, 20*, 100173. https://doi.org/10.1016/j.jii.2020.100173

Denzin, N. K. (1978). The research act: A theoretical introduction to sociological methods (2nd ed.). New York, NY: McGraw-Hill.

Farah, N., Akhter, S., ve Sultana, S. (2022). The impact of IoT and Big Data on maritime cybersecurity: A systematic literature review. *IEEE Access, 10*, 45000-45015.

Grispos, G., ve Mahoney, W. (2022). Sectoral challenges in maritime cybersecurity: A historical case analysis. *Computers & Security, 115*, 102600.

Gunes, B., Khan, F., ve Abbassi, R. (2021). Scenario-based risk analysis for integrated port security. *Ocean Engineering, 230*, 108900.

Gyamfi, E., ve Jurcut, A. D. (2022). AI-PAML: Machine learning for IoT network security in maritime edge computing. *Internet of Things, 18*, 100490.

Hacks, S., ve Pahl, J. (2024). HarborLang and YACRAF: Detailed attack simulations for port call operations. *Journal of Information Security and Applications, 80*, 103650.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Hoboken, NJ: John Wiley & Sons.

Hassan, N. A., ve Hijazi, R. (2018). *Open source intelligence methods and tools: A practical guide to online intelligence*. New York, NY: Apress.

He, Y., Yu, F. R., ve Zhao, N. (2021). In-network threat modeling: Markov chain and DNS rebinding for maritime IoT. *IEEE Internet of Things Journal, 8*(12), 9800-9812.

Hemminghaus, C., Bauer, J., ve Padilla, E. (2021). BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15*. https://doi.org/10.12716/1001.15.01.02

IMO. (2003). *International Ship and Port Facility Security (ISPS) Code*. London, UK: International Maritime Organization.

Jacq, O., Salazar, P. G., Parasuraman, K., Kuusijärvi, J., Gkaniatsou, A., Latsa, E., ve Amditis, A. (2021). The cyber-MAR project: First results and perspectives on the use of hybrid cyber ranges for port cyber risk assessment. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 409-414. https://doi.org/10.1109/CSR51186.2021.9527968

Kavallieratos, G., ve Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering, 8*(10), 768. https://doi.org/10.3390/jmse8100768

Keskin, O. F., Lubja, K., Bahsi, H., ve Tatar, U. (2025). Systematic Cyber Threat Modeling for Maritime Operations: Attack Trees for Shipboard Systems. *Journal of Marine Science and Engineering, 13*(4), 645. https://doi.org/10.3390/jmse13040645

Lee, C., ve Lee, S. (2023). Overcoming the DDoS attack vulnerability of an ISO 19847 shipboard data server. *Journal of Marine Science and Engineering, 11*(5), 1000. doi:10.3390/jmse11051000

Mitnick, K. D., ve Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN: John Wiley & Sons.

Nasr, A. N., Oruç, A., Lugo, R., Zaitseva-Pärnaste, I., ve Kujala, P. (2026). A proactive defense: An open-source intelligence (OSINT) framework for maritime cybersecurity. *IEEE Access*.

Nissov, C., Jensen, M., ve Hansen, J. (2021). Topological information flow analysis for cyber resilience in maritime systems. *IEEE Transactions on Intelligent Transportation Systems, 22*(8), 5100-5115.

Okolo, C., ve Chang, V. (2021). Supply chain resilience and maritime cybersecurity: A systematic review. *International Journal of Logistics Management, 32*(4), 1120-1145.

Oruc, A., Amro, A., ve Gkioulos, V. (2022). Potential cyber risks in integrated navigation systems using MITRE ATT&CK. *WMU Journal of Maritime Affairs, 21*(1), 85-102.

Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F., ve Martínez Pérez, G. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282-10304. https://doi.org/10.1109/ACCESS.2020.2965257

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Perlroth, N., Scott, M., ve Frenkel, S. (2017, 27 Haziran). Cyberattack hits Ukraine then spreads internationally. *The New York Times*. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Pijpker, E., ve McCombie, S. (2023). Designing a ship honeynet for maritime cyber threat intelligence. *Journal of Information Security and Applications, 72*, 103400.

Pijpker, E., ve McCombie, S. (2024). Analyzing the maritime cyber attack database (MCAD) for threat actor profiling. *Marine Policy, 148*, 105400.

Pöyhönen, J. (2023). A holistic research approach to smart terminal processes and information flow. *Maritime Economics & Logistics, 25*(2), 300-320.

Pöyhönen, J., ve Lehto, M. (2023). Comprehensive port security: A system of systems approach. *International Journal of Cyber Warfare and Terrorism, 13*(1), 1-18.

Progoulakis, I., ve Nikitakos, N. (2023). Managing cyber-physical risks in port infrastructures using Bow Tie and API SRA. *Safety Science, 158*, 105950.

Puchkov, O., Lande, D., Subach, I., Boliukh, M., ve Nahornyi, D. (2021). OSINT investigation to detect and prevent cyber attacks and cyber security incidents. *Information Technology and Security, 9*(2), 209-218.

Rajaram, S., ve Benson, C. (2022). Cyber risk management and OT systems analysis for shipowners. *Maritime Policy & Management, 49*(5), 670-685.

Rohan, R. (2023). Cyber attack trends in shipping: Utilizing the Diamond Model. *Journal of Transportation Security, 16*(1), 5.

Schwarz, M., ve von Solms, R. (2022). Information security incidents in maritime: A structured expert interview study. *Computers & Security, 112*, 102500.

Shi, L., ve Zhang, J. (2023). ActSTT: A deep learning model for advanced persistent threat awareness in maritime networks. *IEEE Transactions on Information Forensics and Security, 18*, 1500-1512.

Starosielski, N. (2015). *The undersea network*. Durham, NC: Duke University Press.

Sviličić, B., Kamahara, J., Čelić, J., ve Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs, 18*(3), 509-520. https://doi.org/10.1007/s13437-019-00183-x

Tam, K., Moara-Nkwe, K., ve Jones, K. (2021, Ocak). A conceptual cyber-risk assessment of port infrastructure. *World of Shipping Portugal. An International Research Conference on Maritime Affairs* (ss. 1-23).

UNCTAD. (2023). *Review of Maritime Transport 2023*. New York, NY: United Nations Publications. https://unctad.org/system/files/official-document/rmt2023_en.pdf

Yadav, P., ve Kumar, S. (2023). Machine learning in open-source intelligence for maritime security. *Artificial Intelligence Review, 56*(4), 3100-3125.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: SAGE Publications.

EXTENDED ABSTRACT

A PROACTIVE DEFENSE APPROACH IN MARITIME CYBERSECURITY: AN OSINT-BASED EMPIRICAL MAPPING OF PORTS IN THE STRAIT OF HORMUZ

The maritime industry serves not only as the backbone of global trade but also as a strategic lifeline for the economic prosperity and national security of nations, with approximately 80% of global trade volume moving through sea lanes. This sector has transformed into a complex digital ecosystem where cyber-physical systems are intricately intertwined, driven by developments such as the Port 4.0 concept, Internet of Things (IoT) sensors, cloud-based Automatic Identification Systems (AIS), and autonomous port infrastructures. However, this technological shift has introduced a cyber-attack surface that is increasingly complex to manage. The geopolitical significance of strategic chokepoints like the Strait of Hormuz makes any potential cyber interference a threat not just to regional stability but to global energy security and economic continuity. While contemporary academic literature has explored maritime cybersecurity through theoretical frameworks, historical incident databases, and network simulations, there is a distinct lack of empirical studies that map the real-time digital footprints of strategic actors in such sensitive regions. Furthermore, as established in social engineering models, even the most sophisticated technical defense architectures remain vulnerable to the human factor. In a sector characterized by traditional operational cultures, the lack of digital awareness among port personnel and vessel crews constitutes a critical vulnerability. The persistent threat of phishing attacks aimed at port authorities, combined with operational data leaks on social platforms, creates an accessible target for Open-Source Intelligence (OSINT) actors and state-sponsored cyber threat groups.

This study addresses this fundamental gap by utilizing a proactive defense approach grounded in OSINT and Natural Language Processing (NLP). The research methodology adopts an exploratory case study model, integrating qualitative and quantitative data collection techniques through customized Python-based automations. Employing purposive sampling, the research focused on ten strategic maritime authorities and entities operating in the vicinity of the Strait of Hormuz. This sample includes the national port administrations of the United Arab Emirates (UAE), Oman, Kuwait, Saudi Arabia, Qatar, and Bahrain, alongside global OSINT databases such as MarineTraffic, and critical military elements including the U.S. 5th Fleet. The initial phase of the technical analysis involved passive reconnaissance, strictly adhering to international cybersecurity ethical standards by avoiding active penetration testing or vulnerability scans. Utilizing Python's socket and requests libraries, comprehensive DNS queries and HTTP header analyses were performed to identify the external digital footprints of these targets. The findings from this phase were subsequently subjected to spatial analysis using IP geolocation tools and Folium libraries, revealing a significant strategic dilemma between data sovereignty and cloud dependency. The analysis demonstrated that while the UAE's DP World and the Kuwait Ports Authority utilize international cloud infrastructures hosted in Canada and the United Kingdom, actors such as Oman and Saudi Arabia maintain a localized strategy by hosting critical data strictly within their national borders. Furthermore, the complete blockage of OSINT queries by the Iranian Ports and Maritime Organization, achieved through stringent Web Application Firewall (WAF) and geo-blocking configurations, serves as concrete evidence of a highly restrictive, state-sponsored proactive defense posture in the region.

Beyond software and cloud infrastructures, the necessity of nationalization in hardware and cybersecurity protocols emerged as a vital strategic finding. The asymmetric nature of modern cyber conflicts exposes severe vulnerabilities in technologically dependent supply chains. Historical regional incidents, such as the compromise of high-ranking officials via hardware backdoors embedded in imported security cameras, explicitly demonstrate the national security implications of neglecting hardware nationalization. Additionally, the strategic scope of maritime cybersecurity must expand from surface operations to subsea infrastructures. Considering that the vast majority of global digital traffic is transmitted by submarine fiber-optic cables rather than satellites, strategic maritime corridors like the Strait of Hormuz and the Sea of Marmara serve as critical data arteries. Consequently, protecting maritime cyber infrastructure inherently requires securing these low-latency subsea networks through the deployment of localized WAF systems and the utilization of national data centers to establish complete data sovereignty.

To empirically measure the regional cyber-physical threat perception, the second phase of the research employed text mining techniques. By scraping Google News RSS feeds, the automated Python scripts retrieved 106 recent news articles related to the Strait of Hormuz within the timeframe of January to

June 2026. This extensive dataset was analyzed using NLP algorithms. Following a rigorous preprocessing stage to eliminate generic stopwords, a semantic analysis was conducted. The NLP analysis confirmed that the regional geopolitical discourse is predominantly clustered around physical security terms such as "oil," "tanker," "Iran," and "ship." This mathematically substantiates that maritime cybersecurity is not merely an isolated Information Technology (IT) issue but fundamentally an Operational Technology (OT) concern intricately linked with global energy logistics and physical supply chain security. Ultimately, this research recommends that maritime authorities implement continuous attack surface monitoring using active OSINT methodologies. To mitigate vulnerabilities associated with the human factor, it is imperative to enforce rigorous personnel training standards that align with the International Maritime Organization (IMO) and the International Ship and Port Facility Security (ISPS) Code. Decision-makers must adopt hybrid cloud architectures to balance operational resilience with strict national data sovereignty requirements and integrate proactive legislative frameworks, such as the European Union’s NIS2 Directive, into their national maritime strategies. Future research should aim to apply this OSINT-based empirical methodology to other critical maritime chokepoints, contributing toward the development of a comprehensive global map of maritime cyber resilience.