T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DENİZCİLİK İŞLETMELERİ YÖNETİMİ ANABİLİM DALI
DENİZCİLİK İŞLETMELERİ YÖNETİMİ BİLİM DALI

DENİZCİLİKTE SİBER RİSKLERİN DEĞERLENDİRİLMESİ VE YÖNETİMİ

(YÜKSEK LİSANS TEZİ)

Durmuş Ali YANIK

KOCAELİ 2022

T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DENİZCİLİK İŞLETMELERİ YÖNETİMİ ANABİLİM DALI
DENİZCİLİK İŞLETMELERİ YÖNETİMİ BİLİM DALI

DENİZCİLİKTE SİBER RİSKLERİN DEĞERLENDİRİLMESİ VE YÖNETİMİ

(YÜKSEK LİSANS TEZİ)

Durmuş Ali YANIK

Doç. Dr. Murat YORULMAZ

KOCAELİ 2022

T.C. KOCAELİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DENİZCİLİK İŞLETMELERİ YÖNETİMİ ANABİLİM DALI
DENİZCİLİK İŞLETMELERİ YÖNETİMİ BİLİM DALI

DENİZCİLİKTE SİBER RİSKLERİN DEĞERLENDİRİLMESİ VE YÖNETİMİ

(YÜKSEK LİSANS TEZİ)

Tezi Hazırlayan: Durmuş Ali YANIK
Tezin Kabul Edildiği Enstitü Yönetim Kurulu Karar ve No: 28.09.2022 / 26

KOCAELİ 2022

İÇİNDEKİLER

BİRİNCİ BÖLÜM

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

DÖRDÜNCÜ BÖLÜM

ÖZET

Küresel denizcilik endüstrisi gelişen teknolojiye giderek daha fazla bağımlı hale geldikçe, siber saldırıların kapsamının ve uluslararası denizcilik sektörü üzerindeki olası etkilerinin daha fazla farkında olunması ve anlanması önemlidir. Denizcilik endüstrisinin bilgi ve iletişim teknolojilerine artan bağımlılığı, siber risk yönetimine yüksek bir prim vermektedir. Özellikle gemiler dünya mallarının yüzde 90'ının taşımacılık taleplerini karşılamak için daha sofistike ve bağlantılı hale geldikçe, siber riskler artmakta ve risk yönetimine ihtiyaç duyulmaktadır.

Bir sektördeki tehditleri tanımlamak ve önceliklendirmek için standart risk değerlendirmeleri kullanılır. Bununla birlikte, denizcilikte artan siber güvenlik riskleri, genellikle bir dizi çevresel, teknik ve sosyal faktöre bağlıdır. Bu çalışmada denizcilik sektörüne yönelik tehdit unsuru oluşturan siber risklerin belirlenmesi, değerlendirilmesi ve bu tehditlerin azaltılması veya mümkünse sonlandırılmasına yönelik çözüm önerileri üretilmesi amaçlanmıştır. Bu bağlamda denizcilik sektörünün çeşitli alt dallarında siber tehditlere ilişkin tutumların belirlenebilmesi adına liman, armatör, freight forwarder, acente ve brokerlik işletmelerinden 10 ayrı uzman ile siber risklerin azaltılması ve önlenmesine yönelik değerlendirmeleri talep edilmiştir. Uygulamada karmaşık faktörler arasındaki nedensellik ilişkilerini gösteren yapısal bir model oluşturmak ve analiz etmek için kullanılan bir yöntem olan bulanık DEMATEL kullanılmıştır. Buna ek olarak ağırlıklandırılan kriterler PROMETHEE ve bulanık PROMETHEE yöntemiyle değerlendirilmiş olup kısmi ve net sıralamaları hesaplanmıştır.

Verilerin analizi sonucunda siber risklerin çözümünde yönetim temelli yaklaşım en önemli faktör olarak belirlenmiş, bununla beraber siber güvenlik konusuna en fazla önem veren aktörlerin armatörler ve liman işletmeleri olduğu belirlenirken, değerlendirmeye katılan işletmeler arasında siber risklere karşı en hazırlıksız olanların ise acenteler olduğu tespit edilmiştir. Bu çalışmanın en önemli katkısı denizcilik özelinde siber riskleri belirlemesi ve analiz etmesidir. Siber risklere yönelik çözüm yaklaşımlarının neden-sonuç ilişkilerinin belirlenmesi ve denizcilik sektöründe hizmet gösteren farklı aktörlerin kendi şirketlerindeki uygulamaları

değerlendirerek siber risklerle mücadelede ne durumda olduklarının farkındalığını yaratma konusunda rehberlik etmesi sebebiyle de çalışmanın özel sektör uygulayıcılarına büyük bir fayda sağlaması beklenmektedir. Ayrıca denizcilik alanında bulanık DEMATEL ve bulanık PROMETHEE yöntemlerinin bütünleşik olarak kullanıldığı ilk çalışma olması sebebiyle literatüre önemli bir katkıda bulunmuştur.

Anahtar Kelimeler: Denizcilik, Dijital Dönüşüm, Siber risk, Bulanık Mantık, Dematel, Promethee

ABSTRACT

As the global shipping industry becomes increasingly dependent on emerging technology, it is important to be more aware and understand the extent of cyberattacks and their potential impact on the international shipping industry. The maritime industry's growing dependence on information and communication technologies places a high premium on cyber risk management. Cyber risks are increasing and risk management is needed, especially as ships become more sophisticated and connected to meet the transportation demands of 90 percent of the world's goods.

Standard risk assessments are used to identify and prioritize threats in an industry. However, increasing cybersecurity risks in shipping are often linked to a number of environmental, technical and social factors. This study aims to identify and evaluate the cyber risks that pose a threat to the maritime sector and to offer solutions for minimizing or, if possible, eliminating these threats. In this context, in order to determine the attitudes towards cyber threats in various sub-branches of the maritime industry, evaluations of 10 experts from port, shipowner, freight forwarder, agency, and broker companies on reducing and preventing cyber risks were requested. In application, the fuzzy DEMATEL method, which is a method used to create and analyze a structural model showing the causal relationships between complex factors, was used. In addition, the weighted criteria were evaluated with the PROMETHEE and fuzzy PROMETHEE method and their partial and net rankings were calculated.

As a result of the analysis of the data, it has been determined that the managment based approach has been identified as the most important factor in the solution of cyber risks, also the actors that attach the most importance to cyber security are shipowners and port businesses, while agencies are the most unprepared for cyber risks among the companies participating in the evaluation. This study has made a significant contribution to the literature as it is the first study in which fuzzy DEMATEL and PROMETHEE methods are used in an integrated manner in the maritime sector. Another important contribution of the study is the analysis of cyber

risks. It is expected that the study will provide a great benefit to private sector practitioners, as it will determine the cause-effect relationships of solution approaches to cyber risks and guide managers from different sub-branches serving in the maritime sector to evaluate the practices in their own companies and to raise awareness of their situation in the fight against cyber risks.

Keywords: Maritime, Digital Transformation, Cyber risk, Fuzzy Logic, Dematel, Promethee

SİMGELER VE KISALTMALAR LİSTESİ

AB	**: Avrupa Birliği**
ABD	**: Amerika Birleşik Devletleri**
AEMC	**: Otonom Motor İzleme ve Kontrol**
AI	**: Yapay Zeka**
AIS	**: Otomatik Tanımla Sistemi**
AR	**: Artırılmış Gerçeklik**
ARPA	**: Otomatik Radar Çizme Yardımı**
ASC	**: Otonom Gemi Kontrolörü**
BIMCO	**: Baltık ve Uluslararası Denizcilik Konseyi**
BT	**: Bilgi Teknolojileri**
CC	**: Bulut Bilişim**
CCTV	**: Kapalı Devre Televizyon**
CSP	**: Siber Güvenlik Planı**
DDoS	**: Hizmet Reddi**
DEMATEL	**: The Decision Making Trial and Evaluation Laboratory**
DLP	**: Veri Kaybını Önleme Sistemi**
ECDIS	**: Elektronik Harita Görüntüleme ve Bilgi Sistemi**
ENISA	**: Avrupa Ağ ve Bilgi Güvenliği Ajansı**
EPIRB	**: Tehlike Anında Manuel veya Otomatik Olarak Etkinleştirilebilen Uyarı İşaretleri**
FBI	**: Federal Soruşturma Bürosu**
FMA	**: Çok Faktörlü Kimlik Doğrulama**
GMDSS	**: Küresel Deniz Tehlike ve Güvenlik Sistemi**
GPS	**: Küresel Konumlandırma Sistemi**
ICS	**: Uluslararası Deniz Ticaret Odası**
IEC	**: Uluslararası Elektroteknik Komisyonu**
IMO	**: Uluslararası Denizcilik Örgütü**
INTERCARGO	**: Uluslararası Kuru Yük Armatörleri Birliği**
INTERTANKO	**: Uluslararası Bağımsız Tanker Sahipleri Birliği**
IoT	**: Nesnelerin İnterneti**
IRISL	**: İran İslam Cumhuriyeti Denizcilik Hatları**

ISO	**: Uluslararası Standardizasyon Örgütü**
ISPS	**: Uluslararası Gemi ve Liman Tesisleri Güvenlik Koduna**
IUMI	**: Uluslararası Deniz Sigortaları Birliği**
JNPCT	**: JN Port Container Terminal**
JNPT	**: Jawaharlal Nehru Port Trust**
MASS	**: Deniz Otonom Yüzey Gemisi**
MSI	**: Deniz Güvenlik Bilgileri**
NIST	**: Ulusal Standartlar ve Teknoloji Enstitüsü**
NSA	**: Ulusal Güvenlik Ajansı**
OCIMF	**: Petrol Şirketleri Uluslararası Deniz Forumu**
OECD	**: Ekonomik Kalkınma ve İşbirliği Örgütü**
OT	**: Operasyonel Teknolojiler**
PROMETHEE	**: The Preference Ranking Organization Method for Enrichment Evaluation**
RADAR	**: Radyo Yönü ve Menzil**
RCC	**: Kurtarma Koordinasyon Merkezi**
SART	**: Arama ve Kurtarma Aktarıcısı**
SCC	**: Kıyı Kontrol Merkezi**
SOLAS	**: Uluslararası Denizde Can Güvenliği Sözleşmesi**
SYBASS	**: Süperyat Üreticileri Derneği**
TMSA	**: Tanker Yönetimi ve Öz Değerlendirme Forumu**
UNCTAD	**: Birleşmiş Milletler Ticaret ve Kalkınma Konferansı**
USB	**: Evrensel Seri Veriyolu**
USD	**: Amerika Doları**
WSC	**: Dünya Denizcilik Konseyi**
VDR	**: Seyahat Veri Kaydedici**
VHF	**: Çok Yüksek Frekans**
VPN	**: Sanal Özel Ağ**
VTS	**: Gemi Trafik Hizmeti**

TABLOLAR VE ŞEKİLLER LİSTESİ

GİRİŞ

Deniz taşımacılığı küreselleşen dünyada ticaret için hayati öneme sahip muazzam ulaşım yolları oluşturmakta ve uzak bölgelere neredeyse sınırsız erişim sağlamaktadır. Sürdürülebilir kalkınma, düşük maliyet, verimlilik ve son zamanlarda önemi artan çevre dostu operasyonlar ile talep eden pazarlarda, denizcilik sektörü tüm malların taşınmasının %90'ından sorumludur (Koukaki ve Tei, 2020). Deniz taşımacılığı bağlantıları, müşteriler, tedarikçiler, nakliyeciler, acenteler ve yönetim organları gibi deniz lojistiği varlıklarının yayılması ve birbirine bağlanması için kritik öneme sahiptir (Lee ve Song, 2010). Geniş bir alana sahip olan denizcilik, çok fazla paydaşın bir arada bulunduğu ve büyük ölçüde yönetilmeyen bir alan olan denizcilik, sınırlarının gözetilememesinden yararlanan devlet dışı suç aktörlerinin çoğalmasına eğilimlidir. Özellikle; deniz haydutluğu ve denizde soygun, kaçak balıkçılık faaliyetleri, uyuşturucu, insan ve silah kaçakçılığı, terör faaliyetleri, yasadışı göç ve bazı devletlerin denizde yıkıcı faaliyetleri, 21. yüzyılın deniz güvenliği sorunlarında kilit rol oynamaktadır (Fitton, vd., 2015).

Denizcilik sektörü, yeni teknolojilerin uygulanması veya yeni pazar çözümlerinin geliştirilmesi söz konusu olduğunda genellikle tutucu olarak kabul edilmiştir (Acciaro, vd., 2018). Günümüz denizcilik operasyonlarında dijitalleşme, entegrasyon, otomasyon ve ağ tabanlı sistemlere artan bir güven vardır. Teknoloji ve bağlantı kullanımındaki bu artış, denizdeki operasyonları siber risklere karşı savunmasız hale getirmektedir. (DiRenzo, vd., 2015; McGillivary, 2018). Deniz taşımacılığı teknolojik olarak daha gelişmiş hale geldikçe, limanlarda ve gemilerde uzaktan kontrol özerkliğinin artması siber riskleri de artırmaktadır (Wilshusen, 2015). Büyük kargo gönderileri, nihai varış noktalarına ulaşmadan önce genellikle okyanuslar boyunca haftalarca seyahat eder, bu da suça ilişkin kanıtları ortadan kaldırmak için yeterli zaman yaratır ve kargoları siber saldırılara karşı oldukça savunmasız hale getirir (Jones, vd., 2016).

Teknolojinin hızlı gelişimi yanında küresel olayların siber güvenlik üzerindeki etkisi de oldukça fazladır ve en güncel, çarpıcı örneklerden biri de COVID-19 pandemisinin patlak vermesiyle teknolojideki değişimdir. Pandemi süreci her ne

kadar dijitalleşme üzerinde olumlu etki yaratsa da (Pandey ve Pal, 2020), bazı güvelik sorunlarını da beraberinde getirmektedir (Pranggono ve Arabo, 2021). Şubat 2020'den bu yana, siber suçluların fidye yazılımı ve kimlik avı e-postaları kullanarak bilgisayarları hedef almasıyla denizcilik sektörüne yönelik siber saldırılarda çarpıcı bir artış olduğu ortaya çıkmıştır (Lallie, vd., 2021).

Bir gemide, bilgisayar tabanlı sistemler, bir dizi bilgi teknolojisi bileşeni (örneğin, kişisel bilgisayarlar (PC'ler), dizüstü bilgisayarlar, tablet cihazlar, sunucular ve ağ bileşenleri) ve operasyonel teknolojiden (örneğin, kontrol sistemleri, sensörler, aktüatörler, radar) mevcut gemi kontrol sistemleri, navigasyon ve sevk kontrolü gibi karmaşık işlevleri gerçekleştirmek için önemli düzeyde otomasyon içerir. Otomatik sistemlerin kullanılmasının amacı, maliyeti düşürmek ve performansı artırmak olmuştur. Otomasyon mükemmel faydalar sunarken, aynı zamanda bir dizi siber güvenlikle ilgili riski de beraberinde getirmektedir (Babineau, vd., 2012).

Son yıllarda sektörler otomasyon teknolojileri, Yapay Zeka (AI), büyük veri, bulut bilişim, Nesnelerin İnterneti (IoT) ve siber-fiziksel sistemlerin tanıtılması ve benimsenmesi yoluyla gelişmektedir. Dijitalleşme, denizcilik endüstrisini geleneksel sınırlarının ötesine taşımakta ve lojistiğin üretkenliğini, verimliliğini ve sürdürülebilirliğini artırmak için birçok yeni fırsat sunmaktadır. Dördüncü sanayi devriminin, akıllı gemilerin ve otonom gemilerin yeni ve tamamen birbirine bağlı bir deniz ekosisteminin parçası olduğu deniz taşımacılığı ve denizcilik sektörleri üzerinde radikal değişikliklere sebep olan yıkıcı bir etkiye sahip olması beklenmektedir. Fakat dijital teknolojilerin sektör üzerindeki bu dominasyonu çeşitli tehlikeleri de beraberinde getirmektedir. Özellikle siber güvenlik, çok sayıda ekonomik kayba, kişisel veya şirket bilgilerinin ihlaline vb. neden olan birçok rapor edilen siber saldırı olayı nedeniyle denizcilik endüstrisinde önemli bir konu haline gelmiştir. Bu bağlamda denizcilik sektörüne yönelik tehdit unsuru oluşturan siber risklerin belirlenmesi, değerlendirilmesi ve bu tehditlerin azaltılması veya mümkünse sonlandırılmasına yönelik çözüm önerileri üretilmesi büyük önem taşımaktadır. Çalışmamızın temel amacı akademik literatürde ve sektörel uygulamalarda fayda sağlayabilmek adına denizcilikteki siber riskleri tespit etmek ve sorunların çözümlenmesine katkı sağlayabilecek çözüm önerileri geliştirmektir. Bu amaç

doğrultusunda denizcilikte siber risklere çözüm yaklaşımlarının ağırlıklandırılması bulanık DEMATEL yöntemiyle gerçekleştirilmiş olup denizcilik aktörlerinin bu yaklaşımlara yönelik bakış açıları ise PROMETHEE ve bulanık PROMETHEE yöntemleriyle değerlendirilmiştir. Denizcilikte siber risklere hangi aktörlerin daha fazla önem verdikleri ve kendi aralarındaki üstünlükleri ortaya çıkarılmıştır. Bu çalışma hem kullanılan yöntemler açısından hem de denizcilikte siber risklere karşı çözüm yaklaşımlarını aktörlerin perspektifinden ele alması açısından literatüre katkı sağlamaktadır.

Denizcilikteki sektöründeki siber risklerin tanımlamaları, konuyla ilgili düzenlemeler geliştiren söz sahibi kuruluşların hangileri olduğu ve risklerin azaltılmasına yönelik çalışmalarına ilk bölümde yer verilmiştir.

Siber fiziksel sistemler, siber ve fiziksel bileşenlerin sinerjisine bağlı olan akıllı sistemlerdir. Fiziksel dünyayı (örneğin sensörler, aktüatörler, robotik ve gömülü sistemler aracılığıyla) sanal bilgi işleme dünyası ile ilişkilendirirler. İkinci bölüm denizcilik sektöründe kullanılan önemli siber-fiziksel sistemlerle ilgili çerçeveyi sunmaktadır.

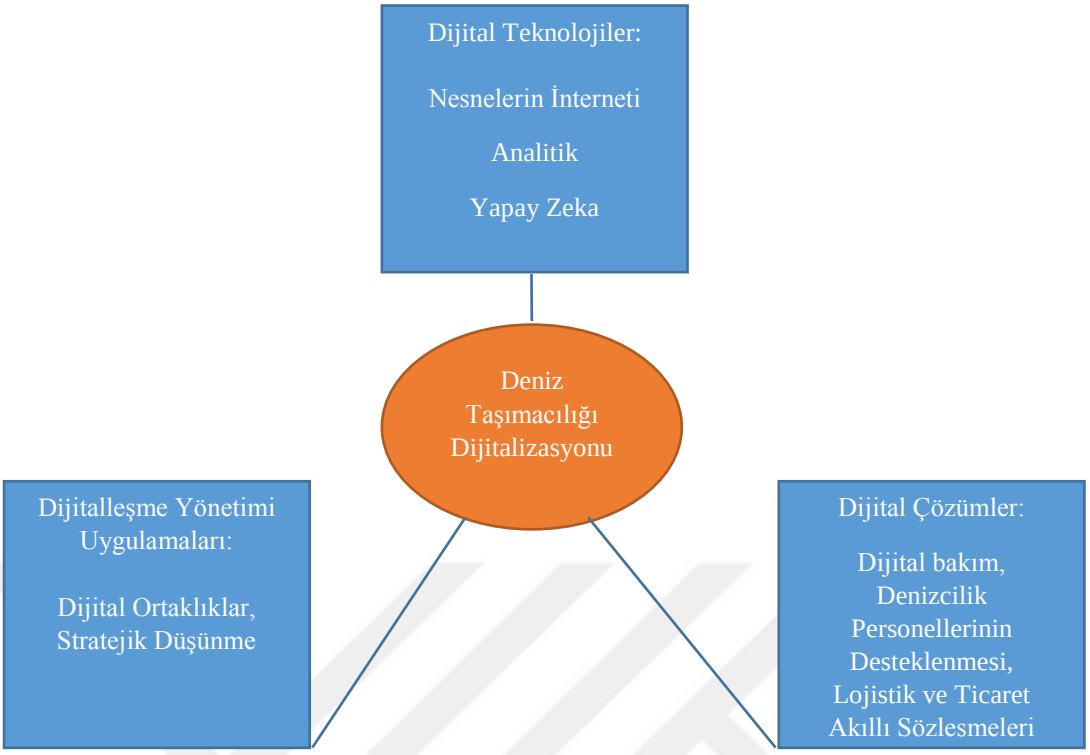
Üçüncü bölümde çalışmanın yöntemine ve uygulanmasına yer verilirken, takip eden son bölümlerde ise çalışmanın bulguları ve sonuçları raporlanmıştır.

BİRİNCİ BÖLÜM

1. DENİZCİLİKTE DİJİTALLEŞME

Endüstri 4.0'a entegrasyona yönelik vizyonlarını ve stratejileri incelemek, denizcilik sektörünün nasıl ilerlediğini ve dolayısıyla denizcilik paydaşlarının birlikte nasıl çalışabileceğini anlamaya yardımcı olacaktır (Ichimura, vd., 2022). Denizcilik sektöründeki çoğu fiziksel işlem artık en azından yarı otomatik mekanik sistemler ve karmaşık yazılım sistemlerinin kontrolü altındaki makineler tarafından gerçekleştirilmektedir (Kuhnb, vd., 2021). Denizde dijitalleşmenin şimdiye kadar denizcilik ortamına sağladığı faydalar oldukça fazladır ve bu faydalar denizcilik operasyonları hakkında daha entegre bir farkındalığa yol açmıştır. Maliyet azalımı ve kazanç artışı, yeni pazarlara giriş, zaman tasarrufu ve en önemlisi can kurtarması denizde dijitalleşmenin ne denli önemli olduğunu ortaya koymaktadır. Teknoloji, hem donanım hem de yazılım olan bilgisayar sistemlerini, gemiler ve limanlar dâhil olmak üzere büyük platformları kapsar. Dijitalleşmenin getirdiği diğer bir konu ise Deniz Otonom Yüzey Gemileridir (MASS). MASS, son zamanlarda akademi, hükümetler ve endüstri genelinde büyük ilgi görmektedir. MASS için gerekliliklerden biri, en azından konvansiyonel gemiler kadar güvenli olmalarıdır (Fan, vd., 2020). Deniz seyir kazalarının çoğunun insan hatasından kaynaklandığı düşünüldüğünde dijitalleşme ile bu durumun azalacağı öngörülebilir (Wróbel, vd., 2017; de Vos, vd., 2021). Ayrıca kazaların büyük çoğunluğunda siber saldırıların etkisi de yadsınamamaktadır (Chang, vd., 2021).

Teknoloji, küresel ekonominin dayandığı deniz taşımacılığının temelidir, ancak aynı zamanda hem fiziksel hem de dijital olarak savunmasızdır (Fitton, vd., 2015). Deniz taşımacılığında dijitalleşmenin temel modeli Şekil 1'de oluşturulmuştur.



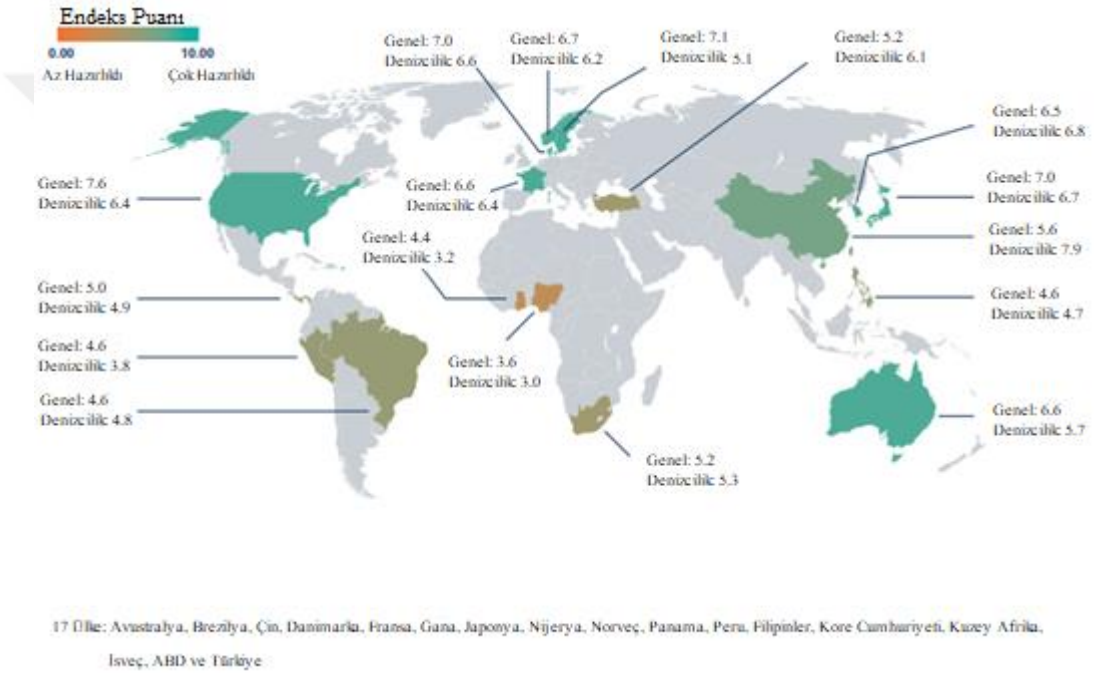
Şekil 1. Deniz Taşımacılığında Dijitalleşme
Kaynak: Lambrou, vd. (2019)

Dijitalleşmenin deniz taşımacılığı üzerindeki etkileri şu üç aşamaya ayrılabilir:

- **Optimizasyon:** Mevcut süreçleri iyileştirmek (ör. akıllı lojistik, liman-çağrı optimizasyonu).
- **Genişleme ve Dönüşüm**: Yeni iş fırsatları yaratmak için bir temel oluşturmak (ör. yakıt ikmali, kargo takibi için blok zinciri teknolojisinin kullanımı).
- **Mevcut Süreçleri İyileştirmek:** Mevcut modellerin yeniden icat edilmesi (UNCTAD, 2018).

Denizcilikte dijital dönüşümün ana itici sebeplerinden olan; yeni teknolojilerin yoğun kullanımı nedeniyle giderek artan siber tehditlere maruz kalma ve güvenliği sağlamak için uygun karşı önlemleri almak olurken (Henriette, vd., 2016; Legner, vd., 2017), ana engellerden ise; teknolojinin hızlı ilerlemesi ve bilginin buna ayak uyduramaması siber tehdit seviyesinin yükselmesi olarak değerlendirilmiştir (Fruth ve Teuteberg, 2017; Agrawal, vd., 2019). Dijital dönüşümü diğer sektörlere kıyasla

yavaşlatan, dikkat çeken diğer engellerden bazıları ise; dijital dönüşümün işletmeyi nasıl etkileyebileceğine dair farkındalık eksikliği ve paydaşlar arasında standardizasyon ve işbirliği eksikliği olarak ortaya çıkmaktadır (Tijan, vd., 2021). Dijital dönüşüm sadece sektörler için değil aynı zaman da ülkeler için de oldukça önemlidir ve bunu kabullenmenin ülkelerin kalkınma durumlarına göre farklılık göstereceği açıktır. Dünya Denizcilik Üniversitesi tarafından yayınlanan yakın tarihli bir rapor, gelişmekte olan ve gelişmiş ekonomiler arasında yeni ve yükselen teknoloji hazırlığındaki boşlukları kabul etmektedir. Buna istinaden Şekil 2'de ülkelerin otomasyon sürecinde yeni teknolojileri kabullenme seviyeleri gösterilmiştir.



17 Ülke: Avustralya, Brezilya, Çin, Danimarka, Fransa, Gana, Japonya, Nijerya, Norveç, Panama, Peru, Filipinler, Kore Cumhuriyeti, Kuzey Afrika, İsveç, ABD ve Türkiye

Şekil 2. Gelişmekte Olan Teknolojiler İçin Hazırlık Seviyesi
Kaynak: Schröder-Hinrichs, vd. (2019).

Yeni teknolojilerin hazırlık seviyesi olarak 0.00-10.00 arasında skala belirlenmiş ve denizcilik teknolojisinin çoğu ülkede genel teknoloji seviyesinin altında kaldığı bulgulanmıştır. Türkiye'de bu durumun tam tersi olduğu dikkat çekmektedir, fakat diğer ülkelere oranla dijitalleşme seviyesi düşük olarak görülmektedir. Ayrıca rapor, denizcileri sistem yönetimi ve operasyonların izlenmesi gibi gerekli becerilerle donatmak için eğitimin uyarlanması ihtiyacına da işaret etmektedir. Bu nedenle, denizcilik endüstrisinde geleceğin işgücü tasarlanırken,

denizcilerin kariyer gelişimi de dahil olmak üzere insan merkezli yaklaşımlar göz önünde bulundurulmalıdır (Baum-Talmor ve Kitada, 2022).

1.1. ENDÜSTRİ 4.0 BİLEŞENLERİ

Endüstriyel dönüşüm, buhar motorlarının icat edilmesinden başlamış, endüstriyel kavramlarda ve işletim yöntemlerinde devrim yaratan teknolojik ve sosyal devrimle bugünkü halini almıştır. Sanayi devriminin gelişimi Tablo 1'de gösterilmiştir.

Tablo 1. Sanayi Devrimi Süreçleri

Sanayi devrimi	***Zaman çizelgesi***	***Özellik***	***Ekonomik ilerleme***
Endüstri 1.0	18'in Sonu - 19'un Başı	Mekanize üretim, buhar motoru	Ekonomi 1.0 (iş gücü ve fiziksel uygunluk)
Endüstri 2.0	19'un Sonu - 20'nin Başı	Seri üretim, elektrik, montaj hatları	Ekonomi 2.0 (enerji kaynakları aracılığıyla çalışma sürecinin iyileştirilmesi)
Endüstri 3.0	20. yüzyılın ikinci yarısı	Bilgi çağı (bilgisayar), otomatikleştirilmiş ürün	Ekonomi 3.0 (hızlı bilgi alışverişi ve iletişim ağı yoluyla performans geliştirme)
Endüstri 4.0	Şimdiki 21. Yüzyıl	BİT Teknolojisi, siber-fiziksel sistem, Nesnelerin İnterneti, ağ oluşturma	Ekonomi 4.0 (yenilikçi bilgi sayesinde benzeri görülmemiş bir değişim dönemi)
Endüstri 5.0	Gelecek	İnsan-robot işbirliği, yüksek düzeyde kişiselleştirme konsepti	Ekonomi 5.0 (rekabet gücü, yaratıcılık ve yenilikçilik yoluyla değer yaratmak)

Kaynak: (Baygin, vd., 2016; Demir, vd., 2019; Nahavandi, 2019; Emad, vd., 2020; Shahbakhsh, vd., 2022)

Endüstri 4.0 fikri 2011'deki Hannover Fuarı'ndan doğdu ve Alman hükümeti, imalat sektöründe öncü bir rol oynamak için 2013'te resmi olarak bunu bir Alman stratejik girişimi olarak duyurdu (Hermann, vd., 2015; Yang ve Gu, 2021). Buna göre, Endüstri 4.0 ile makineler birbirleri arasında veri toplayıp analiz edebilecek, daha hızlı, daha esnek, daha verimli hale gelerek; daha düşük maliyetlerle daha

kaliteli mallar üretme sürecine girebilecek ve aynı zamanda üretim verimliliği, ekonomiyi değiştirme, endüstriyel büyümeyi teşvik etme, profili değiştirme, işgücünün azaltılması nihayetinde şirketlerin ve bölgelerin rekabet gücünü değiştirecektir (Rüßmann, vd., 2015).

Denizcilik sektöründe hemen hemen tüm gemilerin bir Şekilde otomasyona geçmesine rağmen, günümüzde mürettebatsız gemilerin ortaya çıkması ile denizcilik sektörü Endüstri 4.0'a uyum sağlayabilmektedir. (Cross ve Meadow, 2017). Küresel konteyner taşımacılığı endüstrisindeki nakliye maliyetlerinin %15 ila %50'sinin evrak işlerine harcanan zamandan kaynaklandığı tahmin edilmektedir (Groenfeldt, 2017). Evrak işleri nedeniyle katlanılan bu maliyetlerin teknoloji sayesinde çok azalabileceği hatta ortadan kalkabileceği açıktır. Birçok şirket, araştırma merkezleri ve üniversiteler, robotik ve otomasyon teknolojisinin endüstriyel üretimin temeli ve Endüstri 4.0 için önemli bir itici güç olduğunu kabul etmektedir. Dijitalleşmenin uygulanması; blok zinciri ve büyük veri, gerçek zamanlı kontrol, yapay zeka, otonom araçlar ve robotik, ağ bağlantısı, iletişim, sanal gerçeklik ve IoT gibi teknolojilere dayanmaktadır (Bahrin, vd., 2016; Babica, vd., 2019). Bazı deniz kazalarının; bulut bilişim, IoT ve büyük veri analitiğinin eksikliğinden kaynaklandığı bu teknolojilerin diğer teknolojilerle bütünleşerek risk azaltmada önemli bir rol oynayabileceği düşünülmektedir (Sepehri, vd., 2021).

1.1.1. Yapay Zeka (Artificial Intelligence-AI)

AI, verilerden öğrenebilen, belirli veri kümelerinin kalıpları arasındaki korelasyonu tanıyabilen ve nihayetinde insan müdahalesi olmadan eylem yönlerine karar verebilen bir bilgisayar sistemidir (Lambrou, vd., 2019). AI, gemilerin çevresindeki durumunu tanıma, geminin yakınındaki diğer gemilerin ve engellerin tespiti veya manevra ve çarpışmadan kaçınma gibi navigasyonun yürütülmesiyle ilgili birçok görevi desteklemek için kullanılabilir. Ayrıca, bu uygulama, seferlerde en iyi rotaların ve hızın belirlenmesini kolaylaştırabileceğinden, gemilerin özerkliği için bir ön koşul sayılabilir (Msc, vd., 2019; Aslam, vd., 2020). AI ayrıca varlık optimizasyonu, filo planlaması ve çevresel düzenlemelerle ilgili uyumluluk izleme

gibi ticari veya operasyonel faaliyetlerin optimizasyonu için de kullanılabilir (Lambrou, vd., 2019).

1.1.2. Blok Zinciri (Blockchain)

Blok zinciri, son yıllarda bilgi ve veri yönetimi alanında öne çıkan teknolojilerden biri olarak karşımıza çıkıyor. Blok zinciri kavramsal olarak, merkezi olmayan bir yapı ve dağıtılmış depolama olmak üzere iki özelliğe sahiptir (Lei, vd., 2017) ve araştırmacıların yoğun ilgisi ile karşılanmıştır. İlginin kaynağı yalnızca arkasındaki mükemmel teknolojik fikirlerden kaynaklı olmamakla birlikte, Bitcoin gibi kripto para birimlerindeki ticari başarısı da blok zincirine olan ilgiyi üst düzeylere ulaştırmıştır (Nakamoto, 2008).

Blok zinciri mimarisi ve tasarımı; şeffaflık, sağlamlık, denetlenebilirlik ve güvenlik gibi doğal özellikleri sağlar (Christidis ve Devetsikiotis, 2016). Hedef kitleye bağlı olarak, üç nesil blok zinciri oluşturulabilir: Bunlar, dijital kripto para işlemlerini mümkün kılan uygulamaları içeren Blockchain 1.0; akıllı sözleşmeleri ve kripto para birimi işlemlerinin ötesine geçen bir dizi uygulamayı içeren Blockchain 2.0; hükümet, sağlık, bilim ve IoT gibi önceki iki versiyonun ötesindeki alanlardaki uygulamaları içeren Blockchain 3.0'tür (Zhao, vd., 2016). Denizcilik işletmeleri izin verilen (özel) blok zinciri platformları üzerinden akıllı sözleşmeler uygular ve öncelikle ticari dokümantasyon süreçlerini dijitalleştirerek daha az uygulama ile, kargo ve gemi makinelerinin izlenmesi için IoT özellikli blok zincirlerini hesaba katar (Lambrou, vd., 2019).

Blok zinciri gibi yeni teknolojiler, tedarik zinciri yönetimini tamamen devralma ve geleneksel çalışma biçimlerini değiştirme potansiyeline sahiptir (Foerstl, vd., 2017; Kshetri, 2018). Blok zinciri üzerinden ilk kağıtsız, anında finanse edilen ve tamamen kapıdan kapıya paletli konteyner, Blockchain tabanlı platform Naviporta ile Kore'den yola çıkarak Rotterdam Limanı üzerinden Tilburg'daki Samsung SDS deposuna gönderilmiştir (Rotterdam, 2019).

MASS yaygın olarak küresel denizciliğin geleceği olarak kabul ediliyor. Bununla birlikte, siber güvenlik açığı, MASS gelişimini etkileyen potansiyel bir engel olarak tanımlanmıştır. MASS bağlamında blok zinciri kullanımı fikri, MASS operasyonel ortamındaki mobil varlıkların, merkezi olmayan yenilikçi bir fırsat ağı oluşturmasıdır. Bu blok zinciri, varlıkların dinamikleri üzerindeki güveni değerlendirme ve en üst düzeye çıkarma noktasında bir çözüm sağlamak için çekici bir araç haline gelebilir (Wang, vd., 2022).

Blok zincirinin deniz taşımacılığında kullanımına ilişkin yapılan bir ankette; gümrükleme, yönetim, dijitalleştirme, evrak işlerini kolaylaştırma, standardizasyon ve platform geliştirme boyutlarının kullanım niyetini olumlu etkilediğini ortaya çıkarmıştır (Yang, 2019). Blok zincirinin başlıca faydaları arasında; denizcilik tedarik zincirinin şeffaflığı, maliyet ve zaman verimliliği, dijital belge paylaşımı ve imzalanması, bunlara paralel olarak rüşvet, dolandırıcılık ve hırsızlığın azaltılması yer almaktadır.

Blok zinciri uygulamalarında birlikte çalışabilirlik ve standardizasyonun sağlanması, iki ana uygulama zorluğudur. Zorlukların üstesinden gelmek için sağlam bir düzenleyici çerçeve, çalışanların eğitilmesi ve üst yönetimin desteği çok önemlidir (Munim, vd., 2017). Deniz taşımacılığında blok zincirinin benimsenmesindeki engeller; etkili paydaşlardan destek eksikliği, blok zinciri konusunda anlayış eksikliği ve hükümet düzenlemelerinin eksikliği olarak belirlenmiştir (Balci ve Surucu-Balci, 2021).

1.1.3. Nesnelerin İnterneti (Internet of Things-IoT)

İnsanlar nesnelerle az ya da çok, doğrudan veya dolaylı bir Şekilde etkileşime girer; ancak nesnelerin kendi aralarında etkileşime girmesine izin verilirse, nesnelerin kendi ihtiyaçları için veri alışverişinde bulunmaları da mümkün olacaktır. Bu durum, görev bağlamında bağımsız olarak etkileşime girebilecekleri Akıllı Nesneler ağı oluşturacaktır. Bu ağ IoT olarak bilinir (Liu, vd., 2016). IoT, yaygın bilgi işlem, kablolu/kablosuz sensörler, ağlar ve gömülü sistemler dahil olmak üzere çeşitli teknolojileri kapsayan bir paradigmadır (Borgia, 2014). Dahası

iletişim, yapılandırma ve çalıştırma için benzersiz Şekilde tanımlanmış fiziksel ve sanal nesneleri birbirine bağlayan dünya çapında dinamik bir ağ anlamına gelir (Sullivan, vd., 2020). Bu bağlamda IoT, veri analizini kolaylaştırarak denizcilik endüstrilerinin çıktılarını ve üretkenliğini artırmalarına yardımcı olabilir (Wang, vd., 2015).

Denizcilik IoT'si, denizcilik sektöründe navigasyon, güvenlik, uzaktan izleme ve bakım, iletişim ve çevresel verimliliği önemli ölçüde iyileştirme potansiyeline sahip uydu teknolojilerini içermektedir. Bunlar, bir cihazdan bir alıcıya gerçek zamanlı veri aktarımı sağlar. IoT, sensörler, uygulamalar ve insanlar arasında gerçek zamanlı iletişimi kolaylaştırmak için fiziksel nesneleri birbirine bağlayan daha geniş bir konsepti temsil etmektedir (OECD, 2018). Aynı zamanda IoT, güvenlik tehditlerini tespit etmede, ilgili veri ve bilgi alışverişi yoluyla durumsal farkındalığı geliştirmede de yardımcı olur (Jiang, vd., 2019). Deniz trafiği akışını simüle etmek için nesnelerin internetini kullanmak, gemilerin davranış özelliklerini belirlemenin bir yolu aynı zamanda geçidin kapasitesini ölçerek navigasyon risklerini azaltmaya yardımcı olmaktadır (Jiang, vd., 2019).

1.1.4. Büyük Veri (Big Data)

Büyük veri; gelişmiş karar verme, içgörü keşfi ve süreç optimizasyonu sağlamak için yeni işleme biçimleri gerektiren yüksek hacimli, yüksek hızlı ve/veya çok çeşitli bilgi varlıkları şeklinde tanımlanmıştır (Wang, vd., 2015). Bir soruya, herhangi bir yararlı model veya yanıt bulmak için büyük miktarda veriyle ulaşmanın bir yoludur. Hava ve deniz durumu, bir geminin konumu, hız ve elektronik deniz haritası ile ilgili veriler AI tarafından değerlendirilebilir ve böylece anormal algılama ve tehlike tahmini yoluyla güvenli navigasyon sağlanabilir (Ichimura, vd., 2022). Benzer Şekilde, Otomatik Tanımla Sistemi'nden (AIS) elde edilen kayıtlı deniz trafiği verileri, navigasyon için zorlu deniz alanlarını belirtmek için büyük veri sayesinde analiz edilebilir (Zhang, vd., 2021).

Büyük veri bilgisinin makine öğrenimi, yapay zeka, görselleştirme, simülasyon ve artırılmış/sanal gerçeklik de dahil olmak üzere geniş bir uygulama alanı

bulunmaktadır (Lee, vd., 2014). Büyük verinin gücünden yararlanma fırsatları olmasına rağmen, siber tehditlerin gizliliği, bütünlüğü, kullanılabilirliği etkileyebileceği ve nihayetinde rekabet gücünü azaltabileceği için riskin önemli olduğu vurgulanmaktadır (Hutchins, vd., 2015).

1.1.5. Artırılmış Gerçeklik (AR)

Deniz personelinin eğitiminde ve gemi inşa endüstrisinde yaygın olarak uygulanan AR (Liu, vd., 2020), gerçek ortamı daha somut hale getirmek için gerçek dünya veri tabanını kullanılarak ortamın soyut bir görünümünün geliştirilebilmesini ifade etmektedir (Takenaka, vd., 2019). Çoğu gemi kazası, insan hataları, özellikle gemi adamlarının hataları ile ilgili olduğundan gemi adamlarının kararlarını simüle etmek, davranışlarını daha iyi analiz etmeye ve yanlış kararları azaltmaya yardımcı olabilir (Park, vd., 2020).

AR'nin gemilerin rotasını, geleneksel ve otonom olarak insan müdahalesi ile optimize etmek için su yolları ve köprüler tasarlayarak, çarpışma ve karaya oturma risklerinin azaltılmasına yardımcı olabileceği düşünülmektedir (Huang, vd., 2019).

1.1.6. Bulut Bilişim (CC)

Bulut bilişim, minimum yönetim çabası veya hizmet sağlayıcı ile hızlı bir Şekilde sağlanabilen ve serbest bırakılabilen, paylaşılan, yapılandırılabilir bir bilgi işlem kaynakları havuzuna (örneğin ağlar, sunucular, depolama, uygulamalar ve hizmetler) uygun, isteğe bağlı ağ erişimi sağlayan bir modeldir (NISTb, 2022). Güvenli, esnek, erişilebilir ve büyük ölçekli veri depolama sağlayarak modern endüstri 4.0 teknolojilerinin operasyonel hale getirilmesinde önemli bir altyapı rolü oynayan bulut bilişim; bulutta depolanan verileri, sevkiyat karar destek sistemleri ile birlikte kullanılabilmektedir (Dellios ve Papanikas, 2014).

Endüstri 4.0 ile hayatımıza giren teknolojik yeniliklerden bazıları yukarıda açıklanmış olup denizcilik endüstrisinde dijitalleşmeye yönelik hayata geçirilen örnek eylem planı Tablo 2'de gösterilmiştir.

Tablo 2. Şirketlerinin Dijitalleşmeye Yönelik Eylem Planı

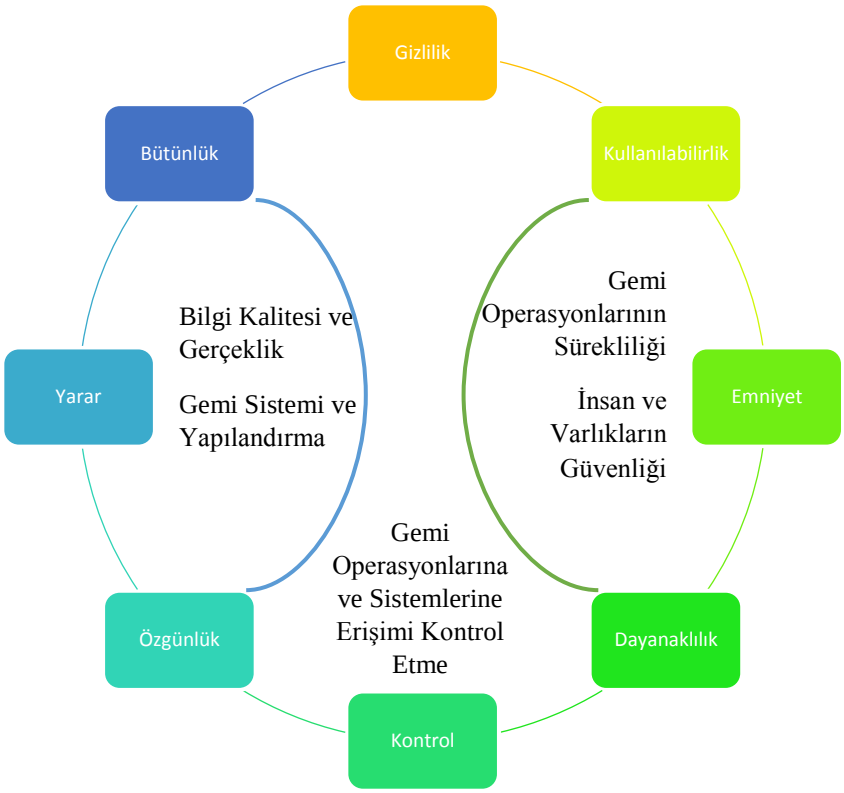
Şirketler	Motivasyon	Tedbir	İlgi Alanları
CMA CGM	Müşteri memnuniyeti Çevresel koruma Gelişmiş denizci eğitimi Rekabet gücünde artış	Teknoloji girişimleriyle işbirliği	Büyük veri Yapay zeka Sanal gerçeklik
EVERGREEN	Müşteri memnuniyeti Geliştirilmiş hizmet kalitesi		Bulut bilişim
HAPAG-LLOYD	Sürdürülebilir değer yaratma Doğru pazarlama	Kültürel değişim Tüm tedarik zincirinde yenilik	Büyük veri
HYUNDAİ MERCHANT MARİNE	Rekabet gücünde artış Maliyet verimliliği Müşteri memnuniyeti	Bilişim şirketi ile işbirliği Özel ekip kurulması	Büyük veri Yapay zeka Nesnelerin İnterneti İleri robotik Bulut bilişim Dijital güvenlik
OCEAN NETWORK EXPRESS	Rekabet gücünde artış Maliyet verimliliği Müşteri memnuniyeti Varlık optimizasyonu Geliştirilmiş hizmet kalitesi	Denizcilik endüstrisinde işbirliği yoluyla standardizasyon Tedarik zincirindeki paydaşlarla ortak araştırma	Büyük veri Yapay zeka Nesnelerin İnterneti Dijital güvenlik
ORİENT OVERSEAS CONTAİNER LİNE	Maliyet verimliliği	Teknoloji girişimleriyle işbirliği Tedarik zincirindeki paydaşlarla işbirliği	Yapay zeka Dijital güvenlik

Kaynak: Ichimura, vd. (2022)

1.2. SİBER GÜVENLİK

En genel anlamıyla siber güvenlik, siber sistemlerin siber tehditlere karşı korunması ile ilgilidir (Refsdal, vd., 2015). Siber güvenlik terimi, "siber uzayın kendisinin, elektronik bilgilerin, siber uzayı destekleyen bilgi teknolojilerinin ve siber uzay kullanıcılarının; kişisel, toplumsal ve ulusal kapasitelerinde, maddi veya manevi çıkarları da dahil olmak üzere, siber uzaydan kaynaklanan saldırılara karşı savunmasız olan durumun korunması" olarak tanımlanabilir (Von Solms ve Van

Niekerk, 2013). Bu tanıma uygun olarak siber güvenliğin sahip olması gerek özellikler Şekil 3'te gösteriştir.



Şekil 3. Siber Güvenlik Özellikleri

Kaynak: Boyes (2015).

Siber güvenlik, yalnızca bilgisayar korsanlarının sistemlere ve bilgilere erişmesini engellemek ve potansiyel olarak gizlilik ve/veya kontrol kaybına neden olmakla ilgili değildir. Aynı zamanda bilgi ve sistemlerin bütünlüğünün, kullanılabilirliğinin korunmasını, iş sürekliliğinin sağlanmasını, dijital varlıkların ve sistemlerin sürekli kullanımını da ele alır. Bunu başarmak için, sadece gemi sistemlerini fiziksel saldırılardan, mücbir sebeplerden vb. korumakla kalmayıp, aynı zamanda sistemlerin tasarımının ve destekleyici süreçlerin esnek olmasını, herhangi güvenlik tehdidine karşı uygun tersine çevirme modlarının mevcut olmasını sağlamak da gerekmektedir (Boyes ve Isbell, 2017).

Avrupa ve Asya endüstrilerinde yapılan bir çalıştayda siber güvenliğin coğrafyalara göre farklı algılandığı ortaya çıksa da siber güvenlik yalnızca ulusal

değil, aynı zamanda küresel bir güvenlik sorunu olarak kabul edilmelidir ifadesine yer verilmiştir (Karamperidis, vd., 2021). Siber güvenlik, siber sistemleri kullanan kişilerin korunmasından siber sistemlere bağlı ulusal altyapının korunmasına kadar her şeyi içeren bilgi güvenliğinden daha geniş bir anlam içermektedir (Von Solms ve Van Niekerk, 2013). Siber uzayın çarpıcı bir yönü, potansiyel olarak son derece geniş kapsamlı ve olası tehdit kaynaklarının, dünyanın herhangi bir yerinde derinlerde hasara neden olma potansiyeline sahip olmasıdır (Refsdal, vd., 2015).

1.2.1. Siber Risk

BT, son on yılda ekonomik büyümeyi destekleyen iyi işleyen ekonomilerin kritik bir bileşeni olmuştur. Hem kamu hem de özel sektördeki her büyüklükteki kuruluş, bulut tabanlı sistemler ve yapay zeka gibi BT ürünlerine ve hizmetlerine giderek daha fazla bağlı ve bağımlı hale gelmektedir. Buna bağlı olarak, siber risklere karşı artan bir maruziyet söz konusudur ve bu tehditlere ilişkin kamuoyu farkındalığı artmaktadır (Aldasoro, vd., 2022).

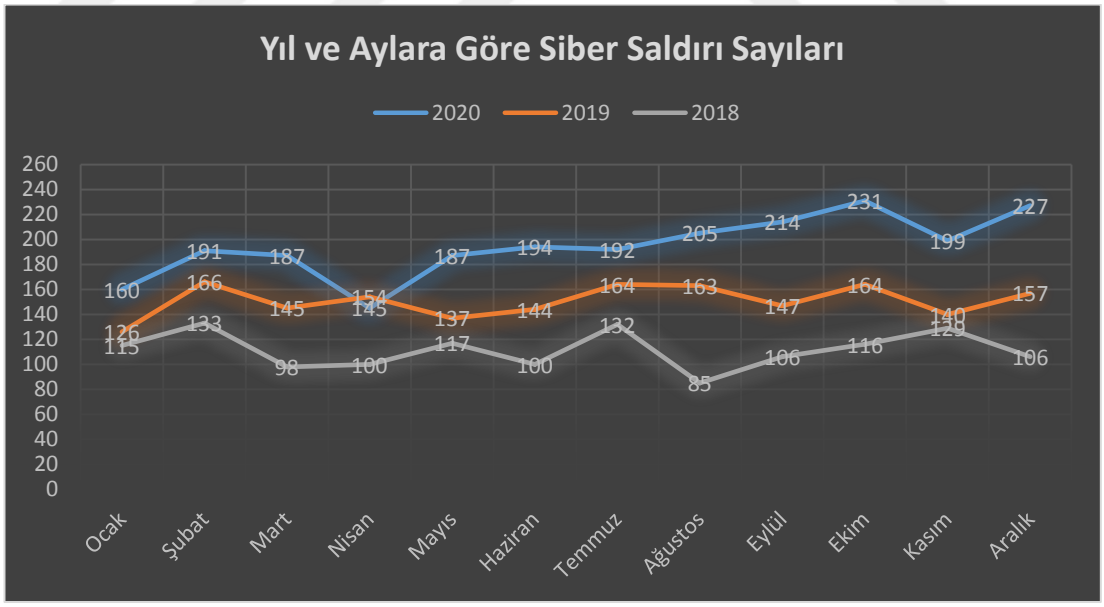
Risk Yönetimi Enstitüsü, siber riski "bilgi teknolojisi sistemlerindeki herhangi bir arıza nedeniyle bir kuruluşun itibarına yönelik finansal kayıp, aksama veya zarar riski" olarak tanımlamaktadır. Jeopolitik ve sosyal itici güçleri tam olarak anlamadan birinin siber riski anlaması ve ona karşı savunma yapması çok zordur. BIMCO'ya (2016, s. 3) göre hem bireylerin hem de kuruluşların siber güvenlik açıklarından faydalanması için birçok neden vardır. Geleneksel olarak siber riskleri ele almanın temel yolu; teknoloji ve insan faktörlerini değerlendirmektir (Giacomello ve Pescaroli, 2019).

Denizcilik, çeşitli nitelikteki risklerden doğrudan etkilenen bir sektördür. Geminin işletilmesi sırasındaki çevresel faktörler, doğal ve iklimsel risklerin birleşimi dış çevre risklerini oluşturur. Buna ek olarak, son olarak, şüphesiz, doğrudan ulaştırma güvenliği seviyesi ile ilgili olan siber riskler, son zamanlarda ağırlaşarak gemi operasyonunun güvenliğini etkilemektedir (Melnyk, vd., 2022). Dolayısıyla denizcilik sektörünü tehdit eden siber riskleri tanımlamak, yönetmek ve bu risklerin azaltılması veyahut elimine edilmesi kritik öneme sahiptir. IMOb (2017:

s. 1), siber risk yönetimini *"siber ilişkili bir riskin belirlenmesi, analiz edilmesi, değerlendirilmesi ve iletilmesi ve bu riski kabul etme, kaçınma, transfer etme veya kabul edilebilir bir düzeye indirme, paydaşlara yapılan eylemlerin maliyet ve faydalarını dikkate alma süreci"* olarak tanımlamaktadır. Bu çalışmanın ilerleyen bölümlerinde siber risklerin belirlenmesi ve yönetilmesine ilişkin detaylı açıklamalara yer verilmiştir.

1.2.2. Siber Saldırı

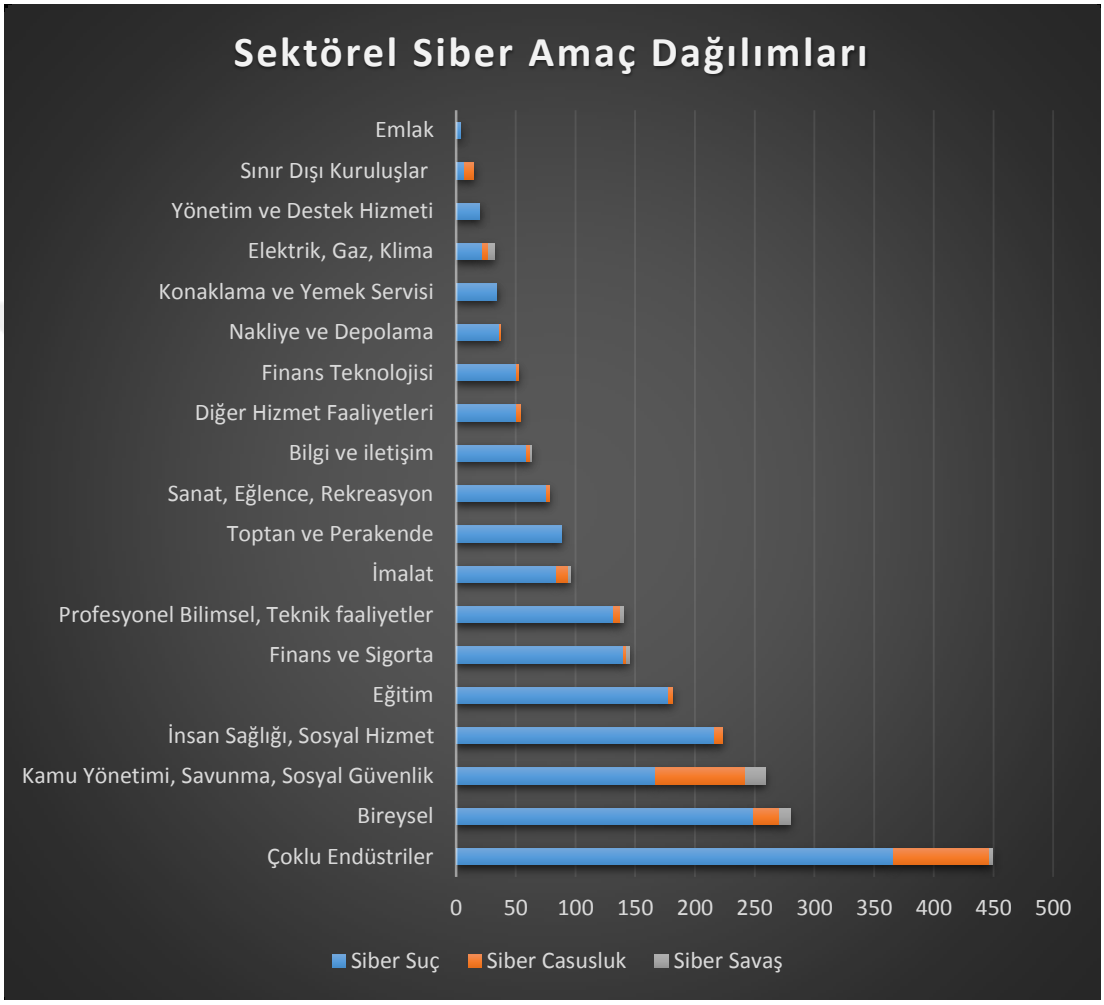
Siber saldırı, şirket ve gemilerin, Bilgi Teknolojileri (BT) ve Operasyonel Teknolojilerini (OT) ele geçirmeye çalışan, bilgisayarı hedef alan, ağları ve/veya kişisel bilgisayar aygıtlarını tehlikeye atmaya, yok etmeye, verilerine erişmeye çalışan her türlü saldırı manevrası olarak tanımlanabilir (BIMCO, 2016). Yıkıcı kötü amaçlı yazılımlar, siber suçlar ve veri sızıntıları dâhil olmak üzere ortaya çıkan siber tehditler, hükümetleri ve endüstriyi benzer Şekilde etkilemektedir. Hackmageddon tarafından yayınlanan son yıllardaki siber saldırı sayıları Şekil 4'te gösterilmiştir.



Şekil 4. Yıllara Göre Siber Saldırı Sayıları
Kaynak: Hackmageddon (2021).

Mevcut göstergelere göre, 2018'in başından 2020'nin son ayına kadar siber saldırılarda artışlar yaşanmış olup ve gerekli önlemlerin alınmaması durumunda bu

artışların ileride daha da fazla olacağı öngörüsünü getirmektedir. Siber saldırıların yıllık maliyetlerinin 375 milyar dolar ile 575 milyar dolar (USD) arasında olduğu tahmin edilmektedir (Dreyer, vd., 2018). Siber tehditlerin sektörel dağılımları ise Şekil 5'te gösterilmiştir.



Şekil 5. Siber Saldırıların Sektörel Dağılımları
Kaynak: Hackmageddon (2021).

Şekil 5'te de görüldüğü üzere farklı sektörlerde işlenen siber suçların sayıları da amaçları da farklılık göstermektedir. Örneğin emlak veya toptan ve perakende sektörlerinde siber casusluk veya siber savaş raporlanmamıştır. Öte yandan çoklu endüstriler daha fazla siber saldırılara maruz kalırken, en çok işlenen suç grubu siber suçlar olmuştur. Siber casusluğun, kamu yönetimi ve savunma sanayide fazlaca işlenen suç olması dikkat çekmektedir.

1.3. DENİZCİLİKTE SİBER SALDIRI

Özellikle ağır makine ve gemi yapımını göz önüne aldığımızda, bu aşırı pahalı platformlar çok uzun süre dayanacak Şekilde tasarlanmıştır, ancak yapım aşamasında kurulan yazılımlar teknolojinin gelişimi sayesinde kötü amaçlı insanlar tarafından ele geçirebilir duruma gelmektedir. Siber saldırılar deniz operasyonlarını sekteye uğratma kabiliyetine sahiptir ve fiziksel saldırılara oranla daha düşük maliyetli alternatif oluşturur. Denizcilik sektörü heyecan verici bir teknik ve ekonomik büyüme dönemiyle karşı karşıyayken, bu büyümenin dezavantajı ise siber risklerin ve suçların daha yaygın hale gelmesidir (Tam ve Jonesb, 2019).

Potansiyel siber tehditlerin doğru bir Şekilde değerlendirilmesi güvenlikle ilgili karar verme için hayati önem taşımaktadır (Meland, vd., 2022). Siber tehditler; bulut tabanlı iletişim, kablosuz veya kablolu iletişim ağları, ağa bağlı akıllı sistemler, sunucular, akıllı donanım cihazları gibi kolaylaştırıcılar sayesinde hareket etme yeteneği elde eder ve siber saldırganlar internetin dünya çapında kullanılabilirliğinden faydalanarak her türlü akıllı sistem ve bileşenlerine herhangi bir yerden, herhangi bir zamanda saldırı başlatma olanağı sağlar (Möller, vd., 2018). Bu tarz saldırıların dış dünyadan gelebileceği gibi içerden de gelmesi mümkündür. Limanlarda veya gemilerde görev yapan; işçiler, kabin görevlileri, ekipman operatörleri, ofis yöneticileri ve hatta güvenlik personelleri dış tehdit aktörleriyle (ör. organize suçlular, teröristler) iş birliği yaparak, konteynerlerin yasa dışı kullanımını düzenlemek için içeriden edindikleri bilgi ve erişim sayesinde casusluk da dahil olmak üzere suç faaliyetleri işleyerek maddi ve manevi hasarlara neden olabilirler (McNicholas, 2012).

Akıllı cihazlara duyulan güven ve bağlanabilirlik; sosyal mühendislik, kimlik hırsızlığı ve istenmeyen e-postalar gibi siber suçları motive etmede çok önemli bir rol oynamaktadır. Yeni nesil denizcilik altyapılarının bütünlüğünün korunması için siber güvenlik, acil bir ihtiyaç olarak gün yüzüne çıkmaktadır (Mednikarov, vd., 2020; de la Peña Zarzuelo, 2021). Bir denizcilik sisteminin normal bir operasyonu nasıl sürdüreceğini ve geliştireceğini öğrenmesinin yanı sıra, bir siber tehdidi

mümkün olan en kısa sürede öngörme, kurtarma ve geliştirme gibi siber esnekliğinin olması gerekmektedir (Erstad, vd., 2021).

Denizde siber güvenlik ve dayanıklılık hakkında daha fazla bilgiye ulaşmak amacıyla Futurenautics tarafından 2018 yılında yapılan mürettebat iletişim anketine 6000 denizci personel katılmış ve ilgi çekici bazı verilere ulaşılmıştır (Futurenautics, 2018):

Denizcilerin %90'ı günlük yaşamlarında kullanılan teknolojinin gemide karşılaştıkları teknolojiden çok daha kolay olduğunu bildirmişlerdir. Gemideki teknolojiyi iki kat daha zor bulanların çoğunun ise gemi zabit olduğu tespit edilmiştir.

Gemi adamları; otomasyon, büyük veri ve analitik ile öngörücü bakımı önümüzdeki 5 yıl içinde sektör için en büyük teknoloji fırsatları olarak gördüklerini belirtmişlerdir.

Gemi adamlarının %38'i insansız gemileri bir fırsat olarak görse de, insansız gemiler, robotikler ve yapay zekâ, önümüzdeki 5 yıl içinde endüstrinin karşı karşıya olduğu en büyük teknoloji tehditleri olarak algılamaktadırlar.

Gemi adamlarının %55'i mürettebat arasındaki iletişimin gemideki güvenliği etkilediğine, hatta bunlardan %95'inin bu etkinin olumlu yönde olduğuna inanmaktadırlar.

Gemi adamlarının yalnızca %15'i herhangi bir siber güvenlik eğitimi almıştır. Günümüzde halen verilen bu tür eğitimlerin büyük bir kısmı, gemi adamının bir sonraki sözleşmesi için mürettebat bulma acenteleri tarafından verilmektedir.

Gemi adamlarının yalnızca %33'ü, en son çalıştıkları şirketin gemide düzenli olarak şifre değiştirme politikası olduğunu ve bunlardan %18'inin ise, en son çalıştıkları şirketin gemideki varsayılan ekipman şifrelerini değiştirme politikası uyguladığını söylemişlerdir.

Bilgi tazeleme eğitimi ile ilgili mevcut eğitim çözümlerinde, mürettebatın %65'i tarafından eksik olduğu bildirilmiş ve bunlardan sadece %20'si siber güvenlik eğitiminden bahsetmiştir.

Gemi adamlarının %47'si, daha önce görev aldıkları bir gemide siber saldırıya maruz kaldıklarını söylemişlerdir.

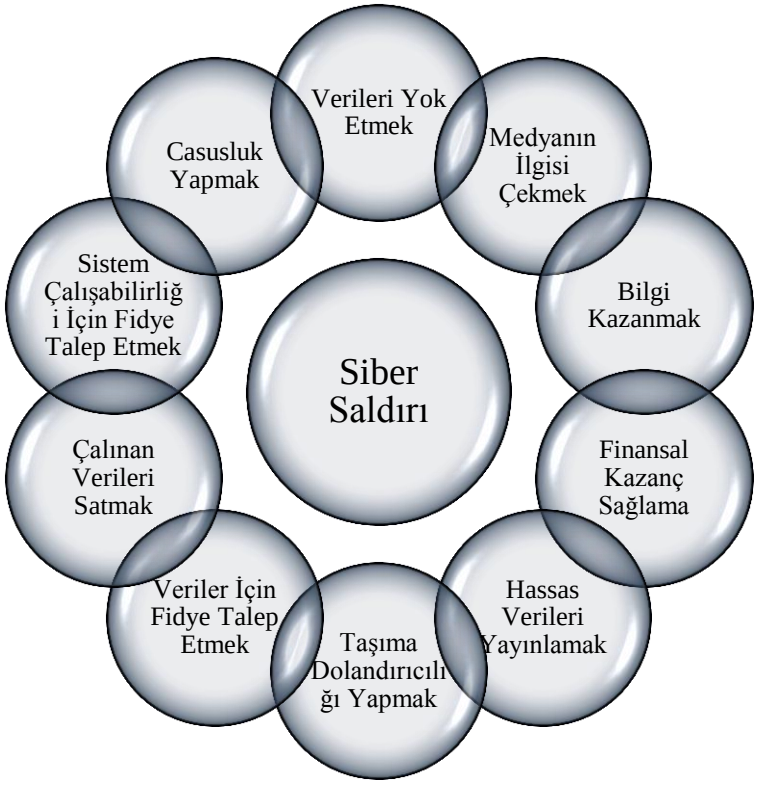
Yukarıda verilen anket bilgilerinden de anlaşılacağı üzere denizde siber saldırılar oldukça sık gerçekleşmektedir, ancak resmi bir raporlama sisteminin olmaması veya itibar kaybı korkusu, bu olayların raporlarının bulunmasını zorlaştırmaktadır (McGillivary, 2018). Denizcilik inovasyon ajansı Thetius tarafından gerçekleştirilen bir diğer ankete; üst düzey yöneticiler, siber güvenlik uzmanları, kıyı yöneticileri ve tedarikçiler dahil olmak üzere 200'den fazla sektör profesyoneli katılmış ve aşağıdaki sonuçlara ulaşılmıştır (Thetius, vd., 2022):

- Bir siber saldırının finansal maliyeti aşırı olabilmektedir. Saldırı fidye ödemesine yol açtığında, armatörlerin ödediği ortalama fidye ücreti 3,1 milyon ABD dolarıdır.
- Çoğu armatör siber güvenlik yönetimine önemli ölçüde yetersiz yatırım yapmakta ve yarısından fazlası yılda 100.000 ABD dolarından az harcamaktadır.
- Sektör profesyonellerinin üçte ikisi, sigortalarının siber saldırıları kapsayıp kapsamadığını bilmemektedir.
- Armatörler, endüstri tedarikçilerinin yalnızca %55'inden siber risk yönetimi prosedürlerine sahip olduklarını kanıtlamalarını istemektedir.
- Gemi adamlarının %25'inden fazlası bir siber olay sırasında hangi eylemlerin yapılması gerektiğini bilmemektedir.

Siber risklerle ilgili ister denizde ister karada hangi pozisyonda bulunulursa bulunsun genel olarak çok fazla bilgi sahibi olunmadığı ve yeterli eğitimin verilmediği açıktır.

1.3.1. Siber Saldırı Aktörleri ve Nedenleri

Siber saldırılar genellikle çıkar amaçlı yapılsa da bazen ideolojik veya politik sebeplerden de gerçekleştirilmesi mümkündür. Bir saldırıyla ilişkili riskler üç bağımlı faktöre ayrılmıştır, bunlar: Tehditler (kim saldırıyor), güvenlik açıkları (saldırdıkları zayıf yönler) ve etkileri (saldırının ne yaptığı) (Androjna, vd., 2020). Bu üç faktör doğru analiz edildiğinde saldırı sonuçlarının daha az yıkıcı olması beklenebilir. Siber saldırı motivasyonları çok az risk ile çok fazla getir elde edilebileceği düşünüldüğünden oldukça fazladır. Günümüzde modern suçlular silah yerine klavye kullanmakta olup onları motive eden nedenler ise Şekil 6'da gösterilmiştir.



Şekil 6. Siber Saldırı Motivasyonları
Kaynak: Fosen (2019)

Siber saldırı aktörleri ve motivasyonlarından bazıları aşağıdaki gibidir (Sen, 2016; Boyes ve Isbell, 2017; Kersten, vd., 2017; Lagouvardou, 2018; Tam ve Jonesa, 2019; Bolbot, vd., 2020).

1.3.1.1. Aktivistler

"Hacktivistler" olarak da bilinen eylemci grupların arzu ettikleri sonuç ideolojik hedeflerine ulaşmaktır. Bu kişiler genellikle, hedeflerinin faaliyetlerini kesintiye uğratır veya bu faaliyetlerde zorunlu değişikliğe yol açarlar. Saldırı sonucu elde edilen bilgiler yayınlanmak amacıyla kullanılır. Nominal olarak saldırgan olmasa da bu faaliyetler, diğer saldırganlara fayda sağlayan veya kazara sızıntılara neden olan fırsatlar yaratabilir. Denizcilik bağlamında, aktivistler tipik olarak çevresel, insani veya politik merkezli etkiler yaratmak isterler. Kısacası; bir mesaj iletmek için aktivizm yapma niyetindedirler.

1.3.1.2. Rakipler

Rakip şirketler ve hatta karşıt ülkeler, siber suç yoluyla küresel ekonomide kendi pazar etkilerini artırmaya çalışabilirler. Amaçları, kurumsal ortamlarda kullanılacak rakibin mevcut teklifleri, nakliye beyannameleri ve müşterileri gibi bilgileri elde etmektir. Bununla birlikte, mali zarar verme amacıyla bir rakibin gemi operasyonlarını kesintiye uğratmak için de teşvik vardır. Ayrıca; Uluslararası Gemi ve Liman Tesisleri Güvenlik Koduna (ISPS) uymama, gemiyi geciktirme, aksamalara yol açarak; dava edilmesine ve itibar kaybı yaşamasına neden olmaktadırlar.

1.3.1.3. Organize Suç Şebekesi

Bu saldırganlar bireylerden farklı büyüklük ve karmaşıklıktaki gruplara kadar çeşitlilik gösterir. Suçluların büyük çoğunluğu, fiziksel ve entelektüel hırsızlık, dolandırıcılık, kaçakçılık, şantaj ve haraç dahil olmak üzere şu veya bu biçimde kâr elde etmek ister. Genellikle gemi veya liman operasyonlarının tekrar faaliyete geçebilmesine izin vermek için fidye talebinde bulunurlar.

1.3.1.4. Teröristler

Siber saldırganlar bazen çizgiyi aşabilir; kasıtsız, gereksiz ölümlere veya hasara neden olabilirken, siber veya siber-fiziksel saldırılar kullanan teröristler genellikle bu sonucu amaç edinirler. Ayrıca, bu saldırgan türü, üye sayısını ve kaynaklarını artırmak isteyebilir, bu da hırsızlık, propagandanın yayılması ve siber araçları kullanarak şantaj ile sonuçlanabilir.

1.3.1.5. Seçkinler

Günümüzün bilgisayar korsanlığı topluluğunun küçük bir bölümünde, geleneksel olarak bilgilerini test etmek veya gösteriş yapmak için sistemleri ele geçirebilirler. Bu tür kar amacı gütmeyen saldırılarda gemi veya liman bilgi ve otomasyon sistemlerini kapatarak dijital korsanlık yapıp elitist görünüm vermek amaçlanabilir.

Siber suçluların ve devlet destekli aktörlerin sahneyi ele geçirdiğini ve para kazanmanın siber saldırıların ana itici güçlerinden biri haline geldiğini iddia ederek siber tehdit ortamına ilişkin raporunu yayınlayan Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA), 15 en sık karşılaşılan siber tehditleri yukarıdakilere benzer Şekilde açıklamıştır (Sfakianakis, vd., 2019).

1.3.2. Siber Saldırı Çeşitleri

Tedarik zinciri boyunca çalışanlar için yapılandırılmış güvenlik bilinci eğitiminin olmaması, önemli bir güvenlik açığını ortaya koymaktadır ve bu eğitimsizliğin sonucu olarak, bilgisayar korsanları başarılı saldırılar elde etmek için spam, e-postalar veya hizmet reddi (DDoS) saldırıları gibi klasik yaklaşımları kullanmaktadırlar. (Mraković ve Vojinović, 2020). Gemilere ve limanlara yapılan saldırı çeşitlerinden bazıları aşağıdaki gibidir (Tam ve Jones, 2018; Ben Farah, vd., 2022).

Oltalama Saldırısı: Spear-phishing olarak bilinen saldırı ile yetkisiz erişim elde etmek için şüpheli bağlantılar içeren e-postalar oluşturularak, verilere veya sistemlere ulaşım sağlanmaya çalışılır ve bu saldırı türü en yaygın saldırılardan biridir. Önemli sayıda hedefli oltalama saldırısı olmasına rağmen, denizcilik sektörünün hassasiyeti nedeniyle, ihlaller sadece bireysel değil, aynı zamanda ülkeler arasındaki ekonomik ilişkileri de etkilediğinden, liman yöneticileri raporlamayı minimumda tutmayı tercih etmektedirler.

DDoS Saldırısı: DDoS saldırıları suç teşkil eden eylemlerdir. Liman bilgi sistemi ağında aşırı trafik oluşturarak ve liman web sitelerine erişimi kapatarak tehlikeye sokabilmektedir. Sonuç olarak, denizcilik hizmetleri ve malları takip etme yeteneği tehlikeli duruma dönüşmektedir.

Bağlantı Noktası Tarama: Saldırganlar, klasik tarama tekniğini kullanarak en savunmasız ağ bağlantı noktalarına ulaşmayı hedefler. Amaçları, hizmetlerin durumunu keşfetmek, veri tabanlarına erişmek için optimum stratejiyi tanımlamak ve hangi kullanıcıların hizmetleri izlediğini belirlemektir.

Tedarik Zinciri Saldırıları: Uçtan uca ağın en savunmasız kısmı aracılığıyla hasar yaratmaya odaklanılır. Uluslararası nakliyenin çıkış noktasından nihai varış noktasına kadar, konteyner takibi, güvencesi ve uluslararası yetkilendirmeler için kilit süreçlere ve paydaşlara dayanır. Bu tip bir saldırının zarar verici sonucunun en kolay anlaşılır örneği, tedarik zinciri hakkında bilgi gerektiren bir konteynerin varış yerinin değiştirilmesidir.

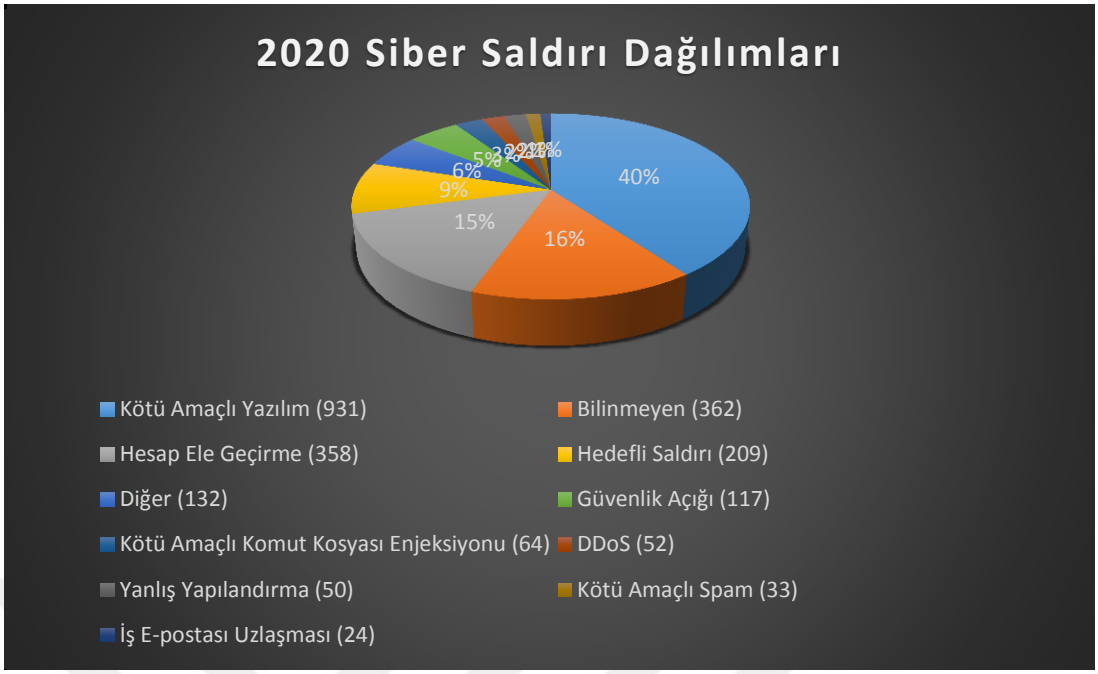
Sosyal Mühendislik: Genel olarak kötü niyetli bir eylem yürütmek için insan merakının veya vicdan azabının istismarına dayanan saldırı çeşididir. İnsan davranışının incelenmesi başarılı bir saldırının özüdür ve bu bağlamda, sosyal medya veya anlık mesajlaşma kullanım kalıpları, bilgisayar korsanlarının liman içi ağ etkinliği hakkında bilgi toplaması için bir araçtır. Örnek olarak, bilgisayar korsanı Facebook/Instagram üzerinden sahte bir kimlik oluşturarak kritik bilgileri elde edebilir. Güvenlik yöneticileri tarafından bir Evrensel Seri Veri Yolu (USB) aracılığıyla yapılan yazılım güncellemeleri, genellikle bilgisayar korsanı tarafından

sisteme erişim elde etmek için kullanılan bir dosya olan kötü amaçlı yazılımı yüklemek için bir araçtır. Kesin olarak uygulanan güvenlik politikalarına dayalı koruma, bu tür saldırıları azaltmada yardımcı olabilmektedir.

Kötü Amaçlı Yazılım/Fidye Yazılım/Truva Atları: Genel olarak, bu saldırı sınıflarının amacı, ağa bağlı bilgisayarları hedef alarak bilgi sistemine veya sunucuya zarar vermektir. Kimlik avı saldırısı olarak da değerlendireceğimiz bu riskler son zamanlarda hızla büyüyerek küresel internet güvenliğinde büyük tehditler oluşturmaktadır (Gupta, vd., 2017).

8 Temmuz 2019'da, Amerika Birleşik Devletleri (ABD) gemisini hedef alan saldırıda, kritik kimlik bilgisi madenciliğine neden olmuştur. Sahil Güvenlik ve Federal Soruşturma Bürosu (FBI), gemideki güvenlik stratejilerinin eksikliğinin böyle bir saldırının gerçekleşmesinin ana nedeni olduğunu bildirerek; gemideki tüm mürettebatın, gemi bilgisayarını aynı kullanıcı adı şifreyle kullandığı tespit edilmiştir. Ayrıca, harici cihazların kullanımı ve antivirüs yazılımı korumasının olmaması, bilgisayar korsanının görevini kolaylaştırmıştır. Denizcilik küresel tedarik zinciri bilgisayar sistemleri ve verileri; yazılım, donanım ve eğitim olmak üzere üç özel yolla Truva atı saldırılarından korunmalıdır. Hal böyle olunca denizcilik sistemlerine yönelik saldırıları önlemek için kapsamlı siber güvenlik önlemlerine ihtiyaç duyulmaktadır. Bu önlemler güvenlik duvarlarını, antivirüs ve casus yazılım önleme programlarını, erişim kontrol sistemlerini, izinsiz giriş tespit sistemlerini, izinsiz giriş koruma sistemlerini ve çok faktörlü kimlik doğrulamayı içermelidir (Shapiro, vd., 2018).

2017'de kripto paraların popülerliğindeki artış ile birlikte, iş hedefli fidye yazılımlarında %90'lık bir artış olduğu ortaya çıkmıştır (Symantec, 2018). 2020 yılında yapılan siber saldırı dağılımları Şekil 7'de gösterilmiştir.



Şekil 7. 2020 Siber Saldırı Çeşitleri
Kaynak: Hackmageddon (2021)

Siber saldırı dağılımlarında en fazla saldırı türü olarak kötü amaçlı yazlımlar ilk sırayı alırken saldırı türü bilinmeyenlerin sayısı da oldukça fazladır. Teknoloji ilerledikçe şimdilik ismi konulamayan saldırılar daha da artacak ve sistemlerde yeni açıklar bularak tehdit oluşturmaya devam edecektir.

1.3.3. Denizcilikte Yaşanmış Siber Olaylar

Küresel tedarik zincirinde önemli bağlantılar olan limanlar ve terminaller, diğer ulaşım, enerji veya telekomünikasyon ağlarıyla ortaklaşa kritik altyapılar olarak kabul edilir. Bu itibarla, suç saldırıları ve terörizm için potansiyel hedeflerdir (Boyes, vd. 2016). Denizcilik sektöründe de diğer sektörlerde olduğu gibi neredeyse her bölüm siber saldırılara maruz kalmış ve başarılı saldırıların sonuçları oldukça maliyetli olmuştur. Günümüze kadar yaşanan bazı önemli siber olaylar aşağıda özetlenmiştir:

2011 yılında İranlı nakliye şirketi İran İslam Cumhuriyeti Denizcilik Hatları'na (IRISL) yönelik gerçekleştirilen siber saldırı, oranlar, yükleme, kargo numarası, tarih ve yer ile ilgili tüm verilere zarar vermiştir. Saldırı aynı zamanda şirketin iç iletişim

ağını da felce uğrattığı ve ciddi mali kayıplara hatta kargo kayıplarına neden olduğu ortaya çıkmıştır (Kim, 2019).

2011-2013 yılları arasında tam 2 sene boyunca devam eden olayda; Antwerp Limanındaki kargo takip sistemi, uyuşturucu ve silah kaçakçıları tarafından kiralanan bilgisayar korsanları aracılığıyla siber saldırıya maruz kalmış ve muz kasalarıyla dolu olarak düşünülen konteynerde silah ve uyuşturucu kaçakçılığı yapıldığı tespit edilmiştir (DNV-GL, 2015). Aynı liman 2018 yılında da aynı saldırıya maruz kalmıştır.

Tarihin en büyük siber felaketlerinden birisi 2017'de nakliye devi Mearsk'ın başına gelmiştir. Vergi muhasebesi yazılımı için bir güncelleme yaması aracılığıyla yayılan NotPetya fidye yazılımı şirketi ciddi Şekilde sekteye uğratmıştır. Virüs, Microsoft Windows'taki güvenlik açıklarından yararlanır ve EternalBlue tabanlıdır; ABD Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilen bir siber saldırı yazılımıdır. Bu saldırı 76 liman dâhil olmak üzere küresel denizcilik operasyonlarının neredeyse beşte birinde sorunlara neden olmuştur. Maersk, olay sonucunda ekonomik kayıplarını 300 milyon USD'ye yakın tahmin ederek, 4000'den fazla sunucu, 45.000 bilgisayar ve 2500 uygulamanın yeniden yüklenmesi gerektiği ortaya çıkmıştır (Catalin, 2018; Singh, 2019)

Merkezi Çin'in Şanghay kentinde bulunan, 1100'ün üzerinde gemi sayısıyla denizcilik sektöründe önemli bir paya sahip olan COSCO, Amerika bölgesindeki iletişimini etkileyen dijital varlıklarına yönelik siber saldırıyı doğrulamıştır. Şirketin e-posta ve telefon sistemleri devre dışı bırakılarak diğer bölgelerle olan bağlantıları kesilmiştir (Naveen, 2018; Marcus, 2018).

İsrail güvenlik ajansı denizcilik sektörüne yönelik siber saldırıların % 400, sektörün operasyonel teknoloji sistemlerine yönelik siber saldırıların ise üç yılda %900 oranında arttığını raporlamıştır. OT sistemlerine yönelik bir diğer saldırı ABD merkezli nakliye şirketi MSC'nin başına gelmiştir. Fidye yazılımı virüsüne maruz kalan şirket ve Cenevre'deki merkezlerini beş gün süreyle kapatmak zorunda kalmıştır (Micheal, 2020).

Carnival şirketine ait bir yolcu gemisi 2020'de yaşadığı siber saldırıda, fidye yazılımı ile müşterilerden, çalışanlardan, hissedarlardan ve düzenleyici kurumlardan potansiyel hak taleplerine yol açabilecek dosyaların çalındığı ortaya çıkmıştır. Şirket kaç yolcunun etkilendiğini ve hangi kişisel verilerin çalındığını açıklamayı ise reddetmiştir (Lucy, 2020).

Bir başka fidye saldırısı, Fransız konteyner taşıyıcı şirketi CMA CGM'nin başına gelmiştir. Şirketin Çin'de bulunan ofislerinin birçoğu etkilenmiş ve çevrimiçi rezervasyon da dâhil olmak üzere bazı çevrimiçi hizmetlerinin kapatılmasına neden olmuştur (Shen ve Baker, 2020). Bunların dışında 2022 yılında yaşanmış bazı siber olay özetleri ise aşağıda gösterilmiştir (Gitlab, 2022).

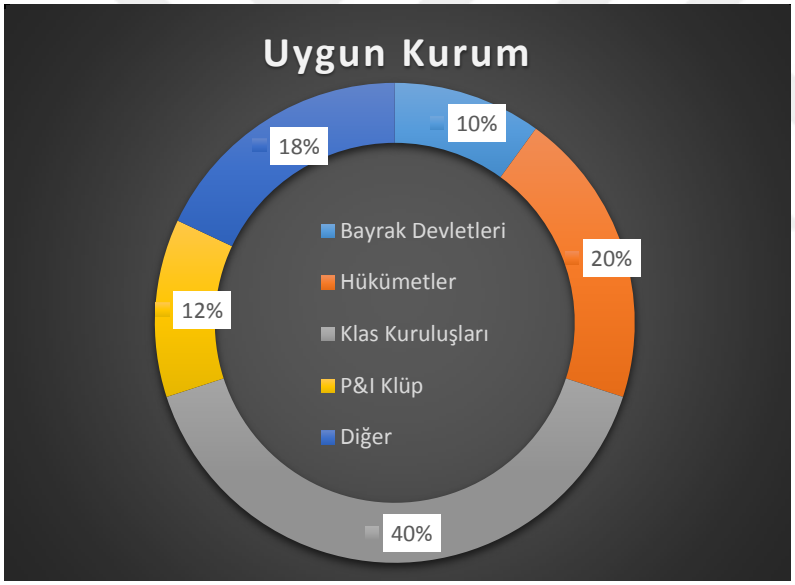
Tablo 3. 2022 Yılı Denizcilikte Siber Saldırı Özetleri

Olay	Ülke	Hedef	Olay Türü	Olay Ayrıntısı
Siber Suç	Birleşik Krallık	Armatör	Virüs/Fidye Yazılımı	Lüks yat kiralama konusunda uzmanlaşmış bir şirket, fidye yazılımı saldırısına uğradığı ortaya çıkmıştır.
Siber Suç	ABD	Liman	Oltalama	ABD Deniz Taşımacılığı Sistemi'nin çeşitli web sitelerine, oltalama yöntemi ile siber saldırılar gerçekleştirilerek müşteriler hedef alınmıştır.
Siber Suç	Almanya	Armatör	Oltalama	Bir gemi sahibinin web sitesi, hedef odaklı kimlik avı saldırısına uğradığı ortaya çıkmıştır (Hapag-Lloyd, 2022).
Siyasi	Birleşik Arap Emirlikleri	Gemi	Küresel Konumlandırma Sistemi (GPS)/AIS sıkışması/sahtekarlığı	Rusya/Ukrayna çatışması bağlamında birkaç AIS sahtekarlığı vakasına rastlanmıştır.
Siber Suç	Hindistan	Liman	Virüs/Fidye Yazılımı	Hindistan'ın en büyük konteyner limanı kompleksi olan Jawaharlal Nehru Port Trust'ta (JNPT), hükümet tarafından işletilen terminal JN Port Container Terminal (JNPCT) tarafından kullanılan bilgi sistemlerinin siber saldırının en son hedefi haline gelmesinden sonra gemi akışı kesintisi yaşanmıştır (JNPT, 2022).
Siber Suç	ABD	Lojistik	Virüs/Fidye Yazılımı	Küresel lojistik devi Expeditors, siber saldırı kurbanı olmuş ve operasyon sistemlerinin çoğunu kapatmak zorunda kalmıştır (Tabak, 2022).
Siber Suç	Birleşik Krallık	Armatör	İzinsiz Giriş	Bir feribot şirketi olan Wightlink, bazı müşterilerinin adları, adresleri, banka bilgileri ve imzalarının, BT altyapılarına yapılan karmaşık bir siber saldırının ardından ele geçirildiğini ifade etmiştir (Toogood, 2022).

Denizcilik endüstrisinde siber tehditler gün geçtikçe daha da çoğaldığı açıktır. Tablo 3'te gösterildiği üzere günümüzde çoğu saldırılar fidye yazılımı olarak gerçekleşmekte ve saldırı mağduru olan şirketler genel itibariyle bu saldırılardan ne kadar kayıpla çıktıklarını ve saldırı sonuçlarının nasıl sonuçlandığını açıklamaktan geri durmaktadırlar.

1.4. DENİZCİLİKTE SÖZ SAHİBİ KURULUŞLAR VE PAYDAŞLARIN SİBER RİSK DEĞERLENDİRMESİ

Denizcilik alanındaki siber güvenlikle ilgili mevcut endüstri ayrıca hükümet standartları ve direktifleri, mevcut OT altyapısı ve sistemlerinde optimum ve güvenli performans için düzenleyici uyumluluğu zorlamaya, siber güvenlik bütünlüğünü güçlendirmeye çalışmaktadır (Progoulakis, vd., 2021). Doğu Asya merkezli büyük bir Ticaret Odası tarafından gerçekleştirilen ve 250'den fazla kıdemli deniz taşımalığı uygulayıcısının katıldığı iki çalıştay sırasında anket yöntemiyle toplanan veriler sayesinde Avrupa ve Asya kıtalarının denizcilikte siber güvelik konusuna bakış açıları araştırılmış siber güvelik konusunda rehberlik edecek kurumlar Şekil 8'deki gibi sonuçlanmıştır.



Şekil 8. Siber Güvelik Konusunda Rehberlik Edecek Kurumlar
Kaynak: Karamperidis, vd. (2021)

Deniz güvenliğinde sektöre yardımcı olarak rehberlik yapması gereken kuruluş yüzde 40 ile klas kuruluşları olarak belirlenmiştir. Denizcilik sektöründe söz sahibi bazı kuruluşların ve paydaşların siber risk konusuna bakış açıları ise aşağıdadır.

1.4.1. Uluslararası Denizcilik Örgütü (IMO)

IMO, denizcilikte siber riski; *bir teknoloji varlığının, bilgi veya sistemlerin bozulması, kaybolması veya kaybolması sonucunda denizcilikle ilgili operasyonel, güvenlik veya güvenlik arızalarına neden olabilecek potansiyel bir durum veya olay tarafından ne ölçüde tehdit edilebileceğinin bir ölçüsü* olarak ifade etmiştir (IMOa, 2022). IMO, siber risk yönetimine ilişkin; deniz taşımacılığında mevcut ve sonradan ortaya çıkan siber tehditlerden, güvenlik açıklarından korumak için denizcilikte siber risk yönetimine ilişkin üst düzey önerilerde bulunmuştur. Mevcut risk yönetimi süreçlerine dâhil edilebilir halihazırda oluşturulmuş emniyet ve güvenlik yönetimi uygulamalarını tamamlayıcı nitelikte olan MSC-FAL.1/Circ.3 kılavuzlarını yayınlamıştı (IMOb, 2017). Deniz Emniyeti Komitesi, Haziran 2017'deki 98. oturumunda Emniyet Yönetim Sistemlerinde Denizcilik Siber Risk Yönetimi - MSC.428(98) kararını kabul ederek, idareleri; 1 Ocak 2021'den sonra şirketin Uygunluk Belgesinin mevcut emniyet yönetim sistemlerinde (Uluslararası Güvenli Yönetim Kodu'nda (ISM) tanımlandığı gibi) siber risklerin uygun Şekilde ele alınmasını sağlamaya teşvik etmiştir (IMOa, 2017).

IMO, son zamanlarda saldırı artışları nedeniyle siber risklerin yönetimi konusunda Baltık ve Uluslararası Denizcilik Konseyi (BIMCO) ile birlikte Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) çerçevesini kabul ederek aşağıdaki gibi önermiştir (IMOb, 2017; NIST, 2018).

Tanımlama: Siber risk için personel rollerini ve sorumluluklarını tanımlamak, yönetmek. Sistemleri, varlıkları, verileri, yetenekleri belirlemek.

Koruma: Risk kontrol süreçleri ve önlemleri ile beklenmedik durumlarda, bir siber olaya karşı koruma sağlamayı ve sevkiyatın sürekliliği için operasyonları planlamak.

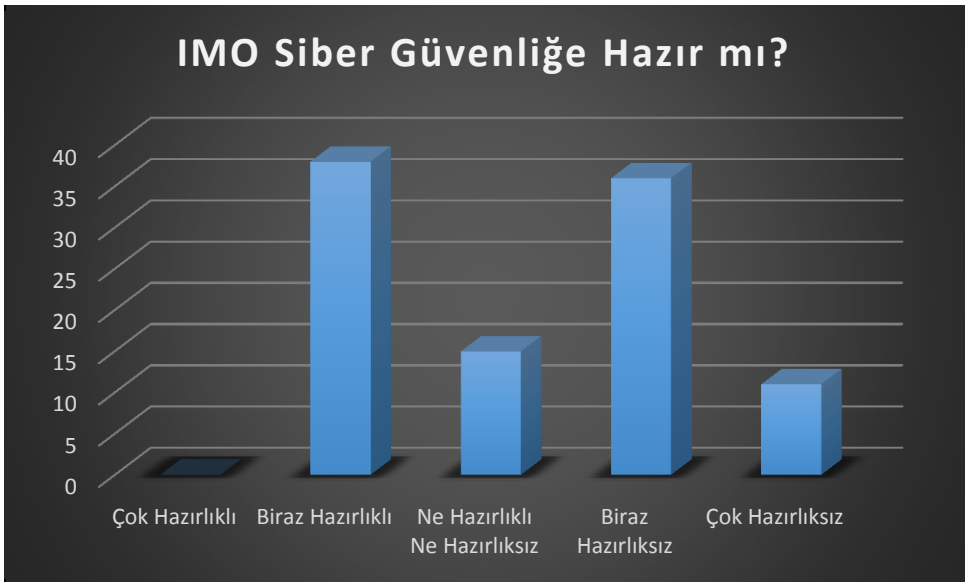
Tespit: Bir siber olayı tespit etmek için gerekli faaliyetlerin geliştirilmesi ve zamanında uygulanmasını sağlamak.

Müdahale: Dayanıklılık sağlamak için planlar geliştirerek uygulamak. Bir siber olay nedeniyle yaşanan bozulmalarda, nakliye operasyonları veya hizmetleri için gerekli sistemlerin geri yüklemesini yapılabilmek.

Kurtarma: Gerekli siber sistemleri yedeklemek ve siber olaydan etkilenen nakliye operasyonları için geri yükleme yapabilmek.

Siber tehlikelerin ne kadar ciddi bir konu olduğu ise Ekim 2020'de IMO'ya yapılan saldırıda bir kez daha anlaşılmıştır. BT sistemlerine yapılan saldırının hizmet kesintilerine neden olduğunu açıklayan IMO saldırının kaynağı ve tekrarı için önlem alacağını bildirmiştir. Gemi sahiplerinin siber güvenliğe yatırım yapmasıyla ilgili alınan karar sonrası böyle bir saldırının gerçekleşmesi ise ironik bir durumu ortaya çıkarmaktadır (Konrad, 2020).

IMO her ne kadar deniz ticaretinin başrol kuruluşlarından olsa da siber güvenlik konusunda yaklaşımı sektör tarafından tatmin edici bulunmamaktadır. *'IMO 2021 gerekliliklerini karşılamaya ve dolayısıyla siber güvenliği ele almaya ne kadar hazır?'* sorusuna verilen cevaplar Şekil 9'da gösterilmiştir.



Şekil 9. IMO'nun Siber Güvenliğe Yaklaşımına Sektörel Bakış
Kaynak: Karamperidis, vd. (2021)

Şekil 9'da görüldüğü üzere IMO'nun siber güvenlik konusuna hazırlıksız olduğu düşünülmektedir. IMO'nun siber güvenlik hakkında aldığı kararlar genel itibariyle öneri niteliği oluşturması ve bu kurallara uyulmaması veya siber önlemlerinin alınmaması durumu sonucunda herhangi bir yaptırım veya yasal bağlayıcılık oluşmaması sektör tarafında ciddiyet oluşturmamaktır.

1.4.2. Avrupa Birliği Siber Güvenlik Ajansı (ENISA)

ENISA, Avrupa Birliği (AB) üye ülkelerine ve özel sektör kuruluşlarına tavsiyelerde bulunmak aynı zamanda kuruluşların kritik bilgi altyapılarının dayanıklılığını artırmak amaçlı kurulmuş ve 2019 yılında limanların siber güvenliği ile ilgili yayınladıkları raporda sektöre bir dizi önerilerde bulunulmuştur (ENISA, 2019). Bir sonraki yıl yayınlanan raporda ise, ortak siber risk ilkelerini takip ederek liman siber risk değerlendirmesinde başarıya ulaşabilmek ve risklerle etkin mücadele için dört aşamalı yaklaşım aşağıdaki 0gibi sunulmuştur (ENISA, 2020):

Aşama 1: Siber bağlantılı varlık ve hizmetlerin belirlenmesi
Aşama 2: Siber bağlantılı risklerin belirlenmesi ve değerlendirilmesi
Aşama 3: Güvenlik önlemlerinin belirlenmesi
Aşama 4: Siber güvenlik olgunluğunun değerlendirilmesi

1.4.3. Petrol Şirketleri Uluslararası Deniz Forumu (OCIMF)

OCIMF, özellikle petrol kaynaklı deniz kirliliği konusunda artan kamuoyu endişesine yanıt olarak Nisan 1970'de kurulmuş olup, bugün 100'den fazla üye şirkete ve IMO'ya danışmanlık statüsüne sahip bir kuruluştur (OCIMF, 2022). OCIMF tarafından şirketlere kendi güvenlik yönetim sistemlerini geliştirmeleri ve ölçmeleri için bir araç sağlayan; Tanker Yönetimi ve Öz Değerlendirme Forumunun (TMSA) 3. versiyonu 1 Ocak 2018 tarihinde yürürlüğe girmiş ve üyelerin siber risk güvenlik politikalarını ve prosedürlerini şirketin/geminin işletim prosedürlerine dâhil etmeleri konusunda aşağıdaki kararlar alınmıştır (TMSA, 2017):

- Yazılım yönetimi prosedürleri oluşturulmalı,
- Siber tehditlerin nasıl belirleneceği ve azaltılacağına dair rehber kılavuzlar edinilmeli,
- Endüstri ve sınıflandırma derneğinden siber güvenlikle ilgili en son yayınlanan kılavuzlar bulundurulmalı,
- Şifre yönetim prosedürleri oluşturulmalı,
- Gemilerde siber farkındalığı artırmak için personelle paylaşılabilecek bir siber güvenlik planı bulunmalıdır.

1.4.4. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)

1901'de kurulan ve şu anda ABD Ticaret Bakanlığı'nın bir parçası olan NIST, kuruluşların siber güvenlik risklerini yönetmelerine yardımcı olmak için endüstri standartlarını ve en iyi uygulamaları bir araya getirerek siber güvenlik riskleri hakkında ortak bir dil oluşturmaya çalışmaktadır (NISTa, 2022). Siber güvenliği; bilgi kaybını önlemek ve korumak için saldırıları tespit etme ve bu saldırılara yanıt verme olarak açıklayan NIST siber güvenlik fonksiyonlarının kategorilerini Tablo 4'te olduğu gibi açıklamıştır.

Tablo 4. NIST Siber Güvenlik Fonksiyonları

Fonksiyonlar	*Kategoriler*
Tanımlamak	Varlık Yönetimi İş Çevresi Yönetim Risk Değerlendirmesi Risk Yönetim Stratejisi Tedarik Zinciri Risk Yönetimi
Korumak	Kimlik Yönetimi ve Erişim Kontrolü Farkındalık ve Eğitim Veri güvenliği Bilgi Koruma Süreçleri ve Prosedürleri Bakım Koruyucu Teknoloji
Tespit etmek	Anomaliler ve Olaylar Güvenlik Sürekli İzleme Tespit İşlemleri
Cevap vermek	Müdahale Planlaması İletişim Analiz Azaltma İyileştirmeler
Kurtarmak	Kurtarma Planlaması İyileştirmeler İletişim

NIST, siber güvenlik çerçevesinde fidye yazılımını; saldırganların bir kuruluşun verilerini şifrelemesi ve erişimi geri yüklemek için ödeme talep etmesi olarak açıklamıştır. Saldırganların ayrıca bir kuruluşun bilgilerini çalabileceğini ve bilgileri rakiplere veya halka açıklamaması karşılığında ek bir ödeme talep etmesi durumu olarak özetleyerek kritik alt yapıların siber güvenliğine ek olarak fidye yazılımı risk yönetim raporunu yayınlamıştır (Fisher, vd., 2022).

1.4.5. Diğer Kuruluşlar

Baltık ve Uluslararası Denizcilik Konseyi (BIMCO), Amerika Deniz Ticaret Odası, Dijital Konteyner Derneği, Uluslararası Kuru Yük Armatörleri Birliği (INTERCARGO), InterManager, Uluslararası Bağımsız Tanker Sahipleri Birliği (INTERTANKO), Uluslararası Deniz Ticaret Odası (ICS), Uluslararası Deniz Sigortaları Birliği (IUMI), Petrol Şirketleri Uluslararası Deniz Forumu (OCIMF), Süperyat Üreticileri Derneği (Sybass) ve Dünya Denizcilik Konseyi (WSC)

tarafından Gemilerde Siber Güvenlik Yönergeleri versiyon 4 yayınlanmış; operasyonel ve teknik süreçlere, ekipmana, personel eğitimine ve siber olaylara müdahaleye, müteakip operasyonel kurtarmaya odaklanarak, ilgili endüstri düzenlemeleri ve en iyi uygulamalara uygun olarak gemide siber risk yönetimi stratejilerini sunulmuş ve Şekil 10'da gösterildiği gibi siber risk yaklaşımları önerilmiştir (BIMCO, vd., 2020).

Şekil 10. Siber Güvenlik Yönergeleri

Kaynak: BIMCO, vd. (2020).

Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) dünya çapında standardizasyon için özel sistem oluşturur. ISO veya IEC üyesi ulusal kuruluşlar, belirli teknik faaliyet alanlarıyla ilgilenmek üzere ilgili kuruluş tarafından kurulan teknik komiteler aracılığıyla Uluslararası Standartların geliştirilmesine katılır. ISO ve IEC teknik komiteleri, karşılıklı ilgi alanlarında işbirliği yapmaktadır. ISO ve IEC ile irtibat halinde olan diğer uluslararası kuruluşlar, hükümet ve hükümet dışı kuruluşlar da çalışmada yer almaktadır (ISO ve IEC, 2021). ISO 90001 kalite yönetim sistemini uygular, süreç odaklı bir yaklaşımla planla-yap-kontrol et-eylem döngüsünü takip eder ve kuruluş genelinde uygulanan her prosedür için risk temelli düşünmeye odaklanır. Bu döngünün amacı, planlı sonuçlara ulaşmak ve sistemin sürekli iyileştirilmesini sağlamaktır (ISO, 2015).

Planlama: Riskleri ve fırsatları ele alarak, belirlenen konular sıraladıktan sonra hedeflere ulaşmak için planlar ve prosedürlerin yapılması.

Yapma: Planlamaya dayalı olarak fiili işin gerçekleştirilmesi.

Kontrol Etme: İlk hedeflerin planlara uygun olarak gerçekleştirilip gerçekleştirilmediğinin doğrulanması ve değerlendirilmesi. Süreçle ilgili sorunların tanımlanması.

Eylem: Bir değerlendirmenin sonucuna göre sürecin ve performansın iyileştirilmesi.

Denizcilik endüstrisini özellikle siber olaylara karşı savunmasız ve siber suçlular için çekici kılan özellikleri aşağıdakiler gibi özetlenebilir (BIMCO, vd., 2020):

- Denizcilik sektörünü hedef alan siber suçlar genellikle kitle iletişim araçlarının ilgisini çekmemektedir. Bu durum sektörün kamuoyu nezdinde görünürlüğünün düşük olmasına ve sektörü siber suçlular için çekici kılmaktadır.
- Günlük işler için büyük para transferleri gerçekleşmektedir.

- Sektördeki birbirine bağlı çok sayıda işletme ve yetkili, iş açısından kritik verileri duyarlı ve ticari açıdan hassas bilgileri paylaşmaktadır.
- Bir geminin işletilmesine birden fazla paydaşın dahil olması, genellikle onu güvenceye almak için hesap verme sorumluluğunun olmamasına neden olmaktadır.
- Gemiler karadan erişilebilir ve izlenebilir durumdadır. Gemi ekipmanı (OT'ye özel sistemler) veya gemi yazılımı için uzaktan destek sağlanabilmektedir.
- Birçok eski BT ve OT sistemi hala kullanılmaktadır. Bu sistemler, artık desteklenmeyen ve güvenliği sağlanamayan eski yazılımları çalıştırmaktadır. Bu sebeple otomasyon sistemleri, siber güvenlik düşünülmeden entegre edilmiş birden fazla alt sistemden oluşabilmektedir.
- Yama uygulanamayan veya güncellenemeyen BT ve OT sistemlerine erişim daha kolay gerçekleşebilmektedir.
- Siber güvenlik, denizcilik için nispeten yeni bir kavramdır, henüz anlaşılmamıştır ve çoğu denizcilik işletmecisi ve yöneticisinin ilgili siber riskler konusunda eğitimi yoktur.

Denizcilik sistemleri ve siber güvenlik konusunda tek bir yönetmelik veya standart bulunmamaktadır. Deniz siber güvenliği, düzenleyicilerin dikkate alması gereken benzersiz bir dizi zorluk teşkil etmektedir. Siber güvenlik standartlarının gelişimini hızlandırmak ve etkin, bütünsel deniz siber risk yönetimini desteklemek için bir Siber Koda ihtiyaç olduğu düşünülmektedir (Hopcraft ve Martin, 2018). Denizcilikte siber tehditler konusunda yayınlanmış çeşitli kılavuzların özeti Tablo 5'te gösterilmiştir.

Tablo 5. Denizcilikte Siber Tehditlerin Çözümüne İlişkin Kılavuzlar

Başlık	**Yayıncı Kuruluş**	**Basım Yılı**	**Başlık**	**Yayıncı Kuruluş**	**Basım Yılı**
Framework for Improving Critical Infrastructure Security	NIST	2016	The Application of Cybersecurity Principles to Marine and Offshore Operations	ABS	2016
Guide to ICS Security	NIST	2015	Guidelines on Maritime Cyber Safety	Indian Register of Shipping	2018
Guidelines on Cybersecurity Onboard Ships	BIMCO	2020	Cybersecurity Guidelines for Shipowners	Polish Register of Shipping	2020
Rules on Cybersecurity for the Classification of Marine Units	Bureau Veritas	2020	Deploying Information and Communications Technology in Shipping	Lloyd's Register	2016
Guidelines for Designing Cybersecurity Onboard Ships	ClassNK	2020	Guidelines on Maritime Cyber Risk Management	IMO	2017
Cybersecurity Resilience Management for Ships and Mobile Offshore Units in Operation	DNV-GL	2016	Cyber Risk Management for Ports	ENISA	2020

Kaynak: Drazovich, vd. (2021)

Deniz siber güvenliği konusunda bölgesel kılavuzlar başta olmak üzere çok sayıda geliştirilmiş kılavuz mevcuttur. Bu kılavuzların her biri tehditlerin tespiti, çözümü ve yanıt verilebilirlik anlamında çok önemli olsa da teknolojinin durmaksızın ilerlemesi ve risklerin kendilerini yenilemesi sebebiyle tam olarak endüstri isteğine karşılık veremedikleri açıktır.

İKİNCİ BÖLÜM

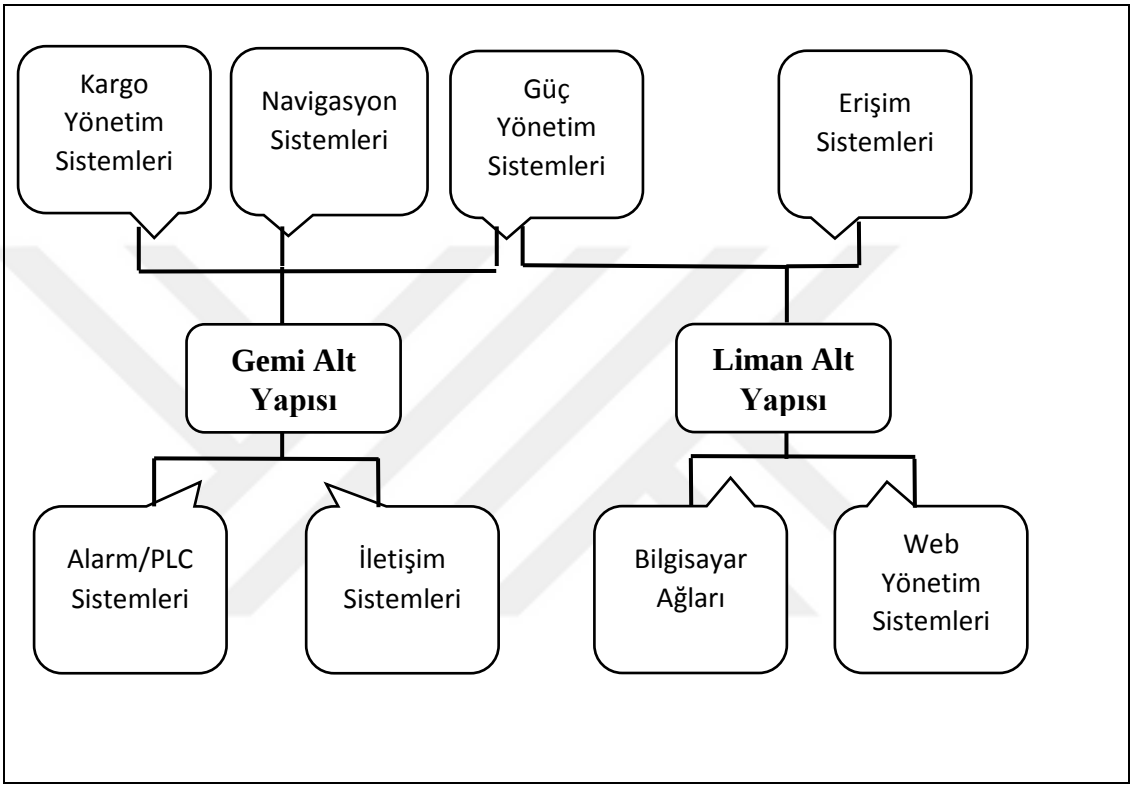
2. DENİZCİLİKTE SİBER RİSK UNSURLARI VE ÇÖZÜM YAKLAŞIMLARI

Siber fiziksel sistemlerin, güvenlik açısından bir dizi kritik uygulama içerdiğinden, insanlara, çevreye ve varlıklara herhangi bir zarar vermeden çalışmalarını sağlamak çok önemlidir (Bolbot, vd., 2019). Denizcilikte siber riskleri azaltmanın veya ortadan kaldırabilmenin olmazsa olmazı neyle karşı karşıya olduğumuzu bilmemizden geçmektedir. Öncelikle siber sistemin ve bileşenlerinin karşılıklı bağımlılıkları şu şekilde açıklanabilir (Kure, vd., 2018):

- **Fiziksel Karşılıklı Bağımlılık:** Bu, bir altyapının çalışması diğerinin fiziksel çıktısına bağlıysa, fiziksel olarak birbirine bağımlı olan iki veya daha fazla altyapıyı ifade eder.
- **Siber Karşılıklı Bağımlılık:** Bilgi altyapısı aracılığıyla iletilen bilgilere bağlı olarak bir altyapının durumunu ifade eder.
- **Mantıksal Karşılıklı Bağımlılıklar:** Bu tür karşılıklı bağımlılık, her bir altyapının durumu, siber, fiziksel veya coğrafi olarak kabul edilemeyen kontroller, mekanizmalar, düzenleyici veya başka yollarla diğerinin durumuna bağlı olduğunda ortaya çıkar.
- **Coğrafi Bağımsızlıklar:** Bu tür karşılıklı bağımlılık, birden çok altyapının öğeleri aynı alanda olduğunda ortaya çıkar. Bu durumda doğal afetler, bir altyapının bir unsurunun yakın çevredeki bir veya daha fazla altyapıda arıza oluşturmasına neden olabilir.

Sistem ilişkilerine ve güvenlik açıklarına dayalı olarak bir gemide bulunan temel işlevlere yönelik potansiyel saldırı yollarını hesaplamak oldukça önemlidir (Enoch, vd., 2021). Siber savunma henüz denizcilik sistemleri mühendisliğinin ayrılmaz bir parçası olmamıştır ve güvenlik düzeylerini sistematik olarak değerlendirmek için diğer alanlarda olduğu gibi yerleşik herhangi bir otomatik araç da bulunmamaktadır (Hemminghaus, vd., 2021). Bir geminin güç dağıtım sistemine

yapılan ve elektrik kesintisine yol açan bir siber saldırı, gemideki mürettebat için ölümcül güvenlik sonuçları doğurabilir. Ayrıca, yangın veya çarpışma gibi bir güvenlik olayı, gemideki sistemleri siber risklere karşı daha savunmasız olabilecekleri bir acil durumda bırakabilir (Larsen ve Lund, 2021). Gemi ve limanların alt yapı özellikleri Şekil 11'de gösterilmiştir.



Şekil 11. Gemi/ Liman Altyapısı

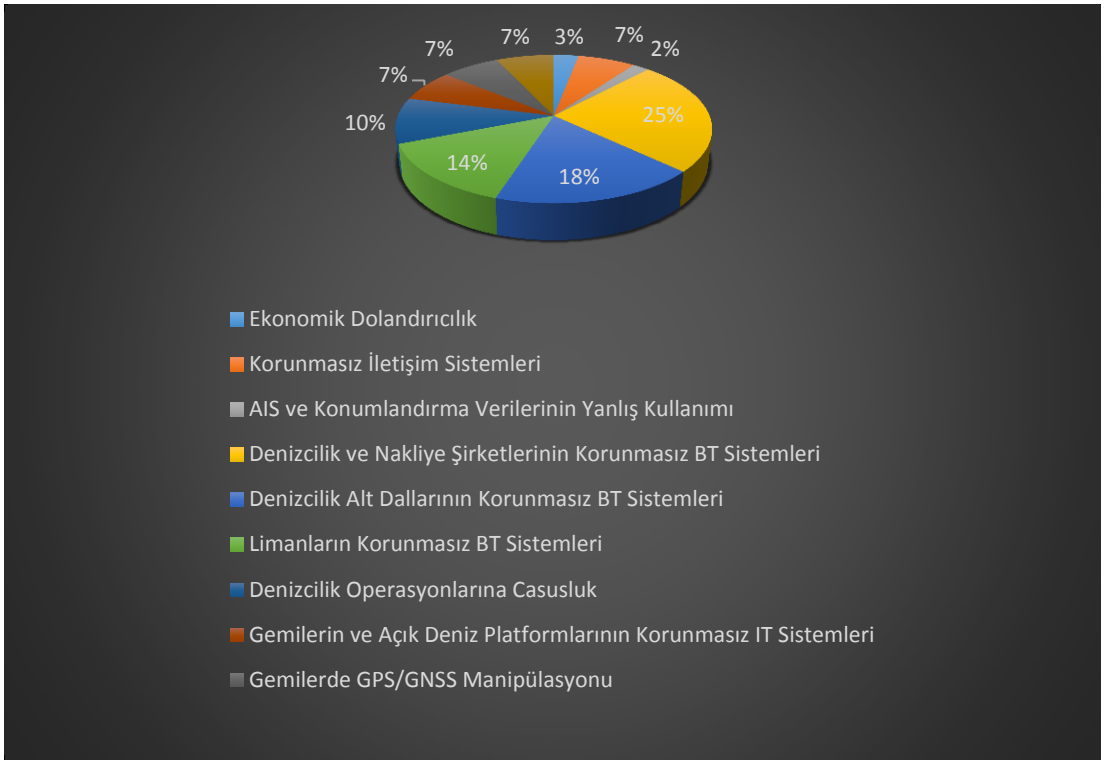
Kaynak: Ben Farah, vd., (2022)

Gemi içi altyapı iki sisteme ayrılabilir: elektro-mekanik ve iletişim. İlki, güvenliği insan gözlemine ve önleyici bakıma bağlı olan motorlar/güç ile ilgili unsurları içerirken, ikincisi, endüstri içindeki süreçlerin kritik aşamalarının yürütülmesini kolaylaştırmak için liman ve gemi arasında bilgi alışverişini sağlar (Ben Farah, vd., 2022).

2.1. DENİZCİLİKTE BİLGİ TEKNOLOJİLERİ (BT) VE OPERASYONEL TEKNOLOJİLER (OT)

Günümüzün küresel denizcilik sektörü giderek artan bir Şekilde dijitalleşmeye, operasyonların entegrasyonuna ve otomasyona bağımlı hale gelmektedir. Bu dijitalleşme yeni fırsatlar yaratırken bir yandan da siber tehditleri ortaya çıkarmaktadır. Siber teknolojiler, sadece gemilerde ve limanlarda çok sayıda sistem ve sürecin işletilmesi, yönetimi için değil, aynı zamanda geminin, mürettebatın, kargonun ve denizciliğin emniyeti, güvenliği ve korunması için de gerekli, hatta çevre kirliliğinin önlenmesi için kritik hale gelmiştir. Bu teknolojiler, ağ oluşturma ve internete bağlantı yoluyla gemilerde BT ve OT'lere entegre edilmiştir (Hareide, vd., 2018). Mürettebatın, gemideki OT teknolojisi üzerindeki kontrollerini kaybetmediklerinden emin olmaları ve denizcilik şirketlerinin finansal kayıpları veya değerli bilgi kaybını önlemek için BT sistemlerini korumaları gerekmektedir. Sistemleri anlamayı kolaylaştırmak ve iyi bir güvenlik muhakemesini teşvik etmek için denizcilik sektörü, insan davranışına ilişkin iç görüye ve mürettebatın kendi gemilerindeki sistemlere yönelik siber riskleri nasıl algıladığını bilmesi oldukça önemlidir (Van Schaik, vd., 2017).

BT veya OT sistemlerine uzaktan erişim sağlamak için geminin uydu, 4G veya Wi-Fi bağlantılarının ihlal edilmesi gerekir (Glomsvoll ve Bonenberg, 2017). İnternet bağlantısının kesilmesi dış tehditleri önler; ancak, bakımı yapılmayan işletim sisteminden kaynaklanan güvenlik açıkları, kasıtsız veya kötü niyetli olarak, dahili aktörler (gemi mürettebatı) tarafından da tetiklenebilirler (Middleton, 2014). Eski BT sistemleri ve genişleyen bir IoT bağlantı noktalarının savunmasız kalmasına neden olabilir (Androjna, vd., 2020). OT ve BT sistemlerine yönelik potansiyel siber saldırılar iki ana gruba ayrılabilir: Hedeflenmemiş siber saldırılar (saldırgan, yaygın güvenlik açıklarını bulmak ve bunlardan yararlanmak için internette mevcut araçları ve teknikleri kullandığında) ve hedefli siber saldırılar (saldırgan, bir nakliye şirketini veya bir gemiyi hedef almak için özel olarak oluşturulmuş karmaşık araçlar ve teknikler kullandığında) (BIMCO, vd., 2020). Siber saldırılara ilişkin denizcilik BT ve OT sistemlerini etkileyen pasta grafiği aşağıda gösterilmiştir.



Şekil 12. Denizcilikte Siber Tehditler

Kaynak: Meland, vd. (2021)

2018 tarihinde denizde siber güvenlikle ilgili yapılan ankette; denizcilik personellerine, "Şirketiniz gemilerinizi OT'ye yönelik siber tehditlerden koruyor mu?" sorusuna %42 evet, %32 emin değilim, %26 ise hayır cevapları ortaya çıktı ve bu sonuçlar bir yıl önce yapılan ankete göre farkındalığın arttığını göstermektedir; çünkü aynı soru cevapları 2017'de %93 hayır, %7 evet şeklindedir. BT sistemi ihlalleri, ofis işlevlerini geçici olarak kesintiye uğratabilir veya veri kaybına yol açarak finansal veya itibar kaybı ortaya çıkarabilir, bu her sektör için geçerlidir. Öte yandan bir OT siber ihlali, fiziksel birinin öldürüldüğü, geminin hasar gördüğü veya okyanusların kirlendiği daha büyük felaketleri beraberinde getirebilir. Bu tür büyük ölçekli sonuçlar sadece bir şirket için değil, potansiyel olarak tüm endüstri için yüksek finansal ve itibar maliyetleri getireceği anlamını taşır (Markit, 2020).

2010-2020 tarihleri arasında denizcilikte yaşanan 46 siber olayın araştırıldığı akademik çalışmada 10 siber tehdidin listesi sunularak, gemilerde ve karada en çok BT sistemlerinin etkilendiğini vurgulanmış ve GPS/GNSS sinyallerinin

manipülasyonunu ve gemideki OT sistemlerini hedefleyen olaylar tanımlanmıştır (Meland, vd., 2021)

2.2. GEMİNİN SİBER FİZİKSEL SİSTEMLERİ

Hassas gemi sistemleri tipi ve işlevine göre değişiklik gösterebilmektedir, ancak genel itibariyle içerdikleri unsurlar; kritik sistemler, can güvenliği ve geminin emniyetli çalışması için gerekli sistemler, kişisel bilgileri tutan sistemler, VDR sistemleri şeklindedir (Boyes ve Isbell, 2017). Modern gemiler; ECDIS (Elektronik Harita Görüntüleme ve Bilgi Sistemi), AIS (Otomatik Tanımlama Sistemi), Radar/ARPA (Radyo Yönü ve Menzil/Otomatik Radar Çizme Yardımı), Pusula (Gyro, Fluxgate, GPS ve diğerleri), VDR (Seyahat Veri Kaydedici –"Kara Kutu"), GMDSS (Küresel Deniz Tehlike ve Güvenlik Sistemi) ve daha birçok gelişmiş birim ve sistem ile donatılmıştır. Güvenli seyrüsefer yardımcılarından olan bu sistemler gemiler için vazgeçilmezdir ancak bu yardımcılarla birlikte seyrüsefer güvenliğini tehlikeye atan siber riskler sorunu önemlidir. Seyrüsefere yardımcı bu sistemlerin tamamı potansiyel olarak siber saldırılara açıktır (DiRenzo, vd., 2015; Lund, vd., 2018). Yolcu ve ticari gemilerdeki bilgi saldırılarına hazırlıksızlık nedeniyle yaşanacak olaylar ve kazalar, mürettebatın ihmali ile daha sık meydana gelmektedir (Nyrkov, vd., 2018).

Güvenlik, denizcilik operasyonları düzenlemelerinde her zaman kritik bir faktör olmuştur ve artık navigasyon sistemleri, navigasyonun etkinliğini ve güvenliğini artırmak için siber teknolojilere giderek daha fazla bağımlı hale geldiğinden, nakliyeyi siber tehditlerden koruma ihtiyacı ortaya çıkmaktadır (Kalogeraki, vd., 2018; Kessler, vd., 2018; Svilicica vd., 2019). AIS, GNSS veya ECDIS gibi en yaygın olarak kullanılan seyrüsefer yardımcılarının verimli çalışmaları için küresel konumlandırma sistemine (GPS) ve çok yüksek frekans (VHF)-radyo iletişimine büyük ölçüde bağımlı olması nedeniyle, güvenlik açıklarını beraberinde getirmektedir. Son derece otomatikleştirilmiş gemiler, radyo frekansı veya uydu iletişimi üzerinden büyük miktarda veri alıp iletecek ve bu da onları gemideki seyir dışı kazaların güvenlik açıklarına ek olarak siber-fiziksel alanın her türlü mevcut tehdidine ve riskine karşı savunmasız hale getirecektir (Sen, 2016). Bir

geminin sistemlerine yapılacak bir saldırı, potansiyel olarak yaşamları tehlikesi, hassas kayıplar, bilgi hırsızlığı, dolandırıcılık, adam kaçırma, korsanlık, kargo hırsızlığı gibi durumları ortaya çıkabileceğinden deniz siber menzili gibi girişimleri ve düzenlemeleri/yönergeleri desteklemek denizcilikte siber güvenliğin artırılmasını sağlamak adına önemlidir (Potamos, vd., 2021). Gemilerin siber fiziksel sistemleri ve oluşabilecek güvenlik açıkları Tablo 6'da gösterilmiştir.

Tablo 6. Gemi Siber Fiziksel Sistemleri Güvenlik Açıkları

Kritik Sistemler	**Varlıklar**	**Tehditler**	**Güvenlik Açıkları**
Köprü navigasyon ve radyokomünikasyon sistemleri	-Radar -ECDIS -Bağlantı -AIS -GPS -VDR -GMDSS	-İnternet bağlantısı güvenliği -Yazılım güvenliği -Siber olay işleme prosedürleri -Erişim kontrolleri -Taşınabilir cihazların kullanımı	-İnternet bağlantısı kurulur -İşletim sistemi ve uygulamalar günceldir -Olay algılama, analiz, yanıtlama -USB ortamının güvenlik durumunun uygulanması
Güç üretim ve dağıtım sistemleri	-Kontrol sistemleri -İzleme sistemleri -Alarm sistemleri	-Fiziksel ve mantıksal erişim kontrolleri -Kimlik doğrulama kontrolleri -Denetim ve günlükler -Yetkili erişim prosedürü	-Tüm erişimler sadece yetkili personele sağlanır -Tüm kontrol mekanizmaları uygulanır -Güvenlikle ilgili olaylar kayıt altına alınır -Çıkış yapma zorunluluğu uygulanır
Kargo yönetim sistemleri	-Kontrol sistemleri -İzleme sistemleri -Alarm sistemleri	-Uzaktan kimlik doğrulama kontrolleri -Yalnızca yetkili personel için fiziksel erişim -Politikalar ve prosedürler periyodik olarak gözden geçirilir -Bir programın fiili kullanımından önce eğitim	-Yalnızca kriptografi kullanarak uzaktan kimlik doğrulama -Tüm varsayılan parolalar değiştirildi -Olay algılama, analiz ve yanıt -Fiziksel ve çevresel koruma

Tablo 6. Gemi Siber Fiziksel Sistemleri Güvenlik Açıkları Devam

Erişim kontrol sistemleri	-Kontrol sistemleri -İzleme sistemleri -Alarm sistemler	-Uzaktan kimlik doğrulama kontrolleri mevcuttur -Yalnızca yetkili personele fiziksel erişim sağlanır -Politikalar ve prosedürler periyodik olarak gözden geçirilir -Bir programın fiili kullanımından önce eğitim	-Yalnızca kriptografi kullanarak uzaktan kimlik doğrulama -Tüm varsayılan parolalar değiştirildi -Olay algılama, analiz ve yanıt -Fiziksel ve çevresel koruma
Yolcu servis ve yönetim sistemleri	-Kontrol sistemleri -İzleme sistemleri -Alarm sistemler	-Erişim kontrol politikası -Yük devretme prosedürleri -Yetkili erişim politikası - Güvenlik önlemleri konusunda eğitim	-Yetkili kullanıcıların ve ayrıcalıkların belgelenmesi -Yedekleme sistemlerinin kurulması -Parola paylaşımı ve ortak hesaplar yasaktır -Olay tanıma ve işleme
İnternet iletişim sistemleri	-Ara bağlantı kontrol ekipmanı -Siber güvenlik yazılımı	-Ağ gizliliği koruması -En son yamalar veya yeni sürüm güncellemeleri -Kötü amaçlı kod koruma mekanizmaları -En son virüs tanımları veya yeni sürümler uygulaması	-Yönlendiriciler ve güvenlik duvarı tasarımları, kuralları ve ilkeleri -Merkezi yönetim ve raporlama -Kötü amaçlı yazılım enfeksiyonları -Merkezi yönetim ve raporlama

Kaynak: Svilicicc, vd. (2019)

2.2.1. Küresel Navigasyon Uydu Sistemleri (GNSS)

Dünyada, konum ve zamanlama hizmetleri sağlayan ana teknoloji haline gelen GNSS birçok uygulama alanında bağımlılık haline gelmiş ve güvenlik açığı konusunda endişeleri beraberinde getirmiştir (Marcos, vd., 2018; Medina, vd., 2019). GNSS sistemleri: Amerika Birleşik Devletleri'ne ait; GPS, Rusya'ya ait; GLONASS, Avrupa Birliği'ne ait; GALILEO, Çin Halk Cumhuriyeti'ne ait; BEIDOU, Japonya'ya ait; QZSS, Hindistan'a ait; IRNSS, bunlardan başlıcalarıdır. Navigasyon sistemlerinin, genel olarak ticari denizcilik operasyonlarında ve Deniz Taşımacılığı Sisteminde kullanılanlarla temelde aynı olduğunu belirtmek önemlidir. GNSS'nin sadece navigasyon olmadığını vurgulayan Dobryakova, vd.,(2018) GNSS güvenlik açıklarının neden olduğu tehditleri araştırdıkları çalışmada, dağıtılmış bir radyo

elektronik cihaz ağında kullanılan senkron zamanın referans sinyalini boğmak için GNSS girişimine ihtiyaç olduğunu yani GNSS'nin bağımsız pasif cihazlarda yüksek doğrulukta zaman senkronizasyonu yaptığına dikkat çekmişlerdir.

Güvenlik açısından, ticari gemiler sivil GNSS sinyallerine güvenir. Ne yazık ki, alıcılarda mesaj kullanılabilirliğini artırmak için sivil GNSS, mesajları herhangi bir gizliliğe veya doğrulama mekanizmasına dayanmadan açık metin olarak iletmek üzere tasarlanmıştır. Bu nedenle, ticari olarak temin edilebilen Yazılım Tanımlı Telsizler kullanılarak kolayca yanıltılabilirler. (Caprolu, vd., 2020). GNSS'ye yönelik siber saldırılar, kimlik doğrulama ve şifreleme eksikliği nedeniyle kolaylaştırılmış ve sistemi ihlallere karşı savunmasız hale getirmektedir (Oligeri, vd., 2020) GNSS sinyallerine yönelik kasıtlı saldırılar geleneksel olarak karıştırma ve yanıltma olarak ikiye ayrılır. (DiRenzo, vd., 2015; Schmidt, vd., 2016; Medina, vd., 2019; Androjna, vd., 2020)

GNSS Karıştırma: Güçlü elektromanyetik dalgaları, konumunu inkar etmek amacıyla kurban alıcıya kasıtlı olarak yönlendirme eylemidir (Borio, vd., 2016; Glomsvoll ve Bonenberg, 2017). GNSS karıştırma nispeten az teknik bilgi gerektirir ve yalnızca rastgele veya rahatsız edici gürültüyle orijinal sinyallerin bastırılmasıyla gerçekleştirilebilir (Huang, vd., 2016).

GNSS Sahtekarlığı: GNSS parazitinden oldukça farklıdır, GNSS işlemlerini bozmadan kurbanın alıcısında yanlış bir konum oluşturmak amacıyla sahte GNSS benzeri sinyallerin iletilmesinden oluşur. Navigasyon sistemleri, bozucuları algıladığında alarm çalarken, sahtekarlık sistemleri, en son GNSS sistemlerini bile karıştıran ve daha ciddi sonuçlara yol açan yanlış sinyaller oluşturur (Middleton, 2014).

GNSS ile ilgili rapor edilen siber olayda; Karadeniz'deki 20 geminin GPS sinyalleri, gemilerin konumlarının Gelendzhik Havalimanı'nda olduklarını göstermiştir (David, 2017).

2.2.2. Elektronik Harita Görüntüleme ve Bilgi Sistemi (ECDIS)

Deniz taşımacılığının güvenli bir şekilde yerine getirilmesinde oldukça yüksek bir paya sahip olan ECDIS bilgisayar tabanlı, kritik operasyonel teknoloji sistemi haline gelmiştir (Svilicica, vd., 2019). Konumları ve yönleri belirlemek için bir navigasyon destek sistemi olan ECDIS, güzergah planlama, yürütme ve izleme için farklı seyir veri kümelerini bağlayarak seyri güvenli hale getirmektedir (Porathe, vd., 2013), ECDIS geminin GNSS bağlantısı ile ara yüzüdür ve bir elektronik deniz haritası içermesinden kaynaklı her iki sistem de siber saldırılara karşı savunmasızdır (Liu, vd., 2018).

Kobe Üniversitesinde eğitim amaçlı kullanılan bir gemiye ECDIS güvenlik açıklarının tespiti için yapılan çalışma sonucu ne kadar savunmasız ve risklere karşı açık bir sistem olduğu ortaya çıkmıştır (Svilicicb, vd., 2019). Gemilerin siber risklerini değerlendirmek için genel bir çerçeve sunan akademisyenler bunları; hazırlık, iletme, sonuçların iletilmesi ve bakım olarak sıralamışlardır. Bir başka ECDIS zafiyeti araştırmalarında güvenlik testi uygulayarak sistemin zayıf yönlerini göstermişlerdir. (Svilicicc, vd., 2019; Svilicica, vd., 2020).

2018'de bir grup araştırmacı, USB çubuğu kullanarak kötü amaçlı yazılım içeren bir virüs ile askeri eğitim gemisinde navigasyon sistemine saldırdıkları ve geminin ECDIS ekranındaki konumunu değiştirmeyi başardıkları bir deney gerçekleştirmişlerdir (Hareide, vd., 2018). ECDIS'e özel güvenlik gereksinimleri aşağıdaki gibidir (Kavallieratos, vd., 2020).

İnsan Kaynakları Güvenliği: ECDIS yöneticisi eğitimli olmalı ve hileli veri paketlerini ayırt edebilmelidir.

Erişim Kontrolü: ECDIS'nin kullanımı yalnızca yetkili ve iyi eğitimli personel ile sınırlandırılmalıdır.

İletişim Güvenliği: i) ECDIS, diğer gemilere ve SCC'ye gönderilen yolculukla ilgili verilerin akışlarını kontrol edebilmelidir; ii) ECDIS, harici aktörlere gönderilen

ve alınan verileri denetleyebilmelidir; iii) ECDIS tarafından iletilen güvenlikle ilgili bilgiler doğrulanmalıdır ve iv) ECDIS ile uydu sistemi arasındaki iletişim sürekli olarak mevcut olmalıdır.

Tusher, vd. (2022) siber güvenlik risklerini otonom gemiler açısından çok kriterli karar verme yöntemlerinden Bayesçi en iyi-en kötü metodunu kullanarak değerlendirmiş, sistem düzeyinde, sonuçlar, seyir sistemlerinin potansiyel siber tehditlere karşı en savunmasız olduğunu, sevk sistemlerinin ise gelecekteki otonom denizcilik operasyonları bağlamında en az savunmasız unsur olduğu sonucuna ulaşmışlardır. Bulgulara göre, bir alt sistem düzeyinde ise, en savunmasız üç parça GNSS, ECDIS ve kara kontrol merkezleri iletişim cihazları iken, en az savunmasız parçalar motor kontrolleri, kara kontrol merkezleri entegrasyon platformları ve kargo elleçleme limanlarıdır.

2.2.3. Otomatik Tanımlama Sistemi (AIS)

AIS, bir geminin yakındaki diğer gemileri, yerel deniz trafiğini (yani 10-20 deniz mili içinde) görebilmesi ve yakınındaki herhangi bir geminin adını, IMO kayıt numarasını, boyutunu (yani uzunluk, kiriş, draft ve gros tonaj) ayrıca konum (enlem ve boylam), rota, kerteriz, varış noktası, durum (örn. demirli, güç altında yolda vb.) ve diğer bilgileri görülmesine izin veren bir izleme sistemidir (Kessler, vd., 2018). Gemilerdeki AIS elektroniği, bilgileri otomatik olarak iletmelidir. Öte yandan, ilgili bilgileri otomatik olarak alabilmeli ve işleyebilmelidirler. Ayrıca, yüksek öncelikli ve güvenlikle ilgili çağrılar minimum gecikme ile cevaplanmalıdır. Operatörler için bilgilerin görüntülenmesi, erişilmesi ve seçilmesi için bir kullanıcı arayüzüne sahip ayrı bir sistem olmalıdır. (Nguyen, vd., 2018). AIS'de gemi ayrıntılarının değiştirilmesine, hayalet gemilerin oluşturulmasına, yanlış uyarıların verilmesine ve sinyal iletim frekansını değiştirmeye izin veren çok sayıda güvenlik açığı bulunmaktadır (Balduzzi, vd., 2014: Guri, vd., 2014; Iphar, vd., 2015). AIS'ye siber saldırı sonucu oluşabilecek potansiyel sonuçlar aşağıdaki gibi olabilir (Katsilieris, vd., 2013; Mazzarella, vd., 2016; Deloitte, 2017):

AIS Sahtekarlığı: Bilgisayar korsanları özel olarak hazırlanan mesajları taklit edebilir ve mevcut bir gemi veya sahte bir gemi oluşturabilirler.

Gemiyi Gasp Etme: Bilgisayar korsanları bir geminin verilerini indirebilir ve bazı parametreleri değiştirerek AIS'ye servis edebilir.

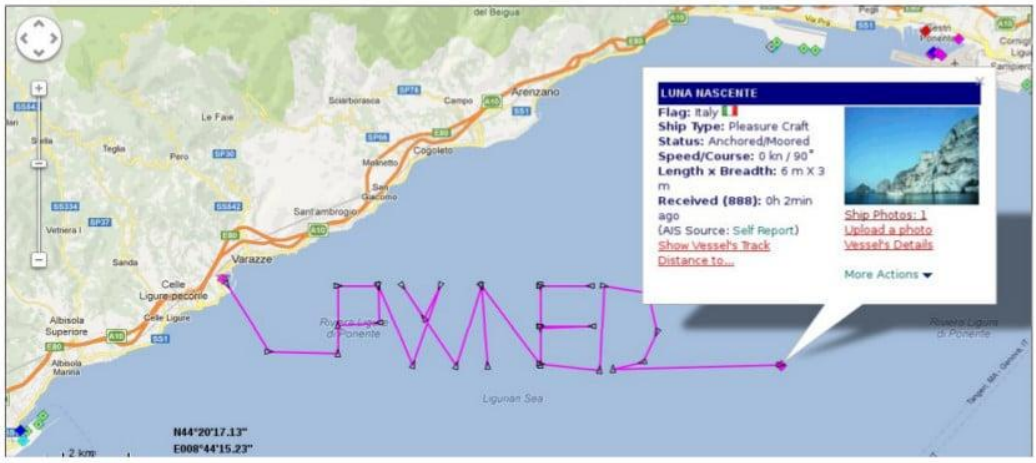
Tekrar Saldırıları: AIS bilgilerini ele geçiren bilgisayar korsanları belirli zaman dilimlerinde sahte mesajlar gönderebilir.

Sudaki Adam: Denizcilik yasaları nedeniyle bu tür bir uyarı ile herkesin uyması gereken durum ortaya çıkarabilirler.

Sahte En Yakın Varış Noktası: Bilgisayar korsanları sahte varış noktaları oluşturabilirler.

Keyfi Hava Tahmini: Bilgisayar korsanları yetkili gibi davranarak yanlış hava tahminlerini iletebilirler.

2014 yılında bir siber güvenlik şirketi tarafından gerçekleştirilen çalışmada Şekil 13'te gösterildiği gibi AIS sahtekârlığı yapılmıştır.



Şekil 13. AIS Verilerinden Sahte Gemiler Oluşturmak
Kaynak: Balduzi, vd. (2014)

Araştırmacılar dizüstü bilgisayara bağlanan kendi AIS aktarıcılarını oluşturdular ve ardından ele geçirilen AIS verileri içindeki çeşitli bileşenleri manipüle ettiler. Ele geçirilen AIS veri akışını manipüle ederek, kritik güvenlik mekanizmalarını kandırmayı ve çevrimiçi/internet AIS veri tabanlarındaki dijital tanımlayıcıları değiştirmeyi başardılar. Belki daha da ürkütücü olan, araştırmacılar seyir verilerine etkili bir Şekilde müdahale etmeyi, bunlara erişmeyi ve onları manipüle etmeyi başardılar ve Akdeniz'de kurgusal da olsa "PWNED" yazarak işin ciddiyetini göstermişlerdir (Balduzzi, vd., 2014). AIS protokolü; yanıltma, korsanlık, veri manipülasyonu ve DDoS dahil olmak üzere farklı saldırılara karşı savunmasızdır (Caprolu, vd., 2020).

AIS'nin sistemi, uygulaması ve protokol spesifikasyonu ile tüm veri iletim zinciri, birçok tehditten etkilenebilir ve birden fazla saldırı olasılığı ortaya çıkabilir. AIS mesajlarındaki anormallikleri belirlemek için belirli davranışların tanımlanmasıyla birlikte mesajların ve gemilerin yörüngelerinin uzun vadeli analizi gerekmektedir (Ray, vd., 2015). AIS'ye özel güvenlik gereksinimleri aşağıdaki gibidir (Kavallieratos, vd., 2020).

Operasyon Güvenliği: i) AIS, sistemi kontrol kaybından veya bilgi sahipliğinden korumak için güvenlik hizmetlerini uygulamalıdır ve ii) varış limanı veya kargo ile ilgili bilgiler gibi yolculuk verileri, düşmanlara olası sızıntıları önlemek için gizli olmalıdır.

Haberleşme Güvenliği: i) radar sistemi ile haberleşme kanalı yedekli olmalıdır ve ii) SCC'ye iletilen yolculukla ilgili veriler, kurcalanmaya veya hasara karşı korunmalıdır.

Giriş Kontrolü: i) AIS verilerini okuyan, değiştiren ve ileten aktörleri benzersiz bir Şekilde tanımlamak ve ayrıca sistemin kendisini ve hizmetlerini doğrulamak için güvenilir kimlik doğrulama mekanizmaları mevcut olmalıdır ve ii) AIS, yönetici tarafından talep edildiğinde veya yapılandırılabilir bir boşta kalma süresinin ardından kilitleme mekanizmalarını (örneğin, HMI ekranını kilitleme) uygulayabilmelidir.

Kriptografi: AIS işlevlerinin (örneğin, istek, okuma, işleme ve gönderme) özgünlüğü, dijital imzalar gibi güvenlik teknikleri kullanılarak sağlanmalıdır.

AIS, dünya çapında gözetleme için güçlü bir araç olduğundan; gelecekte özellikle AIS takibi ve otomatik anomali tespiti konusunda farkındalığın artırılması gerektiğine inanılmakta ayrıca denizdeki bireylerin mahremiyetini ve veri egemenliğini korumak için gemilere hem takma ad hem de gizlilik sağlayan AIS uzantılarına ihtiyaç olduğu vurgulanmaktadır (Wolsing, vd., 2022).

2.2.4. Yolculuk Veri Kaydedicileri (VDR)

Uluslararası Denizde Can Güvenliği Sözleşmesi 1974 (SOLAS), Seyrüsefer Güvenliğine ilişkin bölüm V'de uygulamaları düzenlenen VDR'ler; Uçaklarda taşınan kara kutular gibi, herhangi bir olaydan hemen önce prosedürleri ve talimatları gözden geçirmelerine ve herhangi bir kazanın nedenini belirlemeye yardımcı olmak amacıyla tasarlanmışlardır (IMOb, 2022). Bu sistemin amaçları şunlardır: Geminin teknik ve rota verilerini içeren sefer bilgilerinin kaydedilmesi, kaptan köşkünden alınan ses kayıtları ve bu bilgilerin kaydedilmesidir. Bu cihazlar, genellikle bir mürettebat üyesi tarafından alınan bilgileri değiştirme veya silme olasılığından korunmaz. Ayrıca, sistemin çalışmasını etkileyebilecek ağ üzerinden uzaktan erişim olasılığı da vardır (Kardakova, vd., 2018).

Hindistan'da 2012'de kargo gemisi ile balıkçı teknesi çarpışması sonucu 4 kişinin hayatını kaybettiği olayda; gemide 25 mürettebat üyesi bulunduğu ve en az dördünün olaydan tamamen haberdar olduğunu bilindiği halde VDR dosyalarının yeniden yazılmasına ve ses verilerinin kaybolmasına neden olan bir USB sürücünün yerleştirildiği iddia edilmiştir. Ayrıca ana bilgisayar sistemine de bir virüs bulaştığı ve uygun anti-virüs koruma yazılımına sahip olmadığı tespit edilmiştir (Anand, 2012).

2.2.5. Radyo Algılama ve Menzil (RADAR)

RADAR aslen İngilizce "**RA**dio **D**etecting **A**nd **R**anging" terimsel ifadesinin baş harflerinden türetilmiştir. Konseptin temelinde hedef tespiti ve menzil tayini işlerini gerçekleştirmek vardır. Buna ek olarak pek çok radar sistemi açısal yön ve doppler hızı tahmini işlevlerini de yerine getirir. Bu fonksiyonların gerçekleştirilmesinde radyo dalgaları kullanılmaktadır. Radar sistemleri, genel olarak, yönlendirilmiş bir anten yardımıyla elektromanyetik enerjiyi belirlenen bir yönde havaya doğru göndererek hedef tespitini gerçekleştirmeye çalışır. Arama yönünde radar menzilinin içinde bulunan nesneler, radarın yaydığı elektromanyetik enerjinin bir kısmını geri yansıtır. Buna eko sinyali veya radar dönüşü de denilmektedir. Yansıyan sinyaller radar alıcısı vasıtasıyla işlendiğinde ise hedefe ilişkin hız, menzil açı pozisyonu gibi bilgiler elde edilir (Nathanson, vd., 1999).

SOLAS gemileri olarak sertifikalandırılmış iki petrol/kimyasal tankerde uygulanan gemi radarlarının karşılaştırmalı bir siber güvenlik dayanıklılık testinde, potansiyel siber tehditlerin temel olarak radarların altında yatan işletim sisteminin bakımı ile ilgili olduğunu ve radar sistemlerinin periyodik siber güvenlik testlerinin düzenleyici standardizasyonuna ihtiyaç duyulduğu ortaya çıkmıştır (Svilicicb, vd., 2020).

2.2.6. Küresel Deniz Tehlike ve Güvenlik Sistemi (GMDSS)

Bu sistem denizde ortaya çıkabilecek tehlikelerde kara bazlı iletişim sistemlerinin de kullanılmasıyla kurtarma birimlerini otomatik olarak uyaran, arama-kurtarmayı otomatik olarak hızlı Şekilde sağlayan uluslararası bir sistemdir. Bu fonksiyonu yerine getirebilmek için hem yeryüzü hem de uydu telsiz iletişim teknolojilileri ile gemilerdeki telsiz iletişim sistemleri kullanılır. Sistem her ihtimal göz önünde bulundurularak uyulması istenen koşullar yerine getirildiği takdirde, hiç gecikmeden bir arama-kurtarma ve yardımı temin eder (Korkmaz, 2008).

SOLAS 1974 IV. Bölüm gereği gemilerde istenilen ve kullanılan tüm iletişim ve alarm cihazları (VHF/HF/MF, EPIRB, SART, Navtex alıcısı, DSC Enkoder,

Inmarsat-Cvb.) GMDSS teçhizatını oluşturur. GMDSS'ye uymak için gemiler, aşağıdaki işlevleri yerine getirebilecek donanıma sahip olmalıdır (Johnson, 1999):

- Tehlike uyarılarını, her biri farklı bir radyokomünikasyon hizmeti kullanan en az iki ayrı ve bağımsız mod ile iletmek. Alıcı istasyon ya yakındaki başka bir gemi ya da Kurtarma Koordinasyon Merkezi (RCC) olacaktır. RCC, geniş bir deniz bölgesindeki tüm gemileri gereksiz yere alarma geçirmekten kaçınmak için bir 'alan çağrısı' kullanarak olayın çevresindeki SAR birimlerine ve gemilere alarmı iletecektir.
- Kıyıdan gemiye uyarıların alınması.
- İletim ve alma.

- Uydu veya karasal araçlar kullanarak, telefon veya teleks veya her ikisi yoluyla gemileri ve uçakları içeren arama ve kurtarma iletişimini koordine etmek;

- Normal olarak MF ve/veya VHF bantlarında, yine telefon veya teleks veya her ikisi aracılığıyla, tehlikedeki gemi veya hayatta kalanlar ve gemilere veya uçaklara yardım eden ve tüm gemilerde elde tutulan VHF alıcı-vericilerinin sağlanmasını gerektiren olay yeri iletişimi ve cankurtaran sandalları;

- Tehlike anında manuel veya otomatik olarak etkinleştirilebilen uyarı işaretlerini (EPIRB'ler) veya arama ve kurtarma aktarıcılarını (SART'ler) gösteren acil durum konumundan konum sinyalleri;

- Hava durumu raporları ve seyir uyarıları dahil deniz güvenliği bilgileri (MSI);

- Geminin yönetimi ve işletilmesi ile ilgili olarak, herhangi bir uygun kanalda, kılavuzluk ve römorkör hizmetleri için emirler, onarımlar gibi kamuya açık yazışmalar için olanlar da dahil olmak üzere, kıyıdaki radyo sistemlerine veya ağlarına ve bu ağlardan genel radyo iletişimleri;

- Normalde VHF R/T kullanan gemiler arası güvenlik iletişimi olan köprüden köprüye iletişim (Johnson, 1999).

GMDSS'ye özel güvenlik gereksinimleri aşağıdaki gibidir (Kavallieratos, vd., 2020).

Bilgi Güvenliği Politikaları: GMDSS bileşenlerini geminin ağına kurmak için bir politika mevcut olmalıdır.

Erişim Kontrolü: i) Otonom gemi kontrolörüne (ASC) diğer alt sistemlere ve kıyı kontrol merkezine (SCC) aktarılan GMDSS sinyallerinin ve verilerin gerçekliği sağlanmalıdır ve ii) GMDSS aracılığıyla iletilen sinyalleri, SCC gibi harici aktörler, otonom motor izleme ve kontrol (AEMC), navigasyon sistemleri gibi diğer gemi alt sistemleri tarafından doğrulanmalıdır.

Operasyon Güvenliği: ASC, gerektiğinde GMDSS'ye güvenlik, emniyet ve dinamik veriler sağlayabilmelidir.

İletişim Güvenliği: i) GMDSS aracılığıyla diğer yerleşik sistemlere ve harici aktörlere iletilen emniyet sinyalleri sürekli olarak mevcut olmalıdır, ii) GMDSS'ye, sinyalin/verinin meşru bir kullanıcıdan/sistemden mi yoksa kötü niyetli bir kullanıcıdan mı geldiğini tespit edebilmelidir, iii) harici aktörlere veya alt sistemlere iletilen sinyaller uygun Şekilde şifrelenmelidir.

Sistem Toplama, Geliştirme ve Bakım: GMDSS antenleri uygun Şekilde kurulmalıdır.

2.3. LİMANLARIN SİBER FİZİKSEL SİSTEMLERİ

Limanlarda konteynerlerin yüklenmesi ve boşaltılması veya konteynerlerin demiryolu, karayolu ve denizyolu taşıyıcıları ile taşınması gibi lojistik katmanında veya bankaları, tedarikçileri, müşterileri, perakendecileri içeren işlem katmanında yaşanacak herhangi bir aksama, ortak taşıyıcıya ve konsolidatörlere sahip olan gemiler için milyarlarca doları aşan ekonomik kayıplara neden olacaktır (Rose ve Wei, 2013). Bu aksama limanların siber fiziksel sistemlerinden kaynaklı da olabilmektedir. Denizcilik ve liman operatörleri, hacktivizm, siber suç, siber casusluk , siber terörizm ve siber savaş gibi tehdit kategorileri tarafından hedef alınabilir. Her birinin farklı bir tanımı ve özellikleri vardır. Örneğin; hacktivizm, web sayfalarına ve bilgisayarlara girerek belirli bir nesne üzerinde baskı oluşturmak için farklı hack teknikleri (örneğin kötü amaçlı yazılım) kullanarak siber uzayda operasyon anlamına gelir. Hacktivizm yürütmenin amacı, eylemleriyle dikkat

çekmekten siber uzaydaki savunmasız boşluklar yoluyla işi bozmaya kadar çeşitlilik gösterebilir (Ahokas, vd., 2017).

Limanların BT/OT sistemlerini bütünleşik olarak ele alırsak bu sistemlerin herhangi bir siber saldırıya uğramasının sonucu, oldukça maliyetli bir durumu ortaya çıkarabilecektir (Weaver, vd., 2022). Limandaki dijital teknolojiler, diğer limanlardan, gemilerden, hava servislerinden, kargo göndericilerinden ve diğer kaynaklardan gelen bilgileri işleyebilmekte ve limana giden gemilere, limana en uygun hızlarının ve diğer açık deniz özelliklerine ulaşabilmeleri için sürekli olarak bilgi verebilmektedir (Heilig, vd., 2017). Bunlara ek Gemi Trafik Hizmeti (VTS), AIS ve GPS gibi Küresel Navigasyon Uydu Sistemi limanlarda, örneğin gemilerin ve römorkörlerin faaliyetlerini takip etmek ve hatta vinç yönetimi için yaygın olarak kullanılmaktadır (Jacq, vd., 2021).

Tedarik zinciri BT altyapısının farklı bölümlerinde sürekli donanım ve yazılım değişikliklerinin gerçekleştiği dinamik bir ortamda, liman alt yapılarının rolünü ve tedarik zincirleri üzerindeki etkilerini ele alarak denizcilik sektöründe risk yönetimini yeniden düşünmeye ihtiyaç olduğu düşünülmektedir (Polatidis, vd., 2018). Risk yönetimi ile ilgili saldırı keşif yolları siber tehditlerin anlaşılması ve azaltması yönünde oldukça etkilidir (Polatidis, vd., 2018). Limanlarda başarılı risk yönetimi yapılabilmesi için önemli varlık tanımları şu Şekilde yapılmıştır (Gunes, vd., 2021)

Bina ve Yapılardaki Siber Risk Faktörleri: Güvenlik kontrol noktaları-IT'ye bağlı bina yönetim sistemleri-Kablo geçiş noktaları-Sunucular-Operasyon kontrol noktaları.

Fiziksel Altyapılar: IT ekipmanları-Donanımlar-Boru devreleri-Yük elleçleme ve lojistik sahası-geçiş güzergâhları.

Tesis ve Makine: Otomatik kapı ve bariyer-Mobil vinç ve aracalar-Dijital göstergeler, valfler-Kontrol sistemleri-Kreynler.

Bilgi İletişim Teknolojileri: Konteyner izleme sistemleri-Otomatik plaka tanıma sistemleri-Kapalı devre televizyon (CCTV)-Veri tabanı-Yazılım

Liman kritik altyapısını destekleyen teknolojiler, genel olarak dahili iş sistemleri ve operasyonel sistemler olarak iki kategoriye ayrılabilir. Dahili iş sistemleri; basit sunuculardan veya nispeten küçük bağlantı noktaları için yazılımlardan, yüzlerce sunucu ile yüksek düzeyde ölçeklendirilmiş, çok konumlu veri merkezlerinde çalışan karmaşık kurumsal platformlara kadar geniş bir yazılım, donanım ve ağ bağlantısı yelpazesini kapsarken, operasyonel sistemler; işlemleri izlemek ve yönetmek için çok çeşitli endüstriyel kontrol sistemlerini ve akıllı telefonlara, tabletlere veya bilgisayarlara kablosuz olarak bilgi besleyen kameralar ve sensörler gibi bağlı IoT cihazlarını içerir. Neredeyse tüm altyapının bağlı olduğu hassas navigasyon ve zamanlama yetenekleri sunan uydular gibi ek kategoriler de önemlidir (Trimble, vd., 2017). Polemi (2017), limanların siber güvenliğinin artırılması amacıyla aşağıdaki önerilerde bulunmuştur.

- Limanlardaki ve tüm tedarik zincirindeki güvenlik standartlarındaki güvenlik açıklarını, engelleri ve boşlukları belirleme,
- Tedarik zincirlerindeki potansiyel ardışık etkileri analiz eden liman tehdit senaryolarını belirleme,
- Riske maruz kalmayı değerlendirme,
- Kendini korumayı tanımlama ve önleyici araçları uygulayan tespit önlemleri alma,
- Periyodik güncelleme yapma, siber korumayı denetleme,
- Siber güvenlik olaylarından koşullu ve kurtarma planları geliştirme.

Limanlar ve terminaller endüstri 4.0 ile evrim geçirerek liman yetkililerini, terminalleri, liman kullanıcılarını ve ilgili liman hizmetleri sağlayıcılarını değil aynı zamanda; şehri, limanın hinterlandını ve küresel tedarik zincirinin çok ötesine geçmiştir (de la Peña Zarzuelo, vd., 2020). Günümüzde liman sektöründeki değişimlerin ana itici güçlerinden biri akıllı limanların yaşadığı dijital dönüşümdür. Farklı bağlantı noktaları arasında artan bağlantı ile birlikte farklı cihazların, aracıların ve etkinliklerin entegrasyon düzeyi, yeni risklerin ortaya çıktığı

yeni bir ekosistem yaratmaktadır. Bu durumun siber güvenlik konusunda, endüstrinin zorluklarından biri haline getirmekte ve politika yapıcılar, yeni '4.0 dünyasına geçişte diğerlerinin gerisinde kalmış bir sektörde yeni teknolojilerin tam gelişimini kolaylaştırırken, bu kritik altyapıların yeterince korunmasını sağlamak için özel sektörle birlikte çalışması gerektiği düşünülmektedir (de la Peña Zarzuelo, 2021).

2.4. LİTERATÜR TARAMASI

Siber riskler gün geçtikçe pek çok sektör için daha büyük bir tehdit unsuru olmaya devam edecek. Bu kaçınılmaz sonun gelmesinde elbette ki hayatımızın her alanına dahil olan internet ve dijital sistemler sebep olmakta. Dolayısıyla siber güvenlik risklerine ilişkin akademik çalışmaların da çeşitli sektörler üzerine yoğunlaştığı görülmektedir. Turizm (Paraskevas, 2022); yeme-içme (Latino ve Menegoli, 2022); sağlık (Lehto vd. 2022); eğitim (Agarwal vd., 2022) ; üretim (Hutchins vb., 2015) bunlardan yalnızca birkaçı.

Turk vd. (2022) inşaat sektörüne yönelik çalışmalarında üç tür yanlış eylemi (çalmak, yalan söylemek ve zarar vermek) tanımlayan özgün bir çerçeve geliştirmiş, yanlış faaliyetlerden etkilenebilecek dört unsuru (bilgi varlığı, maddi varlık, kişi ve sistem) belirlemiş ve siber güvenliği, dört tür unsur arasında üç yanlışın olmaması olarak tanımlamışlardır. Siber güvenlik önlemlerinin uygulanması konusunda literatürde verilen bazı tavsiyeler; önlemleri uygularken yukarıdan aşağıya bir yaklaşım benimsenmesi, uluslararası ve bütünsel bir siber güvenlik politikasının geliştirilmesi, karada ve denizde çalışanlar için özel bir eğitim programının uygulanması, şirkete özel prosedürlerin ve risk değerlendirme yöntemlerinin geliştirilmesini ve uygulanmasını içermektedir (Mraković ve Vojinović, 2019; Alcaide ve Llave, 2020).

Pandey vd. (2020) performansı artırmak için küreselleşmiş tedarik zincirlerindeki çeşitli siber güvenlik risklerini ve siber saldırıları belirlemeye çalışmış ve elde ettikleri 16 siber güvenlik riskini, arz riski, operasyonel risk ve talep riski olmak üzere üç kategoriye ayırmıştır. Bu sınıflandırmaya bağlı olarak makale, siber güvenlik risklerinin tedarik zinciri operasyonlarının sürekliliğini nasıl etkilediğine

dair kavrayış sağlamaktadır. Araştırmacılar özelikle tedarik zincirlerini etkileyen siber-fiziksel sistem güvenlik açıklarına odaklandıklarını vurgulamışlardır. Omitola vd. (2019) siber fiziksel sistemlerin etkin bir Şekilde korunabilmesi için güvenlik zorluklarına; gizlilik, bütünlük ve erişebilirlik merceğinden bakılması gerektiğinin altını çizmişlerdir.

Park vd. (2019) denizcilikte siber güvenlik konusuna ilişkin literatür çalışmasına dayalı bir makale hazırlamış, siber güvenlik konusunda eğitim ve uzman eksikliği, çağın gereksinimlerini karşılamayan BT sisteminin kullanımı, bilgisayar korsanlarının hedefi olma riski, sahte web sitesi ve kimlik avı e-postası kullanımını mevcut literatürden denizcilik endüstrisinde siber güvenliği etkileyen temel tehditler olarak belirlemişlerdir. Bu doğrultuda, siber saldırılar için 4 risk kontrol seçeneğini aşağıdaki gibi sıralamışlardır:

- Siber güvenlik sürecini geliştirme.
- Siber güvenlik için eğitim ve öğretim.
- Sistemi yükseltme ve güncelleme.
- Siber güvenlik iklimi yaratma.

Deniz ortamındaki siber tehdidi azaltmak için temel önerilerde bulunan Fitton, vd., (2015) tarafından yayınlanan raporda bilgi, teknoloji ve insan unsurları denizcilikte siber operasyonların ana üçlüsü olarak tanıtılmış ve riskleri azaltabilmek için birbirleriyle etkileşim içinde olmaları gerektiğini vurgulamışlardır. Siber riskleri azaltırken insanları kaynak olarak kullanan çerçeveler, politikalar ve farkındalık eğitim programları geliştirmek için insan davranışını keşfetmek ve anlamak önemli olabilir (He ve Zhang, 2019).

Pöyhönen ve Lehto (2022) ‘Otonom uzaktan kumandalı serbest geçiş operasyonlarının (nehir, kanal vb. su yollarındaki) siber güvenlik riskleri nasıl değerlendirilebilir?’ sorusuna cevap bulmayı amaçladıkları çalışmalarında, alınan tedbirlerin, paydaşların ePilotaj ortamındaki süreçlerini destekleyen sistemlerin genel kullanılabilirliği için oldukça önemli olduğu; operasyonel kullanılabilirliğin, operasyonel sürekliliğin sağlanmasında ve faaliyetlerin güvenilirliğinin

desteklenmesinde kilit bir rol oynadığı; ve siber güvenlik risk yönetimi ve bilgi güvenliğinin, operasyonel güven, süreklilik, güvenilirlik ve esneklik açısından zorunlu özellikler olduğu sonuçlarına varmışlardır.

Beaumont (2018) ise siber güvenlik riskleri odaklı çalışmasında otonom konteyner terminallerine ilişkin bir örnek olay incelemesi sunmuştur. Bu çalışma, Dördüncü Sanayi Devrimi ile bağlantılı teknoloji kullanımından kaynaklanan risklerin hem gerçek hem de tehlikeli olduğunu gösterme amacına sahiptir. Birçok konteyner terminal operasyonunun önemli siber temelli risklere maruz kalma olasılığının yüksek olduğunu ve uygun kontrol önlemleri uygulanmadıkça daha fazla otonom teknolojinin kullanıma sunulmasıyla bu riskin artacağını savunmuştur.

Ashraf vd. (2022) deniz siber güvenliğinin önemini göz önünde bulunduran çalışmalarında, siber güvenlik tehditlerini etki ve kayıp ölçeğini anlamak için sunmuşlardır. Paydaşların etkili önleyici ve düzeltici stratejiler uygulamaları için bir rehber görevi gördüğünü vurgulayan araştırmada, deniz güvenliği, gizlilik, bütünlük ve kullanılabilirlik ile ilgili siber güvenlik riskleri tartışılmış ve etkileri analiz edilmiştir. Bu bağlamda, nesnelerin interneti (IoT) cihazlarının kullanımı, gemiler için modern güvenlik çerçeveleri ve modern gemilerde kullanılan sensörler ve cihazlar ile ilgili olarak dijital dönüşümün eğilimi de analiz edilmiştir. Ayrıca, siber risk azaltma planları ve çerçeveleri ile birlikte potansiyel tehdidi ve ciddiyeti belirlemek için risk değerlendirme yöntemleri tartışmışlardır. Sonuç olarak, siber güvenlik ihlallerinin etkisini hafifletmek için olası öneriler ve karşı önlemler detaylandırılmıştır. Bu yönüyle bizim çalışmamız ile az da olsa benzerlik göstermektedir. Zira takip eden başlıklarda denizcilikte siber risklere çözüm geliştirmek amacıyla çeşitli yaklaşımlar açıklanmaktadır.

2.4.1. Siber Risklere Çözüm Yaklaşımları

Denizcilik endüstrisinin bilgi ve iletişim teknolojilerine artan bağımlılığı, siber risk yönetimine yüksek bir prim vermektedir. Siber sistemler fayda sağlarken risk de yaratır. Bu sistemlerin yanlış kullanımı, istismarı ve hatta basit arızası yaralanmalara veya ölümlere yol açabilir, deniz ortamına zarar verebilir veya hayati ticaret

faaliyetlerini kesintiye uğratabilir. Siber güvenliği uygulayan kuruluşlar üç temel unsur belirlemeleri gerekmektedir: Eğitim, politika ve teknolojiler yoluyla eğitim. Eğitim ve teknolojik eğitim ile siber bağlantılı güvenliği öğretmenin yenilikçi yollarına dair iç görü ve organizasyonun güvence altına alınması sağlanabilir. Yönetim ile stratejiler gözden geçirilerek, araçların, tekniklerin, politikaların, standartların, yetkilerin, yasaların ve en iyi uygulamalar dahil olmak üzere bir çerçeve oluşturulabilir (Dawson, 2018). Mraković ve Vojinović, (2019) siber güvenlik önlemlerinin dayanması gereken üç temel hususu şu Şekilde açıklamışlardır:

İnsan Kaynakları: Personel risklerin farkında, yeterli beceri ve niteliklere sahip olmalıdır. Ayrıca, çalışanlar prosedürlere, yetki seviyelerine, fiziksel güvenlik engellerine aşina olmalı ve riske müdahale konusunda iyi eğitilmiş olmalıdır.

Teknoloji: Yeterli sistem tasarımı bir gerekliliktir ve yazılım yapılandırması, daha fazla inceleme, doğrulama ve test süreçlerini kullanımı çok önemlidir.

Süreçler: Sistemlerin ve ağların yönetimini, yönetim politikalarını ve prosedürlerini, denetimleri, üçüncü taraflarla yapılan sözleşmeleri vb. içermelidir.

2.4.1.1. İnsan Temelli Yaklaşım

İnsanlar genellikle sosyoteknik bir sistemdeki zayıf halka olarak kabul edilse de aynı zamanda acil bir duruma düzen getirebilecek bir sistemin baş karakteri olarak kabul edilmektedir (da Conceição, vd., 2017). Bazı denizcilik eğitim merkezleri artık siber güvenlik konusunda sürekli eğitim programları sunmaktadır (örneğin Fransız Ecole nationale supérieure maritime). Bu sayede denizcilik şirketleri ve mürettebatı siber güvenlik risklerinin giderek daha fazla farkına varıyor ve kriz yönetimi konusunda daha bilgili oluyorlar (Jacq, vd., 2018). Siber saldırıları tespit etme, önleme ve bunlara karşı savunma, saldırılara etkin bir şekilde yanıt verebilme, hataları tespit edebilme ve siber saldırı koşullarında çalışmaya devam edebilmeleri için personelin eğitilmesi gerekmektedir (Fitton, vd., 2015). İnsan faktörünün siber saldırılarda etkinliğine dair yapılan bir akademik çalışmada; insan faktörü ne kadar

düşükse; hacktivizm, siber casusluk, siber terörizm, siber suçluluk ve siber savaşın o kadar yüksek olacağı varsayımında bulunulmuştur (Senarak, 2021). Gemideki veya karadaki personelin; potansiyel siber riskleri yönetmek için siber güvenlik farkındalığı, becerileri ve yetkinlikleri oluşturma, belirli davranışların nasıl istismar edilebileceğini öğretme ve insanları siber güvenlik ihlallerine yeterince yanıt vermeleri için eğitme kapsamına alınması gerekmektedir. Şirketin eğitim ve insan faktörünün farkındalığı ile ilgili çeşitli prosedürleri ve faaliyetleri bulunması gerekir (Kechagias, vd., 2022):

- Denizde ve karada, siber güvenlik sorumlu personeli belirlenmeli ve ilgili görevleri yerine getirmelidir.
- Tüm gemilerde mürettebat üyeleri için siber güvenlik e-öğrenme yazılımı sağlanmalıdır.
- Tüm güvenlik konularının yanı sıra siber güvenlik konusunu da kapsayacak Şekilde gemide resmi alıştırma eğitimi düzenlemelidir.
- Bilgi işlem departmanı tarafından tüm gemi ve ofis personeline siber güvenlik bilgilendirme politikası verilmeli ve personelin benimsenmesi sağlanmalıdır.
- Siber güvenlik konusunda yılda en az 1 kez kurum içi seminer düzenlenmelidir.
- Şirket bünyesindeki tüm personel; farkındalıklarını ve becerilerini geliştirmek için sertifikalı üçüncü şahıslardan düzenli olarak siber güvenlik eğitim seminerleri almalıdır.
- Şirketin sorumlu departmanları siber güvenlik olayları ve tehditleri hakkında farkındalık e-postaları ve memorandumlar göndermelidir.
- Her denetimden önce siber güvenlik prosedürleri uygulanmalıdır.
- Şirketin sistemlerinde kurulu tüm yazılım varlıkları için sorumlu departman tarafından hem kıyı çalışanlarına hem de denizcilere kullanım eğitimi verilmelidir.
- Personel aralıklı olarak siber güvenlik tatbikatı yapılmalıdır.

Pavlinović vd. (2021) Hırvat denizcilerin siber tehditler konusundaki farkındalıklarını incelemişlerdir. Araştırmanın sonuçları, siber tehditlere karşı yüksek düzeyde bir farkındalığın olduğunu göstermektedir. Ancak, teknik ve insan

faktörlerinin ciddi bir tam entegrasyonu ve eğitimli, yetiştirilmiş ve bilinçli personel olmadan, güvenilir bir güvenlik sistemi veya güvenlik zorluklarına dayanabilecek herhangi bir sistem olmadığını vurgulamışlardır.

Denizcilik endüstrisinin siber güvenlik konusunda ne kadar eğitim ve bilgi sahibini ölçmek amacıyla yapılan bir çalışmada ise; ankete katılanların %40'ı kendi aralarında şifre paylaşımı yaptıkları ve herhangi bir önlem almadıkları (eposta, USB, web, vb.), %75'inin siber güvenlikle ilgili bilgi eksikliğinin olduğu ve %33'ünün sektördeki siber tehditlerin büyümesine bağlı olarak geçen yıl bir tür siber olaya maruz kaldıkları ayrıca ankete katılarının çoğunluğunun teknoloji sayesinde siber tehditlerin üstesinden gelinebileceği algısı ortaya çıkmıştır (Alcaide ve Llave, 2020).

2.4.1.2. Teknoloji Temelli Yaklaşım

Denizcilik alanının giderek özerkleşmesi sektördeki (teknik sistemler, insanlar) rol ve sorumluluklarda ciddi Şekilde değişimlere yol açmakta ve sektörün teknoloji ile donatılması insan rolünü azaltmak yerine artıracağı düşünülebilir (Relling, vd., 2018). Yazılım, donanımdan çok daha hızlı yaşlanmaktadır. Örneğin, birçok denizcilik işletmecisi, Microsoft'un 2001'de tanıtılan Windows XP işletim sistemlerine yönelik desteği durdurma kararından olumsuz bir Şekilde etkilenmiştir. XP, denizde çok çeşitli uygulamaları kontrol etmek için yazılımların monte edilebileceği, kullanıcı dostu ve sağlam bir sistemdir. Microsoft için, 2001'de mevcut olmayan yerel dokunmatik ekran desteği ve mobil cihazlarla entegrasyon içeren Windows 8.1 gibi yeni ve daha karmaşık işletim sistemlerini zorlarken eski ürünü korumanın hiçbir ticari anlamı yoktur. Windows XP desteğinin olmaması işletim sisteminin sürekli kullanımının Microsoft güvenlik güncelleştirmeleri tarafından desteklenmeyeceği anlamına gelmektedir. Windows XP sadece 13 yıl sürmüş, daha niş, daha az popüler veya daha az etkili olan birçok yazılım parçası çok daha kısa sürelerde kalmıştır. Yine de platformlar ve onları oluşturan endüstriyel makineler çok daha uzun süre dayanacak Şekilde tasarlanmıştır (Fitton, vd., 2015). Denizcilik endüstrisinin teknoloji faktörünün alt yapısı ile ilgili çeşitli prosedürleri ve faaliyetleri bulunması gerekir (Kechagias, vd., 2022):

E-posta: Virüs ve kötü amaçlı yazılımdan korunma, kimlik doğrulama, güvenli Proxy filtreleri.

Şirket ağı: Fiziksel güvenlik, ağ ayrımı, güvenlik duvarları ve erişim kontrol listeleri, çok faktörlü kimlik doğrulama (FMA), izinsiz giriş önleme sistemleri, uç nokta güvenlik koruması, saldırı tespit sistemleri, güvenli yazılım tasarımı ve yapılandırması, yazılım güncellemeleri ve yamalar, güvenlik açığı taraması ve yama uygulaması, veri kaybını önleme sistemleri (DLP), veri şifreleme önlemleri, merkezi kayıt sunucusu - güvenlik bilgileri ve olay yönetimi, güvenlik operasyonları merkezi - yönetilen algılama hizmeti, gerçek zamanlı tehdit ayıklama için kumlama cihazı, yedeklemeler.

Uzaktan çalışan dizüstü bilgisayarlar: Sanal özel ağ (VPN), kumlama ajanı, sabit disk sürücüsü şifreleme, etki alanı politikasının uygulanması, davranış analizi, host saldırı önleme sistemi, güvenlik duvarı, FMA, DLP.

2.4.1.3. Yönetim Temelli Yaklaşım

Platformlara ve deniz altyapısına yönelik siber saldırılar şu anda kaçınılmazdır. Bu saldırıların etkisi belirsizdir ve tahmin edilmesi zordur. Aynı şey kinetik saldırılar ve fiziksel kazalar için de söylenebilir. Bu durumlarda, insan hayatını ve kritik sistemleri korumak için ayrıntılı ve iyi prova edilmiş prosedürlere ihtiyaç vardır. Bu tür prosedürler siber saldırılar için oluşturulmalı veya var olan prosedürlere uyarlanmalıdır (Fitton, vd., 2015). Denizcilik kritik altyapısını ele alan net standartların ve gereksinimlerin eksikliği, siber riskleri değerlendirmek, kontrol altına almak ve azaltmak için standartlaştırılmış politikalara zorunlu bir ihtiyaç olduğunu göstermektedir (Trimble, vd., 2017). Emniyet ve güvenlikle ilgili risk yönetimine ilişkin siber güvenliğin şirket politikaları ve prosedürleri dahilinde dikkate alınması gerekmektedir (BIMCO, 2016).

Heering (2020), 2017 – 2019 yılları arasında Estonya'da faaliyet gösteren denizcilik şirketleri arasında gerçekleştirdiği siber güvenlik ve siber farkındalık üzerine iki anketin sonuçlarını açıklamaktadır. 19 armatörden 12'sinden geri bildirim

alınan çalışmada sonuçlar en az 7 kuruluşun farklı türde siber saldırıların kurbanı olduğunu göstermektedir. Ayrıca, armatörlerin potansiyel siber tehditlere ve çalışanlarının eğitimine yeterince dikkat etmediğini belgelemektedir. Dahası yazar, armatörlerin kullanabileceği siber risk azaltma için bazı önerilere dikkat çekmektedir. Heering'e göre bilgi teknolojisi ticari sürecin önemli bir parçası haline geldiğinden, kuruluşların atması gereken ilk önemli adım, yönetimin en üst düzeyinde siber güvenlik sorununun var olduğunu ve kimsenin güvende olmadığını kabul etmektir. Ancak o zaman ilerlemek ve sorun hakkında açıkça konuşmak ve BT departmanı, eğitim personeli vb. için yeterli finansal desteğin sağlanması dahil olmak üzere siber riskin azaltılması için gerekli adımları atmak mümkündür.

2018 tarihinde denizcilik şirketlerinden 126 üst düzey yöneticinin; bilgi ve teknoloji görevlilerinin, üst düzey güvenlik ve uyum liderlerinin, kilit yöneticilerin katıldığı ankette %69 oranında endüstrinin bir bütün olarak siber güvenlik ve ilgili tehditleri ele almaya hazır olduğuna inanılırken buna karşılık %36'sı kendi şirketlerinin hazırlıklı olduğu inancana sahip olmadığı ortaya çıkmıştır (Wogan, 2019). Kısacası, yöneticiler siber güvenlik konusunda genel olarak kendilerini hazır hissederken kendi çalıştıkları şirketlerine bu konuda güvenmedikleri algısı ortaya çıkmaktadır. Bir diğer anket çalışması Svilicicb ve ark. (2019) tarafından gemi personelleri üzerinde gerçekleştirilmiş ve siber güvenliğin gemi politika ve prosedürlerine yalnızca kısmen entegre edildiği ve esas olarak siber güvenliğe yönelik politika ve prosedürlerin tam olarak geliştirilmediği ortaya çıkmıştır. Yönetim siber güvenlik konusunda aşağıda örnekleri bulunan protokol ve prosedürlere yer vermelidir (Kechagias, vd., 2022):

Siber Güvenlik Beyanı Oluşturulmalı: BT / OT ekipmanının gizliliği, bütünlüğü ve kullanılabilirliğinin korunması, gemide ve karada, örgüt içindeki kişilerin ve malların emniyeti ve güvenliğinin teşvik edilmesi, personelin siber güvenlik planında (CSP) açıklanan gereksinimlere uyması ve ilgili siber güvenlik görev ve sorumluluklarına aşina olmasının sağlanması, genel müdür ve üst düzey yöneticilerin CSP'de açıklandığı gibi organizasyonun siber güvenlik hedeflerini desteklemek için gemide ve karada gerekli tüm kaynakları sağlaması, mevzuat gerekliliklerini ve sektördeki en iyi uygulamaları izlenmesi ve uygulanması, ilgili

görevleri yerine getirmek için hem karada hem de gemide sorumlu personel atanması, tüm şirket personelinin kapsamlı sürekli eğitiminin gerçekleştirilmesi, tüm şirket personeli arasında siber güvenlik bilincinin teşvik edilmesi, siber güvenlik politikaları, prosedürleri ve teknik altyapı hakkında düzenli olarak belgelenmiş incelemeler ve iç denetimlerin yapılması gerekmektedir.

CSP Oluşturulmalı: Siber güvenlik hedefleri, gerekli ve yasak eylemler, görev ve sorumlulukların belirlenmesi, siber riske maruz kalma değerlendirmesinin faaliyet aşamalarının tanımlanması ayrıca siber güvenlik kontrolü için benimsenen koruma önlemlerinin alınması, acil durum ve olay müdahale planını ve siber güvenlik olay analizi prosedürünün sunulması, gemide ve karada tehditlerin, güvenlik açıklarının belirlenmesi gerekmektedir.

Prosedür Kılavuzu Oluşturulmalı: Bilgi teknolojisi ve veri kontrolü ile şirket içindeki BT faaliyetlerini ve veri kontrollerini tanımlamak, şirket kullanıcıları (genel müdür, BT yöneticisi, BT personeli, bilgi sistemi kullanıcıları) için ilgili sorumlulukları belirlemek, kullanıcı hesapları ve şifreleri oluşturmak, donanım ve yazılım kullanımı, virüsten koruma sistemleri kullanımı, yedekleme gibi çeşitli BT prosedürleri için talimatlar ve gereksinimleri sağlamak, yazılım yönetimi ile ofis binalarında ya da gemilerde şirketin yazılım varlıklarını kontrol etmek, etkin bir yazılım yönetim sistemini sürdürmek için izlenmesi gereken eylemleri tanımlamak, yazılım envanteri, güncellemeler/yükseltmeler, yedekleme süreci, kullanım eğitimi, değişim yönetimi, yazılım edinme, test etme ve devreye alma gibi yazılımın yaşam döngüsü ve alınması gereken kararlar ile ilgili sorumlulukları ve prosedürleri kapsar.

Siber Güvenlik Formları Oluşturulmalı: Ofis BT altyapı envanteri, ofis BT yazılım formu, gemi BT altyapı envanteri, gemi OT altyapı envanteri, gemi BT/OT yazılım kaydı formu, BT/OT yazılım güncelleme formu, yazılım değerlendirme formu, siber güvenlik olayı inceleme formu, antivirüs güncelleme/tarama formu, PC inceleme formu, BT eğitim formu, yedek izleme formu, şifre değişikliği izleme formu oluşturulmalıdır.

Politikalar Oluşturulmalı: Şirket cihazları kullanım politikası, yedekleme politikası, e-posta kullanım politikası, üçüncü şahıs erişim politikası, yazılım yükleme politikası, kullanıcı hesapları kontrol ve kullanıcı erişim yönetimi politikası, parola politikası, çıkarılabilir USB politikası, kişisel cihaz kullanım politikası oluşturulmalıdır.

2.4.2. Literatür Taraması Sonucunda Belirlenen Kriterler

Yukarıda da açıklandığı üzere literatür taraması sonucunda siber risklere karşı çözüm yaklaşımlarını 3 (üç) ana başlık altında ele almak mümkündür. Risklerin yönetilmesi ve azaltılması noktasında daha kapsamlı değerlendirmeler yapılabilmesi için bu ana başlıkları oluşturan temel bileşenlerin de değerlendirilmesi gerekmektedir Bu bağlamda literatürdeki çalışmaların analizi sonucunda her bir ana kriterin altında beş adet olmak üzere toplamda on beş alt kriter belirlenmiştir. Bu kriterler aşağıdaki gibidir:

- **İnsan Temelli Yaklaşım**

Farkındalık: IMO onaylanmış bir emniyet yönetim sisteminin siber riskleri dikkate alması gerektiğini belirten bir karar yayınlayarak, siber riskler ve tehditler hakkında farkındalığı artırmaya yönelik acil ihtiyacı olduğunu vurgulamıştır (Whitman ve Mattord, 2019) Hayata, güvenliğe veya değerli varlıklara yönelik olası risk, tehlike veya gerçek tehditler hakkında, bu riskleri ve tehditleri ele alan eylem veya davranışlara dönüştürülecek bir farkındalık zaruridir. Mürettebatın artan bağlantı ve teknoloji kullanımının potansiyel sonuçları hakkında ne ölçüde farkında olduğu, bir siber olay riskini abartıp abartmadıklarına veya hafife alıp almadıklarının göstergesi olabilmektedir. Mürettebatın kontrol edilebilirlik ve yenilik açısından siber riskleri nasıl deneyimlediği hakkında bilgi, uygun eğitim, prosedürler geliştirmek ve konu hakkında farkındalığı artırmak için gerekli olabilir (Larsen ve Lund, 2021). Dolayısıyla son yıllarda deniz siber güvenliği alanında ortaya çıkan siber risklere odaklanarak, insanların bu risklere ilişkin farkındalıklarını araştıran ve siber güvenlik önlemlerinin uygulanmasına ilişkin önerilerde bulunmaya odaklanan çalışmaların sayısı artmaktadır (Garcia-Perez vd., 2017).

Rol Ayrımı ve Sorumluluk: Siber güvenliği sağlamak ve gizlilik risklerini azaltmak için dengeli ve adil sorumluluk paylaşımı, iki yönlü dinamik iletişim kanalları ve neyin tehdit ve çözüm oluşturduğu konusunda net bir fikir birliğine varılması önerilmektedir (Liu vd., 2020). Müşteriler de dahil olmak üzere taşımacılık sürecine dahil olan tüm aktörlerin rollerine uygun hareket etmesi ve siber risklerle mücadele kapsamında üzerlerine düşen sorumlulukları yerine getirmeleri gerekmektedir.

Eğitim: ABD Sahil Güvenlik'in 2015 Siber Stratejisi, siber eğitim ve öğretimin işgücü geliştirmenin önemli bir bileşeni olması gerektiğini belirtmiştir (Young-McLear vd., 2016). Bir güvenlik işgücünün üyeleri olarak belirli güvenlik işlevlerini (tam veya yarı zamanlı) gerçekleştiren çalışanlar için profesyonel düzeyde eğitim gereklidir (Yıldırım, 2016). Çalışanların bilgi işlem güvenliği davranışlarını tanımalarına ve değiştirmelerine yardımcı olmak için kuruluşların, çalışanlarının güvenlik politikalarına uyma konusunda aktif katılımını teşvik etmek için siber güvenlik eğitimlerine ve farkındalık programlarına yatırım yapması gerekir. Hedeflenen eğitim seviyesi, sürece dahil olan aktörler için gerekli güvenlik becerilerini ve yeterliliklerini üretmeye çalışır. Eğitim ihtiyaç analizi yapılırken, ilgililerin, çalışanların sorumluluk üstlenmesini gerektiren görevleri yetkin bir Şekilde yerine getirip getirmediğini değerlendirmesi çok önemlidir (Bayer ve Brummel, 2015).

Çalışan Yetkinliği: Siber güvenlik rollerinin doğası çalışandan çalışana değişir. Gerekli yetkinlikler, temel farkındalıktan iş süreci becerilerine kadar çeşitlilik gösterebilir. Çalışan personellerde aranan yetkinlikler, teknik riskleri azaltma becerilerini, politika ve yönetişim geliştirme kapasitesini ve mevzuata uyumu sağlamak için özel uygulamaları içerebilir (Bayer ve Brummel, 2015). Bu sebeple personel risklerin farkında olmalı ve yeterli beceri ve niteliklere sahip olmalıdır. Ayrıca, çalışanlar prosedürlere, yetki seviyelerine, fiziksel güvenlik engellerine aşina olmalı ve risk yanıtı konusunda iyi eğitilmiş olmalıdır (Mraković ve Vojinović, 2019).

Çalışan İklimi: Siber güvenlik ortamı, siber tehdit için bir kontrol seçeneğidir. Bu kavram, çalışanların kuruluşlarında güvenlikle ilgili sahip oldukları tutarlı bir dizi algı ve beklenti olarak tanımlanan güvenlik ikliminden uyarlanmıştır. Güvenlik iklimi, bir kuruluşun işle ilgili tehlikeleri belirleme ve iyileştirmedeki etkinliğini proaktif olarak değerlendirmek, böylece işle ilgili hastalık ve yaralanmaları azaltmak veya önlemek için kullanılabilir. Park vd., (2019: 84) siber güvenlik iklimini siber risk farkındalığını artırmak ve siber kazaları önlemek için oluşturulan şirket ortamı olarak tanımlamıştır. Yazarlara göre bir şirkette siber güvenlik ortamını teşvik etmek için, yönetimin siber güvenlik tutumları, siber güvenlik eğitim ve öğretim programı, siber güvenlik yönetmeliği ve güvenlik personelinin durumu gibi güvenlik ortamından çeşitli faaliyetler benimsenir.

- **Teknoloji Temelli Yaklaşım**

Ağ Altyapısı Yönetimi: Gemideki BT ağı, siber saldırılara karşı savunmanın çok önemli bir unsurudur. Şirketlerin, yalnızca iş süreci bağlantısı gibi bariz bağlantılara odaklanmak yerine, olası tüm izinsiz giriş noktaları açısından sınır güvenliğini yeniden değerlendirmesi gerekebilir. İş ağı ve kontrol sistemi ağı arasındaki tek bir güvenlik duvarı, birçok izinsiz girişi muhtemelen gözden kaçıracak ve saldırgan kontrol sistemi ağının içine girdiğinde çok az güvenlik sunacaktır (Byres ve Lowe, 2004). Buna rağmen, gemilerdeki gerçek düzenlemeler ve koruyucu önlemler genellikle uluslararası tavsiyelerde belirtildiği gibi değildir. Dolayısıyla ağ yapılandırması ve koruyucu önlemleri son derece önemlidir (Mraković ve Vojinović, 2019).

Chaudry vd.'ne (2012) göre kuruluşlardaki ağların güvenliğini etkileyen dört faktör vardır: Bunlar erişim kontrolü ve çalışan farkındalığı iken, güvenlik politikalarının dökümantasyonu ve üst düzey yönetim desteğidir. Georgiadou ve arkadaşlarının (2022) yaptığı bir çalışmaya göre koronavirüs döneminde bir dizi siber güvenlik yönergesi sağlayarak daha iyi bir organizasyon kültürü seviyesi ve üst yönetim desteği sergileyen işletmeler, ağırlıklı olarak kurumsal ağ erişim yönetimine (Sanal Özel Ağ, VPN, kablosuz bağlantıların kullanımı ve önlenmesi) odaklanmış ve

varlık güvenliğine (şifre koruması, kilitleme, yazılım güncelleme, kimlik avı e-postaları) daha az odaklanmıştır.

Yazılım Varlıkları Yönetimi: Geleneksel ağlar, siber tehditleri önlemek, tespit etmek ve azaltmak için tipik olarak bağımsız güvenlik çözümlerini (ör. güvenlik duvarı, birleşik tehdit yönetimi, derin paket denetimi) kullanır. Dinamik ve otomatik yapılandırma gerektiren belirli savunma eylemleri maliyetlidir ve bu tür ağlarda yönetilmesi zordur (Kreutz vd., 2013). Gelişen paradigmalar olarak, yazılım tanımlı ağ iletişimi (SDN) ve ağ işlevi sanallaştırması (NFV), son derece esnek ağlar sağlayarak ağ yönetimini basitleştirir ve iyileştirir. Bu tür varlıklar maliyet azaltma, enerji tasarrufu, daha yüksek çeviklik ve daha kolay yönetim gibi faydalar sağlar (Yürekten ve Demirci, 2021).

Yedekleme Mekanizmaları: İster iletişim, ister güç veya internet ağları olsun, orijinal verilerin kaybolması durumunda veri yedeklemesine ihtiyaç vardır. Ağ güvenliği konseptinin gözden geçirilmesi ve çevresel güvenlik konseptinin benimsenmesi sırasında veri yedekleme, bina, cihaz, kurumların davranışları ve bireysel davranışlardan bağımsız olarak tüm unsurların buna dahil edilmesine yardımcı olur (Alhayani vd., 2021).

Erişim Yönetimi: Siber risklerin artması, küresel seyir sistemlerinin artan bağlantı ve bağımlılığının bir sonucudur. Bu nedenle siber güvenlik, bilgi sistemlerinin (donanım, yazılım ve ilgili altyapı), bunlara ait verilerin ve sağladıkları hizmetlerin yetkisiz erişime, zarara veya kötüye kullanıma karşı korunmasını ifade eder. Bu, sistem operatörü tarafından kasıtlı olarak veya güvenlik prosedürlerine uyulmaması sonucunda kazara meydana gelen zararları içerir (Shaikh, 2017).

Şirket merkezindeki ve gemideki her bir kullanıcı, bazı bilgiler, veriler veya sistemin parçaları ile ilgili kullanıcı haklarıyla sınırlandırılmalıdır. Erişim ve kullanıcı haklarının sınırlandırılmasının altında yatan neden, temel olarak bilgi eksikliğinden veya kasıtsız olarak atılan ve sistemin savunmasız kalmasına ve veri hırsızlığı veya benzeri olaylara maruz kalmasına neden olan adımların atılmasıdır (Mraković ve Vojinović, 2019).

Kötü Amaçlı Yazılım Savunması: Ağları saldırılara karşı korumak, mevcut sürekli bağlantı ve bilgi akışı çağında her zamankinden daha önemlidir. Kötü amaçlı yazılım, dağıtılmış hizmet reddi (DDoS), gizli dinleme, web uygulaması saldırıları ve gelişmiş kalıcı tehditler (APT'ler) gibi siber tehditler, tüm ağlar için ciddi tehlikeler oluşturur (Yürekten ve Demirci, 2021).

Kötü amaçlı yazılımın bir geminin sistemlerine bulaşmasının sonucu, konum, kargo bilgileri dahil olmak üzere gemi verilerinde değişiklik olabilir. Örneğin, kötü amaçlı yazılımın etkisi altında, belirli gemilere rota değiştirmeye zorlayan fırtınalı hava koşulları hakkında yanlış bilgiler gönderilebilir. Rota veri kaydedicisini hacklemek, hız, radar istasyonlarından (radar) ve diğer navigasyon ekipmanlarından görüntülenen veriler gibi mevcut gemi parametrelerini değiştirebilir. Siber suçlular, geminin rota kontrol ve dümen sistemlerinden ses kayıtları ve bilgilerin yanı sıra basınçlı tankların, perdelerin, kapıların ve kapakların durumuna ilişkin verileri silebilir. Tüm bunlar deniz kazaları, deniz haydutluğu, can ve mal kayıpları gibi tehlikeleri de beraberinde getirmektedir (Melnyk vd., 2022). Dolayısıyla kötü amaçlı yazılımdan koruma ve virüsten koruma yazılımının uygulanması bir zorunluluktur (Mraković ve Vojinović, 2019).

- **Yönetim Temelli Yaklaşım**

Örgüt Kültürü ve Üst Yönetim Desteği: Organizasyon kültürü, yönetim ve organizasyonel davranış arasındaki aracıdır ve farklı şirketler genellikle farklı organizasyon kültürlerine sahiptir. Örgüt kültürü, bir işletmenin operasyon faaliyetlerini ve bir işletmenin bilgi güvenliği uygulamasının etkinliğini kesinlikle etkileyeceğinden, yöneticiler örgüt kültürünü ISM uygulamasını desteklemek ve yönlendirmek için önemli bir faktör olarak görmelidir. Bilgi güvenliği her organizasyonun karşı karşıya olduğu büyük bir endişe olsa da, güvenlik uygulamalarının organizasyon kültürüne proaktif ve spontane bir şekilde günlük operasyonlar için dahil edilmesi organizasyonun başarısını olumlu yönde etkileyebilir (Chang and Lin, 2007). Üst yönetim desteği, politika ve prosedürler ve farkındalık, siber güvenlik kültürünün oluşturulmasında kritik öneme sahiptir.

Masrek ve arkadaşları (2017), kültürleri yönetim desteği, politika ve prosedür, uyumluluk, farkındalık, bütçe ve teknoloji dahil olmak üzere altı boyuta ayıran kavramsal bir çerçeve önermektedir. Yazarlara göre yönetim desteği iki boyuttan oluşur: bilgi güvenliğine önem verilmesi ve bilgi güvenliğinin taahhüdü. Bu iki boyut üst yönetimin tam desteğine ve katılımına örnek teşkil eder.

***Raporlama Mekanizmalarının Oluşturulması*:** Bir siber güvenlik veya gizlilik ihlali durumunda yapılan herhangi bir rapor veya beyan, mümkün olduğunca kapsamlı ve doğru olmalıdır. Bu sayede aktörler, denizcilikteki siber güvenlik ve gizlilik riskleri hakkında gerçek bilgiler sağlarken, müşteriler de hizmet sağlayıcılara karşılaşacakları güvenlik sorunları hakkında geri bildirimde bulunacak ve sonuçta her iki taraf arasında güven inşa edilebilecektir (Liu vd., 2020). Bu doğrultuda önleyici tedbirler ve bu tür olaylar için raporlama mekanizması hakkında farkındalığın yaygınlaştırılmasına ciddi bir ihtiyaç vardır (Bhardwaj vd., 2021). Siber saldırıların denetlenmesi, değerlendirilmesi, raporlanması için geliştirilecek bir otonom sistem, risk yönetiminde modern kurum ve kuruluşlara yardımcı olabilir (Hosam, 2022).

Politikalar ve Prosedürler: Siber güvenlik önlemleri, sistemlerin ve ağların yönetimini, yönetim politikalarını ve prosedürlerini, denetimleri, üçüncü taraflarla yapılan sözleşmeleri vb. içeren süreçlere dayanmalıdır (Mraković ve Vojinović, 2019). İlgili literatür incelemesindeki öneriler, önlemlerin uygulanmasında yukarıdan aşağıya bir yaklaşımı, uluslararası ve bütünsel bir siber güvenlik politikasının geliştirilmesini, karada ve denizde çalışanlar için özel olarak hazırlanmış bir eğitim programını, şirkete özgü prosedürlerin ve risk değerlendirme yöntemlerinin geliştirilmesini ve uygulanmasını içerir (ör. Di Renzo vd., 2015; BIMCO, 2017; He ve Zhang, 2021; Larsen ve Lund, 2021). Çalışanlar, katı organizasyon politikaları ve prosedürleri kapsamında işletme uygulamalarını takip eder. Bu politika ve prosedürler, tehdit veya olay durumunda acil durum planlarının izlenmesini ve ayrıca saldırıyı önlemek veya saldırıdan zamanında kurtulmak açısından önemlidir.

Yatırım Desteği: Bir şirket için siber güvenliğin toplam maliyeti iki öğeyi içerir: tahmin maliyeti ve başarısızlık maliyeti. Tahmin maliyeti, beklenen siber

tehditleri (ör. izinsiz giriş tespit ve önleme sistemlerinin satın alınması, kurulması ve bakımının yapılması) etkin bir Şekilde önlemek amacıyla şirketin siber güvenlik yatırımını ifade eder; bu yüksek güvenlik derecesini sürdürmek, şirketin tahmin maliyetini artırmasını gerektirir. Ayrıca, her ek güvenlik derecesi için, bir şirket daha büyük bir beklenti maliyetine maruz kalacaktır. Başarısızlık maliyeti, bir şirketin öngörülemeyen siber güvenlik ihlalleri ve tehditleri (örneğin, hizmet reddi saldırısından kaynaklanan gelir kaybı) nedeniyle mali kaybını temsil eder. Şirketin başarısızlık maliyetinin eğrisi, güvenlik derecesine göre azalır (He ve Zhang, 2019). Bu maliyetleri uzun vadede minimize etmek için yeni teknolojilere yapılan büyük yatırımlar için yönetim onayları, siber güvenlik gereksinimlerini karşılamak için çok önemlidir. Üst yönetim, yatırım desteğine öncelik vermeye ve teknoloji yakınsamasını kolaylaştırabilecek bir sistem oluşturmaya ikna edilmelidir (Bag vd., 2018).

Schultz (2005), siber güvenlik açığının, yetersiz BT yatırımları, memnuniyetsiz müşteriler, ekonomik kayıplar ve önemli yasal cezalar dahil olmak üzere kuruluşlar için değer kaybeden sonuçlar doğurduğunu vurguladı. Kechagias, vd., (2022) uzmanlar tarafından siber güvenlikteki en zayıf halkanın insanlar olduğu yaygın olarak tartışıldığını vurgulamış, bunun nedeninin, kuruluşların genellikle tek taraflı olarak teknolojiye siber güvenliğe kaynak yatırmaları, ancak aynı şeyi insan unsuru için yapmayı ihmal etmeleri olduğunun altını çizmiştir. Rotherberger (2016) kuruluşların siber güvenlik liderlerini diğer çalışanlarla çalışmaya daha iyi hazırlamak için liderlik geliştirme programları uygulaması gerektiğini belirmiştir. Yazara göre siber güvenlik liderlerini geliştirmek bir yatırımdır ve bu yatırımın getirisi, azaltılmış siber güvenlik riski şeklini alacaktır.

Paydaşlar İle İş Birliği İçerisinde Olma: Araştırmalar, kilit paydaşlar ve halk arasında yeterli bilgi ve farkındalık eksikliğinin başarılı bir risk önleme önündeki büyük bir engel olduğunu ortaya koymuştur. Bir geminin işletilmesine birden fazla paydaşın dahil olması, genellikle onu güvenceye almak için hesap verme sorumluluğu eksikliği ile sonuçlanır. İletişim yeteneklerindeki gelişmeler, gemilerin rota optimizasyonu, sefer planlaması ve güvenilir hava tahmini için gemideki yazılım programlarını sık sık güncellemelerine, ofis tarafı ile gerçek zamanlı veri alışverişi,

sorunları çözme ve destek yeteneği gibi gemi yöneticileri ile sürekli ve verimli iletişim kurmalarına olanak sağlamıştır. Gelişmeler ayrıca form ve beyan alışverişinde bulunmak için ulusal ve liman yetkililerileriyle daha iyi iletişim ve veri alışverişi sağladılar ve çeşitli paydaşların taleplerini karşılayan sürekli raporlamayı desteklemiştir (Kechagias vd., 2022). Denizcilik sektörü kuruluşları, dernekler, düzenleyiciler ve paydaşlar, açık boşlukları tartışarak ve uygun önlemleri alarak siber güvenliği iyileştirmek için sürekli bir toplu çaba üzerinde anlaşmalıdır. Diğer bir deyişle, denizcilik sektöründeki siber güvenlik ve mahremiyet tehlikeleri, ancak tüm kilit paydaşların kendileriyle ilgili fırsatları ve riskleri iyice anlamaları ve proaktif olarak birlikte çalışarak hataları birbirine paylaştırmak yerine sorumlulukları paylaşmaları halinde azaltılabilir (Liu vd., 2020). Siber risklere karşı çözüm yaklaşımları literatür taraması sonucu elde edilmiş olup Tablo 7'de gösterilmiştir.

Tablo 7. Siber Risklere Karşı Çözüm Yaklaşımlarının Belirlenmesi

Ana Kriterler	**Alt Kriterler**
İnsan Temelli Yaklaşım (İTY) *(Fitton, vd., 2015; Relling, vd., 2018; Giacomello ve Pescaroli, 2019; He ve Zhang, 2019; Mraković ve Vojinović, 2019; Heering, 2020; Mraković ve Vojinović, 2020; LarsenveLund, 2021; Senarak, 2021; Baum-Talmor ve Kitada, 2022; Kechagias, vd., 2022)*	***Farkındalık (K1)*** (Chaudry vd.,2012; Yıldırım, 2016; Garcia-Perez vd., 2017;Jacq, vd., 2018; He ve Zhang, 2019; Mraković ve Vojinović, 2019; Whitman veMattord, 2019; Heering, 2020; Balci ve Surucu-Balci, 2021; LarsenveLund, 2021; Baum-Talmor ve Kitada, 2022; Kechagias, vd., 2022)
	Rol Ayrımı ve Sorumluluk (K2) (Relling, vd., 2018; Mraković ve Vojinović, 2019; Liu vd., 2020, Kechagias, vd., 2022)
	Eğitim (K3) (Bayer ve Brummel, 2015; Fitton, vd., 2015; Yıldırım,2016; Young-McLear vd., 2016; Munim, vd., 2017; Jacq, vd., 2018; He ve Zhang, 2019; Mraković ve Vojinović, 2019; Alcaide ve Llave, 2020; Heering, 2020; Mraković ve Vojinović, 2020; Baum-Talmor ve Kitada, 2022)
	Çalışan Yetkinliği (K4) (Bayer ve Brummel, 2015; Jacq, vd., 2018; Mraković ve Vojinović, 2019)
	Çalışan İklimi (K5) (Park vd., 2019; Wong vd.,2019; Georgiadou vd., 2021)
Teknoloji Temelli Yaklaşım (TTY) *(Fitton, vd., 2015; Relling, vd., 2018; Shapiro, vd., 2018; Giacomello ve Pescaroli, 2019; Mraković ve Vojinović, 2019; Mraković ve Vojinović, 2020; Kechagias, vd., 2022)*	***Ağ Altyapısı Yönetimi (K6)*** (Byres ve Lowe, 2004; Shapiro, vd., 2018; Mraković ve Vojinović, 2019; Georgiadou vd., 2022)
	Yazılım Varlıkları Yönetimi (K7) (Kreutz vd., 2013; Shapiro, vd., 2018; Mraković ve Vojinović, 2019; Yurekten ve Demirci, 2021; Georgiadou vd., 2022)
	Yedekleme Mekanizmaları (K8) (Alhayani vd., 2021; Kechagias, vd., 2022)
	Erişim yönetimi (K9) (Chaudry vd.,2012; Shaikh, 2017; Mraković ve Vojinović, 2019; Kechagias, vd., 2022)

Tablo 7. Siber Risklere Karşı Çözüm Yaklaşımlarının Belirlenmesi Devam

	Kötü Amaçlı Yazılım Savunması (K10) (Shapiro, vd., 2018; Mraković ve Vojinović, 2019; Mraković ve Vojinović, 2020; Yurekten ve Demirci, 2021; Melnyk vd., 2022)
Yönetim Temelli Yaklaşım (YTY) *(Fitton, vd., 2015; Munim, vd., 2017; Dawson, 2018; Mraković ve Vojinović, 2019; Alcaide ve Llave, 2020; Heering, 2020; Balci ve Surucu-Balci, 2021; Potamos, vd., 2021; Kechagias, vd., 2022*	***Örgüt Kültürü ve Üst Yönetim Desteği (K11)*** (Chang ve Lin, 2007; Chaudry vd.,2012; Munim, vd., 2017; Dawson, 2018; Mraković ve Vojinović, 2019; Govander vd. 2021, Georgiadou vd., 2022)
	Raporlama Mekanizmalarının Oluşturulması (K12) (Liu vd., 2020; UN ESCAP, 2020; Bhardwaj vd., 2021; Siyam ve Hussain, 2021; Hosam, 2022)
	Politikalar ve Prosedürler (K13) (Chaudry vd.,2012; BIMCO, 2017; Munim, vd., 2017; Trimble, vd., 2017; Di Renzo vd., 2015; BIMCO, 2017; ; Svilicicb, vd., 2019; Alcaide ve Llave, 2020; He ve Zhang,2021; Larsen ve Lund, 2021; Balci ve Surucu-Balci, 2021; Potamos, vd., 2021;)
	Yatırım Desteği (K14) (Schultz, 2005; Rotherberger, 2016; Bag, 2018; He ve Zhang, 2019; Mraković ve Vojinović, 2019; Govander vd. 2021; Kechagias, vd., 2022)
	Paydaşlar İle İş Birliği İçerisinde Olma (K15) (Liu vd., 2020; Balci ve Surucu-Balci, 2021; Kechagias, vd., 2022)

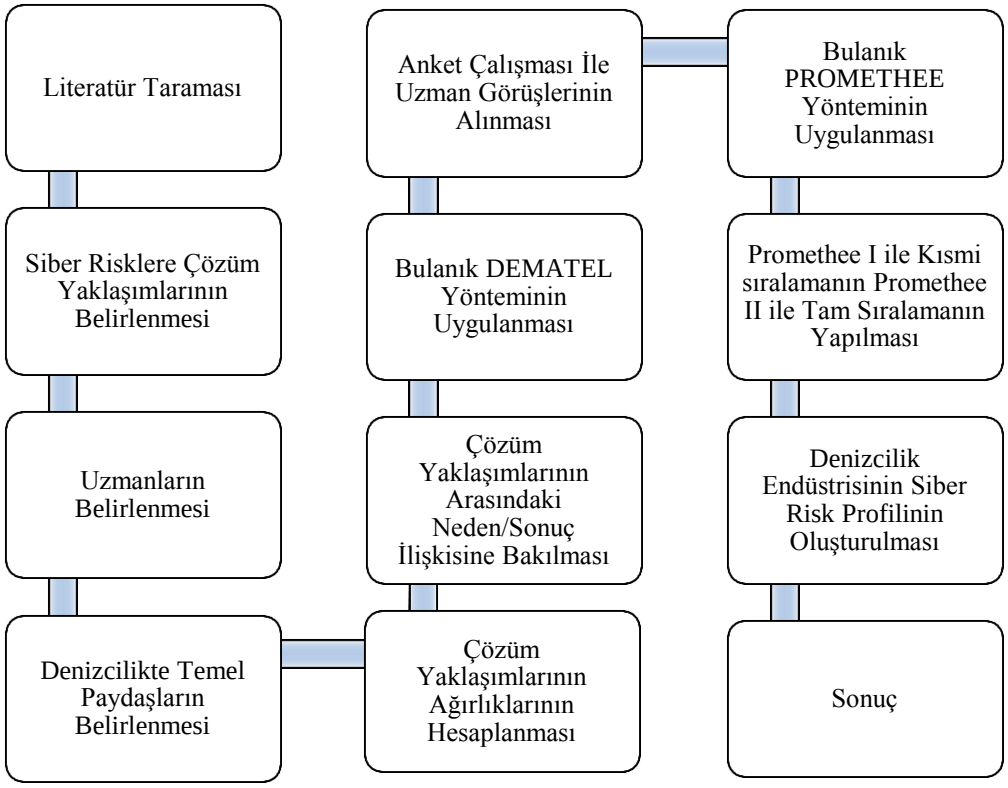
ÜÇÜNCÜ BÖLÜM

3. YÖNTEM

Tezin bu bölümünde araştırmanın önemine değinilerek araştırmanın tasarımına yer verilecektir. Kullanılacak yöntemin adımları tek tek anlatılarak birbirleri ile olan ilişkileri gösterilmiştir.

3.1. ARAŞTIRMANIN AMACI VE TASARIMI

Denizcilik sektörünün çok paydaşlı ve kırılgan yapısı düşünüldüğüne siber risklerin ne denli önemli olabileceği tahmin edilebilmektedir. Bu çalışma; denizcilikte siber risklerin neler olduğuna, aktörlerinin kimlerden oluştuğuna, denizcilikte yaşanmış siber olaylara, denizcilik paydaşlarının bakış açılarına, literatürde ne gibi çözümler sunulduğuna değinerek yeni bir siber güvenlik modeli ortaya koymaktadır. Bu anlamda literatüre ve sektöre katkı sağlaması beklenmektedir. Araştırmanın tasarımı aşağıda gösterildiği gibidir.



Şekil 14. *Araştırmanın Tasarımı*

Araştırmada çok kriterli karar verme yöntemlerinden olan The Decision Making Trial and Evaluation Laboratory (DEMATEL) tercih edilmiştir. Bu yöntemin tercih edilme sebebi belirlenen kriterlerin arasındaki neden sonuç ilişkisini ortaya çıkarmasıdır. Kriter ağırlıkları DEMATEL yöntemiyle belirlendikten sonra denizcilik endüstrisinin bazı alt dallarının siber güvenlik konusuna ne kadar önem verdiklerini belirlemek amacıyla Bulanık The Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE) yöntemiyle sıralama işlemi gerçekleştirilmiştir. Çalışmanın amacını gerçekleştirmek için denizcilik sektöründeki temel paydaşların (aktörlerin) uzman görüşlerine başvurulmuştur. Çalışmada uygulanılacak anket yöntemi, Kocaeli Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurulu'nun 22/09/2022 tarih ve 2022/08 nolu toplantısında alınan 18 sıra sayılı onayı ile gerçekleştirilmiş ve EK 1'de gösterilmiştir.

Çalışmanın amacına uygun temel aktörleri aşağıdaki gibi sıralamak mümkündür.

3.1.1. Liman İşletmeleri

Deniz taşımacılığındaki teknolojik ve yapısal değişimler ve gelişmeler, lojistik zincirinin temel/kilit noktaları olan limanları da değişime adapte olmaya yönlendirmektedir. Limanlarda akıllı algılama sistemlerinin varlığının gerçeğe dönüşmesiyle günümüzde farklı operasyon alanları otomatik modda çalışmaktadır. Limanların BT'lerindeki ve ekipmanlardaki inovasyonlar/yenilikler liman sistemlerine uyarlanarak otomasyon esaslı insansız terminaller işletilmekte, operasyonel/yönetimsel süreçlerde optimizasyon gerçekleştirilerek süreç inovasyonları sağlanmakta, ana liman hizmetlerine ek olarak bütünleşik katma değerli lojistik hizmetleri sunarak hizmet inovasyonları gerçekleştirilmektedir. Limanların rekabet gücü temel olarak emek, sermaye, teknoloji ve enerji gibi üretim unsurları tarafından belirlenir. Bu bağlamda, liman operasyonlarındaki inovasyonların yanı sıra BT'lerden faydalanmayan liman ve terminaller hızla değişen denizyolu taşımacılığı endüstrisinde rekabet etmekte zorlanmaktadır (Karataş ve Çetin, 2014) .

Limanların kullanıcıları için önemli bir değer yarattığı lojistik sistemde limanların rolü giderek daha fazla önem kazanmaktadır. Konteynerleşme, limanları tedarik zinciri sistemlerinin önemli bir parçası haline getirmenin yanı sıra hinterlandındaki dağıtım merkezleriyle entegre hale getirdi (Akbayırlı, vd., 2016). Dolayısıyla limanlara yönelik siber risklerin bir nevi kamçı etkisiyle dolaylı ve doğrudan limanlarla etkileşim içerisinde bulunan diğer paydaş/aktörler için de tehlike arz ettiği aşikardır.

3.1.2. Armatör (Gemi Sahibi) İşletmeler

Armatörler veya gemi sahipleri, ticareti yapılan malın deniz yoluyla belirlenen güzergahlar arasında taşınması faaliyetlerinde taşıyıcı rolünü üstlenen aktörlerdir. Söz konusu aktörler, yüklerinin deniz yoluyla taşınmasını talep eden müşterileri ile navlun sözleşmeleri imzalayarak, nakliye işlerini yürüterek gemilerini ticari kazanç için kullanırlar (Orhon, 2019).

Deveci (2013) gemi sahibini *'kiraya vermek veya denizyolu ile taşıma yapmak için gemisi olan kişi ve işletmeler olarak tarif edilebilir. Gemi sahipleri çoğunlukla gemilerinin işletimi ve yönetimini kendi organizasyonları ile gerçekleştirmekte, bazen de geminin işletimini üçüncü bir tarafa bırakılabilmektedirler. Her iki durumda da bir geminin işletimi ve yönetimi, ulusal ve uluslararası denizcilik otoriteleri tarafından gerekli görülen tescil ve dökümantasyonu içermekte; geminin personel, kumanya, yedek parça, sarf malzemeleri ile donatımı, tamir ve bakımını kapsamakta; geminin sigortalama işleminin yapılması, hak iddialarının çözümü ve tazminat taleplerinin halledilmesine uzanmakta; sörveyörlerin atanması ve geminin uygun bir Şekilde çalışır durumda kalabilmesi için planlanmış olan diğer görevlerin yapılmasına kadar genişlemektedir.*' olarak tanımlamıştır.

Ekonomist Dergisi'nin 2018 yılında yayınladığı bir araştırmaya göre Türkiye'de 548 firma gemi sahibi olarak gemi işletmektedir (Yılmaz, 2018). Deniz Ticaret Odası'nın 2021 tarihli en yeni raporunda Türk Deniz Ticaret Filosunda 1000 gross ton ve üzeri 475 gemi bulunduğu, bu gemilerin ortalama yaşının 23,8 ve toplam deadveyt ton kapasitelerinin 5.857.588 DWT olduğu raporlanmıştır (DTO,

2022). Türk Armatörler Birliği'nin Türk Deniz taşımacılığı tonaj kapasitesinin yaklaşık yarısına sahip olan 198 üyesi bulunmaktadır (Armatörlerbirliği, 2022).

Literatürde de sıklıkla bahsedildiği üzere gemiler başlı başına teknolojik araçlardır ve bu sebeple gerek geminin kendisi gerekse de gemilerin operasyonun ve yönetiminin sağlandığı karadaki ofislerinin kullandıkları sistemler siber tehlikelerin tehdidi altındadır.

3.1.3. Freight Forwarder İşletmeler

Devlet kurumları tarafından gümrük vergisi alınması, tarih boyunca ticaretin temel bir parçası olmuştur. Gümrük vergilerinin toplanmasıyla birlikte, malları gönderici veya alıcı adına taşıyacak aracılara ve acentelere talep geldi. Yük taşımacılığını düzenlemek ve gemilerde yer satın almak için nakliyeciler adına hareket eden gümrük komisyoncuları ve acenteleri, freight forwarderlara dönüştü. Freight forwarder işletmelerinin rolü daha da genişledi ve taşımacılık endüstrisi için sadece aracı olma algısını çoktan terk etti. Kabaca söylemek gerekirse, forwarder şirketleri müşterileri (denizcilik/nakliye şirketleri) için malların sevkiyatını organize eder ve operasyonların sorunsuz çalışmasını sağlamak için operasyonel yardım sağlar.

Forwarderın ana amacı, müşterilere en iyi hizmeti ve en rekabetçi fiyatı sunarken, gönderileri organize etmek, nakliyede gecikme olmamasını sağlamak için gereken tüm işlemleri yönetmektir (Archetti ve Peirano, 2020). Günümüzde freight forwarderlar, tedarik zincirindeki bir dizi hizmetten sorumludur. Geleneksel olarak yükletenin acentesi olarak taşımayı organize eden ve sevkiyat dökümantasyonunu sağlayan forwarderlerın üstlendiği faaliyetler ve sunduğu hizmetler şu şekilde sıralanabilir (Deveci, 2002):

• Depolama, paketleme, dağıtım, envanter yönetimi, konsolidasyon, etiketleme, yeniden paketleme, tartma ve kalite kontrol gibi çeşitli bağımsız hizmetler sunmak,

• Gerekli tüm belgeleri sağlamak ve gümrük işlemlerini düzenlemek,

• Uluslararası sevkiyat dağıtımı ile ilgili danışmanlık hizmetleri sağlamak,

• Yükletenin acentesi olarak yükleten hesabına taşıma organizasyonu (ör. Rezervasyon) sağlamak ve taşıma talimatlarını yürütmek.

Forwarderlık özellikle müşteri yoğun bir hizmet sektörüdür ve alıcıları ve satıcıları birbirine bağlayarak ürünleri müşterilere etkin bir Şekilde teslim ederek ekonomik değer yaratır. Yüksek kaliteli müşteri hizmeti sunmada önemli bir rol oynar ve performansının üreticilerin/tedarikçilerin performansı ile bir bağlantısı vardır. Forwarder firmaları, modern lojistik hizmetlerinde hız, sıklık ve güvenirliği sağlamak için müşterilerine anında bilgi sağlamaya ve etkin müşteri ilişkileri yönetimine ihtiyaç duyarlar. Forwarderlar esnek olmalı ve müşterinin talebine göre çeşitli hizmetler sunabilmelidir. Farklı bölgelerdeki işletmeler hizmet tekliflerinde farklı eğilimler görmektedir. Dolayısıyla bilgi teknolojisi boyutu, freight forwarderlık hizmetlerinde firma performansı ile pozitif olarak ilişkilidir.

Bilgi yönetimi süreci, bir firmanın müşteriler ve pazarlar hakkında bilgi toplamaya (örneğin, doğrudan bir posta kampanyasına müşteri yanıtı ve ikincil kaynaklardan veri elde etmeye) odaklanan, müşterilerin davranışları ve piyasa koşullarıyla ilgili eğilimleri ve kalıpları belirlemek için analiz tekniklerini kullanan ve müşteri ile doğrudan temasa odaklanan faaliyetlerini ifade eder (Shang, vd., 2012). Forwarderların talep yönünde değişen ihtiyaçlara cevap verebilmesi noktasında teknolojik araçlara ve broker/acente gibi diğer aracılarla ortak oldukları ağları başarılı bir Şekilde yönetmeleri gerekmektedir.

3.1.4. Broker İşletmeler

Broker, bir ücret veya komisyonculuk karşılığında gemi kiralayan ile gemi sahibi (armatör) arasında aracı olarak çalışan taraftır. Bu tür aktörlerin en temel işlevi, gemi kiralayan ile armatörü bir araya getirmek ve acentelik yapmaktır. Bir brokerin kargo yetkilisini temsil ettiği durumlardaki rolü, müvekkilinin (kiralayan) taşımak istediği yük için uygun gemileri bulmaktır. Bu işlev, gemi ve kargolar, limanlar, çeşitli kargoların yükleme ve boşaltma yöntemleri, hava durumu modelleri, gemi talebi ve arzı vb. konularda derinlemesine bilgi gerektirir (Prasad, 2008). Dolayısıyla etkin bir broker, "knowhow" dedikleri şeye sahip olmalıdır, yani ne

hakkında konuştuğunu bilmeli, güncel piyasa bilgilerine hakim olmalı ve değişen durumlara uyum sağlamalıdır (Sayed ve Akter, 2022). Bu rol, özellikle ileri BT çağından önce kritikti. Gemi sahipleri için gemi kiralayanlara ulaşmak veya gemi kiralayanların uygun bir gemi bulması gerçekten zaman alıcı ve pahalıydı. Ancak günümüz bilişim çağında gemi sahipleri ve kiracılar akıllı telefon uygulamaları aracılığıyla dahi birbirlerine çok rahat bir şekilde ulaşabilmektedir (Balcı, 2016).

Pisanias ve Wilcocks (1999), brokerlerin gemi kiralama sözleşmesi için gemi kiralayan ve sahiplerini eşleştirmenin yanı sıra 4 farklı görevi olduğunu belirtmektedir:

- Bilgi edinme ve yayma
- Pazar bilgisi yoluyla danışmanlık rolü
- Müzakereler ve temsil
- Gayri resmi tahkim

Pisanias ve Wilcocks ayrıca gemi brokerliği işinin aslında bir bilgi ağı olduğunu ancak bilgi miktarından çok bilginin niteliğinin önemli olduğunu belirtmektedir. Colins (2000) ise brokerlerin rolünü "bilgi, piyasa tavsiyesi, stratejik tavsiye, müzakere tamponu, sözleşmenin yönetimi ve anlaşmazlıkların çözümünde yardım" olarak listeler. Gemiyi bağladıktan sonra müşteriyi istatistiksel bilgilerle desteklemek ve navlun ve demuraj hesaplamaları gibi hizmetler sunmak da brokerin asli görevlerindendir (Coulson, 1991).

Armatör veya gemi kiralayan adına hareket eden broker, müşterileri için anlaşmayı müzakere eder. Müzakere aşamasından önce, kiralama acentesi son işlemlerin raporlarıyla aktif olarak ilgilenir. Bu işlem, acenteye navlun oranıyla ilgili bilgileri sağlar çünkü oranlar piyasa koşullarına göre belirlenir. Broker, araştırmasının bir sonucu olarak, mevcut navlun oranlarının seviyesi hakkında bir ön genel bakışa sahip olur ve sunacağı navlun miktarı hakkında kararlarını verir. Gemi brokeri, kiralamaya uygun gemiler ve kiralama kabiliyetleri ile armatörün komisyoncusu tarafından sağlanan bilgileri karşılaştırdıktan sonra, karşı tarafla uygun temasları kurar ve gemiyi kiralamak için görüşmeleri başlatır. İşlem için

uygun bir gemi bulduğunda, ortaya çıkan işte ortak çıkarları olmasını sağlamak için taraflar birbirleriyle iletişim kurar. İşlem tarihleri, navlun oranı ve kargonun miktarı hakkında bilgi alışverişinde bulunurlar (Fiotakis, 2005). Dolayısıyla broker kiralama sürecinin tüm prosedürünü ve bir kiralama sözleşmesinin tamamlanması ve nihai anlaşması için gereken büyük miktarda bilgiyi dikkate almak zorundadır.

Gemi brokerliği mesleği, birçok beklenti ve görevi içeren denizcilik işinin önemli bir parçasıdır. Brokerlerin iş prosedürlerinde aracı olarak rolü, Bilgi Merkezleri gibi çeşitli kaynaklardan piyasa bilgilerinin edinilmesini gerektirir ve iletişimi gerektirir. Bilgi Teknolojilerinin adaptasyonu denizcilik endüstrisinin tüm sektörlerinde yeni standartların uygulanması, brokerler için yeni bir çalışma ortamı yaratarak değişiklikleri ve reformları da beraberinde getirmektedir. E-ticaret ve İnternet, aracılara birçok fırsat sunarken aynı zamanda birçok tehdit de getirmektedir. Tüm brokerler için veritabanlarının ve bilgilerin mevcudiyeti büyük önem taşımaktadır.

3.1.5. Acente İşletmeler

Son yıllarda deniz araçlarına yönelik gereksinimler artmış, gemilerin durumlarını, çevre, sıhhi ve radyasyon güvenliğini izleme yöntemleri daha karmaşık hale gelmiş ve bu değişiklikler nedeniyle bir gemi/liman acentelerinin rolü önemli ölçüde artmıştır. Uluslararası ticaret hacminin büyümesi aynı zamanda deniz acenteliği piyasasının gelişmesine de katkıda bulunmaktadır (Iarmolovych, 2018). Deniz ticaretinin gelişmeye başladığı ilk zamanlarda gemi sahibinin tüm haklarını, uğradığı limanlarda yalnızca kaptan temsil ediyordu, ilerleyen zamanlarda ise bu hizmetin sınırları genişledi ve kontrol gemi acente işletmelerine devredildi (Ayan, 2005).

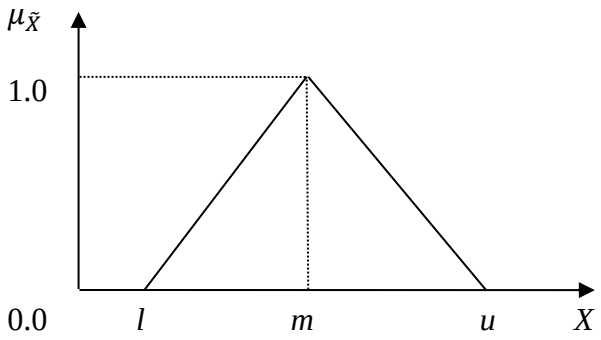
Acentelerin Türk Ticaret Kanunu'ndaki tanımlarını esas alan Karaman (2009, s. 23), gemi acentelerini *'temsil ettiği donatan, taşıyan ve kaptan adına bir mukaveleye dayanarak, bir ticari işletmeyi ilgilendiren akitlerde aracılık eden veya o işletme adına akit yapmayı meslek edinen ve bulundukları liman veya ülkede temsilcisi olduğu kişilerin yasal hak ve çıkarlarını kollayıp koruyan gemi ve yük için*

yapılması gerekli ve zorunlu olan hizmetleri temsil ettikleri donatan ve kaptan adına gereken zaman veya sürede yerine getiren, hizmetlerinin karşılığını gerek gemi ve gerekse yükte alan tüccar kişi ve kuruluşlar' olarak tanımlamıştır.

Gemi acenteleri, özellikle armatörleri ve yük ilgililerini temsil etmekte ve ticari, operasyonel, hukuki vb. birçok önemli işlevi yerine getirmektedirler (Özaydın, 2016). Bir gemi acentesinin birincil amacı, üstlenilen gemi operasyonlarını en düşük maliyet ve optimum verimlilikle gerçekleştirmek için gemi sahibinin ve geminin çıkarlarını korumaktır (Baran ve Arabelen, 2018). Deniz Ticaret Odası'nın 2019 verilerine göre Ulaştırma ve Altyapı Bakanlığı'ndan gemi acenteliği yetki belgesi alan firma sayısı 1251'dir (DTO, 2019). Öte yandan, liman acenteleri tarafından rezervasyondan, pazarlama ve satışa, dokümantasyondan konteyner takibine, liman hizmetleri ve müşteri ilişkilerine kadar geniş bir hizmet yelpazesi sunulmaktadır (Deveci, 2002). Acenteler, diğer işletmelerden ticari hizmet sağlayıcılara olduğu gibi, giderek daha rekabetçi ve küreselleşen bir iş ortamında sürdürülebilirliği sağlamak için kusursuz hizmetler sunmalıdır.

3.2. BULANIK MANTIK

Gerçek dünyada, birçok karar, hedefler, kısıtlamalar ve olası eylemler tam olarak bilinmediğinden dolayı belirsizliği içerir (Bellman ve Zadeh, 1970). Zadeh(1965), bazı belirsiz problemleri, yani bulanık belirsizliği çözmek için, sistematik bir bulanık küme teorisi ortaya koymuştur (Zadeh, 1965). İnsanların düşünceleri, çıkarımları ve algıları açısından belirli bir derecede bulanıklık mevcuttur. Bulanık küme teorisi, insan önyargısını yakalayarak belirsiz ve dilsel ifadeler için değerlendirme prosedürünü kolaylaştırır. Dilsel değişken, değerleri doğal bir dilde tümceler veya cümleler biçiminde olan bir değişkendir (Von Altrock, 1997). Pratikte, dilsel değerler bulanık sayılarla temsil edilebilir ve üçgen bulanık sayı yaygın olarak kullanılır (Jeng ve Tzeng, 2012). Bu nedenle uygulamada karar verme aşamasında bulanık sayılar üretmek gerekmektedir. Bu bağlamda üçgen bulanık sayı üçlü olarak tanımlanabilir. $\tilde{A} = (l, m, u)$ burada l, m ve u bulanık kümelerin alt, orta ve üst sayılarını gösterir $(x \leq y \leq z)$. Üçgen bulanık sayıları Şekil 15'te gösterilmektedir.



Şekil 15. Üçgensel Bulanık Sayılar

Bir üçgen bulanık sayının üyelik fonksiyonu aşağıdaki gibi ifade edilebilir.

$$\mu_{\tilde{A}} = \begin{cases} 0, & x < 1, \\ (x-l)/(m-l), & l \le x \le m, \\ (u-x)/(u-m), & m \le x \le u, \\ 0, & x > u. \end{cases} \quad (1)$$

Üçgen bulanık sayıların özelliklerine ve Zadeh (1965) tarafından ortaya konan genişleme ilkesine göre, İki üçgen bulanık sayıdan herhangi biri için $\tilde{A}_1 = (l_1, m_1, u_1)$ ve $\tilde{A}_2 = (l_2, m_2, u_2)$, bunların matematiksel hesaplaması şu şekilde tanımlanabilir:

İki bulanık sayının eklenmesi; $\tilde{A}_1 + \tilde{A}_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2)$ (2)

İki bulanık sayının çıkarılması; $\tilde{A}_1 - \tilde{A}_2 = (l_1 - l_2, m_1 - m_2, u_1 - u_2)$ (3)

İki bulanık sayının çarpımı ; $\tilde{A}_1 * \tilde{A}_2 = (l_1 * l_2, m_1 * m_2, u_1 * u_2)$ (4)

Üçgen bulanık sayıların aritmetik ortalamaları;

$k * \tilde{A}_1 = (k * l_1, k * m_1, k * u_1), (k > 0)$ (5)

$\frac{\tilde{A}_1}{k} = \left(\frac{l_1}{k}, \frac{m_1}{k}, \frac{u_1}{k} \right), (k > 0)$ (6)

3.3. BULANIK DEMATEL YÖNTEMİ

DEMATEL yöntemi, 1972-1976 tarihleri arasında Battelle Memorial Enstitüsü'nün Cenevre Araştırma Merkezi'nden geliştirilmiş (Gabus and Fontela, 1972; Fontela and Gabus, 1976), dünya toplumlarının önemli sorunlarıyla ilgilenmek üzere tasarlanmış matematiksel bir prosedürdür (Chauhan vd., 2018). Bu yöntem, özellikle bir sayının her bir öğenin etkisinin gücünü temsil ettiği bir sistemin öğeleri

arasında bağlamsal bir ilişki gösteren matrisler veya digraflarla karmaşık nedensel ilişkilerin yapısını görselleştirmek için pratik ve etkili bir araç olmuştur (Chang vd., 2011; Jassbi vd., 2011; Patil ve Kant, 2014; Jeng, 2015). DEMATEL analizi için seçilen ölçek 0-4 arasında değişmektedir (Yang vd., 2008).

Bulanık DEMATEL metodolojisinde yer alan adımlar aşağıdaki gibi açıklanmıştır (Akyuz ve Celik, 2015):

Adım 1: İkili bir karşılaştırma matrisi oluşturmak için araştırma katılımcılarını araştırmak.

Bu adımda problemle ilgili unsurlar ve elemanlar arasındaki etki derecesi oluşturulur. İkili karşılaştırma ölçeği, 0, 1, 2, 3 ve 4 puanlarının "Etki yok", "Çok Düşük Etki", "Düşük Etki", "Yüksek Etki" ve "Çok Etkileyici"yi temsil ettiği beş seviye olarak belirlenebilir. Sırasıyla Yüksek Etki". Daha sonra yöneticilerin tercihlerinin değerlendirmesini elde etmeli ve ortalamasını kullanmalıdır.

Adım 2. İlk doğrudan ilişki bulanık matrisi

$\tilde{Z}$ Kriterler arasındaki etkiler ve yönler açısından ikili karşılaştırmalarla elde edilen bir $n \times n$ matrisidir; burada $\tilde{Z}_{ij}$, i kriterinin j kriterini etkileme derecesi olarak gösterilir.

$$\tilde{Z} = \begin{bmatrix} 0 & \tilde{Z}_{12} \dots \dots & \tilde{Z}_{1n} \\ \tilde{Z}_{21} & 0 \dots \dots & \tilde{Z}_{2n} \\ & \cdot & \\ & \cdot & \\ & \cdot & \\ \tilde{Z}_{n1} & \tilde{Z}_{n2} \dots \dots & 0 \end{bmatrix} \quad (7)$$

$\tilde{Z}_{ij} = (l_{ij,}\, m_{ij,}\, u_{ij})$üçgen bulanık sayılar olan ve $\tilde{Z}_{ij}$ = (i = 0,1,2,….,n) köşegen üzerinde (0, 0, 0) üçgensel sayılara denk gelir.

Adım 3. Normalleştirilmiş ilk doğrudan ilişki matrisinin oluşturulması

İlk doğrudan ilişki bulanık matrisini normalize ederek, normalleştirici doğrudan ilişki bulanık matrisini $\tilde{X}$ aşağıdaki gibi elde edilebilir.

$$S = \frac{1}{\max_{1 \le i \le n} \sum_{j=1}^{n} z_{ij}}, \; i, j = 1,2,\ldots,n \text{ and } X = s.Z \tag{8}$$

$$\tilde{X} = \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} \ldots & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} \ldots & \tilde{x}_{2n} \\ & \vdots & \\ \tilde{x}_{n1} & \tilde{x}_{n2} \ldots & \tilde{x}_{nn} \end{bmatrix} \tag{9}$$

Adım 4. Toplam bulanık ilişki matrisinin oluşturulması

Normalleştirilmiş yönlü ilişki matrisi oluşturulduktan sonra $\tilde{X}$, bulanık toplam ilişki matrisi $\tilde{T}$ aşağıdaki denklemlerden kurulabilir.

$$\tilde{T} = \lim_{n \to \infty} (\tilde{X} + \tilde{X}^2 + \cdots + \tilde{X}^k) = X(1 - X)^{-1} \tag{10}$$

Adım 5. Neden sonuç ilişkilerinin (Gönderici alıcı grupların) belirlenmesi

$\tilde{T}$ matrisini üreterek, $\tilde{D}_i + \tilde{R}_i$ ve $\tilde{D}_i - \tilde{R}_i$ sonra hesaplanır ve hangisinde $\tilde{D}_i$ ve $\tilde{R}_i$ satırların toplamı ve sütunların toplamıdır.

Bu adımda, toplam ilişki matrisinde her sütun ve her satırdaki değerlerin toplamı hesaplanır. Böylece, D_i, i. satırın toplamını ve R_j, j. sütunun toplamını gösterir. Faktörler arasındaki doğrudan ve dolaylı etkiler sırasıyla D_i ve R_j ile gösterilmiştir.

$$D_i = \sum_{j=1}^{n} t_{ij} \; (i=1,2,\ldots.n) \tag{11}$$

$$R_i = \sum_{j=1}^{n} t_{ij} \; (j=1,2,\ldots.n) \tag{12}$$

Prosedürü tamamlamak için, tüm hesaplanan $\widetilde{D}_i + \tilde{R}_i$ ve $\widetilde{D}_i - \tilde{R}_i$ uygun durulaştırma yöntemiyle durulaştırılır. Ardından, iki sayı kümesi olacaktır: $(\widetilde{D}_i + \tilde{R}_i)^{\text{def}}$ stratejik hedeflerin ne kadar önemli olduğunu gösteren ve $(\widetilde{D}_i - \tilde{R}_i)^{\text{def}}$ hangi stratejik hedefin sebep, hangisinin sonuç olduğunu gösterir. Genel olarak, eğer değer $(\widetilde{D}_i - \tilde{R}_i)^{\text{def}}$ pozitifse, hedefler neden grubuna aittir ve eğer değer $(\widetilde{D}_i - \tilde{R}_i)^{\text{def}}$ negatif ise, hedefler etki grubuna aittir.

Adım 6. Kriter Ağrlıklarının Hesaplanması

Bulanık DEMATEL yönetminin son adımı olarak kriter ağırlıkları aşağıdaki formül yardımıyla hesaplanır.

$$w_i = \{(\widetilde{D}_i^{\,def} + \tilde{R}_i^{\,def})^2 + (\widetilde{D}_i^{\,def} - \tilde{R}_i^{\,def})^2\}^{1/2} \quad (13)$$

$$W_i = \frac{w_i}{\sum_{i=1}^{n} w_i} \quad (14)$$

3.4. BULANIK PROMETHEE YÖNTEMİ

Karar verme problemlerinde sıkça kullanılan bir diğer yöntem olan PROMETHEE (Preference Ranking Organisation Method for Enrichment Evaluation), Brans (1982) tarafından ilk defa kullanılmış daha sonra Brans ve Vincke'nin (1985) yaptığı çalışmalarla geliştirilerek literatüre kazandırılmıştır. PROMETHEE yöntemi; birden fazla kriter ile en doğru alternatifin belirlenmesinde kullanılarak karar vericilere fikir vermektedir. Yöntem birden fazla alternatifler arasında kısmı sıralama (PROMETHEE I) ve net sıralama (PROMETHEE II) yapabilmesine imkan sağlamaktadır. (Brans vd., 1986). PROMETHEE yönteminin bir uzantısı olan GAIA ile karar vericilere görsel olarak farklı bakış açıları kazandırılmaktadır.

Bulanık PROMETHEE yöntemi ilk olarak Le Teno ve Mareschal (1998) tarafından önerilmiş bulanık mantığın PROMETHEE methoduna eklenmesi ile ortaya çıkmıştır. Bulanık PROMETHEE yöntemi ile PROMETHEE yönteminin uygulama adımları arasında fark olmaması nedeniyle kısaca PROMETHEE yönteminin adımları aşağıdaki gibidir.

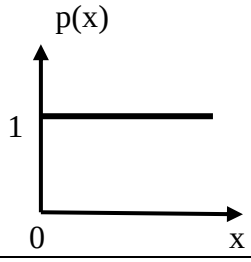
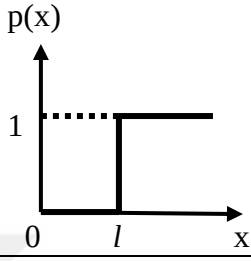
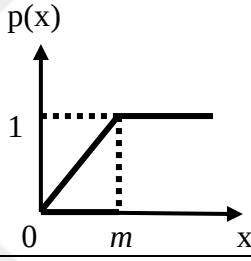
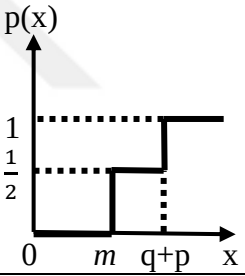
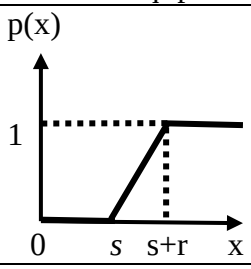
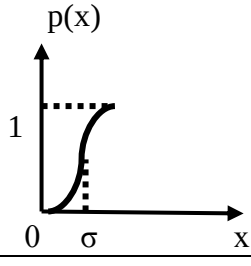
Adım 1: w=(w_1, w_2,…, w_k) ağırlıklarına sahip k kriter c=(f_1, f_2,…, f_k) tarafından değerlendirilen alternatiflere A=(a,b,c,…) ilişkin Tablo 8'de verilen Şekilde veri matrisi oluşturulur.

Tablo 8. Veri Matrisi Gösterimi

Kriterler	*a*	*B*	*c*	...	*W*
f_1	$f_1(a)$	$f_1(b)$	$f_1(c)$	...	w_1
f_2	$f_2(a)$	$f_2(b)$	$f_2(c)$	...	w_2
…	…	…	…	...	…
f_k	$f_k(a)$	$f_k(b)$	$f_k(c)$	...	w_k

Adım 2: Kriterlerin temel özelliklerine göre tercih fonksiyonları Tablo 9'da gösterilen 6 farklı tercih tipleri arasından belirlenir.

Tablo 9. Tercih Fonksiyonları

Tip	Parametreler	Fonksiyon	Grafik P(x)
Birinci Tip (Olağan)	-	$p(x)=\begin{cases}0, & x \le 0\\ 1, & x > 0\end{cases}$	
İkinci Tip (U-Tipi)	l	$p(x)=\begin{cases}0, & x \le l\\ 1, & x > l\end{cases}$	
Üçüncü Tip (V-Tipi)	m	$p(x)=\begin{cases}x/m, & x \le m\\ 1, & x \ge m\end{cases}$	
Dördüncü Tip (Seviyeli)	q, p	$p(x)\begin{cases}0, & x \le q\\ \frac{1}{2}, & q < x \le q+p\\ 1, & x > q+p\end{cases}$	
Beşinci Tip (Lineer)	s, r	$p(x)\begin{cases}0, & x \le s\\ \frac{x-s}{r}, & s \le x \le s+r\\ 1, & x \ge s+r\end{cases}$	
Altıncı Tip (Gaussian)	σ	$p(x)=\begin{cases}0, & x \le 0\\ 1-e^{-x^2/2\sigma^2}, & x \ge 0\end{cases}$	

3. Adım: Tercih fonksiyonlarından yararlanılarak her bir kritere göre alternatifler kümesindeki her alternatif çifti için ortak tercih fonksiyonları aşağıdaki gibi hesaplanır.

$$p(a,b)=\begin{cases}0, & f(a) \leq f(b) \\ p[f(a)-f(b)], & f(a) > f(b)\end{cases} \quad (13)$$

4. Adım: Her alternatifn ortak tercih fonksiyonlarına bakılarak çok kriterli tercih indekseleri aşağıdaki gibi hesaplanır.

$$\pi(a,b)=\frac{\sum_{i=1}^{k} w_i x P_i(a,b)}{\sum_{i=1}^{k} w_i} \quad (14)$$

5. Adım: Her a ∈ A alternatifleri için pozitif üstünlük ve negatif üstünlük değerleri aşağıdaki gibi hesaplanır.

$$\phi^{+}(a) = \sum \pi(a,x) \quad x=(b,c,d\ldots\ldots) \quad (15)$$

$$\phi^{-}(a) = \sum \pi(x,a) \quad x=(b,c,d\ldots\ldots) \quad (16)$$

6. Adım: Alternatiflere ait kısmi sıralama PROMETHEE I ile gerçekleştirilir. Bu adımda farksızlık, üstünlük ve kıyaslanmama şeklindeki üç durum ile alternatifler karşılaştırılır.

Denklem (17), (18) ve (19)'daki koşul sağlanırsa a alternatifi b alternatifine tercih edilmelidir.

$$\phi^{+}(a) > \phi^{+}(b) \text{ ve } \phi^{-}(a) < \phi^{-}(b) \quad (17)$$

$$\phi^{+}(a) > \phi^{+}(b) \text{ ve } \phi^{-}(a) = \phi^{-}(b) \quad (18)$$

$$\phi^{+}(a) = \phi^{+}(b) \text{ ve } \phi^{-}(a) < \phi^{-}(b) \quad (19)$$

Denklem (20)'deki durum gerçekleşirse a alternatifi ile b alternatifi birbirinden farksız demektir.

$\phi^+(a) = \phi^+(b)$ ve $\phi^-(a) = \phi^-(b)$ (20)

Denklem (21) ve (22)'deki durumlardan birisi gerçekleşirse a ve b alternatifi kıyaslanamaz demektir.

$\phi^+(a) > \phi^+(b)$ ve $\phi^-(a) > \phi^-(b)$ (21)

$\phi^+(a) < \phi^+(b)$ ve $\phi^-(a) < \phi^-(b)$ (22)

Adım 7. Uygulamanın bu adımında PROMETHEE II ile tam sırlama işlemi yapılır. Her alternatif için net üstünlük değerleri hesaplanır.

$\phi(a) = \phi^+(a) - \phi^-(a)$ (23)

Bütün alternatiflerin üstünlük değerleri aşağıdaki iki duruma göre değerlendirilir.

$\phi(a) > \phi(b)$; a alternatifi b alternatifne göre daha üstündür.
$\phi(a) = \phi(b)$; alternatifler birbirlerinden farksızdır.

Buraya kadar anlatılan adımlar PROMETHEE yönetimine ait olan klasik adımlardır. Bulanık PROMETHEE yönteminde ise farklı olarak parametrelerin bulanık sayılarla ifade edilmesi ile tercih fonksiyonları ve diğer hesaplamalar güncellenebilmektedir. Bu çalışmada tercih fonksiyonlarından doğrusal fonksiyon kullanılmış olup tercih eşik değeri (p, q) ve kriter ağırlıkları kesin sayılarla ifade edilmiştir. Çalışmada üçgensel sayılara karşılık gelen sözel ifadeler ise aşağıdaki Tablo 10'da gösterilmiştir (Goumas ve Lygerou, 2000).

Tablo 10. Üçgensel Sayı İfadeleri

Sözel İfadeler	Üçgensel Karşılığı
Çok İyi (Çİ)	(1.00-0.20-0.00)
İyi(İ)	(0.80-0.15-0.20)
Biraz İyi (Bİ)	(0.65-0.15-0.15)
Orta (O)	(0.50-0.20-0.15)
Biraz Kötü (BK)	(0.30-0.15-0.20)
Kötü (K)	(0.15-0.15-0.15)
Çok Kötü (ÇK)	(0.00-0.00-0.15)

Çalışmada doğrusal tercih fonksiyonu tercih edilmesi nedeniyle aşağıdaki denklemde a ve b değerlerinin arasındaki sapmayı gösteren d farkı x=(n,c,d) bulanık sayısı olarak ifade edilmiştir.

$$p(a,b) = \begin{cases} 0, & n - c < q \\ \frac{(n,c,d)-q}{p-q}, & q \le n - c \; ve \; n + d < p \\ 1, & n + d \ge p \end{cases} \quad (24)$$

Bu çalışmada temel matematik işlemleri için Goumas ve Lygerou (2000) tarafından önerilen LR bulanık işlemler kullanılmış olup gerekli formüller aşağıdaki tabloda gösterilmiştir.

Tablo 11. Temel Bulanık İşlemleri

Toplama	$(\boldsymbol{m,a,b})_{\boldsymbol{LR}} + (\boldsymbol{n,c,d})_{\boldsymbol{LR}} = (\boldsymbol{m+n, a+c, b+d})_{\boldsymbol{LR}}$
Çıkarma	$(m,a,b)_{LR} - (n,c,d)_{LR} = (m-n, a+d, b+c)_{LR}$
Negatifi	$-(m,a,b)_{LR} = (-m,a,b)_{LR}$
Çarpma	$(m,a,b)_{LR}\; x\; (n,0,0)_{LR} = (mn, an, bn)_{LR}$
Bulanık Çarpma	
m>0, n>0	$(m,a,b)_{LR}\; x\; (n,c,d)_{LR} = (mn, mc+an, md+bn)_{LR}$
m<0, n>0	$(m,a,b)_{LR}\; x\; (n,c,d)_{LR} = (mn, an-md, bd-mc)_{LR}$
m<0, n<0	$(m,a,b)_{LR}\; x\; (n,c,d)_{LR} = (mn, -bn-md, -an-mc)_{LR}$

Bulanık sayılarla yapılan işlemler sonucunda yine bulanık sayılar elde edileceğinden iki bulanık sayının karşılaştırılması sorun yaratacaktır. Bu nedenle durulaştırma işlemi için Yager (1981) tarafından önerilen Yager indeksi yöntemi kullanılmıştır. Yager indeksine göre x = (m,a,b) bulanık sayı denklemi aşağıda gösterilmiştir.

$$F(m,a,b) = (3m-a+b)/3 \quad (25)$$

Durulaştırma işleminden sonraki adımlar PROMETHEE yöntemiyle eş değer olup, pozitif ve negatif üstünlüklerin hesaplanması ile bulanık PROMETHEE I (kısmi sıralama) ve bulanık PROMETHEE II (tam sıralama) sıralamaları yapılır.

DÖRDÜNCÜ BÖLÜM

4. BULGULAR

Tezin bu bölümünde siber risklere çözüm yaklaşımları belirlenerek uzman görüşleri doğrultusunda elde edilen bilgiler ile uygulama gerçekleştirilmiştir. Öncelikle bulanık DEMATEL yönteminde kullanılmak üzere belirlenen kriterlerin ağırlıklarını hesaplamak için denizcilik sektörünün farklı alt dallarında görev yapan kişilerle e-posta yoluyla iletişime geçilmiş ve anket yöntemiyle kriterlerin karşılaştırılması istenmiştir. Uzmanlar; farklı liman işletmelerinden olmak üzere 2, armatör firmalarından 2, acente firmalarından 2, forwarder firmalarından 2, brokerlik firmalarından 2 olmak üzere toplam 10 yöneticiden oluşmaktadır. Hogarth'a (1978) göre en iyi sonuçları elde etmek için uzman görüşlerinin 8-12 kişi arasında olması gerekmektedir. Uzman görüşleri sonucu elde edilen dilsel ifadeler üçgensel sayılara çevrilerek bulanık DEMATEL yöntemiyle değerlendirilmiş olup kriterler arasındaki neden sonuç ilişkileri incelenmiş ve kriter ağırlıkları hesaplanmıştır.

Kriter ağırlıklarının hesaplanmasından sonra denizcilik sektörünün alt dallarından hangilerinin siber risklere karşı daha fazla önem verdiğinin belirlenmesi amacıyla sıralama yöntemi olan bulanık PROMETHEE yönteminden faydalanılmıştır. Bu amaçla Marmara bölgesinden faaliyet gösteren liman, armatör, broker, forwarder ve acente işletmelerinin yöneticileri ile görüşülmüş olup daha önce belirlenen siber risk kriterlerinin şirketlerinde uygulanıp uygulanmadığı beşli ölçek olarak anket yöntemiyle sorulmuştur. Elde edilen bilgiler doğrultusunda yöntemlerin uygulanması ve sonuçları aşağıda anlatılmıştır.

4.1. BULANIK DEMATEL YÖNTEMİNİN UYGULANMASI

Uzman görüşleri sonucu ana kriterler ve alt kriterler karşılaştırılmış ve aşağıda gösterildiği gibi bulanık DEMATEL yönteminin adımları uygulanmıştır.

Tablo 12. Ana Kriterlerin İkili İlişki Matrisleri

	İTY			*TTY*			*YTY*		
İTY	0.00	0.00	0.00	0.34	0.56	0.78	0.31	0.53	0.72
TTY	0.16	0.38	0.59	0.00	0.00	0.00	0.22	0.44	0.63
YTY	0.34	0.56	0.78	0.38	0.59	0.78	0.00	0.00	0.00

Uygulamanın birinci aşamasında uzman görüşleri sonucu elde edilen dilsel ifadeler üçgensel bulanık sayılara çevrilmiş ve elde edilen sonuçların ortalamaları alınarak Tablo 12'de gösterildiği ana kriterlerin karşılaştırılmaları gerçekleştirilmiştir.

Tablo 13. Ana Kriterlerin Normalleştirilmiş ilişki Matrisi

	İTY			*TTY*			*YTY*		
İTY	0.00	0.00	0.00	0.22	0.36	0.50	0.20	0.34	0.46
TTY	0.10	0.24	0.38	0.00	0.00	0.00	0.14	0.28	0.40
YTY	0.22	0.36	0.50	0.24	0.38	0.50	0.00	0.00	0.00

İkili karşılaştırmalar yapıldıktan sonra ana kriterlere normalleştirme işlemi için Denklem (8) uygulanır ve Tablo 13'te gösterildiği gibi normalleştirilmiş bir ilişki matrisi elde edilir.

Tablo 14. Ana Kriterlerin Toplam Bulanık Direkt İlişki Matrisi

	l	*l*	*l*	*I-l Matrisi*			*Tersi*			*Çarpımı*		
İTY	0.00	0.22	0.20	1.00	-0.22	-0.20	1.09	0.30	0.26	0.00	0.07	0.05
TTY	0.10	0.00	0.14	-0.10	1.00	-0.14	0.15	1.08	0.18	0.01	0.00	0.03
YTY	0.22	0.24	0.00	-0.22	-0.24	1.00	0.27	0.32	1.10	0.06	0.08	0.00
	m	*m*	*m*	*I-m Matrisi*			*Tersi*			*Çarpımı*		
İTY	0.00	0.36	0.34	1.00	-0.36	-0.34	1.45	0.79	0.71	0.00	0.29	0.24
TTY	0.24	0.00	0.28	-0.24	1.00	-0.28	0.55	1.42	0.59	0.13	0.00	0.16
YTY	0.36	0.38	0.00	-0.36	-0.38	1.00	0.73	0.83	1.48	0.26	0.31	0.00
	u	*u*	*u*	*I-u Matrisi*			*Tersi*			*Çarpımı*		
İTY	0.00	0.50	0.46	1.00	-0.50	-0.46	4.15	3.79	3.43	0.00	1.90	1.58
TTY	0.38	0.00	0.40	-0.38	1.00	-0.40	3.01	4.00	2.98	1.14	0.00	1.19
YTY	0.50	0.50	0.00	-0.50	-0.50	1.00	3.58	3.89	4.21	1.79	1.95	0.00

Tablo 14. Ana Kriterlerin Toplam Bulanık Direkt İlişki Matrisi Devam

	İTY			TTY			YTY		
İTY	0.00	0.00	0.00	0.07	0.29	1.90	0.05	0.24	1.58
TTY	0.01	0.13	1.14	0.00	0.00	0.00	0.03	0.16	1.19
YTY	0.06	0.26	1.79	0.08	0.31	1.95	0.00	0.00	0.00

Normalleştrime işlemi yapıldıktan sonra ana kriterlerin bulanık direk ilişki matrisi Denklem (10) yardımıyla oluşturulmuş ve Tablo 14'te gösterilmiştir.

Tablo 15. Ana Kriterlerin Neden Sonuç İlişkilerinin Değerleri

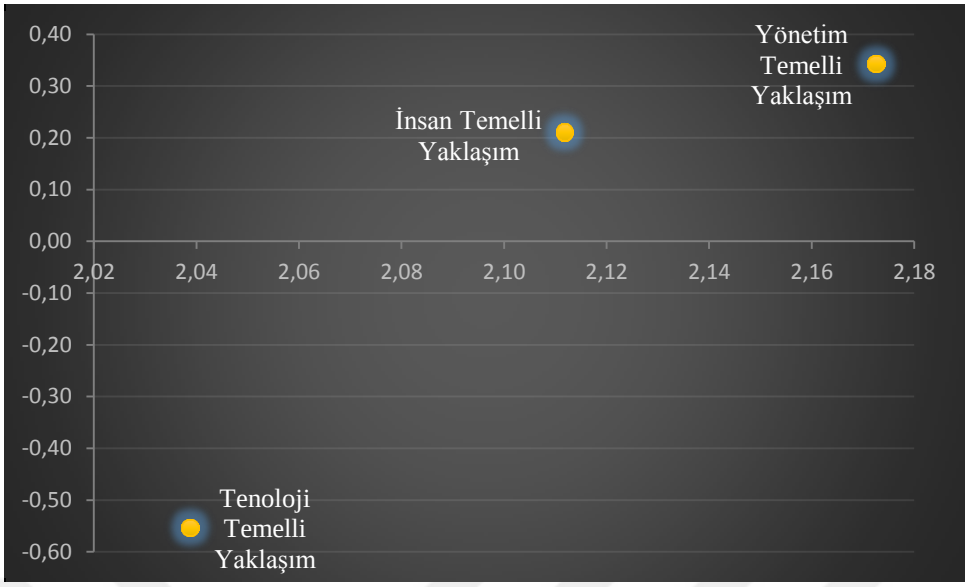
	D_i			R_i			$D_i + R_i$			$D_i - R_i$		
İTY	0.12	0.53	3.47	0.08	0.40	2.94	0.19	0.92	6.41	0.04	0.13	0.54
TTY	0.04	0.30	2.34	0.14	0.60	3.84	0.18	0.90	6.18	-0.10	-0.30	-1.50
YTY	0.14	0.58	3.74	0.08	0.41	2.77	0.22	0.98	6.51	0.06	0.17	0.97

Uygulamanın bu adımında alıcı ve gönderici kriterleri belirlemek için Denklem (11) ve Denklem (12) yardımıyla Tablo 15'te gösterildiği gibi neden sonuç değerleri hesaplanır.

Tablo 16. Ana Kriterlerin Durulaştırma ve Ağırlık Değerleri

	$(\widetilde{D}_i + \widetilde{R}_i)^{\text{def}}$	$(\widetilde{D}_i - \widetilde{R}_i)^{\text{def}}$	w_i	W_i
İTY	2.11	0.21	2.25	0.33
TTY	2.04	-0.55	2.23	0.32
YTY	2.17	0.34	2.42	0.35

Uygulamanın son adımında ise $D_i + R_i$ ve $D_i - R_i$ değerleri durulaştırılarak kriterlerin önem ağırlıkları Tablo 16'daki gibi hesaplanır. Kriterler arasındaki neden sonuç ilişki diyagramı ise aşağıda gösterilmiştir.



Şekil 16. Ana Kriterlerin Neden Sonuç Diyagramı

Şekil 16'daki neden sonuç diyagramına göre; *teknoloji temelli yaklaşım* en çok etkilenen ve alıcıyken, *yönetim temelli yaklaşım* ise en çok etkileyen ve gönderici konumunda olup en önemli ana kriterdir.

Tablo 17. İnsan Temelli Yaklaşımın Alt Kriterlerinin İkili Karşılaştırma Matrisi

	K1			*K2*			*K3*			*K4*			*K5*		
K1	0.00	0.00	0.25	0.39	0.64	0.89	0.29	0.54	0.79	0.21	0.46	0.71	0.36	0.61	0.82
K2	0.36	0.61	0.82	0.00	0.00	0.25	0.18	0.39	0.64	0.21	0.46	0.71	0.39	0.64	0.89
K3	0.61	0.86	0.96	0.43	0.68	0.93	0.00	0.00	0.25	0.43	0.68	0.86	0.25	0.50	0.75
K4	0.46	0.71	0.93	0.54	0.79	1.00	0.43	0.68	0.89	0.00	0.00	0.25	0.39	0.64	0.89
K5	0.18	0.39	0.64	0.25	0.50	0.75	0.11	0.32	0.57	0.21	0.46	0.71	0.00	0.00	0.25

İnsan temelli yaklaşımının alt kriterlerinin dilsel ifadeler sonucunda ikili karşılaştırmaları Tablo 17'de gösterildiği gibidir.

Tablo 18. İnsan Temelli Yaklaşımın Normalleştirilmiş ilişki Matrisi

	K1			*K2*			*K3*			*K4*			*K5*		
K1	0.00	0.00	0.06	0.10	0.16	0.23	0.07	0.14	0.20	0.05	0.12	0.18	0.09	0.15	0.21
K2	0.09	0.15	0.21	0.00	0.00	0.06	0.05	0.10	0.16	0.05	0.12	0.18	0.10	0.16	0.23
K3	0.15	0.22	0.24	0.11	0.17	0.23	0.00	0.00	0.06	0.11	0.17	0.22	0.06	0.13	0.19
K4	0.12	0.18	0.23	0.14	0.20	0.25	0.11	0.17	0.23	0.00	0.00	0.06	0.10	0.16	0.23
K5	0.05	0.10	0.16	0.06	0.13	0.19	0.03	0.08	0.14	0.05	0.12	0.18	0.00	0.00	0.06

İkili karşılaştırmalar yapıldıktan sonra insan temelli yaklaşımın alt kriterlerine normalleştirme işlemi yapılarak Tablo 18'de gösterildiği gibi normalleştirilmiş bir ilişki matrisi elde edilir.

Tablo 19. İnsan Temelli Yaklaşımın Bulanık Toplam Direkt İlişki Matrisi

	l	*l*	*l*	*l*	*l*	*m*	*m*	*m*	*m*	*m*	*u*	*u*	*u*	*u*	*u*
K1	0.00	0.10	0.07	0.05	0.09	0.00	0.16	0.14	0.12	0.15	0.06	0.23	0.20	0.18	0.21
K2	0.09	0.00	0.05	0.05	0.10	0.15	0.00	0.10	0.12	0.16	0.21	0.06	0.16	0.18	0.23
K3	0.15	0.11	0.00	0.11	0.06	0.22	0.17	0.00	0.17	0.13	0.24	0.23	0.06	0.22	0.19
K4	0.12	0.14	0.11	0.00	0.10	0.18	0.20	0.17	0.00	0.16	0.23	0.25	0.23	0.06	0.23
K5	0.05	0.06	0.03	0.05	0.00	0.10	0.13	0.08	0.12	0.00	0.16	0.19	0.14	0.18	0.06
	I-l Matrisi					*I-m Matrisi*					*I-u Matrisi*				
K1	1.00	-0.10	-0.07	-0.05	-0.09	1.00	-0.16	-0.14	-0.12	-0.15	0.94	-0.23	-0.20	-0.18	-0.21
K2	-0.09	1.00	-0.05	-0.05	-0.10	-0.15	1.00	-0.10	-0.12	-0.16	-0.21	0.94	-0.16	-0.18	-0.23
K3	-0.15	-0.11	1.00	-0.11	-0.06	-0.22	-0.17	1.00	-0.17	-0.13	-0.24	-0.23	0.94	-0.22	-0.19
K4	-0.12	-0.14	-0.11	1.00	-0.10	-0.18	-0.20	-0.17	1.00	-0.16	-0.23	-0.25	-0.23	0.94	-0.23
K5	-0.05	-0.06	-0.03	-0.05	1.00	-0.10	-0.13	-0.08	-0.12	1.00	-0.16	-0.19	-0.14	-0.18	0.94
	Tersi					*Tersi*					*Tersi*				
K1	1.04	0.13	0.09	0.08	0.12	1.18	0.33	0.26	0.26	0.31	2.34	1.54	1.31	1.33	1.47
K2	0.12	1.04	0.07	0.08	0.13	0.30	1.18	0.22	0.25	0.31	1.41	2.35	1.23	1.28	1.43
K3	0.19	0.16	1.04	0.14	0.11	0.40	0.37	1.17	0.33	0.32	1.59	1.66	2.28	1.45	1.56
K4	0.17	0.18	0.14	1.04	0.14	0.38	0.40	0.32	1.19	0.36	1.65	1.74	1.47	2.38	1.65
K5	0.07	0.09	0.04	0.07	1.02	0.23	0.26	0.19	0.22	1.14	1.25	1.33	1.11	1.17	2.17
	Çarpımı					*Çarpımı*					*Çarpımı*				
K1	0.00	0.01	0.01	0.00	0.01	0.00	0.05	0.04	0.03	0.05	0.15	0.35	0.26	0.24	0.30
K2	0.01	0.00	0.00	0.00	0.01	0.05	0.00	0.02	0.03	0.05	0.29	0.15	0.20	0.23	0.32
K3	0.03	0.02	0.00	0.01	0.01	0.09	0.06	0.00	0.06	0.04	0.39	0.39	0.14	0.31	0.29
K4	0.02	0.02	0.01	0.00	0.01	0.07	0.08	0.06	0.00	0.06	0.39	0.44	0.33	0.15	0.37
K5	0.00	0.01	0.00	0.00	0.00	0.02	0.03	0.02	0.03	0.00	0.20	0.25	0.16	0.21	0.14

Tablo 19. İnsan Temelli Yaklaşımın Bulanık Toplam Direkt İlişki Matrisi Devam

	K1			*K2*			*K3*			*K4*			*K5*		
K1	0.00	0.00	0.15	0.01	0.05	0.35	0.01	0.04	0.26	0.00	0.03	0.24	0.01	0.05	0.30
K2	0.01	0.05	0.29	0.00	0.00	0.15	0.00	0.02	0.20	0.00	0.03	0.23	0.01	0.05	0.32
K3	0.03	0.09	0.39	0.02	0.06	0.39	0.00	0.00	0.14	0.01	0.06	0.31	0.01	0.04	0.29
K4	0.02	0.07	0.39	0.02	0.08	0.44	0.01	0.06	0.33	0.00	0.00	0.15	0.01	0.06	0.37
K5	0.00	0.02	0.20	0.01	0.03	0.25	0.00	0.02	0.16	0.00	0.03	0.21	0.00	0.00	0.14

Normalleştrime işlemi yapıldıktan sonra insan temelli yaklaşımın alt kriterlerinin bulanık direk ilişki matrisi Denklem (10) yardımıyla oluşturulmuş ve Tablo 19'da gösterilmiştir.

Tablo 20. İnsan Temelli Yaklaşımın Neden Sonuç İlişkilerinin Değerleri

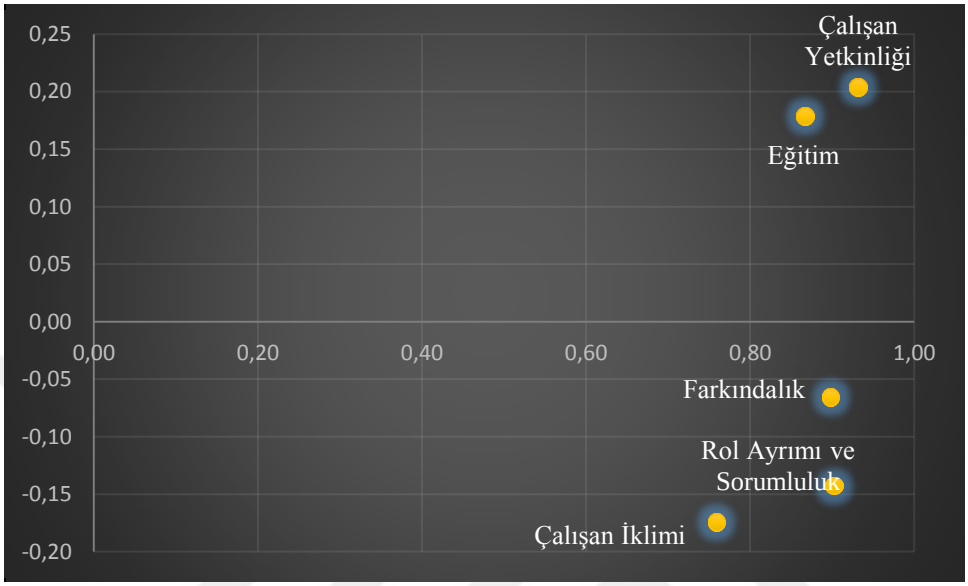
	D_i			R_i			$D_i + R_i$			$D_i - R_i$		
K1	0.03	0.17	1.30	0.06	0.22	1.41	0.10	0.39	2.71	-0.03	-0.06	-0.12
K2	0.03	0.15	1.19	0.06	0.23	1.57	0.09	0.38	2.77	-0.03	-0.08	-0.38
K3	0.07	0.25	1.53	0.03	0.13	1.09	0.09	0.38	2.62	0.04	0.12	0.43
K4	0.07	0.26	1.68	0.03	0.14	1.15	0.10	0.40	2.82	0.05	0.12	0.53
K5	0.01	0.10	0.96	0.04	0.20	1.43	0.06	0.29	2.39	-0.03	-0.10	-0.47

Uygulamanın bu adımında alıcı ve gönderici kriterleri belirlemek için Denklem (11) ve Denklem (12) yardımıyla Tablo 20'de gösterildiği gibi neden sonuç değerleri hesaplanır.

Tablo 21. İnsan Temelli Yaklaşımın Durulaştırma ve Ağırlık Değerleri

	$(\tilde{D}_i + \tilde{R}_i)^{\text{def}}$	$(\tilde{D}_i - \tilde{R}_i)^{\text{def}}$	w_i	W_i
K1	0.90	-0.07	0.41	0.21
K2	0.90	-0.14	0.42	0.21
K3	0.87	0.18	0.39	0.20
K4	0.93	0.20	0.45	0.23
K5	0.76	-0.17	0.30	0.15

Uygulamanın son adımında ise D_i + R_i ve D_i - R_i değerleri durulaştırılarak kriterlerin önem ağırlıkları Tablo 21'deki gibi hesaplanır. Kriterler arasındaki neden sonuç ilişki diyagramı ise aşağıda gösterilmiştir.



Şekil 17. İnsan Temelli Yaklaşımın Neden Sonuç Diyagramı

Şekil 17'deki neden sonuç diyagramına göre; *çalışan iklimi* en çok etkilenen ve alıcıyken, *Çalışan yetkinliği* ise en çok etkileyen ve gönderici konumundadır. Diğer en çok etkileyen ve gönderici konumunda olan *eğitim* kriteri olarak ortaya çıkmış *farkındalık* ile *rol ayrımı ve sorumluluk* kriterleri ise etkilenen ve alıcı grubunda yer almışlardır.

Tablo 22. Teknoloji Temelli Yaklaşımın Alt Kriterlerinin İkili Karşılaştırma Matrisi

	K6			*K7*			*K8*			*K9*			*K10*		
K6	0.00	0.00	0.22	0.47	0.69	0.84	0.47	0.69	0.88	0.28	0.50	0.72	0.34	0.53	0.69
K7	0.25	0.44	0.66	0.00	0.00	0.22	0.34	0.56	0.72	0.38	0.59	0.75	0.31	0.53	0.69
K8	0.25	0.44	0.66	0.28	0.50	0.69	0.00	0.00	0.22	0.09	0.31	0.53	0.19	0.41	0.63
K9	0.31	0.50	0.69	0.34	0.56	0.75	0.34	0.56	0.78	0.00	0.00	0.22	0.28	0.50	0.72
K10	0.34	0.53	0.69	0.44	0.66	0.81	0.41	0.59	0.72	0.22	0.44	0.66	0.00	0.00	0.22

Teknoloji temelli yaklaşımının alt kriterlerinin dilsel ifadeler sonucunda ikili karşılaştırmaları Tablo 22'de gösterildiği gibidir.

Tablo 23. Teknoloji Temelli Yaklaşımın Normalleştirilmiş İlişki Matrisi

	K6			*K7*			*K8*			*K9*			*K10*		
K6	0.00	0.00	0.07	0.14	0.21	0.25	0.14	0.21	0.26	0.08	0.15	0.21	0.10	0.16	0.21
K7	0.07	0.13	0.20	0.00	0.00	0.07	0.10	0.17	0.21	0.11	0.18	0.22	0.09	0.16	0.21
K8	0.07	0.13	0.20	0.08	0.15	0.21	0.00	0.00	0.07	0.03	0.09	0.16	0.06	0.12	0.19
K9	0.09	0.15	0.21	0.10	0.17	0.22	0.10	0.17	0.23	0.00	0.00	0.07	0.08	0.15	0.21
K10	0.10	0.16	0.21	0.13	0.20	0.24	0.12	0.18	0.21	0.07	0.13	0.20	0.00	0.00	0.07

İkili karşılaştırmalar yapıldıktan sonra teknoloji temelli yaklaşımın alt kriterlerine normalleştirme işlemi yapılarak Tablo 23'te gösterildiği gibi normalleştirilmiş bir ilişki matrisi elde edilir.

Tablo 24. Teknoloji Temelli Yaklaşımın Bulanık Toplam Direkt İlişki Matrisi

	l	*l*	*l*	*l*	*l*	*m*	*m*	*m*	*m*	*m*	*u*	*u*	*u*	*u*	*u*
K6	0.00	0.14	0.14	0.08	0.10	0.00	0.21	0.21	0.15	0.16	0.07	0.25	0.26	0.21	0.21
K7	0.07	0.00	0.10	0.11	0.09	0.13	0.00	0.17	0.18	0.16	0.20	0.07	0.21	0.22	0.21
K8	0.07	0.08	0.00	0.03	0.06	0.13	0.15	0.00	0.09	0.12	0.20	0.21	0.07	0.16	0.19
K9	0.09	0.10	0.10	0.00	0.08	0.15	0.17	0.17	0.00	0.15	0.21	0.22	0.23	0.07	0.21
K10	0.10	0.13	0.12	0.07	0.00	0.16	0.20	0.18	0.13	0.00	0.21	0.24	0.21	0.20	0.07
	I-l Matrisi					*I-m Matrisi*					*I-u Matrisi*				
K6	1.00	-0.14	-0.14	-0.08	-0.10	1.00	-0.21	-0.21	-0.15	-0.16	0.93	-0.25	-0.26	-0.21	-0.21
K7	-0.07	1.00	-0.10	-0.11	-0.09	-0.13	1.00	-0.17	-0.18	-0.16	-0.20	0.93	-0.21	-0.22	-0.21
K8	-0.07	-0.08	1.00	-0.03	-0.06	-0.13	-0.15	1.00	-0.09	-0.12	-0.20	-0.21	0.93	-0.16	-0.19

Tablo 24. Teknoloji Temelli Yaklaşımın Bulanık Toplam Direkt İlişki Matrisi Devam

K9	-0.09	-0.10	-0.10	1.00	-0.08	-0.15	-0.17	-0.17	1.00	-0.15	-0.21	-0.22	-0.23	0.93	-0.21
K10	-0.10	-0.13	-0.12	-0.07	1.00	-0.16	-0.20	-0.18	-0.13	1.00	-0.21	-0.24	-0.21	-0.20	0.93
	Tersi					*Tersi*					*Tersi*				
K6	1.06	0.20	0.20	0.13	0.15	1.23	0.46	0.46	0.36	0.38	3.11	2.52	2.52	2.22	2.25
K7	0.12	1.06	0.16	0.14	0.13	0.33	1.26	0.40	0.36	0.35	2.07	3.17	2.31	2.07	2.09
K8	0.10	0.12	1.04	0.06	0.08	0.29	0.34	1.21	0.25	0.28	1.89	2.10	2.98	1.85	1.90
K9	0.13	0.16	0.16	1.04	0.12	0.34	0.40	0.40	1.20	0.35	2.14	2.39	2.39	3.00	2.16
K10	0.15	0.18	0.18	0.11	1.05	0.36	0.43	0.42	0.33	1.22	2.11	2.36	2.34	2.08	3.00
	Çarpımı					*Çarpımı*					*Çarpımı*				
K6	0.00	0.03	0.03	0.01	0.02	0.00	0.09	0.09	0.05	0.06	0.20	0.63	0.66	0.48	0.46
K7	0.01	0.00	0.02	0.02	0.01	0.04	0.00	0.07	0.06	0.06	0.41	0.21	0.50	0.46	0.43
K8	0.01	0.01	0.00	0.00	0.00	0.04	0.05	0.00	0.02	0.03	0.37	0.43	0.20	0.29	0.36
K9	0.01	0.02	0.02	0.00	0.01	0.05	0.07	0.07	0.00	0.05	0.44	0.53	0.56	0.20	0.46
K10	0.01	0.02	0.02	0.01	0.00	0.06	0.08	0.07	0.04	0.00	0.43	0.57	0.50	0.41	0.20
	K6			*K7*		*K8*			*K9*			*K10*			
K6	0.00	0.00	0.20	0.03	0.09	0.63	0.03	0.09	0.66	0.01	0.05	0.48	0.02	0.06	0.46
K7	0.01	0.04	0.41	0.00	0.00	0.21	0.02	0.07	0.50	0.02	0.06	0.46	0.01	0.06	0.43
K8	0.01	0.04	0.37	0.01	0.05	0.43	0.00	0.00	0.20	0.00	0.02	0.29	0.00	0.03	0.36
K9	0.01	0.05	0.44	0.02	0.07	0.53	0.02	0.07	0.56	0.00	0.00	0.20	0.01	0.05	0.46
K10	0.01	0.06	0.43	0.02	0.08	0.57	0.02	0.07	0.50	0.01	0.04	0.41	0.00	0.00	0.20

Normalleştrime işlemi yapıldıktan sonra teknoloji temelli yaklaşımın alt kriterlerinin bulanık direk ilişki matrisi Denklem (10) yardımıyla oluşturulmuş ve Tablo 24'te gösterilmiştir.

Tablo 25. Teknoloji Temelli Yaklaşımın Neden Sonuç İlişkilerinin Değerleri

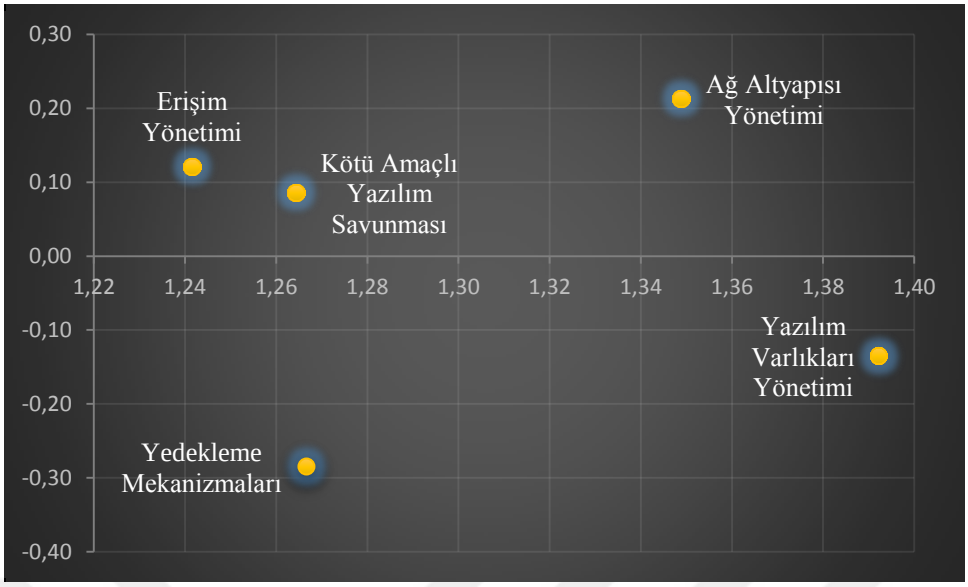
	D_i			R_i			$D_i + R_i$			$D_i - R_i$		
K6	0.08	0.30	2.44	0.04	0.19	1.85	0.13	0.49	4.29	0.04	0.11	0.59
K7	0.05	0.23	2.00	0.08	0.30	2.38	0.13	0.53	4.39	-0.02	-0.07	-0.38
K8	0.02	0.15	1.65	0.08	0.30	2.41	0.11	0.45	4.06	-0.06	-0.16	-0.77
K9	0.06	0.24	2.19	0.04	0.18	1.84	0.09	0.42	4.03	0.02	0.05	0.36
K10	0.07	0.26	2.12	0.04	0.20	1.91	0.11	0.46	4.03	0.02	0.06	0.21

Uygulamanın bu adımında alıcı ve gönderici kriterleri belirlemek için Denklem (11) ve Denklem (12) yardımıyla Tablo 25'te gösterildiği gibi neden sonuç değerleri hesaplanır.

Tablo 26. Teknoloji Temelli Yaklaşımın Durulaştırma ve Ağırlık Değerleri

	$(\tilde{D}_i + \tilde{R}_i)^{\text{def}}$	$(\tilde{D}_i - \tilde{R}_i)^{\text{def}}$	w_i	W_i
K6	1.35	0.21	0.93	0.22
K7	1.39	-0.14	0.98	0.23
K8	1.27	-0.28	0.84	0.19
K9	1.24	0.12	0.78	0.18
K10	1.26	0.09	0.80	0.19

Uygulamanın son adımında ise $D_i + R_i$ ve $D_i - R_i$ değerleri durulaştırılarak kriterlerin önem ağırlıkları Tablo 26'daki gibi hesaplanır. Kriterler arasındaki neden sonuç ilişki diyagramı ise aşağıda gösterilmiştir.



Şekil 18. Neden Sonuç Diyagramı

Şekil 18'de gösterildiği üzere neden sonuç diyagramına göre; *yedekleme mekanizmaları* en çok etkilenen ve alıcıyken *ağ altyapısı yönetimi* ise en çok etkileyen ve gönderici konumunda en önemli kriterdir. Etkileyen diğer kriterler *erişim yönetimi* ve *kötü amaçlı yazılım savunması* iken etkilenen diğer kriter ise *yazılım varlıkları yönetimi* kriteridir.

Tablo 27. Yönetim Temelli Yaklaşımın Alt Kriterlerinin Hesaplanması

	K11			*K12*			*K13*			*K14*			*K15*		
K11	0.00	0.00	0.25	0.50	0.75	0.93	0.43	0.68	0.86	0.50	0.75	0.89	0.43	0.68	0.93
K12	0.36	0.61	0.82	0.00	0.00	0.25	0.39	0.64	0.86	0.25	0.50	0.71	0.39	0.64	0.86
K13	0.39	0.64	0.89	0.46	0.71	0.93	0.00	0.00	0.25	0.29	0.54	0.75	0.39	0.64	0.86
K14	0.29	0.54	0.79	0.43	0.68	0.93	0.25	0.50	0.75	0.00	0.00	0.25	0.32	0.57	0.82
K15	0.32	0.57	0.79	0.21	0.46	0.71	0.25	0.50	0.75	0.36	0.61	0.82	0.00	0.00	0.25

Yönetim temelli yaklaşımının alt kriterlerinin dilsel ifadeler sonucunda ikili karşılaştırmaları Tablo 27'de gösterildiği gibidir.

Tablo 28. Yönetim Temelli Yaklaşımın Normalleştirilmiş ilişki Matrisi

	K11			*K12*			*K13*			*K14*			*K15*		
K11	0.00	0.00	0.06	0.13	0.19	0.24	0.11	0.18	0.22	0.13	0.19	0.23	0.11	0.18	0.24
K12	0.09	0.16	0.21	0.00	0.00	0.06	0.10	0.17	0.22	0.06	0.13	0.19	0.10	0.17	0.22
K13	0.10	0.17	0.23	0.12	0.19	0.24	0.00	0.00	0.06	0.07	0.14	0.19	0.10	0.17	0.22
K14	0.07	0.14	0.20	0.11	0.18	0.24	0.06	0.13	0.19	0.00	0.00	0.06	0.08	0.15	0.21
K15	0.08	0.15	0.20	0.06	0.12	0.19	0.06	0.13	0.19	0.09	0.16	0.21	0.00	0.00	0.06

İkili karşılaştırmalar yapıldıktan sonra yönetim temelli yaklaşımın alt kriterlerine normalleştirme işlemi yapılarak Tablo 28'de gösterildiği gibi normalleştirilmiş bir ilişki matrisi elde edilir.

Tablo 29. Yönetim Temelli Yaklaşımın Bulanık Toplam Direkt İlişki Matrisi

	l	*l*	*l*	*l*	*l*	*m*	*m*	*m*	*m*	*m*	*u*	*u*	*u*	*U*	*u*
K11	0.00	0.13	0.11	0.13	0.11	0.00	0.19	0.18	0.19	0.18	0.06	0.24	0.22	0.23	0.24
K12	0.09	0.00	0.10	0.06	0.10	0.16	0.00	0.17	0.13	0.17	0.21	0.06	0.22	0.19	0.22
K13	0.10	0.12	0.00	0.07	0.10	0.17	0.19	0.00	0.14	0.17	0.23	0.24	0.06	0.19	0.22
K14	0.07	0.11	0.06	0.00	0.08	0.14	0.18	0.13	0.00	0.15	0.20	0.24	0.19	0.06	0.21
K15	0.08	0.06	0.06	0.09	0.00	0.15	0.12	0.13	0.16	0.00	0.20	0.19	0.19	0.21	0.06
	I-l Matrisi					*I-m Matrisi*					*I-u Matrisi*				
K11	1.00	-0.13	-0.11	-0.13	-0.11	1.00	-0.19	-0.18	-0.19	-0.18	0.94	-0.24	-0.22	-0.23	-0.24
K12	-0.09	1.00	-0.10	-0.06	-0.10	-0.16	1.00	-0.17	-0.13	-0.17	-0.21	0.94	-0.22	-0.19	-0.22
K13	-0.10	-0.12	1.00	-0.07	-0.10	-0.17	-0.19	1.00	-0.14	-0.17	-0.23	-0.24	0.94	-0.19	-0.22
K14	-0.07	-0.11	-0.06	1.00	-0.08	-0.14	-0.18	-0.13	1.00	-0.15	-0.20	-0.24	-0.19	0.94	-0.21
K15	-0.08	-0.06	-0.06	-0.09	1.00	-0.15	-0.12	-0.13	-0.16	1.00	-0.20	-0.19	-0.19	-0.21	0.94
	Tersi					*Tersi*					*Tersi*				
K11	1.06	0.19	0.16	0.18	0.17	1.26	0.45	0.41	0.43	0.43	3.57	2.84	2.66	2.64	2.83
K12	0.13	1.05	0.14	0.11	0.15	0.36	1.24	0.36	0.34	0.38	2.50	3.48	2.47	2.41	2.61
K13	0.14	0.17	1.05	0.12	0.15	0.38	0.41	1.23	0.36	0.39	2.61	2.74	3.43	2.52	2.71
K14	0.11	0.15	0.10	1.04	0.13	0.34	0.38	0.33	1.22	0.36	2.51	2.65	2.46	3.32	2.62
K15	0.12	0.10	0.10	0.13	1.04	0.33	0.33	0.32	0.34	1.22	2.39	2.48	2.34	2.34	3.36

Tablo 29. Yönetim Temelli Yaklaşımın Bulanık Toplam Direkt İlişki Matrisi

	Çarpım														
K11	0.00	0.02	0.02	0.02	0.02	0.00	0.09	0.07	0.08	0.08	0.23	0.68	0.59	0.61	0.68
K12	0.01	0.00	0.01	0.01	0.01	0.06	0.00	0.06	0.04	0.06	0.53	0.23	0.55	0.45	0.58
K13	0.01	0.02	0.00	0.01	0.02	0.06	0.08	0.00	0.05	0.07	0.61	0.66	0.22	0.49	0.60
K14	0.01	0.02	0.01	0.00	0.01	0.05	0.07	0.04	0.00	0.05	0.51	0.64	0.48	0.22	0.56
K15	0.01	0.01	0.01	0.01	0.00	0.05	0.04	0.04	0.05	0.00	0.49	0.46	0.46	0.50	0.22
	K11			*K12*		*K13*			*K14*		*K15*				
K11	0.00	0.00	0.23	0.02	0.09	0.68	0.02	0.07	0.59	0.02	0.08	0.61	0.02	0.08	0.68
K12	0.01	0.06	0.53	0.00	0.00	0.23	0.01	0.06	0.55	0.01	0.04	0.45	0.01	0.06	0.58
K13	0.01	0.06	0.61	0.02	0.08	0.66	0.00	0.00	0.22	0.01	0.05	0.49	0.02	0.07	0.60
K14	0.01	0.05	0.51	0.02	0.07	0.64	0.01	0.04	0.48	0.00	0.00	0.22	0.01	0.05	0.56
K15	0.01	0.05	0.49	0.01	0.04	0.46	0.01	0.04	0.46	0.01	0.05	0.50	0.00	0.00	0.22

Normalleştrime işlemi yapıldıktan sonra yönetim temelli yaklaşımın alt kriterlerinin bulanık direk ilişki matrisi Denklem (10) yardımıyla oluşturulmuş ve Tablo 29'da gösterilmiştir.

Tablo 30. Yönetim Temelli Yaklaşımın Neden Sonuç İlişkilerinin Değerleri

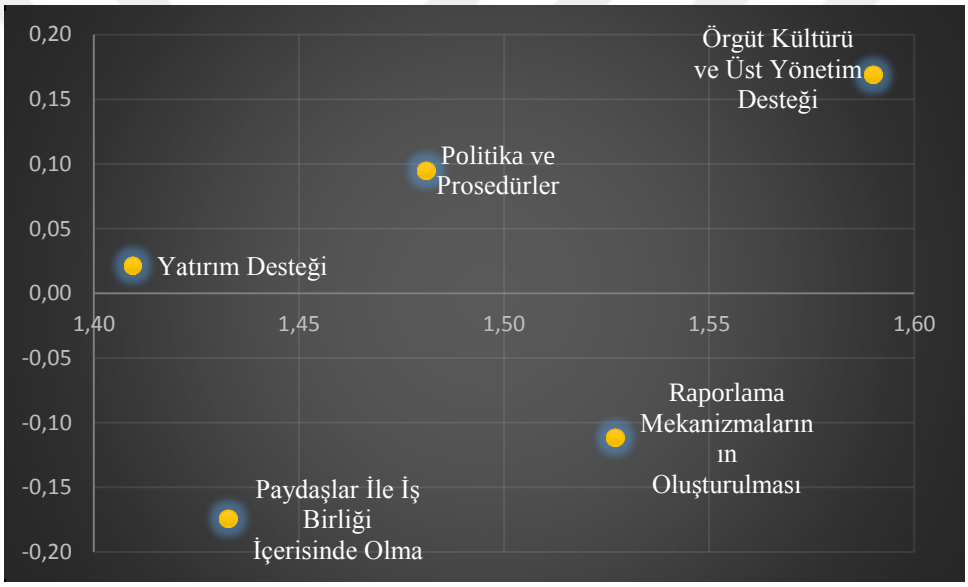
	D_i			R_i			$D_i + R_i$			$D_i - R_i$		
K11	0.08	0.32	2.80	0.04	0.22	2.37	0.13	0.53	5.17	0.04	0.10	0.44
K12	0.05	0.23	2.33	0.07	0.27	2.67	0.11	0.50	5.00	-0.02	-0.04	-0.34
K13	0.06	0.26	2.58	0.04	0.22	2.30	0.10	0.47	4.88	0.01	0.04	0.29
K14	0.04	0.21	2.40	0.05	0.23	2.26	0.09	0.44	4.66	-0.01	-0.02	0.14
K15	0.03	0.18	2.12	0.06	0.26	2.64	0.09	0.44	4.76	-0.03	-0.07	-0.52

Uygulamanın bu adımında alıcı ve gönderici kriterleri belirlemek için Denklem (11) ve Denklem (12) yardımıyla Tablo 30'da gösterildiği gibi neden sonuç değerleri hesaplanır.

Tablo 31. Yönetim Temelli Yaklaşımın Durulaştırma ve Ağırlık Değerleri

	$(\tilde{D}_i + \tilde{R}_i)^{def}$	$(\tilde{D}_i - \tilde{R}_i)^{def}$	w_i	W_i
K11	1.59	0.17	1.28	0.23
K12	1.53	-0.11	1.17	0.21
K13	1.48	0.09	1.10	0.20
K14	1.41	0.02	0.99	0.18
K15	1.43	-0.17	1.04	0.19

Uygulamanın son adımında ise D_i + R_i ve D_i - R_i değerleri durulaştırılarak kriterlerin önem ağırlıkları Tablo 31'deki gibi hesaplanır. Kriterler arasındaki neden sonuç ilişki diyagramı ise aşağıda gösterilmiştir.



Şekil 19. Neden Sonuç Diyagramı

Şekil 19'da gösterildiği üzere neden sonuç diyagramına göre; *paydaşlar ile iş birliği içerisinde olma* en çok etkilenen ve alıcıyken *örgüt kültürü ve üst yönetim desteği* ise en çok etkileyen ve gönderici konumunda en önemli kriterdir. Etkileyen diğer kriterler *politika ve prosedürler* ile *yatırım desteği* iken etkilenen diğer kriter ise *raporlama mekanizmalarının oluşturulması* kriteridir.

Tablo 32. Alt Kriterlerin Nihai Ağırlıklarının Belirlenmesi

Ana Kriterler	**Alt Kriterler**	**Ağırlıklar (w_i)**
İnsan Temelli Yaklaşım (0.33)	Farkındalık (0.21)	0.07
	Rol Ayrımı ve Sorumluluk (0.21)	0.07
	Eğitim (0.20)	0.06
	Çalışan Yetkinliği (0.23)	0.08
	Çalışan İklimi (0.15)	0.05
Teknoloji Temelli Yaklaşım (0.32)	Ağ Altyapısı Yönetimi (0.22)	0.07
	Yazılım Varlıkları Yönetimi (0.23)	0.07
	Yedekleme Mekanizmaları (0.19)	0.06
	Erişim yönetimi (0.18)	0.06
	Kötü Amaçlı Yazılım Savunması (0.19)	0.06
Yönetim Temelli Yaklaşım (0.35)	Örgüt Kültürü ve Üst Yönetim Desteği (0.23)	0.08
	Raporlama Mekanizmalarının Oluşturulması (0.21)	0.07
	Politikalar ve Prosedürler (0.20)	0.07
	Yatırım Desteği (0.18)	0.06
	Paydaşlar İle İş Birliği İçerisinde Olma (0.19)	0.07

Bulanık DEMATEL'in bütün adımları uygulandıktan sonra ana kriterlere ve alt kriterlere ait nihai ağırlıklar Tablo 32'de gösterilmiştir.

4.2. PROMETHEE VE BULANIK PROMETHEE YÖNTEMİNİN UYGULANMASI

Bulanık DEMATEL yönteminin uygulanmasının ardından elde edilen kriter ağırlıkları ile Uzman görüşleri sonucu oluşturulan denizcilik sektörünün paydaşlarının karşılaştırma adımları aşağıdaki gibi gösterilmiştir.

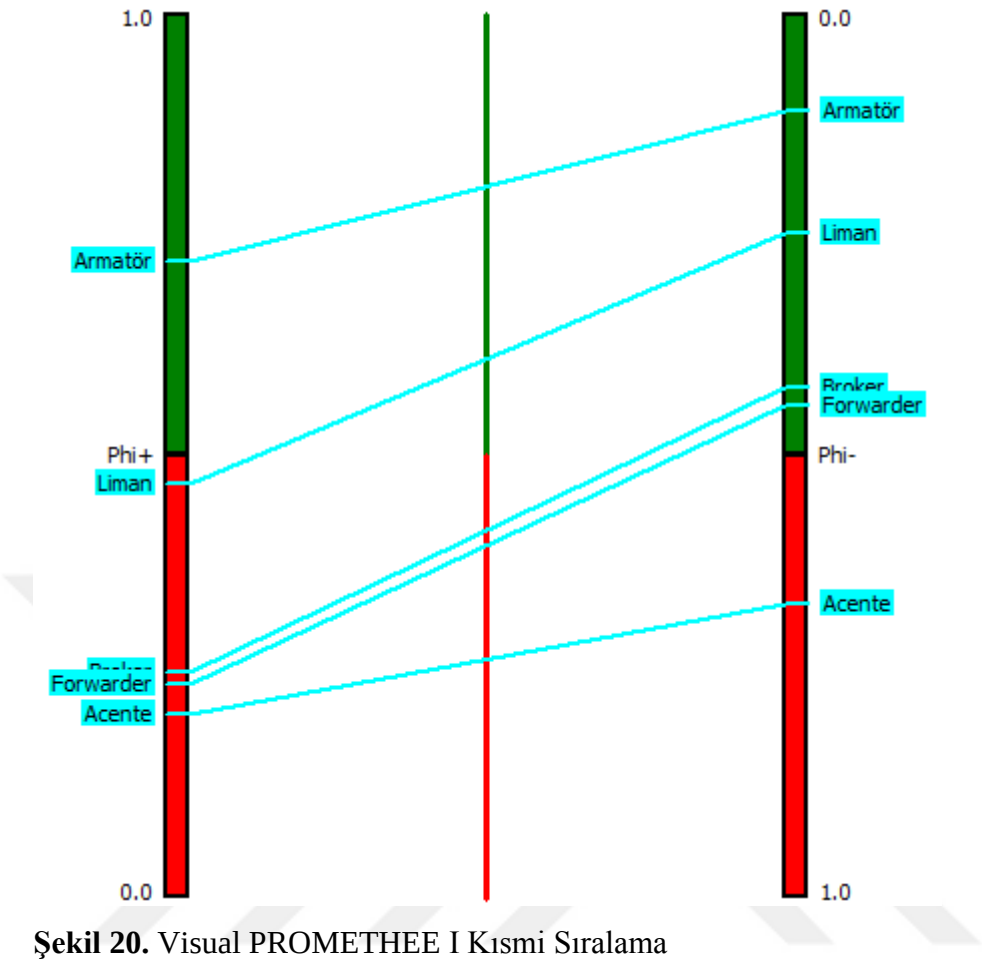
Tablo 33. Alternatiflerin Siber Risk Değerlendirmelerinin Dilsel Değişkenleri

Kriterler	**Firma Tipi**	**Liman (P1)**	**Armatör (P2)**	**Forwarder (P3)**	**Acente (P4)**	**Broker (P5)**
Eğitim (K1)		O (0.50-0.20-0.15)	Bİ (0.65-0.15-0.15)	K (0.15-0.15-0.15)	O (0.50-0.20-0.15)	K (0.15-0.15-0.15)
Farkındalık (K2)		O (0.50-0.20-0.15)	O (0.50-0.20-0.15)	O (0.50-0.20-0.15)	K (0.15-0.15-0.15)	O (0.50-0.20-0.15)
Rol Ayrımı ve Sorumluluk (K3)		O (0.50-0.20-0.15)	Bİ (0.65-0.15-0.15)	BK (0.30-0.15-0.20)	K (0.15-0.15-0.15)	ÇK (0-0-0.15)
Çalışan Yetkinliği (K4)		BK (0.30-0.15-0.20)	İ (0.80-0.15-0.20)	Bİ (0.65-0.15-0.15)	Bİ (0.65-0.15-0.15)	Bİ (0.65-0.15-0.15)
Çalışan İklimi (K5)		Bİ (0.65-0.15-0.15)	K (0.15-0.15-0.15)	Bİ (0.65-0.15-0.15)	İ (0.80-0.15-0.20)	O (0.50-0.20-0.15)

Tablo 33. Alternatiflerin Siber Risk Değerlendirmelerinin Dilsel Değişkenleri Devam

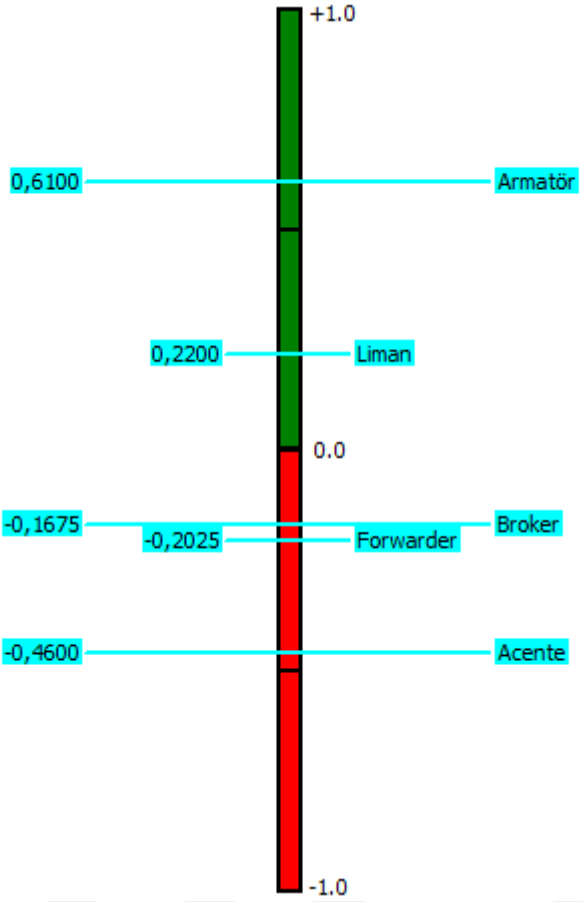
Ağ Alt Yapısı Yönetimi (K6)	O (0.50-0.20-0.15)	Bİ (0.65-0.15-0.15)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)
Yazılım Varlıkları Yönetimi (K7)	O (0.50-0.20-0.15)	O (0.50-0.20-0.15)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)	BK (0.30-0.15-0.20)
Yedekleme Mekanizmaları (K8)	Bİ (0.65-0.15-0.15)	O (0.50-0.20-0.15)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15))
Erişim Yönetimi (K9)	O (0.50-0.20-0.15)	İ (0.80-0.15-0.20)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)
Kötü Amaçlı Yazılım Savunması (K10)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)
Örgüt Kültürü ve Üst Yönetim Desteği (K11)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)	K (0.15-0.15-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)
Raporlama Mekanizmalarının Oluşturulması (K12)	Bİ (0.65-0.15-0.15)	Bİ (0.65-0.15-0.15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)	BK (0.30-0.15-0.20)
Politikalar ve Prosedürler (K13)	O (0.50-0.20-0.15)	İ (0.80-0.15-0.20)	O (0.50-0.20-0.15)	ÇK (0-0-0.15)	K (0.15-0.15-0.15)
Yatırım Desteği (14)	O (0.50-0.20-0.15)	Bİ (0.65-0.15-0.15)	ÇK (0-0-0.15)	K (0.15-0.15-0.15)	K (0.15-0.15-0.15)
Paydaşlar İle İş Birliği İçerisinde Olma (K15)	BK (0.30-0.15-0.20)	O (0.50-0.20-0.15)	ÇK (0-0-0.15)	K (0.15-0.15-0.15)	BK (0.30-0.15-0.20)

Uzman görüşleri sonucu elde edilen dilsel ifadeler üçgensel verilere çevrilerek Tablo 33'de gösterilmiştir. PROMETHEE yönteminin tercih fonksiyonlarından beşinci tip Liner fonksiyon tercih edilmiş olup, verilere en uygun olarak q değeri 0, p değeri ise 0.7 olarak alınmıştır. Bulanık PROMETHEE yönteminden önce dilsel değişkenler Visual PROMETHEE programı ile değerlendirilmiş ve sonuçlar aşağıdaki gibidir.



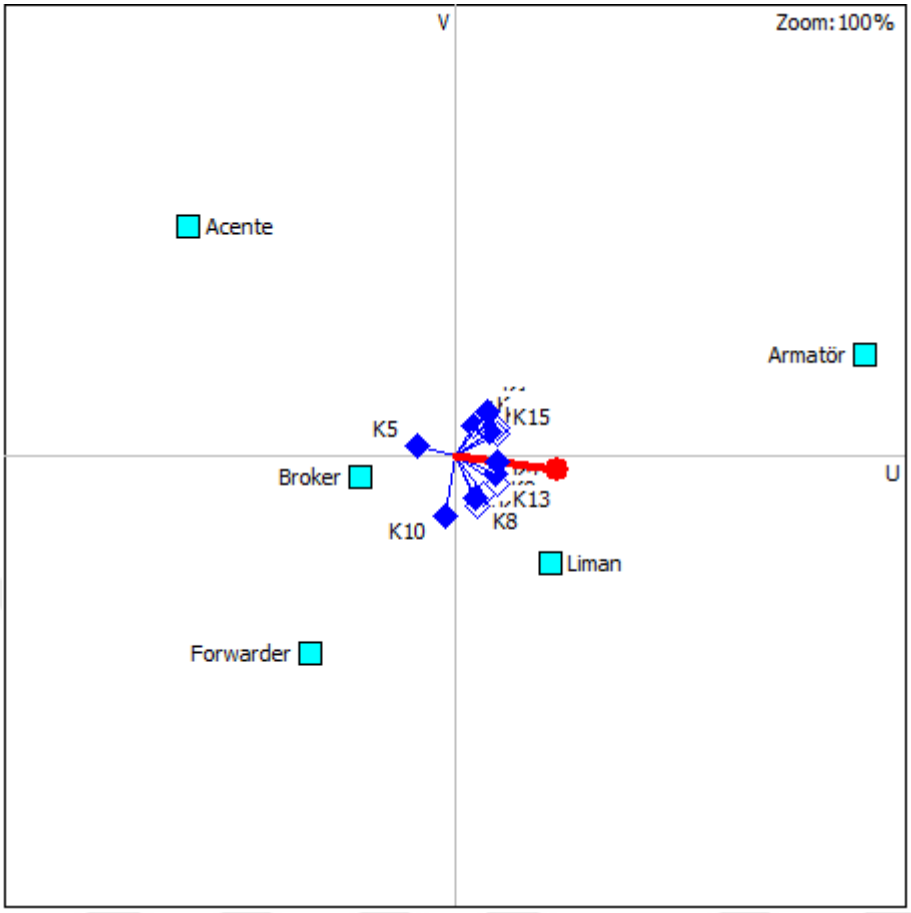
Şekil 20. Visual PROMETHEE I Kısmi Sıralama

Kısmi sıralamalar Şekil 20'de gösterilmiş olup pozitif akımlar ile değerlendirilen alternatiflerin bir diğerine olan üstünlükle gözükmektedir. Kısmi sıralama önceliklerinde *armatör* ve *liman* paydaşları diğerlerine göre daha üstün gözükmektedir.



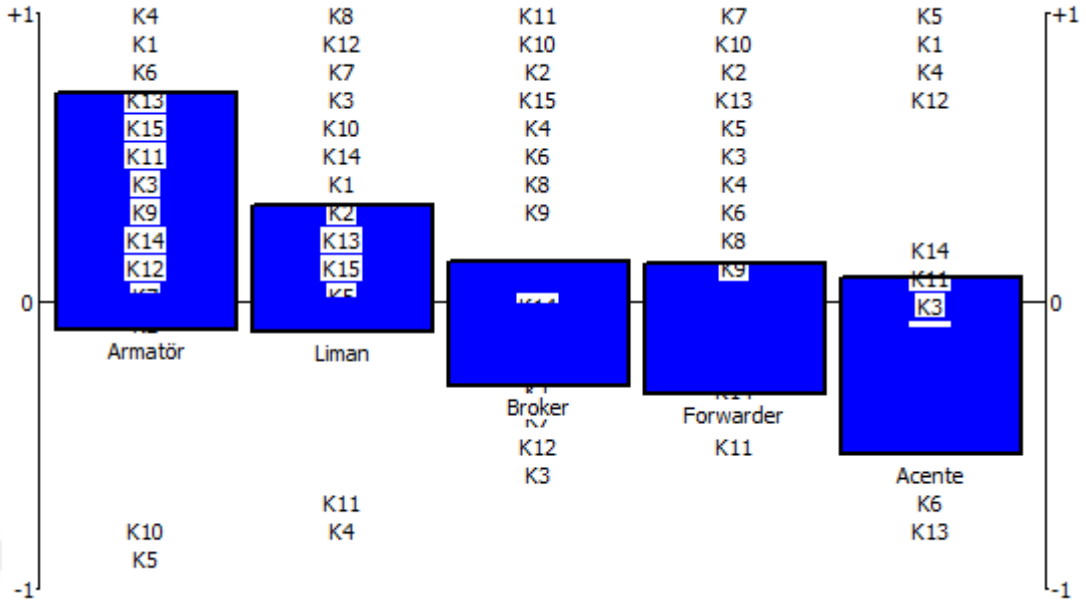
Şekil 21. Visual PROMETHEE II Tam Sıralama

Şekil 21'de görüldüğü üzere pozitif ve negatif akımlara bakılarak net bir sırlama yapılmıştır. Negatif akımlarda *broker*, *forwarder* ve *acente* paydaşları gözükmektedir. 0 ile 1 arasında ise pozitif akımlarda sırasıyla *armatör* ve *liman* paydaşları bulunmakta ve negatif akımlarda bulunan paydaşlara göre net üstünlükleri gözükmektedir.



Şekil 22. Visual PROMETHEE GAIA Ekranı

GAIA ekranı ile problemin çözümü iki boyutlu olarak Şekil 22'de gösterilmiş olup kriterler incelendiğinde çoğunluğunun birbirine yakın olduğu yani aralarında çok fazla birbirine üstünlüklerinin bulunmadığı gözlenmektedir. Kriterlerin çoğunluk olarak *armatör* ve *liman* paydaşlarının etrafında kümelenmekte olduğu gözlenmekte ayrıca kırmızı kalın doğru en optimal seçimleri göstermektedir. Bu düzlemde tek tek veya toplu olarak kriterlere bakılarak en doğru seçim gerçekleştirilebilmektedir.



Şekil 23. Visual PROMETHEE Rainbow Ekranı

Yukarıdaki Şekil 23 incelendiğinde paydaşlara göre hangi kriterlerin negatif yönlü hangilerinin pozitif yönlü oldukları görülmektedir. Örneğin; *armatör* paydaşını incelediğimizde *çalışan iklimi* ve *kötü amaçlı yazılım savunması* kriterleri negatif yönlü iken diğer kriterler pozitif yönlüdür.

	action	Phi	Phi+	Phi-
1	Armatör	0,6100	0,7200	0,1100
2	Liman	0,2200	0,4675	0,2475
3	Broker	-0,1675	0,2550	0,4225
4	Forwarder	-0,2025	0,2400	0,4425
5	Acente	-0,4600	0,2075	0,6675

Şekil 24. Visual PROMETHEE Akış Değerleri

Şekil 24'te görüldüğü üzere paydaşların birbirlerine pozitif ve negatif üstünlük değerleri ve net üstünlük değerleri hesaplanmış olup her ne kadar *broker* ve *forwarder* paydaşlarının üstünlük değerleri birbirine çok yakın olsa da *Armatör>Liman>Broker>Forwarder>Acente* şeklinde sıralanmıştır.

Paydaşlar ve kriterlere ilişkin veriler Tablo 33'te gösterildiği Şekilde oluşturulmuş ve dilsel ifadelerin üçgensel karşılıkları Tablo 10'dan yararlanılarak

karşılıkları yazılmıştır. Bulanık PROMETHEE'nin çözümünde öncelikle paydaşların kriterlere göre sapma değerleri aşağıdaki gibi bulunmuştur.

Tablo 34. Paydaşların Kriterlere Göre Sapma Değerleri

	K1			K2			K3			K4			K5		
P1-P1	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.30	0.40	0.00	0.30	0.30
P1-P2	-0.15	0.35	0.30	0.00	0.40	0.30	-0.15	0.35	0.30	-0.50	0.30	0.40	0.50	0.30	0.30
P1-P3	0.35	0.35	0.30	0.00	0.40	0.30	0.20	0.35	0.35	-0.35	0.30	0.35	0.00	0.30	0.30
P1-P4	0.00	0.40	0.30	0.35	0.35	0.30	0.35	0.35	0.30	-0.35	0.30	0.35	-0.15	0.30	0.35
P1-P5	0.35	0.35	0.30	0.00	0.40	0.30	0.50	0.20	0.30	-0.35	0.30	0.35	0.15	0.35	0.30
	K6			K7			K8			K9			K10		
P1-P1	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.30	0.30	0.00	0.40	0.30	0.00	0.40	0.30
P1-P2	-0.15	0.35	0.30	0.00	0.40	0.30	0.15	0.35	0.30	-0.30	0.35	0.35	0.20	0.35	0.35
P1-P3	0.00	0.40	0.30	0.00	0.40	0.30	0.15	0.35	0.30	0.00	0.40	0.30	0.00	0.40	0.30
P1-P4	0.20	0.35	0.35	0.20	0.35	0.35	0.35	0.30	0.35	0.20	0.35	0.35	0.20	0.35	0.35
P1-P5	0.00	0.40	0.30	0.20	0.35	0.35	0.15	0.35	0.30	0.00	0.40	0.30	0.00	0.40	0.30
	K11			K12			K13			K14			K15		
P1-P1	0.00	0.30	0.40	0.00	0.30	0.30	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.30	0.40
P1-P2	-0.20	0.35	0.35	0.00	0.30	0.30	-0.30	0.35	0.35	-0.15	0.35	0.30	-0.20	0.35	0.35
P1-P3	0.15	0.30	0.35	0.35	0.30	0.35	0.00	0.40	0.30	0.50	0.20	0.30	0.30	0.15	0.35
P1-P4	0.00	0.30	0.40	0.15	0.35	0.30	0.50	0.20	0.30	0.35	0.35	0.30	0.15	0.30	0.35
P1-P5	-0.20	0.35	0.35	0.35	0.30	0.35	0.35	0.35	0.30	0.35	0.35	0.30	0.00	0.30	0.40
	K1			K2			K3			K4			K5		
P2-P1	0.15	0.35	0.30	0.00	0.40	0.30	0.15	0.35	0.30	0.50	0.30	0.40	-0.50	0.30	0.30
P2-P2	0.00	0.30	0.30	0.00	0.40	0.30	0.00	0.30	0.30	0.00	0.30	0.40	0.00	0.30	0.30
P2-P3	0.50	0.30	0.30	0.00	0.40	0.30	0.35	0.30	0.35	0.15	0.30	0.35	-0.50	0.30	0.30
P2-P4	0.15	0.35	0.30	0.35	0.35	0.30	0.50	0.30	0.30	0.15	0.30	0.35	-0.65	0.30	0.35
P2-P5	0.50	0.30	0.30	0.00	0.40	0.30	0.65	0.15	0.30	0.15	0.30	0.35	-0.35	0.35	0.30
	K6			K7			K8			K9			K10		
P2-P1	0.15	0.35	0.30	0.00	0.40	0.30	-0.15	0.35	0.30	0.30	0.35	0.35	-0.20	0.35	0.35
P2-P2	0.00	0.30	0.30	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.30	0.40	0.00	0.30	0.40
P2-P3	0.15	0.35	0.30	0.00	0.40	0.30	0.00	0.40	0.30	0.30	0.35	0.35	-0.20	0.35	0.35
P2-P4	0.35	0.30	0.35	0.20	0.35	0.35	0.20	0.35	0.35	0.50	0.30	0.40	0.00	0.30	0.40
P2-P5	0.15	0.35	0.30	0.20	0.35	0.35	0.00	0.40	0.30	0.30	0.35	0.35	-0.20	0.35	0.35
	K11			K12			K13			K14			K15		
P2-P1	0.20	0.35	0.35	0.00	0.30	0.30	0.30	0.35	0.35	0.15	0.35	0.30	0.20	0.35	0.35
P2-P2	0.00	0.40	0.30	0.00	0.30	0.30	0.00	0.30	0.40	0.00	0.30	0.30	0.00	0.40	0.30
P2-P3	0.35	0.35	0.30	0.35	0.30	0.35	0.30	0.35	0.35	0.65	0.15	0.30	0.50	0.20	0.30
P2-P4	0.20	0.35	0.35	0.15	0.35	0.30	0.80	0.15	0.35	0.50	0.30	0.30	0.35	0.35	0.30
P2-P5	0.00	0.40	0.30	0.35	0.30	0.35	0.65	0.30	0.35	0.50	0.30	0.30	0.20	0.35	0.35
	K1			K2			K3			K4			K5		
P3-P1	-0.35	0.35	0.30	0.00	0.40	0.30	-0.20	0.35	0.35	0.35	0.30	0.35	0.00	0.30	0.30
P3-P2	-0.50	0.30	0.30	0.00	0.40	0.30	-0.35	0.30	0.35	-0.15	0.30	0.35	0.50	0.30	0.30
P3-P3	0.00	0.30	0.30	0.00	0.40	0.30	0.00	0.30	0.40	0.00	0.30	0.30	0.00	0.30	0.30
P3-P4	-0.35	0.35	0.30	0.35	0.35	0.30	0.15	0.30	0.35	0.00	0.30	0.30	-0.15	0.30	0.35
P3-P5	0.00	0.30	0.30	0.00	0.40	0.30	0.30	0.15	0.35	0.00	0.30	0.30	0.15	0.35	0.30
	K6			K7			K8			K9			K10		
P3-P1	0.00	0.40	0.30	0.00	0.40	0.30	-0.15	0.35	0.30	0.00	0.40	0.30	0.00	0.40	0.30
P3-P2	-0.15	0.35	0.30	0.00	0.40	0.30	0.00	0.40	0.30	-0.30	0.35	0.35	0.20	0.35	0.35
P3-P3	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30
P3-P4	0.20	0.35	0.35	0.20	0.35	0.35	0.20	0.35	0.35	0.20	0.35	0.35	0.20	0.35	0.35
P3-P5	0.00	0.40	0.30	0.20	0.35	0.35	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30
	K11			K12			K13			K14			K15		
P3-P1	-0.15	0.30	0.35	-0.35	0.30	0.35	0.00	0.40	0.30	-0.50	0.20	0.30	-0.30	0.15	0.35
P3-P2	-0.35	0.35	0.30	-0.35	0.30	0.35	-0.30	0.35	0.35	-0.65	0.15	0.30	-0.50	0.20	0.30

Tablo 34. Paydaşların Kriterlere Göre Sapma Değerleri Devam

P3-P3	0.00	0.30	0.30	0.00	0.30	0.40	0.00	0.40	0.30	0.00	0.00	0.30	0.00	0.00	0.30
P3-P4	-0.15	0.30	0.35	-0.20	0.35	0.35	0.50	0.20	0.30	-0.15	0.15	0.30	-0.15	0.15	0.30
P3-P5	-0.35	0.35	0.30	0.00	0.30	0.40	0.35	0.35	0.30	-0.15	0.15	0.30	-0.30	0.15	0.35
	K1			K2			K3			K4			K5		
P4-P1	0.00	0.40	0.30	-0.35	0.35	0.30	-0.35	0.35	0.30	0.35	0.30	0.35	0.15	0.30	0.35
P4-P2	-0.15	0.35	0.30	-0.35	0.35	0.30	-0.50	0.30	0.30	-0.15	0.30	0.35	0.65	0.30	0.35
P4-P3	0.35	0.35	0.30	-0.35	0.35	0.30	-0.15	0.30	0.35	0.00	0.30	0.30	0.15	0.30	0.35
P4-P4	0.00	0.40	0.30	0.00	0.30	0.30	0.00	0.30	0.30	0.00	0.30	0.30	0.00	0.30	0.40
P4-P5	0.35	0.35	0.30	-0.35	0.35	0.30	0.15	0.15	0.30	0.00	0.30	0.30	0.30	0.35	0.35
	K6			K7			K8			K9			K10		
P4-P1	-0.20	0.35	0.35	-0.20	0.35	0.35	-0.35	0.30	0.35	-0.20	0.35	0.35	-0.20	0.35	0.35
P4-P2	-0.35	0.30	0.35	-0.20	0.35	0.35	-0.20	0.35	0.35	-0.50	0.30	0.40	0.00	0.30	0.40
P4-P3	-0.20	0.35	0.35	-0.20	0.35	0.35	-0.20	0.35	0.35	-0.20	0.35	0.35	-0.20	0.35	0.35
P4-P4	0.00	0.30	0.40	0.00	0.30	0.40	0.00	0.30	0.40	0.00	0.30	0.40	0.00	0.30	0.40
P4-P5	-0.20	0.35	0.35	0.00	0.30	0.40	-0.20	0.35	0.35	-0.20	0.35	0.35	-0.20	0.35	0.35
	K11			K12			K13			K14			K15		
P4-P1	0.00	0.30	0.40	-0.15	0.35	0.30	-0.50	0.20	0.30	-0.35	0.35	0.30	-0.15	0.30	0.35
P4-P2	-0.20	0.35	0.35	-0.15	0.35	0.30	-0.80	0.15	0.35	-0.50	0.30	0.30	-0.35	0.35	0.30
P4-P3	0.15	0.30	0.35	0.20	0.35	0.35	-0.50	0.20	0.30	0.15	0.15	0.30	0.15	0.15	0.30
P4-P4	0.00	0.30	0.40	0.00	0.40	0.30	0.00	0.00	0.30	0.00	0.30	0.30	0.00	0.30	0.30
P4-P5	-0.20	0.35	0.35	0.20	0.35	0.35	-0.15	0.15	0.30	0.00	0.30	0.30	-0.15	0.30	0.35
	K1			K2			K3			K4			K5		
P5-P1	-0.35	0.35	0.30	0.00	0.40	0.30	-0.50	0.20	0.30	0.35	0.30	0.35	-0.15	0.35	0.30
P5-P2	-0.50	0.30	0.30	0.00	0.40	0.30	-0.65	0.15	0.30	-0.15	0.30	0.35	0.35	0.35	0.30
P5-P3	0.00	0.30	0.30	0.00	0.40	0.30	-0.30	0.15	0.35	0.00	0.30	0.30	-0.15	0.35	0.30
P5-P4	-0.35	0.35	0.30	0.35	0.35	0.30	-0.15	0.15	0.30	0.00	0.30	0.30	-0.30	0.35	0.35
P5-P5	0.00	0.30	0.30	0.00	0.40	0.30	0.00	0.00	0.30	0.00	0.30	0.30	0.00	0.40	0.30
	K6			K7			K8			K9			K10		
P5-P1	0.00	0.40	0.30	-0.20	0.35	0.35	-0.15	0.35	0.30	0.00	0.40	0.30	0.00	0.40	0.30
P5-P2	-0.15	0.35	0.30	-0.20	0.35	0.35	0.00	0.40	0.30	-0.30	0.35	0.35	0.20	0.35	0.35
P5-P3	0.00	0.40	0.30	-0.20	0.35	0.35	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30
P5-P4	0.20	0.35	0.35	0.00	0.30	0.40	0.20	0.35	0.35	0.20	0.35	0.35	0.20	0.35	0.35
P5-P5	0.00	0.40	0.30	0.00	0.30	0.40	0.00	0.40	0.30	0.00	0.40	0.30	0.00	0.40	0.30
	K11			K12			K13			K14			K15		
P5-P1	0.20	0.35	0.35	-0.35	0.30	0.35	-0.35	0.35	0.30	-0.35	0.35	0.30	0.00	0.30	0.40
P5-P2	0.00	0.40	0.30	-0.35	0.30	0.35	-0.65	0.30	0.35	-0.50	0.30	0.30	-0.20	0.35	0.35
P5-P3	0.35	0.35	0.30	0.00	0.30	0.40	-0.35	0.35	0.30	0.15	0.15	0.30	0.30	0.15	0.35
P5-P4	0.20	0.35	0.35	-0.20	0.35	0.35	0.15	0.15	0.30	0.00	0.30	0.30	0.15	0.30	0.35
P5-P5	0.00	0.40	0.30	0.00	0.30	0.40	0.00	0.30	0.30	0.00	0.30	0.30	0.00	0.30	0.40

Ortak tercih fonksiyonlarının kriterlere göre karşılaştırılabilmesi için her bir paydaşın kriterlere göre sapma değerleri Tablo 34'te gösterilmiştir.

Tablo 35. Ortak Tercih Fonksiyonlarının Durulaştırılmış Ağırlıksız Değerleri

Ağr.	0.07	0.07	0.06	0.08	0.05	0.07	0.07	0.06	0.06	0.06	0.08	0.07	0.07	0.06	0.07
	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14	K15
P1-P1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1-P2	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P1-P3	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.52	0.00	1.00	0.53
P1-P4	0.00	0.48	0.48	0.00	0.00	0.00	0.00	0.52	0.00	0.00	0.00	0.00	1.00	0.48	0.00
P1-P5	0.48	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.52	0.48	0.48	0.00
P2-P1	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.43	0.00	0.00	0.00	0.43	0.00	0.00
P2-P2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P2-P3	1.00	0.00	0.52	0.00	0.00	0.00	0.00	0.00	0.43	0.00	0.48	0.52	0.43	1.00	1.00
P2-P4	0.00	0.48	1.00	0.00	0.00	0.52	0.00	0.00	1.00	0.00	0.00	0.00	1.00	1.00	0.48
P2-P5	1.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.43	0.00	0.00	0.52	1.00	1.00	0.00
P3-P1	0.00	0.00	0.00	0.52	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P3-P2	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P3-P3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P3-P4	0.00	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00
P3-P5	0.00	0.00	0.53	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.48	0.00	0.00
P4-P1	0.00	0.00	0.00	0.52	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P4-P2	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P4-P3	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.29	0.29
P4-P4	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P4-P5	0.48	0.00	0.29	0.00	0.43	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P5-P1	0.00	0.00	0.00	0.52	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P5-P2	0.00	0.00	0.00	0.00	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
P5-P3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.48	0.00	0.00	0.29	0.53
P5-P4	0.00	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.29	0.00	0.00
P5-P5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Sapma değerlerden yola çıkılarak Denklem (24)'e göre paydalşarın ortak tercih fonksiyonları karşılaştırılarak Denklem (25) ile Yager İndeksine göre durulaştırılmış değerleri ve kriterlerin ağırlıklıları Tablo 35'te gösterilmiştir.

Tablo 36. Paydaş Çiftlerinin Ortak Tercih İndeks Değerleri

	P1	P2	P3	P4	P5
P1	0.000	0.050	0.167	0.193	0.192
P2	0.136	0.000	0.362	0.354	0.322
P3	0.042	0.050	0.000	0.104	0.065
P4	0.042	0.050	0.071	0.000	0.072
P5	0.042	0.024	0.093	0.054	0.000

Denklem (14) yardımıyla paydaş çiftlerinin ortak tercih indeks değerleri hesaplanarak Tablo 36'da gösterilmiştir.

Tablo 37. PROMETHEE I İle Kısmi PROMETHEE II İle Tam Sıralamaların Hesaplanması

	$\phi^+(a)$	$\phi^-(a)$	ϕ_{net}	Tam Sıralama
Liman (P1)	0.150	0.065	0.085	2
Armatör (P2)	0.293	0.044	0.249	1
Forwarder (P3)	0.065	0.173	-0.108	3
Acente (P4)	0.059	0.176	-0.117	5
Broker (P5)	0.053	0.163	-0.110	4

PROMETHEE I ile pozitif ve negatif değerlerinin *armatör* ve *liman* paydaşları diğer paydaşlara, *forwarder* ise *acente* paydaşına Denklem (17), Denklem (18), Denklem (19) şartını sağlamıştır. Denklem (21)' göre *forwarder* ve *acente* paydaşı *broker* paydaşı ile kıyaslanamaz demektir. PROMETHEE II ile net sıralamalar Denklem (23)'ten yararlanılarak pozitif üstünlüklerin negatif üstünlüklerden çıkartılması sonucu elde edilmiştir ve paydaşların üstünlükleri şu şekildedir: *Armatör>Liman>Forwarder>Broker>Acente.* PROMETHEE ve bulanık PROMETHEE yöntemiyle elde edilen üstünlükler arasında bir, iki ve beşinci sıralar aynı sıralamaya sahipken üç ve dördüncü sıralamalarda farklılık olduğu aynı zamanda visual PROMETHEE'ye benzer şekilde üstünlük değerlerinin çok yakın oldukları gözlemlenmektedir.

SONUÇ

Denizcilik sektörünün; zaman tasarrufu, maliyet düşürme, verimlilik gibi hedefler nedeniyle dijitalleşmesi siber riskleri de beraberinde getirmiştir. Gemilerde, limanlarda kullanılan teknolojik sistem ve ekipmanlar, paydaşlar arasında kullanılan iletişim araçları göz önünde bulundurulduğunda denizcilik sektörünün teknolojiye bağımlı hale geldiğini söylemek yanlış olmaz. Özellikle bilgi teknolojilerinde yaşanacak herhangi bir arıza, denizcilik paydaşlarının operasyonel faaliyetlerinde aksamaya, finansal kayıplara ve itibarlarının zedelenmesine sebep olabilir. Siber risklere karşı tetikte olunması, risklerin önüne geçilmesi ve olası zararların minimize edilmesi şirketler açısından stratejik önem arz etmektedir.

Bu çalışmada denizcilik sektöründeki siber risklerin belirlenmesi ve risklerin çözümüne yönelik benimsenmesi gereken yaklaşımların önceliklendirilmesi amaçlanmıştır. Literatür taraması sonucunda siber riskleri ele almanın başlıca yolunun teknolojik, yönetimsel ve insana temelli faktörleri değerlendirmek gerektiği bulgulanmıştır. Dolayısıyla denizcilik sektörünün başlıca aktörleri/temel paydaşları olarak görülen liman işletmeleri, acenteler, brokerler, armatörler ve freight forwarderlerdan oluşan 10 (on) uzmanın görüşü alınarak İnsan Temelli, Teknoloji Temelli ve Yönetim Temelli Yaklaşımın bileşenlerini oluşturan 15 (on beş) alt kriteri değerlendirmeleri talep edilmiş, elde edilen veriler Bulanık DEMATEL yöntemi kullanılarak analiz edilmiştir. Bu yöntem aracılığıyla kriterin ağırlıkları ve aralarındaki neden-sonuç ilişkileri belirlenmiştir. Analiz sonucunda *teknoloji temelli yaklaşımın* en çok etkilenen ve alıcıyken, *yönetim temelli yaklaşımın* ise en çok etkileyen ve gönderici konumunda olup en önemli ana kriter olduğu bulunmuştur.

Yönetim Temelli Yaklaşım'ın alt kriterlerinin analizinde *örgüt kültürü ve üst yönetim desteğinin* en önemli bileşen olduğu görülmektedir. Örgüt kültürü, işletmelerin operasyonel faaliyetlerini ve bilgi güvenliği uygulamalarının verimliliğini etkileyeceğinden, yöneticiler örgüt kültürünü güvenlik uygulamalarını desteklemek ve yönlendirmek için araç olarak kullanabilirler. Masrek ve arkadaşlarının (2017) tanımladığı gibi yönetim desteğinin boyutları bilgi güvenliğine önem verilmesi ve bilgi güvenliğinin taahhüdüdür. Chang ve Lin (2007)'nin de

vurguladığı üzere güvenlik uygulamalarının organizasyon kültürüne proaktif ve spontane bir şekilde günlük operasyonlar için dahil edilmesi organizasyonun başarısını olumlu yönde etkileyebilir. Bu bağlamda Bag vd. (2018)'nin önerdiği üzere üst yönetim, yatırım desteğine öncelik vermeye ve teknoloji yakınsamasını kolaylaştırabilecek bir sistem oluşturmaya ikna edilmelidir. Bag vd.'in önerisi çalışmamızın sonucunu desteklemektedir. Zira *politika ve prosedürler* ile *yatırım desteğinin* de diğer yönetim bileşenlerini etkileyen önemli kriterler olduğu bulanık DEMATEL analizinin sonuçlarındandır. Siber risklerin neler olabileceği ve maruz kalınması durumunda nasıl bir yol haritası çizilmesi gerektiği ile ilgili politikalar ve prosedürler geliştirilmesi işleri oldukça daha kolay kılacaktır. Bu konuda örgüt kültürünün ve üst yönetimin desteği oldukça önemlidir. Gelişen teknolojiyi yakalamak hiç kolay olmasa dahi bu gelişimin beraberinde gelen risklerin çözümü için gerekli yatırımı yapmak sektörü siber risklere karşı koruma noktasında en önemli adımlardan birisidir.

Öte yandan siber risklere karşı İnsan Temelli Yaklaşım geliştirmek çözüm sürecinde ikinci sırada değerlendirilmiştir. Yaklaşımın alt kriterleri değerlendirildiğinde *çalışan yetkinliğinin* diğer alt kriterleri en çok etkileyen kritik faktör olduğu, *eğitim* kriterinin ise onu takip eden diğer etkileyici faktör olduğu bulgulanmıştır. Literatürde sıklıkla atıf yapılmasına rağmen farkındalık etkileyen değil, *rol ayrımı ve sorumluluk ve çalışan iklimi* gibi etkilenen faktör konumunda olduğu sonucuna varılmıştır. Pavlinović vd. (2021)'nin çalışmasında da açıkladığı gibi denizcilerin siber tehditler konusundaki farkındalıkları yüksek olsa dahi teknik ve insan faktörlerinin ciddi bir tam entegrasyonu ve eğitimli, yetiştirilmiş ve bilinçli personel olmadan, güvenilir bir güvenlik sistemi veya güvenlik zorluklarına dayanabilecek herhangi bir sistem olması mümkün değildir. Personelin siber risklerin farkında olması beklenilen bir durumdur, ancak personel aynı zamanda yeterli beceri ve niteliklere de sahip olmalıdır. Bununla beraber, Mraković ve Vojinović (2019)'un da belirttiği gibi, prosedürlere, yetki seviyelerine, fiziksel güvenlik engellerine aşina olmalı ve risk yanıtı konusunda iyi eğitilmiş olmalıdır. İnsan temelli yaklaşıma ilişkin gerekli eğitimler verildiğinde çalışanların algıladığı ikliminin de olumlu hale geleceği ve personelin kendisini daha güvende hissedeceği yorumu yapılabilir. Kechagias, vd. (2022)'nin önerileri de çalışmanın bulgularını kapsamaktadır.

Yazarlara göre gemideki veya karadaki personelin; potansiyel siber riskleri yönetmek için siber güvenlik farkındalığı, becerileri ve yetkinlikleri oluşturma, belirli davranışların nasıl istismar edilebileceğini öğretme ve insanları siber güvenlik ihlallerine yeterince yanıt vermeleri için eğitme kapsamına alınması gerekmektedir. Şirketin eğitim ve insan faktörünün farkındalığı ile ilgili çeşitli prosedürleri ve faaliyetleri bulunması gerekir.

Siber risklerin çözümünde bir diğer yaklaşım olan Teknoloji Temelli Yaklaşım her ne kadar sıralamada son sırada yer alsa da çözüm sürecinde vazgeçilmez bir araçtır. *Ağ altyapısı yönetimi*, teknolojik çözümler arasında ilk sırada yer almakta ardından *erişim yönetimi* ve *kötü amaçlı yazılım savunması* gelmektedir. Burada akıllara ilk 'safety first' ifadesi gelebilir. Açıkça görülen odur gibi ağların ve verilerin kontrollü bir şekilde korunmaya çalışması denizcilik sektöründeki aktörler açısından önem arz etmektedir. Chaudry vd. (2012)'nin çalışmalarında da açıkladıkları üzere erişim kontrolü ve çalışan farkındalığı, güvenlik politikalarının dökümantasyonu ve üst düzey yönetim desteği ağların güvenliğini etkileyen dört temel faktördür. Bu çalışma ve literatür taramasına bağlı olarak alt kriterlerin açıklandığı 2.4.2. başlıkta da açıkça görüldüğü üzere bu üç çözüm yaklaşımının birbirinden bağımsız olamayacağı, bütünsel olarak değerlendirilmesi esas olmalıdır. Gelişen teknolojiyi yakından takip etmek ve sektöre uyarlanmak gelecek saldırılara karşı önlem almada da oldukça önemlidir. Teknolojik riskler ancak yönetimsel önceliklendirme ve insan odaklı bir yaklaşımla çözümlenebilir.

Denizcilik sektörünün alt dallarında hangi tip işletmelerin siber riskler ile mücadeleye daha fazla önem verdiğinin anlaşılması için bir sıralama yöntemi olan bulanık PROMETHEE yöntemi kullanılmış olup liman, armatör, freight forwarder, broker ve acente işletmelerinin siber güvenlik uygulamaları açısından kısmi ve net sıralamaları yapılarak hangilerinin daha fazla tedbirli oldukları ortaya konmuştur. PROMETHEE yönteminin bir uzantısı olan GAIA geometrik gösterimi ile belirlenen kriterlerin küme şeklindeki dağılımı incelendiğinde iki işletme grubu arasında çok fazla farkın bulunmadığı ve kümesel gösterimde kriterlere en yakın olduğundan hem armatör hem de liman işletmelerinin bu kriterlere fazla önem verdiği görülmektedir. Diğer bir ifadeyle, armatör firmalar ve liman işletmeleri siber risklerin yönetimi için

belirlenen kriterlere daha fazla önem verirken, sırası ile forwarder, broker ve acentelerin ise diğerlerine kıyasla negatif yönlü kaldığı ve güvenlik çalışmalarına daha az önem verdikleri ortaya çıkmıştır. Armatör firmaların ve liman işletmelerinin ticari olarak daha büyük ve kurumsallaşmaya daha elverişli olmaları sebebiyle de bu sonuçların elde edilmesi şaşırtıcı değildir.

Siber risklerin yönetiminin, ticari büyüklüklerine bakılmaksızın denizcilik sektörünün alt dallarının her biri için ciddi öneme sahip olması gerekmektedir. Her ne kadar forwarder, broker ve acentelerin siber güvenlik konusuna daha az önem verdikleri gözlemlense de birden fazla paydaş ile ortak çalışma yürütmeleri sebebiyle siber saldırılara uğramaları oldukça olasıdır ve bu durumun sonucunda büyük finansal kayıplara ve sektörel itibar zedelenmelerine maruz kalacakları aşikardır. Bu sebeple denizcilik sektörünün hangi alt dalı olduğu fark etmeksizin siber riskler ile mücadele konusu tüm işletme kolları açısından önem arz etmelidir. Zira armatör ve limanların bu hususa önem veriyor olması bu işletmelerle doğrudan veya dolaylı olarak paydaş olan acente, broker veyahut forwarderlerin de elini taşın altına koymalarını gerektirecek, aksi takdirde herhangi bir zayıf halkanın olması lojistik zinciri hatta tedarik zinciri boyunca diğer tüm işletmelerin de saldırı ve kayıplara maruziyetini de beraberinde getirecektir.

Literatürdeki çalışmalar incelendiğinde denizcilikte siber risklerin zorlukları ve siber riske maruz kalabilecek siber fiziksel sistemlerin açıklandığı bazı çalışmalar olsa da siber risklerle başa çıkmak için dikkat edilmesi gereken kriterler ve bu kriterlerin arasında nasıl bir neden sonuç ilişkisi içerisinde olduklarını belirten bir çalışmaya rastlanmamıştır. Ayrıca denizcilik sektörünün alt dallarının siber risklere bakış açılarının nasıl olduğu konusunda da daha önce herhangi bir çalışmanın yapılmamış olduğu tespit edilmiştir. Çalışma hem bu yönüyle ve hem de kullanılan yöntemlerin bütünleşik olarak denizcilik sektöründe kullanıldığı ilk çalışma olması sebebiyle literatüre katkı vermesi beklenmektedir. Diğer yandan şirket yöneticilerinin de siber risklere ilişkin yaklaşımlarını belirlerken dikkate almaları gereken faktörleri değerlendirmesi sayesinde bu çalışma özel sektör uygulayıcılarının karar alma sürecinde fayda sağlayabilecekleri bir çalışma olmuştur.

Çalışmada denizcilik sektöründeki beş temel paydaş grubuna yer verilmiş olmasına rağmen gelecek çalışmalarda deniz sigorta şirketleri, gemi tedarik firmaları, klas kuruluşları gibi farklı aktörlerin de uzman görüşleri alınarak daha kapsamlı değerlendirmelere yer verilebilir. Türkiye'deki işletmelerin esas alınması çalışmanın temel kısıtıdır. Dolayısıyla ilerleyen dönemlerdeki çalışmalar farklı ülkeler bazında da değerlendirmeler yapabilir. Buna rağmen bulguların anlamlı olması ve faydalı sonuçlar üretmesi çalışmanın amacına uygun olarak sonuçlandığının göstergesidir.

KAYNAKÇA

1. Kitaplar

Agarwal, Nidhi, Ruchika Gupta and Puneet Kumar (2022). Role of ICT in Imparting Quality Education and Curbing Cyber Security Risks During COVID-19 Pandemic. Cyber Security in Intelligent Computing and Communications. Singapore: 337-353, Springer Singapore.

Babica, V., Deniss Sceulovs, Elvira Rustenova (2019. September). Digitalization in maritime industry: prospects and pitfalls. In Workshop on ICTE in Transportation and Logistics (pp. 20-27). Springer, Cham.

Beaumont, Peter (2018). Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR. Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution. UK: 497-516 IGI Global.

Boyes, Hugh and Roy Isbell (2017). Code of practice: Cyber security for ships. UK: Institution of Engineering and Technology.

Boyes, Hugh, Roy Isbell, and Alexandra Luck (2016). Code of practice: cyber security for ports and port systems. London: Department for Transport.

Brans, Jean-Pierre (1982). L'ingénierie de la décision: l'élaboration d'instruments d'aide a la décision. Canada: Université Laval, Faculté des sciences de l'administration.

Collins, Nick (2000). The essential guide to chartering and the dry freight market. United Kingdom: Clarkson Research Studies.

Coulson, E. C. (1991). A Guide For Tanker Brokers. United Kingdom: Clarkson Research Studies Limited.

Fitton, Oliver, Prince Daniel, Germond Basil and Lacy Mark M. (2015). The future of maritime cyber security. Lancaster: Lancaster University.

Fontela, E., ve Gabus, A. (1976). The DEMATEL observer. Geneva: Battelle Geneva Research Center.

Giacomello, G., and Gianluca Pescaroli (2019). Managing human factors. In Cyber resilience of systems and networks (pp. 247-263). Springer, Cham.

Hermann, Mario, Tobias Pentek, and Boris Otto (2015). Design principles for Industrie 4.0 scenarios: a literature review. Dortmund: 45, Technische Universität Dortmund.

Kersten, W., Thorsten Blecker and Christian M. Ringle (2017). Digitalization in supply chain management and logistics: smart and digital solutions for an industry 4.0 environment. Berlin: epubli GmbH.

Korkmaz, Yakup (2008). GMDSS ve Deniz Telsiz İletişimleri. İstanbul: Kendi Yayını.

McNicholas, Michael (2012). Terrorism and commercial transportation: use of ships, cargoes, containers to transport terrorists and materials. Maritime security and defence against terrorism, 98, 51. Amsterdam: IOS Press.

Nathanson, Fred E., J. Patrick Reilly, Marvin N. Cohen (1999). "Radar Design Principles", Second Edition, Mc Graw-Hill, USA: Scitech Publishing, Inc.

Nyrkov, A., Konstantin P. Goloskokov, Elena G. Koroleva, Sergei S. Sokolov, Anton A. Zhilenkov and Sergei Chernyi (2018). Mathematical models for solving problems of reliability maritime system. In Advances in Systems, Control and Automation (pp. 387-394). Singapore: Springer.

Paraskevas, Alexandros (2022). Cybersecurity in travel and tourism: a risk-based approach. In Handbook of e-Tourism (pp. 1605-1628). Cham: Springer International Publishing.
Polemi, Nineta (2017). Port cybersecurity: securing critical information infrastructures and supply chains. Elsevier.
Refsdal, Atle, Bjørnar Solhaug & Ketil Stølen (2015). Cybersecurity. In Cyber-risk management (pp. 29-32). Springer, Cham.
Refsdal, Atle, Bjørnar Solhaug & Ketil Stølen (2015). Cyber-risk management. In Cyber-risk management (pp. 33-47). Springer, Cham.
Schröder-Hinrichs, J. U., Dong-Wook Song, Tiago Fonseca, Khanssa Lagdami, Xiaoning Shi, Karsten Loer (2019). Transport 2040: Automation, technology, employment-The future of work. World Maritime University, Transport, 2040.
Sen, R. (2016). Cyber and information threats to seaports and ships. Maritime Security, 281-302. Elsevier.
Shaikh, Siraj A. (2017). Future of the sea: Cyber security. London United Kingdom: Foresight, Government Office for Science.
Von Altrock, Constantin (1997). Fuzzy logic and neurofuzzy applications in business and finance. USA: Pearson P T R.

2. Makaleler, Bildiriler, Diğer Basılı Yayınlar

Abawajy, Jemal (2014). "User preference of cyber security awareness delivery methods." Behaviour & Information Technology, 33.3, 237-248.
Acciaro, M., Claudio Ferrari, Jasmine SL Lam, Rosario Macario, Athena Roumboutsos, Christa Sys, Alessio Tei & Thierry Vanelslander (2018) "Are the innovation processes in seaport terminal operations successful?" Maritime Policy & Management, 45:6, 787-802, DOI: 10.1080/03088839.2018.1466062
Agrawal, P., Rakesh Narain, and Inayat Ullah (2020). "Analysis of barriers in implementation of digital transformation of supply chain using interpretive structural modelling approach." Journal of Modelling in Management, 15.1, 297-317.
Akbayırlı, K., Durmuş Ali Deveci, Gökçay Balcı, Ercan Kurtuluş (2016). "Container port selection in contestable hinterlands." Journal of ETA Maritime Science, 4(3), 249-265.
Akyuz, E., and Erkan Celik (2015). "A fuzzy DEMATEL method to evaluate critical operational hazards during gas freeing process in crude oil tankers." Journal of Loss Prevention in the Process Industries, 38, 243-253.
Alcaide, J. I., and Ruth Garcia Llave (2020). "Critical infrastructures cybersecurity and the maritime sector." Transportation Research Procedia, 45, 547-554.
Aldasoro, I., Leonardo Gambacorta, Paolo Giudici, Thomas Leach (2022). "The drivers of cyber risk." Journal of Financial Stability, 60, 100989.
Alhayani, B., Sara Taher Abbas, Dawood Zahi Khutar, Husam Jasim Mohammed (2021). "Best ways computation intelligent of face cyber attacks." Materials Today: Proceedings, ISSN 2214-7853, 26-31.
Androjna, A., Tanja Brcko, Ivica Pavic, Harm Greidanus (2020). "Assessing cyber challenges of maritime navigation." Journal of Marine Science and Engineering, 8(10), 776.
Archetti, C., and Lorenzo Peirano (2020). "Air intermodal freight transportation: The freight forwarder service problem." Omega 94, 102040.

Ashraf, I., Yongwan Park, Soojung Hur, Sung Won Kim, Roobaea Alroobaea, Yousaf Bin Zikria, Summera Nosheen 2022). "A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry." IEEE Transactions on Intelligent Transportation Systems, 1-14.

Aslam, S., Michalis P. Michaelides, and Herodotos Herodotou (2020). "Internet of ships: A survey on architectures, emerging applications, and challenges." IEEE Internet of Things journal, 7.10, 9714-9727.

Ayan, Mustafa Serdar (2005). Denizcilik işletmelerinde örgüt kültürü ve İzmir bölgesine yönelik bir araştırma. Yayınlanmamış Doktora Tezi, İzmir: Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.

Babineau, G. L., Rick A. Jones, and Barry Horowitz (2012). "A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions." 2012 IEEE Conference on Technologies for Homeland Security (HST). (pp. 99-104). IEEE.

Bag, S., Arnesh Telukdarie, J.H.C. Pretorius, Shivam Gupta (2018). "Industry 4.0 and supply chain sustainability: framework and future research directions." Benchmarking: An International Journal, 28(5), 1410-1450.

Balcı, Gökçay (2016). "Shipbroker selection criteria of charterers in dry bulk shipping." PROCEEDINGS BOOK, 587.

Balci, G., and Ebru Surucu-Balci (2021). "Blockchain adoption in the maritime supply chain: Examining barriers and salient stakeholders in containerized international trade." Transportation Research Part E: Logistics and Transportation Review, 156, 102539.

Balduzzi, M., Alessandro Pasta, and Kyle Wilhoit (2014). "A security evaluation of AIS automated identification system." Proceedings of the 30th annual computer security applications conference, p. 436-445.

Baran, E., and Gamze Arabelen (2018). "How Demographic Factors Affect Job Satisfaction in Shipping Agencies?: A Research Through İzmir-Based Liner Shipping Agencies." Journal of ETA Maritime Science, 6.3, 229-242.

Baum-Talmor, P., and Momoko Kitada (2022). "Industry 4.0 in shipping: Implications to seafarers' skills and training." Transportation research interdisciplinary perspectives, 13, 100542.

Baygin, M., Hasan Yetis, Mehmet Karakose, Erhan Akin (2016). "An effect analysis of industry 4.0 to higher education." In 2016 15th international conference on information technology based higher education and training (ITHET) (pp. 1-4). IEEE.

Bellman, R. E., and Lotfi Asker Zadeh (1970). "Decision-making in a fuzzy environment." Management science, 17.4, B-141.

Ben Farah, M. A., Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic and Xavier Bellekens (2022). "Cyber security in the maritime industry: a systematic survey of recent advances and future trends." Information, 13(1), 22.

Beyer, R. E., and B. Brummel (2015). "Implementing effective cyber security training for end users of computer networks." Society for Human Resource Management and Society for Industrial and Organizational Psychology, 1-22.

Bhardwaj, G., Ruchika Gupta, Arun Pratap Srivastava, S. Vikram Singh (2021). "Cyber Threat Landscape of G4 Nations: Analysis of Threat Incidents and Response Strategies." In 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 75-79). IEEE.

BIMCO, C., ICS, I., Intermanager, I., ve IUMI, O. (2020). “World Shipping Council: The Guidelines on Cyber Security onboard Ships.” Version 4.

BIMCO, C., ICS, I., ve Intertanko, O. C. I. M. F. (2017). IUMI,“Guidelines on cyber security onboard ships.” Verison 3.

BIMCO (2016). “The Guidelines on Cyber Security Onboard Ships.” Version 2.0.

Bolbot, V., Gerasimos Theotokatos, Evangelos Boulougouris, Dracos Vassalos (2020). “A novel cyber-risk assessment method for ship systems.” Safety Science, 131, 104908.

Bolbot, V., Gerasimos Theotokatos, Luminita Manuela Bujorianu, Evangelos Boulougouris, Dracos Vassalos (2019). “Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review.” Reliability Engineering ve System Safety, 182, 179-193.

Borgia, Eleonora (2014). "The Internet of Things vision: Key features, applications and open issues." Computer Communications, 54, 1-31.

Borio, D., Fabio Dovis, Heidi Kuusniemi, Letizia Lo Presti (2016). “Impact and detection of GNSS jammers on consumer grade satellite navigation receivers.” Proceedings of the IEEE 104(6), 1233-1245.

Boyes, Hugh (2015). “Cybersecurity and cyber-resilient supply chains.” Technology Innovation Management Review, 5(4), 28

Brans, J. P., Ph Vincke, and Bertrand Mareschal (1986). "How to select and how to rank projects: The PROMETHEE method." European journal of operational research, 24.2, 228-238.

Brans, Jean-Pierre, Roy, B., Vincke Ph. (1975). Aide a la decision multicritere. Rev. Belge Statisti., d’Informatique et de Recherche Operationnelle, 15(4).

Caprolu, M., Roberto Di Pietro, Simone Raponi, Savio Sciancalepore, Pietro Tedeschi (2020). “Vessels cybersecurity: Issues, challenges, and the road ahead.” IEEE Communications Magazine, 58(6), 90-96.

Chang, B., Chih-Wei Chang, and Chih-Hung Wu (2011). "Fuzzy DEMATEL method for developing supplier selection criteria." Expert systems with Applications, 38.3, 1850-1858.

Chang, C. H., Christos Kontovas, Qing Yu, Zaili Yang (2021). “Risk assessment of the operations of maritime autonomous surface ships.” Reliability Engineering ve System Safety, 207, 107324.

Ernest, C. S., and Chin-Shien Lin (2007). "Exploring organizational culture for information security management." Industrial management & data systems, 107.3, 438-458.

Chaudhry, P. E., Sohail Chaudhry, and Ronald Reese (2012). “Developing a model for enterprise information systems security.” Economics, Management, and Financial Markets, 7(4), 587–599

Chauhan, A., Amol Singh, and Sanjay Jharkharia (2018). "An interpretive structural modeling (ISM) and decision-making trail and evaluation laboratory (DEMATEL) method approach for the analysis of barriers of waste recycling in India." Journal of the Air & Waste Management Association, 68.2, 100-110.

Christidis, K., and Michael Devetsikiotis (2016). "Blockchains and smart contracts for the internet of things." Ieee Access 4, 2292-2303.

Cross, J. F., and Gordon Meadow (2017). "Autonomous ships 101." Journal of Ocean Technology, 12.3, 23-27.

da Conceição, V. P., Joakim Dahlman, and Ana Navarro (2017). "What is maritime navigation? Unfolding the complexity of a Sociotechnical

System." Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol. 61. No. 1. Sage CA: Los Angeles, CA: SAGE Publications. pp. 267-271.

Dawson, Maurice (2018). "Applying a holistic cybersecurity framework for global IT organizations." Business Information Review, 35(2), 60-67.

de la Peña Zarzuelo, Ignacio (2021). "Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue." Transport Policy, 100, 1-4.

de la Peña Zarzuelo, I., María Jesús Freire Soeane, and Beatriz López Bermúdez (2020). "Industry 4.0 in the port and maritime industry: A literature review." Journal of Industrial Information Integration, 20, 100173.

de Vos, J., Hekkenberg, and Osiris A. Valdez Banda (2021). "The impact of autonomous ships on safety at sea–a statistical analysis." Reliability Engineering ve System Safety, 210, 107558.

Dellios, K., and Dimitrios Papanikas (2014). "Deploying a maritime cloud." IT Professional, 16(5), 56-61.

Demir, K. A., Gözde Döven, and Bülent Sezen (2019). "Industry 5.0 and human-robot co-working." Procedia computer science, 158, 688-695.

Deveci, Durmuş Ali (2002). Konteyner taşımacılığı gemi acenteliği hizmet hatalarını ölçmeye yönelik bir araştırma: İzmir limanındaki gemi acentelerine yönelik uygulama, (Yayınlanmamış Doktora Tezi) İstanbul Üniversitesi Deniz Bilimleri ve İşletmeciliği Ensititüsü, İstanbul.

Deveci, Durmuş Ali (2013). "Deniz ulaştırması: İşletmeler ve işlevler (Maritime transportation: Businesses and functions)." CeritA. DeveciA. EsmerS.(Eds.), Denizcilik İşletmeleri Yönetimi (Maritime Business Management), 23-34.

DiRenzo, J., Dana A. Goward, and Fred S. Roberts (2015). "The little-known challenge of maritime cyber security." In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE.

Dobryakova, L. A., Łukasz S. Lemieszewski, and Evgeny F. Ochin (2018). "GNSS spoofing detection using static or rotating single-antenna of a static or moving victim." IEEE Access, 6, 79074-79081.

Drazovich, L., Liam Brew, and Susanne Wetzel (2021). "Advancing the State of Maritime Cybersecurity Guidelines to Improve the Resilience of the Maritime Transportation System." In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 503-509). IEEE.

Dreyer, P., Therese Jones, Kelly Klima, Jenny Oberholtzer, Aaron Strong, Jonathan William Welburn, Zev Winkelman (2018). "Estimating the global cost of cyber risk." Research Reports RR-2299-WFHF, Rand Corporation.

Emad, G. R., M. Khabir, and M. Shahbakhsh (2020). "Shipping 4.0 and training seafarers for the future autonomous and unmanned ships." In Proceedings of the 21th Marine Industries Conference (MIC2019), Qeshm Island, Iran (pp. 1-2).

Enoch, S. Y., Jang Se Lee, and Dong Seong Kim (2021). "Novel security models, metrics and security assessment for maritime vessel networks." Computer Networks, 189, 107934.

Erstad, E., Runar Ostnes, and Mass Soldal Lund (2021). "An operational approach to maritime cyber resilience." TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.

ESCAP UN (2020). "Enhancing cybersecurity in Asia and the Pacific."

Fan, C., Krzysztof Wróbel, Jakub Montewka, Mateusz Gil, Chengpeng Wan, Di Zhang (2020). "A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships." Ocean Engineering 202, 107188.

Fiotakis, Dimitrios (2004). "Impact of Information Technology upon the Shipbroking Profession, The." Tul. Mar. LJ, 29, 237.

Fisher, W., William C. Barker, Karen Scarfone, Murugiah Souppaya (2022). "Ransomware Risk Management: A Cybersecurity Framework Profile." NISTIR, 8374.

Foerstl, K., Martin C. Schleper and Michael Henke (2017). "Purchasing and supply management: From efficiency to effectiveness in an integrated supply chain." Journal of Purchasing and Supply Management, 23(4).

Fruth, M., and Frank Teuteberg (2017). "Digitization in maritime logistics—What is there and what is missing?." Cogent Business ve Management, 4(1), 1411066.

Gabus, A., ve Fontela, E. (1972). "World problems, an invitation to further thought within the framework of DEMATEL." Battelle Geneva Research Center, Geneva, Switzerland, 1(8).

Garcia-Perez, A., Mick Thurlbeck, and Eddie How (2017). "Towards cyber security readiness in the Maritime industry: A knowledge-based approach." Semantic Scholar, 1-7.

Georgiadou, A., Spiros Mouzakitis, Kanaris Bounas, and Dimitrios Askounis (2020). "A cyber-security culture framework for assessing organization readiness." Journal of Computer Information Systems, 1-11.

Georgiadou, A., Spiros Mouzakitis and Dimitris Askounis (2022). "Working from home during COVID-19 crisis: a cyber security culture assessment survey." Security Journal, 35(2), 486-505.

Glomsvoll, O., and Lukasz K. Bonenberg (2017). "GNSS jamming resilience for close to shore navigation in the Northern Sea." The Journal of Navigation, 70(1), 33-48.

Goumas, M., and V. Lygerou (2000). "An extension of the PROMETHEE method for decision making in fuzzy environment: Ranking of alternative energy exploitation projects." European Journal of Operational Research 123(3), 606-613.

Govender, S. G., Elmarie Kritzinger, and Marianne Loock. (2021). "A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture." Personal and Ubiquitous Computing, 25(5), 927-940.

Gunes, B., Gizem Kayisoglu, and Pelin Bolat (2021). "Cyber security risk assessment for seaports: A case study of a container port." Computers ve Security, 103, 102196.

Guri, M., Gabi Kedma, Assaf Kachlon, Yuval Elovici (2014, October). "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies." In 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE) (pp. 58-67). IEEE.

Hareide, O. S., Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes and Kirsi Helkala (2018). "Enhancing navigator competence by demonstrating maritime cyber security." The Journal of Navigation, 71(5), 1025-1039.

He, W., and Zuopeng Zhang (2019). "Enterprise cybersecurity training and awareness programs: Recommendations for success." Journal of Organizational Computing and Electronic Commerce, 29(4), 249-257.

Heering, D. (2020). "Ensuring cybersecurity in shipping: Reference to Estonian shipowners." TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 14(2).

Heilig, L., Eduardo Lalla-Ruiz, and Stefan Voß (2017). "Digital transformation in maritime ports: analysis and a game theoretic framework." Netnomics: Economic research and electronic networking, 18(2), 227-254.

Hemminghaus, C., J. Bauer, and E. Padilla (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.

Henriette, E., Mondher Feki, and Imed Boughzala (2016, September). "Digital Transformation Challenges." In MCIS (p. 33).

Hogarth Robin, M. (1978). "A note on aggregating opinions." Organizational behavior and human performance, 21(1), 40-46.

Hopcraft, R., and Keith M. Martin (2018). "Effective maritime cybersecurity regulation–the case for a cyber code." Journal of the Indian Ocean Region, 14(3), 354-366.

Hosam, Osama (2022, February). "Intelligent Risk Management using Artificial Intelligence." In 2022 Advances in Science and Engineering Technology International Conferences (ASET) (pp. 1-9). IEEE.

Huang, J. C., Chung-Yuan Nieh, and Hsin-Chuan Kuo (2019). "Risk assessment of ships maneuvering in an approaching channel based on AIS data." Ocean Engineering, 173, 399-414.

Huang, J., Letizia Lo Presti, Beatrice Motella, Marco Pini (2016). "GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky." Ict Express, 2(1), 37-40.

Hutchins, M. J., Raunak Bhinge, Maxwell K. Micali, Stefanie L. Robinson, John W. Sutherland, David Dornfeld (2015). "Framework for identifying cybersecurity risks in manufacturing." Procedia Manufacturing, 1, 47-63.

Iarmolovych, D. Yu (2018). "Maın Characterıstıcs Of Agreements Of Marıne Shıp Agent." Innovation and Entrepreneurship, 53.

Ichimura, Y., Dimitrios Dalaklis, Momoko Kitada, Anastasia Christodoulou (2022). "Shipping in the era of digitalization: Mapping the future strategic plans of major maritime commercial actors." Digital Business, 2(1), 100022.

Iphar, C., Aldo Napoli, and Cyril Ray (2015, October). "Detection of false AIS messages for the improvement of maritime situational awareness." In Oceans 2015-mts/ieee washington (pp. 1-7). IEEE.

Jacq, O., Xavier Boudvin, David Brosset, Yvon Kermarrec, Jacques Simonin (2018, October). "Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre." In 2018 2nd Cyber Security in Networking Conference (CSNet) (pp. 1-8). IEEE.

Jacq, O., Pablo Gimenez Salazar, Kamban Parasuraman, Jarkko Kuusijärvi, Andriana Gkaniatsou, Evangelia Latsa, Angelos Amditis (2021, July). "The Cyber-MAR Project: First Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Cyber Risk Assessment." In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 409-414). IEEE.

Jassbi, J., Farshid Mohamadnejad, and Hossein Nasrollahzadeh (2011). "A Fuzzy DEMATEL framework for modeling cause and effect relationships of strategy map." Expert systems with Applications, 38(5), 5967-5973.

Jeng, Don Jyh-Fu (2015). "Generating a causal model of supply chain collaboration using the fuzzy DEMATEL technique." Computers ve Industrial Engineering, 87, 283-295.

Jeng, D. J. F., and Gwo-Hshiung Tzeng (2012). "Social influence on the use of clinical decision support systems: revisiting the unified theory of acceptance and use of technology by the fuzzy DEMATEL technique." Computers ve Industrial Engineering, 62(3), 819-828.

Jiang, L., Guangyu Huang, Chuanchao Huang, Wei Wang (2019). "Data mining and optimization of a port vessel behavior behavioral model under the Internet of Things." IEEE Access, 7, 139970-139983.

Johnson, Barry (1999). "English in the global maritime distress and safety system." World Englishes, 18(2), 145-157.

Jones, K.D., Kimberly Tam, and Maria Papadaki (2016). "Threats and Impacts in Maritime Cyber Security." Engineering ve Technology Reference, 1-3.

Kalogeraki, E. M., Dimitrios Apostolou, Nineta Polemi, Spyridon Papastergiou (2018). "Knowledge management methodology for identifying threats in maritime/logistics supply chains." Knowledge management research ve practice, 16(4), 508-524.

Karaman, Zehra (2009). İzmir'de gemi acentelerinde çalışanların iş doyumlarının belirlenmesi (Doctoral dissertation, DEÜ Sosyal Bilimleri Enstitüsü), İzmir.

Karamperidis, S., Chronis Kapalidis, and Tim Watson (2021). "Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches." Journal of Marine Science and Engineering, 9(12), 1323.

Karataş, Ç., ve Pelin Sait (2014). "Liman inovasyonları ve bilgi sistemleri: Türkiye limanları üzerine bir araştırma." Journal of Entrepreneurship and Innovation Management, 3(2).

Kardakova, M., Ilya Shipunov, Anatoly Nyrkov, Tatyana Knysh (2018, December). "Cyber security on sea transport." In Energy Management of Municipal Transportation Facilities and Transport (pp. 481-490). Springer, Cham.

Katsilieris, F., Paolo Braca, and Stefano Coraluppi (2013, July). "Detection of malicious AIS position spoofing by exploiting radar information." In proceedings of the 16th international conference on information fusion (pp. 1196-1203). IEEE.

Kavallieratos, G., Vasiliki Diamantopoulou, and Sokratis K. Katsikas (2020). "Shipping 4.0: Security requirements for the cyber-enabled ship." IEEE Transactions on Industrial Informatics, 16(10), 6617-6625.

Kechagias, E., Georgios Chatzistelios, Georgios A. Papadopoulos, Panagiotis Apostolou (2022). "Digital Transformation of the Maritime Industry: A Cybersecurity Systemic Approach." International Journal of Critical Infrastructure Protection, 100526..

Kessler, G. C., J. Philip Craiger, and Jon C. Haass (2018). "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system." TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 12(3), 429.

Koukaki, T., and Alessio Tei (2020). "Innovation and maritime transport: A systematic review." Case Studies on Transport Policy, 8(3), 700-710.

Kreutz, D., Fernando MV Ramos and Paulo Verissimo (2013). "Towards secure and dependable software-defined networks." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking vol. 42.

Kshetri, Nir (2018). "1 Blockchain's roles in meeting key supply chain management objectives." International Journal of Information Management, 39, 80-89.
Kuhna, K., Salih Bicakci, and Siraj Ahmed Shaikh (2021). "COVID-19 digitization in maritime: understanding cyber risks." WMU Journal of Maritime Affairs, 20(2), 193-214.
Kuhnb, K., Jeptoo Kipkech, and Siraj Shaikh (2021). "Maritime Ports and Cybersecurity." Maritime Transport and ITS Solutions in Port Logistics; Fiorini, M., Gupta, N., Eds.
Kure, H. I., Shareeful Islam, and Mohammad Abdur Razzaque (2018). "An integrated cyber security risk management approach for a cyber-physical system." Applied Sciences, 8(6), 898.
Lagouvardou, Sotiria (2018). "Maritime Cyber Security: concepts, problems and models." Master Thesis, Kongens Lyngby, Copenhagen.
Lallie, H. S., Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Bellekens (2021). "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." Computers ve Security, 105, 102248.
Lambrou, M., Daisuke Watanabe and Junya Iida (2019). "Shipping digitalization management: conceptualization, typology and antecedents." Journal of Shipping and Trade, 4(1), 1-17.
Larsen, M. H., and Mass Soldal Lund (2021). "Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review." IEEE Access, 9 144895-144905.
Latino, M. E., and Marta Menegoli (2022). "Cybersecurity in the food and beverage industry: A reference framework." Computers in Industry, 141, 103702.
Lee, E. S., ve and Dong-Wook Song (2010). "Knowledge management for maritime logistics value: discussing conceptual issues." Marit. Pol. Mgmt., 37(6), 563-583.
Le Téno, J. F., and Bertrand Mareschal (1998). "An interval version of PROMETHEE for the comparison of building products' design with ill-defined data on environmental quality." European Journal of Operational Research, 109(2), 522-529.
Legner, C., Torsten Eymann, Thomas Hess, Christian Matt, Tilo Böhmann, Paul Drews, Alexander Mädche, Nils Urbach & Frederik Ahlemann (2017). "Digitalization: opportunity and challenge for the business and information systems engineering community." Business ve information systems engineering, 59(4), 301-308.
Lehto, M., Pekka Neittaanmäki, Jouni Pöyhönen, Aarne Hummelholm (2022). "Cyber Security in Healthcare Systems." In Cyber Security (pp. 183-215). Springer, Cham.
Lei, A., Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P. Anyigor Ogah, Zhili Sun (2017). "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems." IEEE Internet of Things Journal, 4(6), 1832-1843.
Liu, G., Rodrigo Perez, Jesus A. Muñoz, Francisco Regueira (2016). "Internet of ships: the future ahead." World Journal of Engineering and Technology, 4(03), 220.
Liu, N., Alexandros Nikitas, and Simon Parkinson (2020). "Exploring expert perceptions about the cyber security and privacy of Connected and

Autonomous Vehicles: A thematic analysis approach." Transportation research part F: traffic psychology and behaviour, 75, 66-86.
Liu, Y., Zirui Lan, Jian Cui, Gopala Krishnan, Olga Sourina, Dimitrios Konovessis, Hock Eng Ang, Wolfgang Mueller-Wittig (2020). "Psychophysiological evaluation of seafarers to improve training in maritime virtual simulator." Advanced Engineering Informatics, 44, 101048.
Liu, Y., Sihai Li, Qiangwen Fu and Zhenbo Liu (2018). "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system." Sensors, 18(5), 1433.
Lund, M. S., Odd Sveinung Hareide, and Øyvind Jøsok (2018). "An attack on an integrated navigation system." Necesse 2018, Vol 3, Issue 2, 149-163
Marcos, E. P., Stefano Caizzone, Andriy Konovaltsev, M. Cuntz, Wahid Elmarissi, Kazeem A. Yinusa, M. Meurer (2018, April). "Interference awareness and characterization for GNSS maritime applications." In 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS) (pp. 908-919). IEEE.
Mazzarella, F., Michele Vespe, Dario Tarchi, Giuseppe Aulicino, Antonio Vollero (2016, July). "AIS reception characterisation for AIS on/off anomaly detection." In 2016 19th International Conference on Information Fusion (FUSION) (pp. 1867-1873). IEEE.
McGillivary, Phil (2018). "Why maritime cybersecurity is an ocean policy priority and how it can be addressed." Marine Technology Society Journal, 52(5), 44-57.
Mednikarov, B., Yuliyan Tsonev, and Andon Lazarov (2020). "Analysis of Cybersecurity Issues in the Maritime Industry." Information ve Security, 47(1), 27-43.
Medina, D., Christoph Lass, Emilio Perez Marcos, Ralf Ziebold, Pau Closas, Jesus Garcia (2019, July). "On GNSS jamming threat from the maritime navigation perspective." In 2019 22th International Conference on Information Fusion (FUSION) (pp. 1-7). IEEE.
Meland, P. H., K. Bernsmed, E. Wille, Ø.J. Rødseth & D.A. Nesheim (2021). "A retrospective analysis of maritime cyber security incidents." TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.
Meland, P. H., Dag Atle Nesheim, Karin Bernsmed, Guttorm Sindre (2022). "Assessing cyber threats for storyless systems." Journal of Information Security and Applications, 64, 103050.
Melnyk, O., Svitlana Onyshchenko, Nataliia Pavlova, Oleksandra Kravchenko, Svitlana Borovyk (2022). "Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System." International Journal of Computer Science and Network Security, 22(03), 135-140.
Middleton, Allison (2014). "Hide and seek: managing automatic identification system vulnerabilities." Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea, 71(4).
Möller, D. P., Isabell A. Jehle, Jens Froese, Andreas Deutschmann, Tobias Koch (2018, May). "Securing Maritime Traffic Management." In 2018 IEEE International Conference on Electro/Information Technology (EIT) (pp. 0453-0458). IEEE.
Mraković, I., and Ranko Vojinović (2019). "Maritime cyber security analysis–How to reduce threats?" Transactions on maritime science, 8(01), 132-139.

Mraković, I., and Ranko Vojinović (2020). "Evaluation of Montenegrin Seafarer's Awareness of Cyber Security." Transactions on Maritime Science, 9(02), 206-216.

Msc, E. E. L., E. Eric den Breejen Msc, and J. Hans van den Broek PhD (2019, October). "A Business Process Framework and Operations Map for Maritime Autonomous and Unmanned Shipping: MAUSOM." In Journal of Physics: Conference Series (Vol. 1357, No. 1, p. 012017). IOP Publishing.

Munim, Z. H., Okan Duru, and Enna Hirata (2021). "Rise, Fall, and Recovery of Blockchains in the Maritime Technology Space." Journal of Marine Science and Engineering, 9(3), 266.

Nahavandi, Saeid (2019). "Industry 5.0—A human-centric solution." Sustainability, 11(16), 4371.

Nakamoto, Satoshi (2008). "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review, 21260.

Nguyen, D., Rodolphe Vadaine, Guillaume Hajduch, René Garello, Ronan Fablet (2018, October). "A multi-task deep learning architecture for maritime surveillance using AIS data streams." In 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA) (pp. 331-340). IEEE.

NIST (2018). "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology, Version 1.1.

Omitola, T., Abdolbaghi Rezazadeh, and Michael Butler (2019, August). "Making (implicit) security requirements explicit for cyber-physical systems: A maritime use case security analysis." In International Conference on Database and Expert Systems Applications (pp. 75-84). Springer, Cham.

Orhon, D. (2019). Avrupa Birliği ve Türkiye'de Denizcilik Sektöründe Rekabet Hukuku Düzenlemelerinin İncelenmesi. (Avrupa Birliği Uzmanlığı Tezi). T.C. Ulaştırma ve Altyapı Bakanlığı Avrupa Birliği ve Dış İlişkiler Genel Müdürlüğü, Ankara.

Özaydın, Nazlı Gülfem Gidener (2016). "Gemi Acenteliği Sektöründe Yaşanan Hizmet Problemlerinin İncelenmesi." Dokuz Eylül Üniversitesi Denizcilik Fakültesi Dergisi, 8(1), 83-96

Pandey, N., and Abhipsa Pal (2020). "Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice." International journal of information management, 55, 102171.

Park, D. J., Jeong-Bin Yim, Hyeong-Sun Yang, Chun-ki Lee (2020). "Navigators' errors in a ship collision via simulation experiment in South Korea." Symmetry, 12(4), 529.

Patil, S. K., and Ravi Kant (2014). "A hybrid approach based on fuzzy DEMATEL and FMCDM to predict success of knowledge management adoption in supply chain." Applied Soft Computing, 18, 126-135.

Pavlinović, M., Maja Račić, and Ivan Karin (2021, August). "Cyber Risks in Maritime Industry–Case Study of Croatian Seafarers." In International Conference on Human Interaction and Emerging Technologies (pp. 108-113). Springer, Cham.

Polatidis, N., Michalis Pavlidis, and Haralambos Mouratidis (2018). "Cyber-attack path discovery in a dynamic supply chain maritime risk management system." Computer Standards ve Interfaces, 56, 74-82.

Potamos, G., Adamantini Peratikou and Stavros Stavrou (2021, July). "Towards a Maritime Cyber Range training environment." In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 180-185). IEEE.

Prasad, Krishna (2008). "Changıng Role Of Shıp-Brokers A study of the impact of modern communication in practical ship-broking."

Pisanias, N., and Leslie Willcocks (1999). "Understanding slow Internet adoption:'infomediation'in ship-broking markets." Journal of Information Technology, 14(4), 399-413.

Park, C., Wenming Shi, Wei Zhang, Christas Kontovas , Chia-Hsun Chang (2019). "Cybersecurity in the maritime industry: A literature review." In 20th Commemorative Annual General Assembly, AGA 2019-Proceedings of the International Association of Maritime Universities Conference, IAMUC 2019 (pp. 79-86).

Pöyhönen, J., and Martti Lehto (2022). "Assessment of Cybersecurity Risks: Maritime Automated Piloting Process." In The proceedings of the 17th international conference on cyber warfare and security (Vol. 17). Academic Conferences International Ltd.

Pranggono, B., and Abdullahi Arabo (2021). "COVID-19 pandemic cybersecurity issues." Internet Technology Letters, 4(2), e247.

Progoulakis, I., Paul Rohmeyer, and Nikitas Nikitakos (2021). "Cyber Physical Systems Security for Maritime Assets." Journal of Marine Science and Engineering, 9(12), 1384.

Ray, C., Romain Gallen, Clément Iphar, Aldo Napoli, Alain Bouju (2015, May). D"eAIS project: Detection of AIS spoofing and resulting risks." In OCEANS 2015-Genova (pp. 1-6). IEEE.

Relling, T., Margareta Lützhöft, Runar Ostnes & Hans Petter Hildre. (2018, July). "A human perspective on maritime autonomy." In International Conference on Augmented Cognition (pp. 350-362). Springer, Cham.

Rose, A., and Dan Wei (2013). "Estimating the economic consequences of a port shutdown: the special role of resilience." Economic Systems Research, 25(2), 212-232.

Rothenberger, Kenneth E. (2016). A quantitative study of perceptions about leadership competencies of IT project managers (Doctoral dissertation, Capella University).

Rüßmann, M., Markus Lorenz, Philipp Gerbert, Manuela Waldner, Jan Justus, Pascal Engel, and Michael Harnisch (2015). "Industry 4.0: The future of productivity and growth in manufacturing industries." Boston consulting group, 9(1), 54-89.

Sayed, M. A. A., and Mansura Akter (2022). "An Overview of Ship Brokering and Chartering and its Challenges in Bangladesh." ZENITH International Journal of Multidisciplinary Research, 12(5), 1-18.

Schmidt, D., Kenneth Radke, Seyit Camtepe, Ernest Foo, Michał Ren (2016). "A survey and analysis of the GNSS spoofing threat and countermeasures." ACM Computing Surveys (CSUR), 48(4), 1-31.

Senarak, Chalermpong (2021). "Port cybersecurity and threat: A structural model for prevention and policy development." The Asian Journal of Shipping and Logistics, 37(1), 20-36.

Sepehri, A., Hadi Rezaei Vandchali, Atiq W. Siddiqui, Jakub Montewka (2021). "The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review." Ocean Engineering, 110162.

Sfakianakis, A., Christos Douligeris, Louis Marinos, Marco Lourenço, and Omid Raghimi (2019). "Enisa threat landscape report 2018: 15 top cyberthreats and trends." DOI, 10, 622757.

Singh, Hansdeep (2019). Cyber Securıty In Marıtıme Industry The Exposures, Risks, Preventions and Legal Scenario (Master's thesis).

Shahbakhsh, M., Gholam Reza Emad, and Stephen Cahoon (2022). "Industrial revolutions and transition of the maritime industry: The case of Seafarer's role in autonomous shipping." The Asian Journal of Shipping and Logistics, 38(1), 10-18.

Shang, K. C., and Chin-Shan Lu (2012). "Customer relationship management and firm performance: an empirical study of freight forwarder services." Journal of Marine Science and Technology, 20(1), 8.

Shapiro, L. R., Marie-Helen Maras, Lucia Velotti, Susan Pickman, Hung-Lung Wei & Robert Till (2018). "Trojan horse risks in the maritime transportation systems sector." Journal of Transportation Security, 11(3), 65-83.

Siyam, N., and Malak Hussain (2021). "Cyber-safety policy elements in the era of online learning: a content analysis of policies in the UAE." TechTrends, 65(4), 535-547.

Sullivan, B. P., Shantanoo Desai, Jordi Sole, Monica Rossi, Lucia Ramundo, Sergio Terzi (2020). "Maritime 4.0–opportunities in digitalization and advanced manufacturing for vessel development." Procedia manufacturing, 42, 246-253.

Svilicica, B., Brčić, D., Žuškin, S., ve Kalebić, D. (2019). "Raising awareness on cyber security of ECDIS." TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 13(1).

Svilicica, B., Miho Kristić, Srđan Žuškin & David Brčić (2020). "Paperless ship navigation: cyber security weaknesses." Journal of Transportation Security, 13(3), 203-214.

Svilicicb, B., Junzo Kamahara Rooks, Matthew Rooks and Yoshiji Yano (2019). "Maritime cyber risk management: An experimental ship assessment." The Journal of Navigation, 72(5), 1108-1120.

Svilicicb, B., Igor Rudan, Vlado Frančić and Djani Mohović (2020). "Towards a cyber secure shipboard radar." The Journal of Navigation, 73(3), 547-558.

Svilicicc, B., Junzo Kamahara, Jasmin Celic & Johan Bolmsten (2019). "Assessing ship cyber risks: A framework and case study of ECDIS security." WMU Journal of Maritime Affairs, 18(3), 509-520.

Tam, K., and Kevin Jones (2019, June). "Factors affecting cyber risk in maritime." In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-8). IEEE.

Tam, K., and Kevin Jones (2019, June). "Forensic readiness within the maritime sector." In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-4). IEEE.

Takenaka, M., Chihiro Nishizaki, and Tadatsugi Okazaki (2019, October). "Development of Ship Collision Prevention Device with Augmented Reality Toolkit." In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) (pp. 4290-4295). IEEE.

Thetius, HFW, CYBEROWL. (2022). "The Great Dısconnect." The state of cyber risk management in the maritime industry, 1-44.

Tijan, E., Marija Jović, Saša Aksentijević, Andreja Pucihar (2021). "Digital transformation in the maritime transport sector." Technological Forecasting and Social Change, 170, 120879.

Trimble, D., Jonathon Monken, and Alexander FL Sand (2017, November). "A framework for cybersecurity assessments of critical port infrastructure." In 2017 International Conference on Cyber Conflict (CyCon US) (pp. 1-7). IEEE.

Turk, Ž., Borja García de Soto, Bharadwaj R.K. Mantha, Abel Maciel, Alexandru Georgescu (2022). "A systemic framework for addressing cybersecurity in construction." Automation in Construction, 133, 103988.

Tusher, H. M., Ziaul Haque Munim, Theo E. Notteboom, Tae-Eun Kim, Salman Nazir (2022). "Cyber security risk assessment in autonomous shipping." Maritime Economics ve Logistics, 1-20.

Wang, H., Ottar L. Osen, Guoyuan Li, Wei Li, Hong-Ning Dai, Wei Zeng (2015, November). "Big data and industrial internet of things for the maritime industry in northwestern norway." In TENCON 2015-2015 IEEE Region 10 Conference (pp. 1-5). IEEE.

Wang, Y., Peng Chen, Bing Wu, Chengpeng Wan, Zaili Yang (2022). "A trustable architecture over blockchain to facilitate maritime administration for MASS systems." Reliability Engineering ve System Safety, 219, 108246.

Weaver, G. A., Brett Feddersen, Lavanya Marla, Dan Wei, Adam Rose, Mark Van Moer (2022). "Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach." Transportation Research Part C: Emerging Technologies, 137, 103423.

Wilshusen, Gregory C. (2015). "Maritime critical infrastructure protection: Dhs needs to enhance efforts to address port cybersecurity" (No. GAO-16-116T).

Wogan, H. P. (2019). "Survey Reveals That Most Marıtıme Companıes Are Unprepared For Cybersecurıty Threats." Ocean News ve Technology, 14.

Wolsing, K., Linus Roepert, Jan Bauer, Klaus Wehrle (2022). "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches." Journal of Marine Science and Engineering, 10(1), 112.

Wong, W. P., Hwee Chin Tan, Kim Hua Tan, Ming-Lang Tseng (2019). "Human factors in information leakage: mitigation strategies for information sharing integrity." Industrial Management ve Data Systems, 119(6), 1242-1267.

Wróbel, K., Jakub Montewka, and Pentti Kujala (2017). "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety." Reliability Engineering ve System Safety, 165, 155-169.

Van Schaik, P., Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, Petko Kusev (2017). "Risk perceptions of cyber-security and precautionary behaviour." Computers in Human Behavior, 75, 547-559.

Von Solms, R., and Johan Van Niekerk (2013). "From information security to cyber security." computers ve security, 38, 97-102.

Yang, Chung-Shan (2019). "Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use." Transportation Research Part E: Logistics and Transportation Review, 131, 108-117.

Yang, F., and Sai Gu (2021). Industry 4.0, a revolution that requires technology and national strategies. Complex ve Intelligent Systems, 7(3), 1311-1325.

Yang, Y. P. O., How-Ming Shieh, Jun-Der Leu, Gwo-Hshiung Tzeng (2008). "A novel hybrid MCDM model combined with DEMATEL and ANP with applications." International journal of operations research, 5(3), 160-168.
Yildirim, Ebru (2016). "The importance of information security awareness for the success of business enterprises." In Advances in human factors in cybersecurity (pp. 211-222). Springer, Cham.
Young-McLear, K., Grant Wyman, Joseph Benin & Yamasheka Young-McLear (2016). "A white hat approach to identifying gaps between cybersecurity education and training: a social engineering case study." In Advances in human factors in cybersecurity (pp. 229-237). Springer, Cham.
Yurekten, O., and Mehmet Demirci (2021). "Citadel: Cyber threat intelligence assisted defense system for software-defined networks." Computer Networks, 191, 108013.
Zadeh, Lotfi A. (1965). "Fuzzy sets." Information and control, 8(3), 338-353.
Zhang, M., Jakub Montewka, Teemu Manderbacka, Pentti Kujala, Spyros Hirdaris (2021). "A big data analytics method for the evaluation of ship-ship collision risk reflecting hydrometeorological conditions." Reliability Engineering ve System Safety, 213, 107674.
Zhao, J. L., Shaokun Fan, and Jiaqi Yan (2016). "Overview of business innovations and research opportunities in blockchain and introduction to the special issue." Financial innovation, 2(1), 1-7.

3. Elektronik Kaynaklar

Anand, N. (2012). Voyage Data Recorder of Prabhu Daya may have been tampered with, https://www.thehindu.com/news/national/tamil-nadu/voyage-data-recorder-of-prabhu-daya-may-have-been-tampered-with/article2982183.ece Erişim Tarihi: 25.03.2022.
Armatörlerbiliği (2022). Türk Armatörler Birliği. https://armatorlerbirligi.org.tr/uyelerimiz Erişim Tarihi: 01.11.2022.
Catalin Cimpanu (2018). Ransomware Infection Cripples Shipping Giant COSCO's American Network. https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/ Erişim Tarihi: 26.02.2022.
David, Hambling. (2017). Ships fooled in GPS spoofing attack suggest Russian cyberweapon https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/#ixzz7RHcKBTfZ Erişim Tarihi: 25.02.2022.
Deloitte (2017). Cyber Security in the Shipping Industry. Capital Link Cyprus Shipping Forum. https://globalmaritimehub.com/wp-content/uploads/attach_852.pdf Erişim Tarihi: 27.02.2022.
DNV-GL (2015). Dig¡tale Sårbarheter Maritim Sektor. Lysneutvalget. 2015-0569, Rev. 1. https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/7.pdf Erişim Tarihi: 23.02.2022.
DTO (2019). Izmir Deniz Ticaret Odası Denizden Merhaba Dergisi, 21, pp. 1-40. Available at http://www.dtoizmir.org.

tr/dosyalar/denizdenmerhaba/PDF%20SAYILAR/s21.pdf Erişim Tarihi: 23.02.2022.
DTO (2022). Denizcilik Sektör Raporu. https://www.denizticaretodasi.org.tr/media/SharedDocuments/sektorraporu/sektor_raporu_tr_2021.pdf Erişim Tarihi: 01.11.2022.
ENISA (2019). Port Cybersecurity - Good practices for cybersecurity in the maritime sector, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector Erişim Tarihi: 23.02.2022.
ENISA (2020). Guidelines - Cyber Risk Management for Ports, https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports Erişim Tarihi: 23.02.2022.
Fosen, Jarle (2019). Cyber Security Awareness-in the maritime industry. https://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%201418279).pdf Erişim Tarihi: 23.03.2022.
Groenfeldt, Tom (2017). IBM and Maersk apply blockchain to container shipping. Forbes. https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/?sh=20c8bf5f3f05 Erişim Tarihi: 28.04.2022.
Hackmageddon (2021). Cyber Attacks Statistics. https://www.hackmageddon.com/category/security/cyber-attacks-statistics/ Erişim Tarihi: 26.02.2022.
Hapag-Lloyd (2022). Cyber threat: possible spear phishing attack against Hapag-Lloyd. https://www.hapag-lloyd.com/en/services-information/news/2022/03/mar07-cyber-threat-phishing-attack.html Erişim Tarihi: 20.04.2022.
IMOa, MSC, 428(98), 2017, Marıtıme Cyber Rısk Management In Safety Management Systems, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf Erişim Tarihi: 21.02.2022.
IMOb, MSC-FAL, 1/Circ.3. (2017). Guıdelınes On Marıtıme Cyber Rısk Management, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf Erişim Tarihi: 21.02.2022.
IMOa (2022). Maritime Cyber Risk, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx Erişim Tarihi: 21.02.2022.
IMOb (2022). Voyage Data Recorders, https://www.imo.org/en/OurWork/Safety/Pages/VDR.aspx Erişim Tarihi: 21.02.2022.
ISO (2015). THE PROCESS APPROACH IN ISO 9001:2015. https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso9001-2015-process-appr.pdf Erişim Tarihi: 28.03.2022.
ISO ve IEC. (2021). Information technology, cybersecurity and privacy protection-Cybersecurity framework development. https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27110:ed-1:v1:en Erişim Tarihi: 28.03.2022.

JNPT (2022). Cyber attack hits state-owned terminal at India's JNPT. https://container-news.com/cyber-attack-hits-state-owned-terminal-at-indias-jnpt/ Erişim Tarihi: 24.04.2022.

Kim, Link Wills (2019). Cybersecurity rises to surface of maritime industry concerns. https://www.freightwaves.com/news/cybersecurity-rises-to-surface-of-maritime-industry-concerns Erişim Tarihi: 27.02.2022.

Konrad, John (2020). IMO Cyber-attack Has Serious Implications. https://gcaptain.com/imo-cyberattack-has-serious-implications/ Erişim Tarihi: 20.02.2022.

Lucy, White (2020). Carnival hit by cyber attack: Hackers steal personal information of cruise giant's passengers and staff. https://www.thisismoney.co.uk/money/markets/article-8640269/Carnival-hit-ransomware-attack-Hackers-steal-passenger-information.html Erişim Tarihi: 20.02.2022.

Marcus, Williams (2018). Cosco Shipping Lines hit by cyber-attack. https://www.automotivelogistics.media/cosco-shipping-lines-hit-by-cyber-attack/21276.article Erişim Tarihi: 20.02.2022.

Markit, Ihs (2019). Safety at Sea and BIMCO cyber security white paper. Supported by ABS Group. https://cdn.ihsmarkit.com/www/pdf/1019/Safety-at-Sea-and-bimco-cyber-security-white-paper.pdf Erişim Tarihi: 27.03.2022.

Micheal, Grinter (2020). Maritime cyber-attacks up 900% in three years. http://www.hongkongmaritimehub.com/maritime-cyber-attacks-up-900-in-three-years/ Erişim Tarihi: 20.02.2022.

Naveen, Goud (2018). Cyber Attack on COSCO. https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/ Erişim Tarihi: 20.02.2022.

NISTa (2022). Cybersecurity Framework. https://www.nist.gov/industry-impacts/cybersecurity-framework Erişim Tarihi: 22.03.2022.

NISTb (2022). NIST Cloud Computing Program – NCCP. https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp Erişim Tarihi: 22.03.2022.

OCIMF (2022). The Oil Companies International Marine Forum. https://www.ocimf.org/ Erişim Tarihi: 26.03.2022.

OECD (2018). Information Sharing for Efficient Maritime Logistics, International Transport Forum. https://www.itf-oecd.org/sites/default/files/docs/information-sharing-maritime-logistics.pdf Erişim Tarihi: 25.02.2022.

Rotterdam (2019). First blockchain container shipped to Rotterdam. https://www.portofrotterdam.com/en/news-and-press-releases/first-blockchain-container-shipped-rotterdam Erişim Tarihi: 26.03.2022.

Shen, C. and Bajer James Bajer (2020). CMA CGM confirms ransomware attack. https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack Erişim Tarihi: 21.02.2022.

Symantec (2018). ISTR Internet Security Threat Report. Internet Security Threat Report https://docs.broadcom.com/doc/istr-23-executive-summary-en Erişim Tarihi: 25.02.2022.

Tabak, Nate (2022). Global logistics giant Expeditors suffers cyberattack, shuts down operations systems. https://www.freightwaves.com/news/global-logistics-giant-expeditors-suffers-cyberattack-shuts-down-operations-systems Erişim tarihi: 21.04.2022.

TMSA (2017). Tanker Management and Self Assessment version 3. https://www.ocimf.org/publications/books/tanker-management-and-self-assessment-3 Erişim Tarihi: 25.02.2022.

Toogood, Darren (2022). Wıghtlınk Suffers 'Sophıstıcated' Cyber Attack Exposıng Customers' Detaıls. https://www.islandecho.co.uk/wightlink-suffers-sophisticated-cyber-attack-exposing-customers-details/ Erişim Tarihi: 22.04.2022.

UNCTAD (2018). United Nations Conference on Trade and Development: Review of Maritime Transport. https://unctad.org/en/PublicationsLibrary/rmt2018_en.pdf Erişim Tarihi: 25.03.2022.

Yılmaz, Özlem (2018). Gemicilik sektörünün en büyük armatörleri. https://www.ekonomist.com.tr/haberler/gemicilik-sektorunun-en-buyuk-armatorleri.html Erişim Tarihi: 22.04.2022.

ETİK KURUL İZNİ

T.C.
KOCAELİ ÜNİVERSİTESİ
Sosyal ve Beşeri Bilimler Etik Kurulu

Sayı : E-10017888-100-292542
Konu : Ali Yanık'ın etik kurul izni hk.

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 12.09.2022 tarihli, 284103 sayılı ve "Ali Yanık'ın etik kurul izni hk." konulu yazı

Sosyal ve Beşeri Bilimler Etik Kurulu'nun 22/09/2022 tarih ve 2022/08 no lu toplantısında alınan 18 sıra sayılı kararı aşağıda sunulmuştur.

Bilgilerinize arz ederim.

Karar No 18: Sosyal Bilimler Enstitüsü Müdürlüğünün 12.09.2022 tarih ve 284103 sayılı yazısı görüşüldü. Denizcilik İşletmeleri Yönetimi Anabilim Dalı yüksek lisans programı öğrencisi Ali YANIK'ın, Doç. Dr. Murat YORULMAZ'ın danışmanlığında yürüttüğü "Denizcilikte Siber Risklerin Değerlendirilmesi ve Yönetimi" başlıklı yüksek lisans tez çalışması için yapacağı anket uygulamasında, bilimsel araştırma ve yayın etiği açısından bir sakınca olmadığına oy birliği ile karar verildi.

Prof.Dr. İbrahim ŞİRİN
Kurul Başkanı