T.C.

ALANYA ALAADDİN KEYKUBAT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

İŞLETME MÜHENDİSLİĞİ ANA BİLİM DALI

DENİZCİLİK SEKTÖRÜNDE DİJİTAL OLGUNLUK MODELİ VE SİBER GÜVENLİK FARKINDALIĞI

Yüksek Lisans Tezi

Lemi KAYA

Danışman
Doç. Dr. Gülin İdil S. BOLATAN

ALANYA
2024

T.C.

ALANYA ALAADDİN KEYKUBAT ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DENİZCİLİK SEKTÖRÜNDE DİJİTAL OLGUNLUK MODELİ VE SİBER GÜVENLİK FARKINDALIĞI

Yüksek Lisans Tezi

Lemi KAYA

İşletme Mühendisliği Ana Bilim Dalı

İşletme Mühendisliği Programı

Danışman

Doç. Dr. Gülin İdil S. BOLATAN

ALANYA

2024

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilemeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Alanya Alaaddin Keykubat Üniversitesi tarafından kullanılan "bilimsel intihal tespit programıyla tarandığını ve "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.

Lemi KAYA

TEŞEKKÜR SAYFASI

Tez çalışmam sırasında bilgisi, sabrı, hoşgörüsüyle yol gösteren, değerli büyüğüm Doç. Dr. Gülin İdil Sönmeztürk Bolatan'a saygı ve teşekkürlerimi sunarım.

Hayatım boyunca her türlü desteklerini aldığım canım annem, babam ve kız kardeşime minnettarım.

Tüm zorluklara karşı hayatıma baharlar getiren, hep yanımda olan sevgili eşim Bahar Kirşan Kaya'ya sonsuz teşekkür ederim.

Lemi KAYA

ÖZET

DENİZCİLİK SEKTÖRÜNDE DİJİTAL OLGUNLUK MODELİ VE SİBER GÜVENLİK FARKINDALIĞI

Lemi KAYA
İşletme Mühendisliği Anabilim Dalı
Alanya Alaaddin Keykubat Üniversitesi, Lisansüstü Eğitim Enstitüsü,
Haziran, 2024 (96 Sayfa)

Dijitalleşme, denizcilik sektörünü geleneksel sınırlarının ötesine taşımakta ve firmaların üretkenliğini, verimliliğini ve sürdürülebilirliğini artırmak için birçok yeni fırsat sunmaktadır. Dijital olgunluk, firmaların pazarda rekabetçi kalmak için kalıpları değiştirme ve uygulama konusundaki hazırlığını ve kapasitesini göstermektedir. Denizcilik şirketlerinin, dijital dönüşümün yeteneklerinden rekabetçi avantajlar elde etmek için dijital olgunluk durumlarını modeller aracılığıyla bilmesi gerekmektedir. Bu çalışma ile denizcilik sektörünün ve firmaların dijital olgunluk seviyesini ölçmek amacıyla 5 ana boyut ve 25 alt boyuttan oluşan dijital olgunluk modeli geliştirilmiştir. Tüm boyutların önemi AHP (Analitik Hiyerarşi Prosesi) yöntemi kullanılarak belirlenmiştir. AHP ile Ağırlıklandırılmış Olgunluk Yaklaşımı ile de olgunluk seviyeleri ortaya çıkartılmıştır. Sonuçlar, strateji ve yönetimin en önemli kriter olduğunu göstermektedir. Öte yandan denizcilik sistemlerinin artan karmaşıklığı, dijitalleşmesi, tüm denizcilik sektörü için yeni siber güvenlik gereksinimleri ortaya çıkarmaktadır. Siber güvenliğin ciddiyeti, şirketler üzerindeki etkileri göz önüne alındığında küresel bir dikkat ve bilinç gerektirmektedir. Bu çalışma ile, internet kullanıcılarının siber güvenlik farkındalığını etkileyen faktörlerin belirlenmesi ve değerlendirilmesi için bir yöntem oluşturulması amaçlanmıştır. Denizcilik sektöründe çalışanlara odaklanılarak, kullanıcıların siber güvenlik farkındalığı ile ilişkili faktörleri belirlemek ve ölçmek için tutum, bilgi, deneyim, eğitim ve cinsiyet dahil olmak üzere yedi ayrı farklı faktör kullanılmıştır. Her faktörün ağırlığını çıkarmak için AHP karar verme tekniği uygulandıktan sonra, sonuçlar en önemli faktörün bilgi olduğunu göstermektedir.

Anahtar Sözcükler: Denizcilik sektörü, Dijital olgunluk modeli, Siber farkındalık, AHP.

ABSTRACT

DİGİTAL MATURİTY MODEL AND CYBER SECURİTY AWARENESS İN THE MARİTİME SECTOR

Lemi KAYA

Department of Management Engineering

Graduate School of Alanya Alaaddin Keykubat University,

June, 2024

Digitalization is pushing the maritime industry beyond its traditional boundaries and offers many new opportunities to increase firms productivity, efficiency and sustainability. Digital maturity demonstrates the readiness and capacity of firms to change and apply patterns to remain competitive in the market. Maritime companies need to know their digital maturity status through models to gain competitive advantages from the capabilities of digital transformation. In this study, a digital maturity model consisting of 5 main dimensions and 25 sub-dimensions was developed to measure the digital maturity level of the maritime industry and companies. The importance of all dimensions was determined using the AHP (Analytic Hierarchy Process) method. The maturity levels were also revealed with the AHP Weighted Maturity Approach. The results show that strategy and management are the most important criteria. On the other hand, the increasing complexity and digitalization of maritime systems creates new cyber security requirements for the entire maritime industry. The seriousness of cybersecurity requires global attention and awareness given its impact on companies. This study aims to establish a methodology for identifying and evaluating the factors affecting the cyber security awareness of internet users. Focusing on those working in the maritime industry, seven distinct different factors, including attitude, knowledge, experience, education and gender, were used to identify and measure the factors associated with users cybersecurity awareness. After applying the AHP decision-making technique to extract the weight of each factor, the results show that the most important factor is knowledge.

Keywords: Maritime industry, Digital maturity model, Cyber awareness, AHP.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

SİMGELER VE KISALTMALAR

IoT	Nesnelerin interneti
CPS	Siber fiziksel sistemler
GPS	Küresel konumlama sistemi
RFID	Radyo frekansı ile tanımlama
AI	Yapay zekâ
AIS	Otomatik tanımlama sistemi
AHP	Analitik hiyerarşi prosesi
IT	Bilişim teknolojileri
IMO	Uluslararası denizcilik örgütü
BIMCO	Baltık ve uluslararası denizcilik konseyi

1. GİRİŞ

Son yıllarda neredeyse tüm sektörlerdeki firmalar, yeni dijital teknolojileri keşfetmek ve bunların faydalarından yararlanmak için bir dizi girişimde bulunmuşlardır. Bunlar sıklıkla temel iş operasyonlarının dönüşümünü içermekte ve ürünleri, hizmetleri ve süreçlerin yanı sıra organizasyon yapılarını ve yönetim kavramlarını da etkilemektedir (Matt vd., 2015).

Dijitalleşme, analog teknolojilerle simgelenen geleneksel süreçlerden, dijital teknolojiler ve otomatikleştirilmiş iş süreçleriyle karakterize edilen bir çağa doğru yaşanan güçlü değişimi ifade etmektedir (Bloomberg, 2018).

Dijital dönüşüm, dijital teknolojinin uygulanması ve kullanılmasıyla geleneksel iş uygulamalarında köklü değişikliklere neden olmaktadır. İş süreçlerindeki değişiklikleri aşmakta, yeni organizasyon türlerinin yaratılmasına olanak tanımakta, organizasyon kültüründe, ilişkilerde, değer yaratmada, müşteri erişiminde ve ayrıca pazar konumunda değişiklikler getirmektedir (Dehning vd., 2003).

Tüm sektörleri sınırlarının ötesine zorlayan dijitalleşme, sektörlerin değişen ekosistemdeki değerlerini, etkileşimlerini sürekli olarak yeniden değerlendirmelerini gerektirmektedir (Heilig vd., 2017).

Yeni dijital teknolojilerin geliştirilmesi ve dijitalleşme, farklı sektör uzmanları, akademisyenler, araştırmacılar ve önde gelen uluslararası denizcilik kuruluşlarının yeni iş fırsatları, ticaretin kolaylaştırılması ve tedarik zincirlerinin dönüştürülmesini sağlarken, mevcut süreçlerin dijitalleşme yoluyla nasıl optimize edilebileceğini araştırmasıyla denizcilik sektöründe giderek daha fazla tartışma ve araştırma konusu haline gelmiştir (UNCTAD, 2019).

Günümüzün iş ortamı hızla değişmekte ve dijital çağ tarafından devrim yaratmaktadır. Teknoloji daha hızlı ilerlemekte ve benimsenmesi her zamankinden daha az zaman almaktadır. Uluslararası ticarette önemli bir yeri olan denizcilik sektörü de farklı alanlarda farklı hızlarda dijitalleşmeye devam etmektedir.

Denizcilik sektörü, ekonomik büyümenin temel itici gücü olarak kabul edilen güçlü ve gelişen bir sektördür. Birleşmiş Milletler Ticaret ve Kalkınma Konferansı (UNCTAD), dünya çapındaki ticaret faaliyetlerinin %90'ının deniz taşımacılığı endüstrisiyle bağlantılı olduğunu ve yıllık navlun oranlarının 380 milyar ABD dolarından fazla olduğunu tahmin etmektedir (UNCTAD, 2022).

Dijitalleşme, coğrafi ve zamansal sınırların öneminin azaldığı durumlarda neredeyse sınırsız fırsatlar sunmaktadır. Aynı zamanda güvenlik açığı da artmaktadır. Denizcilik sektöründeki sistemlerin artan karmaşıklığı, dijitalleşmesi, entegrasyonu ve otomasyonu, tüm denizcilik sektörü için yeni siber güvenlik gereksinimlerini ortaya çıkarmaktadır. Sektörün gelen değişikliklere uyum sağlaması kaçınılmazdır. Denizcilik sektöründe bağlantılı paydaşlar arasında diyaloğu ve bilgi alışverişini teşvik etmek, siber güvenlik farkındalığını artırmak gerekmektedir.

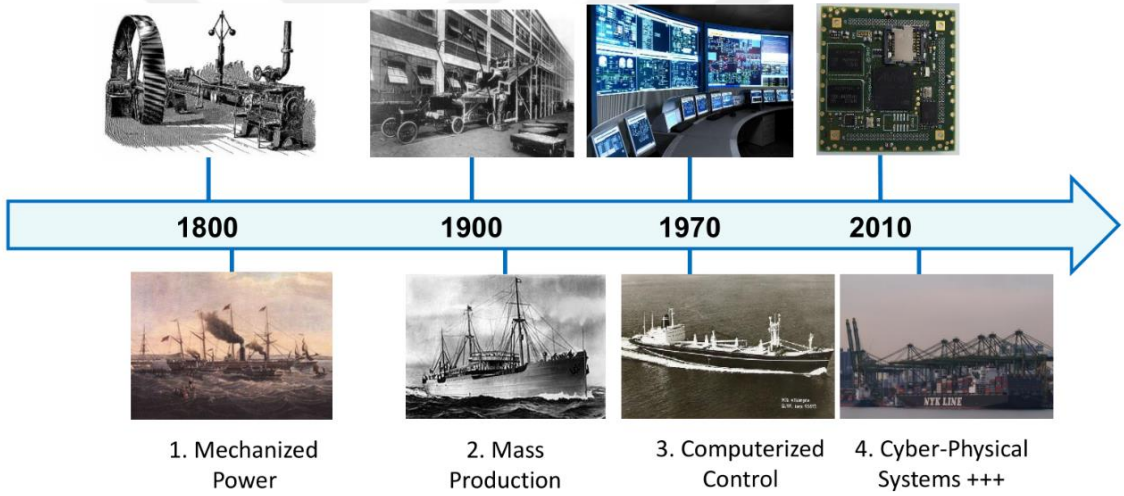
2. LİTERATÜR

2.1. Sanayi Devrimlerinin Gelişim Aşamaları

İnsanlar, su ve buharla çalışan mekanizmaların mal üretimini hızlandırdığı 18. yüzyılın sonlarından bu yana birçok sanayi devrimi yaşamışlardır (Kaufman, 2020).

Sanayi devrimi, üretimin atölye el işçiliğinden makine sanayisine geçişini tamamladığı bir aşamadır. İnsan gücünün yerini makinelerin aldığı ve bireysel atölyelerdeki manuel üretimin yerini büyük ölçekli fabrika üretiminin aldığı üretim ve teknoloji devrimidir. Bu süreç bazı engelleri ve tehditleri beraberinde getirmiş, ancak aynı zamanda departman için fırsatlar ve güç de sağlamıştır. Sanayi devriminden bu yana, teknolojik ilerleme endüstriyel üretkenlikte keskin bir artışa yol açmıştır (Qi, 2021).

Endüstri 1.0-4.0 arasında, endüstriyel teknoloji ilerlemesi kademeli bir büyüme modeli göstermiştir. Dört sanayi devriminin evrimi Şekil 2.1'de gösterilmektedir.



Şekil 2.1 Dört sanayi devriminin seyri (Qi, 2021)

2.1.1. Sanayi devriminin birinci aşaması

İlk sanayi devrimi 1860'lar ile 19. yüzyılın ortalarında buhar makinesinin icat edilmesiyle başlamıştır. Endüstri 1.0 ilk olarak İngiltere'de meydana gelmiştir ve bu sırada sanayi devrimi el sanatları aşamasında idi. Uzmanlaşmış manuel işlemlerin makineleşmesi gerçekleştirilerek, Endüstri 1.0 olarak adlandırılan teknolojik gelişmeyi teşvik etmek için mekanize üretimde buhar gücü kullanılmıştır (Rüßmann vd., 2015).

Endüstri 1.0'ın toplum üzerinde önemli bir etkisi olmuştur. Malların üretim biçimi dönüştürülmüştür ve üretkenliğin, ekonomik büyümenin artmasına yol açmıştır. Ancak aynı zamanda kötü çalışma koşulları ve kirlilik gibi sosyal ve çevresel sorunlara da yol açmıştır (Kamaruzaman vd., 2019).

2.1.2. Sanayi devriminin ikinci aşaması

On dokuzuncu yüzyılın sonlarından yirminci yüzyılın başlarına kadar, teknolojik devrim olarak da bilinen ikinci sanayi devrimi, hızlı bir bilimsel keşif, standardizasyon, seri üretim ve sanayileşme dönemidir. On dokuzuncu yüzyılın ortasında sona eren ilk sanayi devrimi, 1870'te başlayan ikinci sanayi devrimi öncesinde önemli icatlarda bir yavaşlamayla damgasını vurmuştur (Atkeson & Kehoe, 2001). Demiryolu ağının gelişmesi, malların daha hızlı ve daha ucuz taşınmasına olanak tanımıştır ve uluslararası ticaretin büyümesine yol açmıştır. Telgraf ve telefon, bireyler ve işletmeler arasında daha hızlı ve daha verimli iletişime olanak tanıyarak iletişimde devrim yaratmıştır. Henry Ford tarafından icat edilen montaj hattı, otomobillerin ve diğer tüketim mallarının seri üretimine eskisinden çok daha hızlı bir şekilde izin vererek mal üretiminde devrim yaratmıştır (Salah, 2021).

2.1.3. Sanayi devriminin üçüncü aşaması

Yaklaşık olarak ikinci dünya savaşından sonra 1969 yılında Modicon firması, Amerika Birleşik Devletleri'nde ilk programlanabilir mantık denetleyicisini (PLC) tasarlamıştır. Büyük ölçekli endüstriyel üretime geçilmiştir ve insanlık elektronik ve bilgi teknolojisini kullanarak otomasyonu gerçekleştirmiştir. Böylece 20. yüzyılın ikinci yarısında Endüstri 3.0 sanayi devrimi dönemine girilmiştir (Qi, 2021).

Endüstri 3.0, gerçek ilerleme verimi, ana itici güçler ve mekanik karşılıklı bağımlılıklar için yeni kaydedilen bir mikro veri tabanından yararlanmıştır (Taalbi, 2019). Bilgi teknolojisinin birleşik güçleri, yalnızca çalışma şeklimizi değil, aynı zamanda dünyayı nasıl algıladığımızı ve onu nasıl tanımladığımızı da değiştiren üçüncü sanayi devrimini ortaya çıkarmıştır. Üçüncü sanayi devriminden sonra toplumun yerini küresel bir ortam almıştır. İnsanlar, teknoloji ve bilgi sağlayıcıları tarafından, verileri hayatlarını iyileştirecek şekillerde bulma, alma, değiştirme ve kullanma konusunda güçlendirilmiştir (Qureshi vd., 2020).

Enerji yapısındaki değişiklikler taşımacılık yöntemlerinde de değişikliklere neden olmuştur. Geleneksel büyük ölçekli nakliye yöntemleri, esnek ve özelleştirilmiş nakliye yöntemlerine dönüşmüştür (Zhen, 2017).

2.1.4. Sanayi devriminin dördüncü aşaması

Endüstri 4.0'ın teknolojik temeli, ilk kez 1999'da MIT (Massachusetts Institute of Technology) tarafından önerilen Nesnelerin İnternetidir (IoT). Alman hükümeti

tarafından veri yönetimi, cihaz iletişimi ve dijitalleşme alanlarındaki gelişmeleri ele almak ve geliştirmek amacıyla 2011 yılında ortaya çıkışından bu yana dünya çapında büyük ilgi görmüştür. Endüstri 4.0, IoT ve IoS'nin imalat endüstrisine dahil edilmesiyle karakterize edilen dördüncü sanayi devrimini ifade etmektedir. Endüstriyel dönüşüm, katma değerli süreçler sunmak için Siber- Fiziksel Sistemlerden (CPS), büyük veriden, yapay zekâdan, bulut bilişimden, internetten, geleceğe yönelik teknolojilerden ve gelişmiş insan-makine etkileşimi paradigmalarından yararlanmaktadır (Sanders vd., 2016).

Devrim niteliğinde bir süreç olarak endüstri 4.0, dijitalleşmeyi ve bilgi odaklı endüstriyel kalkınmayı teşvik ederken, bilgi ve iletişim teknolojisinin çeşitli boyutlarını entegre etmeyi amaçlamaktadır (Mohd Salleh vd., 2021).

2011 yılındaki başlangıcından bu yana, endüstri 4.0'ın teori ve pratikte güncel bir konu olduğu kanıtlanmıştır. Endüstri 4.0 uygulamaları denizcilik sektörü de dahil olmak üzere farklı endüstriyel sektörlerde kullanılmaktadır. Endüstri 4.0'ın etkileri deniz taşımacılığı, gemi inşası, limanlar ve terminaller dahil olmak üzere denizcilik sektörünün ayrılmaz yönlerinde daha belirgin hale gelmektedir.

2.2. Denizcilik Sektörü ve Dijitalleşme

Akademik literatürde, dijitalleşmenin hala birleşik bir tanımı yoktur ve terimin kapsamı değişebilmektedir. Bazı yazarlar dijitalleşmeyi, dijital teknolojilere daha fazla güvenme ve yaratılan değerin internet uyumlu veri paketlerine dönüştürülmesi süreci olarak tanımlamaktadır (Banalieva & Dhanaraj, 2019). Buna karşılık dijitalleşme, dijital teknoloji kullanımı nedeniyle firmanın geçirebileceği organizasyonel değişiklikler olarak da tanımlanabilmektedir (Westerman vd., 2011).

Dijitalleşme, teknik bir evrimden çok daha fazlasıdır ve kuruluştaki tüm faaliyetleri ve kaynak yapılandırmalarını değiştiren bir eğilimdir (Bharadwaj vd., 2013). Faaliyetler arasındaki uyumu değiştiren firma, değer yaratma ve değer yakalama süreçlerinin mekanizmasını değiştirmekte ve piyasayı bozabilecek tamamen yeni ürün ve hizmet önerileri geliştirmektedir. Dolayısıyla, dijitalleşme yalnızca faaliyetlerin daha iyi kontrol edilmesi yoluyla operasyon verimliliğini artırmanın bir yolu değil, aynı zamanda iş modellerinin inovasyonu yoluyla firmanın genel etkinliğini artırmak için bir fırsattır (Chesbrough, 2010).

Denizcilik sektöründe gemicilik terimi, malların gemilerle okyanusta taşınmasını ifade etmektedir (Munim, 2019). Denizcilik sektörü, ticaret endüstrisinin en önemli

oyuncusu olduğu için küresel ticaretle de eş anlamlıdır (Struck, 2020). Küresel ticaretin %90'ının deniz yoluyla gerçekleşmesi, denizcilik sektörünün dünya ekonomisinin bel kemiği olma rolünü vurgulamaktadır (Emad vd., 2021). Ayrıca, denizcilik sektörü sosyal, iklim değişikliği, ekonomik ve daha da önemlisi hızlı teknolojik gelişim gibi farklı zorluklarla karşı karşıya kalmıştır ve bu da sektörün bu zorlukları bir tehditten ziyade bir fırsat olarak görmeye hazır olmasını gerektirmektedir (Zaman vd., 2017). Bu nedenle, otonom gemiler gibi yeni nesil Endüstri 4.0 teknolojileri, denizcilik alanındaki zorlukların üstesinden gelme potansiyeline sahiptir (Gu vd., 2021).

Dünya giderek daha bağlantılı hale dönüşmekte ve müşterilerin ihtiyaçları daha zorlu ve dinamik hale gelmektedir. Tasarım, gemi inşası ve bakımdan, kargo rotalarının optimizasyonuna kadar denizcilik sektörü ekonomik, politik, demografik ve teknolojik eğilimlere yanıt olarak gelişmeye devam etmektedir. Buna göre dijital teknolojilerin kullanılması bu trendlerin önleyici ve sorumlu bir şekilde karşılanmasına olanak tanımaktadır.

2.2.1. Limanlar

Limanlar bölgesel, ulusal ve uluslararası alanları kapsamakta, çeşitli düzeylerde lojistik, tedarik zinciri yönetimi ve ekonomik faaliyetlerin kolaylaştırılmasında önemli bir rol oynamaktadır. Limanlar, temel kaynakların taşınmasını, enerji, sağlık hizmetleri, iş gücü, yolcu hareketliliği ve erişilebilirlik gibi temel hizmetleri sağlamaktadırlar. Ayrıca bu limanlar, bölgesel ekonomik kalkınmayı destekleyen, sosyal katılımı teşvik eden ekonomik ve sosyal etkileşim merkezleri olarak hareket etmektedir. Küresel ticaretin birbirine bağlılığının artmasıyla ve güvenlik, ekonomik verimlilik, yasal uyumluluk ve sosyal adalet için dengeleme çabalarını içeren bir dizi sorumlulukla eşit derecede boğuşan limanlar, dijital dönüşüme, dijitalleşmeye acil bir ihtiyaçla karşı karşıyadırlar (Klein & Spychalska-Wojtkiewicz, 2023).

Küresel denizcilik endüstrisi daha verimli, uygun maliyetli ve sürdürülebilir bir geleceğe doğru ilerledikçe limanlarda dijitalleşmenin önemi artmıştır. Limanlarda dijitalleşme, maliyetlerin azaltılmasına, güvenliğin artırılmasına ve verimliliğin artırılmasına yardımcı olabilir. Dijitalleşmenin müşteri hizmetlerini iyileştirmede, evrak işlerini azaltmada ve verilere daha iyi erişim sağlamada rolü vardır. Ayrıca limanlardaki dijitalleşme, emisyon kontrolünü azaltacak ve çevresel sürdürülebilirliğin kalitesini artıracaktır (González-Cancelas vd., 2020).

Limanlar kıyı bölgelerinin sürdürülebilir kalkınmasında etkin bir role sahip olduğundan, bu limanların akıllı çıkış ekosistemlerine dönüştürülmesi de önemlidir. İlk üç nesil limanlar tipik olarak liman hizmetleri ve üretimine güçlü bir vurgu yapmaktadır. Dördüncü nesil limanlar ise bilgi hizmetlerine öncelik vermekte ve limanların küresel tedarik zincirlerine entegrasyonunu artırmaktadır. Dördüncü nesil limanlarda mevcut olan tüm hizmetler beşinci nesil limanlarda da mevcuttur ve beşinci nesil limanlar yeşil ve akıllı teknolojileri entegre etmektedir (Philipp, 2020).

İnovasyon, liman üretimi ve hizmetlerinde yeşil çevrenin korunması ve en son teknolojinin önemini vurgulamaktadır. Son dört nesil limanlar yeşil ve düşük karbonlu büyümeyi başaramamış ve iklim değişikliği ve kirlilik gibi konuları göz ardı etmiştir. Akıllı liman fikri, toplama, dağıtım ve taşıma sistemlerinin yeni teknolojilerle geliştirilmesi, lojistik için arz ve talebin entegrasyonu ve toplama, dağıtım ve taşıma sistemlerinin kaynakları en iyi şekilde tahsis etme becerisi etrafında dönmektedir. Bu sayede yeni bir çevresel limanın temel biçimi akıllı denetim, akıllı hizmet ve kendi kendine yükleme ve boşaltma olacaktır. İletişim, ağ oluşturma ve akıllı teknoloji dahil olmak üzere yüksek ve yeni düzey teknolojilerin hızlı gelişimi nedeniyle yirmi birinci yüzyılın başından bu yana kurulan otomatik limanların sayısı artmıştır (Mi & Liu, 2022).

Limanlar her zaman önemli bir stratejik nesne olmuştur. Farklı şehirleri ve kıtaları birbirine bağlamış, yerel hinterlantların bölgesel merkezleri ve vatandaşların tüm ekonomik, kültürel ve sosyal yaşamının kalbi olmuşlardır. Son on yıllar, her türlü işletmenin dijitalleşme ve otomasyon yoluyla karmaşık dinamik kalite değişiklikleriyle karakterize edilmektedir. Geleneksel iş biçimleri, blok zincir, yapay zekâ, e-platformlar, gelişmiş analitik, nesnelerin interneti, otonom araçlar, robotik, makine öğrenimi ile desteklenerek temel bir ilgi alanı haline gelmiştir (Maydanova vd., 2019).

Ülkemizin deniz ve kıyılarının büyük bir kısmı, deniz ve karadaki hâkim coğrafi yapı ve iklim özelliklerinin yanı sıra, jeopolitik gelişmeler gibi üretimi mümkün kılan ve destekleyen karakteristik özellikler sayesinde birçok farklı sanayi koluna hizmet vermek üzere kullanılabilmektedir. Ülkemizde Kasım 2022 itibarıyla liman ve iskele tesisi, marina yat limanı, bağlama yeri, tersane, tekne imalathanesi, kayıkhane, balıkçı kıyı yapısı ve gemi söküm tesisi olmak üzere farklı fonksiyon ve faaliyetlere sahip toplam 957 kıyı yapısı bulunmaktadır (IMEAK Maritime Sector Report 2023).

Ülkemizdeki bazı limanlarda kullanılan dijital teknoloji uygulamaları Tablo 2.1'de gösterilmiştir.

Tablo 2.1 Türkiye'deki konteyner limanlarında kullanılan dijital teknoloji uygulamaları (Yorulmaz vd., 2023)

Asya Port	• Ardiye Hesaplama
	• DBA/VGM Sorgulama (Konteynerin içindeki yük ve kendi ağırlığı ile birlikte toplam ağırlığı)
	• Rıhtım Planı Uygulaması
	• Konteyner Takip Uygulaması
DP World Yarımca	• Uzaktan Vinç Kontrolü
	• ARS (Araç Rezervasyon Sistemi)
	• OCR (Optical Character Recognition)
	• AGS (Automated Gate System)
	• CFS Hizmetleri İçin On-line Talep Oluşturma
	• Çevrimiçi Portal Sorgulama Hizmetleri
	• Konteyner Stok Sorgulama
	• Konteyner Takibi
	• Gemi Programı
	• İthalat Tartım Sonucu
	• Doğrulanmış Brüt Ağırlık (DBA) Sorgulama
Mersin Limanı	• Terminal Operasyon Sistemi
	• Konteyner Operasyon Sistemi
	• On-line Hizmetler
	• Tarife ve Ardiye Hesaplama
	• ARS (Araç Rezervasyon Sistemi)
	• Rıhtım Planı
	• Konteyner takibi
	• Mobil Uygulama Üzerinden Tren Takip
	• Tartım Raporu Alma
Qterminals Antalya	• Yapay zekâ (İş güvenliği)
	• Terminal Operasyon Sistemi
	• On-line Hizmetler
	• Online konteyner operasyonları
	• Gemi operasyonları anlık takip
	• Saha operasyon takibi
	• Stok takibi
	• Booking Sorgulama (İhracat konteynerlerin liman sahasına girişine ait rezervasyon bilgisi)
	• CFS İç Dolum Talebi Yapma
	• Ardiye Hesaplama
	• Konteyner talep takibi
	• Gemi Programı
	• Araç Rezervasyon
	• Doğrulanmış Brüt Ağırlık (DBA) Sorgulama

2.2.2. Deniz taşımacılığı

Dünya ticaret operasyonlarının merkezinde nakliye şirketleri bulunmaktadır (Muhammad vd., 2018). Deniz taşımacılığı ekosistemindeki verimlilik bu nedenle küresel ekonomi için büyük önem taşımaktadır (Lind vd., 2018). Şu anda dünya ekonomisinde küreselleşme göz önüne alındığında, ekonomik büyüme seviyelerini korumak için deniz taşımacılığının verimli, emniyetli ve güvenilir olması gerekmektedir (Sanchez-Gonzalez vd., 2019). Nakliye şirketleri endüstriyel tedarik zincirinin temel taşlarındandır ve küresel ticareti kolaylaştırmada önemli bir rol oynamaktadır (Grzelakowski, 2019). Genel olarak deniz taşımacılığı sektörü oldukça değişkendir ve pazarda rekabetçidir. Yakıt fiyatlarındaki dalgalanmalar ve tutarsız navlun oranları, sektörün faaliyet gösterdiği ortamı karakterize etmektedir. Denizcilik şirketlerinin çoğunluğu, maliyetleri düşürmek ve kar marjlarını maksimuma çıkarmak konusunda muazzam bir baskı altındadır. Bunu, piyasadaki rekabetin gerektirdiği esneklik ve dayanıklılık dikkate alınarak yapmak zorundadırlar. Nakliye şirketleri, dijital teknolojilerin sağladığı paylaşılan veriler aracılığıyla rol oyuncularıyla iş birliği yaparak daha da verimli olabilir ve böylece kar marjlarını artırabilmektedir (Feibert vd., 2018).

Denizcilik işi uluslararası niteliktedir. Kaynakları veya hizmetlerinin satışı açısından coğrafi olarak sınırlı değildir ve bu nedenle, her bir denizcilik şirketi ile aynı yük pazarına katılan ve ortak özellik veya özelliklere sahip gemileri işleten diğer şirketler arasında yüksek rekabet vardır. Nakliye şirketleri, yönetim görevlerinin daha az karmaşık olduğu dijital çağda faaliyet gösterse de bu şirketler ve yönetim konusunda hala sınırlamalar bulunmaktadır. Nakliye şirketleri, işletme maliyetlerinin azaltılması veya müşterilere sunulan değer artışı yoluyla rekabet avantajından yararlanmaktadır (Nikitakos & Thoetokas, 2001).

Dijital devrim, son yıllarda denizcilik sektöründeki değişimin ana itici güçlerinden biri olarak ortaya çıkmıştır. Cihazlar, acenteler ve faaliyetler arasında yüksek düzeyde entegrasyon gerektirmektedir. Deniz taşımacılığı, küresel ticaretin ve imalat tedarik zincirinin omurgası olmayı sürdürmektedir. Küresel mal ticaretinin (hacim olarak) beşte dördünden fazlası deniz yoluyla taşınmaktadır. Denizcilik sektörü uzun mesafelerde en ekonomik ve güvenilir taşıma yöntemini sunmaktadır (World Bank 2020). Tedarik zincirleri ve ulaşım maliyetleri, dijitalleşmenin getirdiği verimlilik sayesinde optimize edilmiştir. Dijitalleşme entegre süreçleri ve entegre tedarik zinciri yeteneklerine sahip şirketler iş performanslarında iyileşmeler elde etmişlerdir (Nwankpa & Datta, 2017).

Deniz taşımacılığı sektöründeki endüstri oyuncularının büyük bir kısmı dijitalleşmenin işlerini önemli büyük ölçüde değiştirdiğini düşünmektedirler ve yüksek teknoloji ile büyük değişiklikler yaşamışlardır. Deniz taşımacılığında dijitalleşmenin son durumunu doğrulamış ve dijitalleşmenin şu anda otonom araçlar, robotik, yapay zekâ, büyük veri, sanal gerçeklik, artırılmış ve karma gerçeklik, nesnelerin interneti, bulut ve uç bilişim, dijital güvenlik, 3D baskı ve katkı mühendisliği dijital alanları için geçerli olduğunu belirtmişlerdir (Tijan vd., 2021).

Denizcilik taşımacılığı aynı zamanda daha sürdürülebilir olmak ve rekabetçi kalabilmek için artan baskılarla karşı karşıyadır. Hızlanan küreselleşme gibi dış etkenler ve küresel itici güçler, deniz taşımacılığında verimliliğin artırılmasına yönelik baskıyı artırmaktadır. Daha sürdürülebilir operasyon modlarına yönelik arayışlar, dijital teknolojilerin benimsenmesi yoluyla değer elde edilmesini destekleyen yeni iş modellerini teşvik etmektedir (Gavalas vd. 2022).

2.2.3. Tersaneler

Tersaneler karmaşık ve dinamik ortamlardır. Çok çeşitli gemilerin inşa edildiği ve onarımlarının yapıldığı geniş alanlardır. Gemilerin kendileri devasa ürünlerdir ve içleri oldukça karmaşıktır. Çok katlı kapalı bir binayı andırır ve metal duvarlardan oluşmaktadır. Tersane sektörü de diğer sektörler gibi Endüstri 4.0 ilkelerini uygulayarak gelişmelerden faydalanmak istemekte ve dijitalleşmeyi gerçekleştirmek için mücadele etmektedir. Tersanelerdeki nesnelerin konumlandırılması bu sürecin ilk adımıdır ve dijitalleşmenin temelini oluşturmaktadır. Bu, konumlandırma sistemleri ile gerçekleştirilmektedir. Konumlandırma, radyo dalgaları, manyetik alanlar, akustik sinyaller ve mobil cihazlar tarafından toplanan sensör verileri kullanılarak kapalı bir alandaki nesnelerin veya insanların konumunun belirlenmesi olarak tanımlanmaktadır (Cil vd., 2022).

Japon ve Kore tersanelerinde, plakaların birleştirilmesi aşamasından boylamasına takviyelerin montajı ve kaynağına kadar robotlaştırmayı başaran karmaşık kavisli blokların montaj hattı faaliyettedir. Bu, kavisli blokların üretiminde tam otomasyon için bir ara adımdır. Endüstri 4.0 teknolojilerinin uygulanması konusunda sektörde belirli bir görüş birliği bulunmaktadır. Bu, standartlaştırılmış bir tasarımı sağlamlaştırmak ve geminin inşasında yer alan farklı ara ürünlerin üretim süreçlerinin istatistiksel kontrolüne ulaşmak için gereklidir (Munin-Doce vd., 2020).

Birçok gemi yapımcısı robotlara kucak açmaya başlamıştır. Örneğin Hyundai Heavy Industries, gemi inşa etmek için robotik teknolojiyi kullanan ilk şirket olacağını açıklamıştır. Şirket, Ulsan'daki tersanesinde bir geminin 3 boyutlu kavisli yüzeyini otomatik olarak şekillendirecek robotik bir sistemin test edildiği bir yılı kısa süre önce tamamlamıştır. Bu insansız sistem, sektörün nesnelerin internetini benimsediğinin bir işaretidir. Hyundai bu sistemin el işçiliğine kıyasla üretkenliği üç kat arttırmasını beklemektedir. Daewoo şirketi de dev konteyner gemilerinin kritik bölümlerini inşa etmek için robot teknolojisini kullanmaktadır. Şirket, 2016' dan bu yana beş tanesi teslim edilen buz kırıcı sıvılaştırılmış doğal gaz taşıyıcılarının parçalarını kaynaklamak için 16 kg'lık bir robot kol kullanmaktadır. Şirket tarafından "Caddy" olarak adlandırılan bu kollar, dar bir alanda çelik yapıları birbirine kaynaştırmak için gövde üzerinde çalışabilmektedir (Munin-Doce vd., 2020).

Türkiye'de tersane sektörünün yaklaşık 700 yıllık bir geçmişi vardır. Türk gemi inşa sektörü hem miktar hem de tonaj olarak dünyanın en büyük üreticilerinden biridir. Son yirmi yılda Türk gemi inşa sanayisi küresel boyutta önemli bir büyüme yaşamıştır. Bu bağlamda Türkiye'de gemi inşa sanayi hem üretim hem de tersane üretimi açısından büyük bir gelişme göstermiştir (Cil vd., 2021).

Tersanelerin yerel yönetmelikteki tesis tanımına göre 2002 yılında 37 olan işletme sayısı Mart 2022 itibarıyla 84'e çıkmıştır. AB Yeşil Anlaşması tersanelerimize elektrikli ve hibrit gemi siparişlerini artırmıştır. Ayrıca tersanelerimiz özel amaçlı gemi inşasında da önemli başarılara imza atmıştır. İlk yüzer enerji gemisi, elektrikli römorkör, elektrikli-hibrit yolcu gemileri, elektrikli-hibrit feribotlar, balıkçı tekneleri gibi projeler tersanelerimizin başarıları arasında yer almaktadır. Bilgi teknolojilerindeki gelişmeler ve Endüstri 4.0 olarak adlandırılan yeni dönem, sektörde de etkisini göstermiştir. Günümüzde dünya gündeminde ön sıralarda yer alan "otonom gemiler" üzerine araştırmalar devam etmektedir ve savunma amaçlı insansız deniz araçları üzerinde çalışmalar yapılmaktadır. Savunma sanayisine yönelik projeler son birkaç yılda büyük bir ivme kazanmıştır. Özellikle MİLGEM Projesi'nin kayda değer kazanımlarıyla Türk tersaneleri, yüksek oranda yerli sanayi katılımının bulunduğu askeri gemi inşa projeleri için yurt dışından sipariş almaya başlamıştır. Bugün Türkiye'nin donanma ihtiyacı kendi ülkesinin tersanelerinden karşılanmaktadır (IMEAK Maritime Sector Report 2023).

2.2.4. Devlet kurumları

Türkiye'de Ulaştırma ve Altyapı Bakanlığı (UAB)'na bağlı düzenleme, denetim, kanun oluşturma ve uygulamada faaliyet gösteren birçok devlet kuruluşu bulunmaktadır. Bunlar; Kıyı Emniyeti Genel Müdürlüğü, Denizcilik Genel Müdürlüğü, Tersaneler ve Kıyı Yapıları Genel Müdürlüğü, Liman Başkanlıkları ve diğer ilgili kuruluşlardır (https://www.uab.gov.tr).

Kıyı Emniyeti Genel Müdürlüğünün genel görev ve sorumlulukları şunlardır (https://www.kiyiemniyeti.gov.tr/hakkimizda):

- Türkiye kıyılarında kurulmuş ve kurulacak güvenli seyir ile ilgili sistem ve tesisleri, fenerleri, deniz işaretlerini, sis düdüklerini ve benzeri seyir emniyeti ile ilgili her türlü cihaz ve tesisleri kurmak ve tekel şeklinde işletmek
- Kılavuzluk, römorkörcülük, palamar ve balıkadam hizmetlerini yapmak, işletmecilik esasları çerçevesinde batık çıkartmak, çıkarttırmak
- Denizlerimizde ve karasularımızda güvenli seyre yönelik kurulmuş ve kurulacak olan sahil telsiz istasyonları, otomatik tanımlama sistemi ve benzeri sistemlerle ilgili her türlü yatırımı yapmak ve tekel şeklinde işletmek
- Seyir emniyeti, gemi kurtarma ve deniz güvenliği ile ilgili hava, deniz ve kara vasıtalarını temin etmek ve bu vasıtaların her türlü bakım, onarım, yenileme ve donatımlarını sağlamaktır.

Denizcilik Genel Müdürlüğünün genel görev ve sorumlulukları şunlardır (https://denizcilik.uab.gov.tr/gorevler):

- Deniz ulaştırması faaliyetlerinin ticari, ekonomik, sosyal ihtiyaçlara ve teknik gelişmelere bağlı olarak ekonomik, seri, elverişli, güvenli, kaliteli, çevreye olumsuz etkilerini önleyecek ve kamu yararını gözetecek tarzda serbest, adil ve sürdürülebilir bir rekabet ortamında yapılmasını ve bu faaliyetlerin diğer ulaştırma türleriyle birlikte ve birbirlerini tamamlayıcı olarak hizmet vermesini sağlamak
- Deniz ulaştırması alanında hizmet üretenler ile hizmetten yararlananların hak, yükümlülük ve sorumluluklarını belirlemek
- Gemi adamlarının sicilinin tutulmasına ilişkin usul ve esasları belirlemek ve bunların sicilini tutmak, gemi adamlarının istihdamını desteklemek amacıyla ilgili kurum ve kuruluşlarla iş birliği yapmak
- Her türlü amatör denizcilik faaliyetine ilişkin usul ve esasları belirlemek, bu faaliyetleri yapacakları yetkilendirmek ve denetlemektir.

Tersaneler ve Kıyı Yapıları Genel Müdürlüğünün genel görev ve sorumlulukları şunlardır (https://tkygm.uab.gov.tr/gorevler):

- Tersaneler ile gemi geri dönüşüm tesisleri ve liman, iskele ve benzeri kıyı yapıları, kıyı yapılarıyla irtibatlı boru, kablo, kanal ve benzeri yapıların kapasitelerinin artırılmasına veya modernizasyonuna yönelik tevsi yatırımlarına izin vermek ve bunları denetlemek,
- Gemi ve diğer deniz araçlarının yapımı, bakımı, onarımı, donatımı, geri dönüşümü ve yan sanayinin gelişmesi için gerekli tedbirleri almak,
- Tersaneler ile gemi ve diğer deniz araçlarının projelerini incelemek, incelettirmek, onaylamak, yapımına izin vermek, projelere uygunluk bakımından denetlemek ve belgelendirmektir.

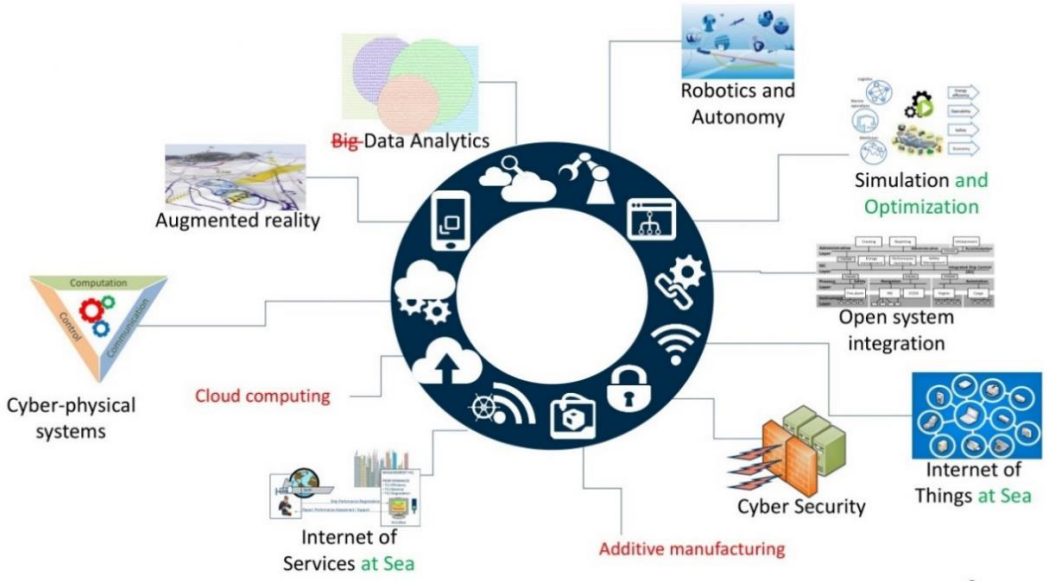
Liman Başkanlıklarının genel görev ve sorumlulukları şunlardır (https://manavgatliman.uab.gov.tr/baskanligin-gorev-ve-yetkileri):

- Denizde seyir güvenliğini sağlamak amacıyla, her türlü seyir yardımcılarını denetlemek, gerektiğinde yenilerinin tesisi için Bölge Müdürlüğüne teklifte bulunmak.
- Gemi adamı, balıkadam, yardımcı gemi adamlarının yeterliliği, sınavları, belgelendirme işlemleri ve başvurularını almak, neticelendirmek, arşiv dosyası oluşturmak,
- Liman Başkanlığı yetki sınırları içinde bulunan gemi inşa bakım, onarım, söküm ve çekek yerlerinin bakımlı ve elverişli olmasını gözetmek ve sağlamaktır.

2.2.5. Denizcilik sektöründeki dijital teknolojiler

Denizcilik 4.0, yeni pazara giriş, yatay ve dikey entegrasyon, yeni emniyet ve güvenlik çözümleri vb. için yeni fırsatlar sunmaktadır. Denizcilik alanı büyük insan kaynakları ve büyük veri işleme iş yükleri gerektirmektedir. Endüstri 4.0'ın denizcilik alanında ortaya çıkardığı insansız gemi teknolojisi ve veri analizi teknolojisi, denizcilik IoT'si, denizcilik IoS'si, siber-fiziksel sistemler, açık sistem entegrasyonu vb. denizcilik alanının el emeğinin azalmasına ve bunun yerine otonom makineler, yapay zekâ kullanmasına yardımcı olmaktadır (Pacchini vd., 2019).

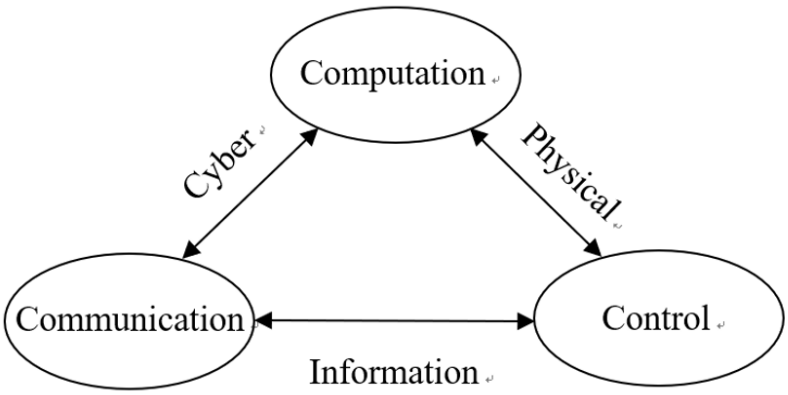
Denizcilik alanındaki endüstri 4.0 dijital teknolojiler Şekil 2.2'de gösterilmektedir.



Şekil 2.2 Denizcilik alanında endüstri 4.0 teknolojileri (Qi, 2021).

2.2.5.1. Siber fiziksel sistemler

Bilgi işlem teknolojisi, iletişim teknolojisi ve kontrol teknolojisinin hızlı gelişimi, insanın sosyal yaşamında büyük değişikliklere neden olmuştur. Bilişim ve sanayileşmenin derinlemesine entegrasyonu ve gelişmesiyle birlikte, geleneksel tek noktalı teknoloji artık yeni nesil üretim ekipmanlarının bilişim ve ağ oluşturma ihtiyaçlarını karşılayamamaktadır. Bu bağlamda Cyber-Physical Systems (CPS) olarak adlandırılan siber-fiziksel sistemler ortaya çıkmıştır. Almanya'nın "Endüstri 4.0 Uygulama Önerileri" CPS'yi Endüstri 4.0'ın temel teknolojisi olarak görmektedir. CPS, bilgi işlem, ağ ve fiziksel ortamları entegre eden çok boyutlu ve karmaşık bir sistemdir. Hesaplama, iletişim ve kontrol teknolojilerinin organik entegrasyonu ve derinlemesine iş birliği sayesinde, büyük ölçekli mühendislik sistemleri için gerçek zamanlı algılama, dinamik kontrol ve bilgi hizmetleri gerçekleştirmektedir (Guo & Jia, 2017).



Şekil 2.3 Siber fiziksel sistemler bileşenleri

CPS, geleneksel güvenlik sorunları temelinde daha fazla fiziksel sistem faktörü ortaya koyan, bilgi sistemleri ve fiziksel sistemlerle yakından ilişkili bir sistemdir. CPS, insan-bilgisayar etkileşimi ara yüzü aracılığıyla fiziksel süreçle etkileşimi gerçekleştirir ve fiziksel bir varlığı uzaktan, güvenilir, gerçek zamanlı, güvenli ve iş birliğine dayalı olarak kontrol etmek için ağa bağlı alanı kullanmaktadır. CPS'nin temel bileşimi Şekil 2.3'te görüldüğü gibi sensör, kontrol yürütme birimi ve hesaplama işlem birimini içerir. Bununla birlikte, CPS, ağ teknolojisini ve iletişim teknolojisini geleneksel fiziksel sistemlerin kontrolüne dahil eder ve bu da uygulamadaki mevcut kontrol yöntemlerinin sağlamlığı ve güvenilirliği konusunda zorlukları beraberinde getirmektedir (Li, vd., 2019).

CPS, sistemi daha güvenilir, verimli ve gerçek zamanlı iş birliği yapabilen bilgi işlem, iletişim ve fiziksel sistemlerin entegre tasarımını gerçekleştirir ve önemli ve kapsamlı uygulama olanaklarına sahiptir (Du & Pang, 2015).

CPS, denizcilik alanında CPS'in farklı uygulamaları için ileriye dönük fikirler sağlayabilecek beş temel teknik unsura sahiptir. Bunlar, algılama ve otomatik kontrol teknolojisi, endüstriyel yazılım teknolojisi, endüstriyel iletim ağı teknolojisi, hibrit bulut platformu teknolojisi, akıllı yönetim ve hizmet platformudur. Algı ve otomatik kontrol teknolojisi kapsamlı algı, otonom biliş ve uygulama odaklı otonom karar desteğine uygulanmaktadır. Endüstriyel yazılım teknolojisi veri alımı, depolama, dönüştürme ve temizleme vb. işlemlere uygulanmaktadır. Endüstriyel iletim ağı teknolojisi, cihazlar arasında her yerde bulunan bağlantıya ve ara bağlantıya uygulanmaktadır. Hibrit bulut platformu teknolojisi, sistem özerkliğine uygulanmaktadır. Akıllı yönetim ve hizmet platformu, kuruluşlar arasında ve kuruluşun çeşitli departmanlarının iş süreçleri arasında iş birliği ile ilgili kaynak entegrasyonu, faaliyet optimizasyonu ve karar desteği için kullanılmaktadır (Li, vd., 2019).

Özetle, CPS, denizcilik alanında büyük bir uygulama potansiyeline sahiptir. Örneğin, seyir aletleri uygulamasında, CPS elektronik haritaların optimizasyonunu güçlendirecek ve grafik görüntüleme, bilgi sorgulama, veri tabanı yönetimi, bilgi analizi ve diğer işlevler dahil olmak üzere yeni işlevler geliştirecektir. Ayrıca, çok modlu taşımacılığın verimli modunu teşvik edecek, GPS gibi gelişmiş sistemlerle birlikte bilgi paylaşımını, kaynak paylaşımını kullanacak ve denizcilik alanında dijitalleşme, bilişim ve istihbaratın gelişimini teşvik edecektir. Gelecekteki pratik uygulamalarda veri tabanı güncellenecek, sistem iyileştirilecek ve uygulama kapsamı genişletilecektir (Pacchini vd., 2019).

2.2.5.2. Blok zincir

Blok zinciri, dağıtılmış veri depolama, noktadan noktaya iletim, mutabakat mekanizması ve şifreleme algoritması gibi bilgisayar teknolojisinin yeni bir uygulama modudur (Li, 2020). Teknolojik açıdan bakıldığında, blok zinciri matematik, kriptografi, internet ve bilgisayar programlama gibi birçok bilimsel ve teknolojik konuyu içermektedir. Uygulama açısından bakıldığında, basit bir ifadeyle blok zinciri, veri bloklarını kronolojik sırayla birleştiren zincirleme bir veri yapısıdır. Kurcalanamaz ve sahteciliğe karşı kriptografi ile garanti edilir. Ademi merkeziyetçilik, kurcalamama, tam iz saklama, izlenebilirlik, toplu bakım, açıklık ve şeffaflık vb. özelliklere sahiptir. Halka açık blok zinciri, ortak (endüstri) blok zinciri ve özel blok zinciri olmak üzere üç türe ayrılmaktadır (Zou, 2020).

Blok zincirinin temel teknolojileri arasında dağıtık defterler, asimetrik şifreleme, mutabakat mekanizmaları ve akıllı sözleşmeler yer almaktadır (Zou, 2020). Blok zincirinin ana uygulama alanları arasında finans alanı, IoT ve lojistik, kamu hizmeti alanı, sigorta alanı bulunmaktadır (Song, 2020). Bununla birlikte, çeşitli alanlarda yaygın olarak kullanılmasına rağmen, mevcut kavramlar, sistemler ve yasalar tarafından kısıtlanması, teknik zorluklar ve rekabetçi teknik zorluklar gibi birçok zorlukla da karşı karşıyadır (Li, 2020).

Şu anda, Endüstri 4.0'ın ortaya çıkmasıyla birlikte, blok zincir teknolojisi denizcilik yönetiminde uygulanmıştır, ancak denizcilik alanında yaygın olarak kullanılmamıştır. Blok zinciri temel olarak evrak işlerini, takip ve izlemeyi, gümrükleme ve yönetimi dijitalleştirmek ve basitleştirmek için kullanılmaktadır. Veri paylaşımını teşvik edebilir, iş süreçlerini optimize edebilir, işletme maliyetlerini azaltabilir, iş birliği verimliliğini artırabilir ve güvenilir sistemler oluşturabilmektedir. Blok zinciri veri paylaşım modeli kullanılarak, denizcilik kurumları hizmet verileri de departmanlar ve bölgeler arasında ortaklaşa muhafaza edilebilir ve kullanılabilir. Akıllı liman uygulaması esas olarak blok zinciri teknolojisinin uygulanmasına, elektronik belgelerin teşvik edilmesine, çevrimiçi iş işlemeye, tehlikeli malların tam zincir denetimine ve tam lojistik görselleştirmeye yansımaktadır. Buna ek olarak, blok zincir mürettebat yönetimi, gemi yönetimi, navigasyon yönetimi, tehlikeli madde yönetimi, kirlilik önleme yönetimi ve denizcilik acil yardım gibi denizcilik denetimi ve hizmet işlerinde uygulanmaktadır (Ellingsen & Aasland, 2019).

2.2.5.3. Nesnelerin interneti

İnternet 1969'da Amerika Birleşik Devletleri'nin ARPANET (Advanced Research Projects Authority Net)'i ile başlamıştır. İnternetin doğuşundan bu yana netizen sayısı hızla artmış, uygulama alanları da her geçen yıl artmıştır. Küresel İnternet, 1990'lı yıllarda ticari kullanıma girdiğinden bu yana hızla genişlemiş ve bugün dünyada ekonomik kalkınmayı ve sosyal ilerlemeyi teşvik etmek için önemli bir bilgi altyapısı haline gelmiştir. İnternet birden fazla bilgisayar ağının buluşmasıyla oluşan bir ağdır. Son yıllarda Endüstri 4.0'ın hızlı gelişimi ve yeni nesil bilgi teknolojisiyle birlikte Nesnelerin İnterneti (IoT), dünyada ekonomik ve teknolojik gelişmenin yeni döneminin stratejik yönlerinden biri haline gelmiştir. IoT, internete dayalı olarak yüksek hızda geliştirilen yeni bir uygulama teknolojisidir. Bilgisayar ve internetten sonra bilişimin üçüncü dalgası olarak kabul edilmektedir (Dong & Liu, 2010).

Gemilerin İnterneti, IoT'nin denizcilik alanında yeni bir uygulamasıdır. Inmarsat (The International Maritime Satellite Organization)'ın araştırması, denizcilik işlerinde internete yapılan harcamaların diğer sektörlerin harcamalarını aştığını ve denizcilik sektörünün IoT'ye yaptığı sermaye yatırımının diğer sektörlerinkini çok aştığını göstermektedir Hibrit web/masaüstü uygulamalarının gelişme eğilimi devam ettikçe, RIA'nın (Zengin İnternet Uygulamaları) kullanım ve işlevsellik bakımından ilerleyebileceği öngörülmektedir. Denizcilik alanında IoT/IoS hizmetlerinin uygulanması, akıllı ulaşım sistemlerini, deniz depolama yönetimini, nakliye denetimini, dijital liman ve nakliye inşaatını, denizcilik uydu çağrı merkezi platformu inşaatını ve denizcilik işlerini içermektedir. Bunların arasında Akıllı Ulaşım Sistemi (ITS), modern bilgi teknolojisini temel olarak kullanır ve AIS (Automatic Identification System), VTS, LRIT, okuyucular, sensörler, navigasyon yardımcıları, uzaktan algılama, GPS'yi iletmek için gelişmiş iletişim, bilgisayar, otomatik kontrol ve sensör teknolojilerini kullanmaktadır (Du & Pang, 2015).

Gelecekte internet teknolojisine dayalı olarak uzak bilgisayar odaları, uzaktan pilotaj, uzaktan köprüler vb. gerçekleştirmek mümkündür. Buna ek olarak, denizcilik ağ teknolojisinin uygulanması, denizcilik denetimi, deniz güvenliği ve kapsamlı yönetimde denizcilik yönetimiyle yakından ilgili olan mürettebat, gemiler ve yükleri, navigasyon ortamı ve navigasyon yardım hizmetleri gibi denizcilik yönetimiyle ilgili dinamik ve statik yönetim bilgilerini entegre etmek için teknolojik yeniliğe dayanacaktır (Dong & Liu, 2010).

IoT/IoS hizmetleri, BT operasyonlarına daha iyi, daha verimli, daha çevre dostu ve daha sürdürülebilir bir şekilde yardımcı olmak için yeni birbirine bağlı teknolojilere

odaklanacaktır. İnternet teknolojisinin ve radyo frekansı tanımlama (RFID) teknolojisi ile temsil edilen Nesnelerin İnterneti teknolojisinin denizcilik alanında uygulanması uzun vadeli önem taşımaktadır. İlk olarak, deniz taşımacılığı tesisleri ve ekipmanlarının bilgilenme derecesi hızlandırılacak ve mevcut tesis ve ekipmanlar, deniz taşımacılığının bilgilendirme sürecini teşvik edecek şekilde güncellenecek, optimize edilecek ve geliştirilecektir. İkincisi, denizcilik sistemleri arasında bilgi kaynağı paylaşımının ve iş birliğinin gerçekleştirilmesi hızlandırılacaktır. Üçüncüsü, entegre ulaşım sisteminin gelişiminin ilerletilmesi için gerekli bir teknik destek haline gelmiştir. Dördüncüsü, deniz taşımacılığı güvenliği denetiminin ve acil durum müdahale yeteneklerinin iyileştirilecektir. Beşincisi, denizcilik bilişim algısının inşasını, denizcilik bilgi temel ve özel ağlarının inşasını, temel veri tabanlarının inşasını ve denizcilik bilişim uygulamalarının geliştirilmesini teşvik etmeye yardımcı olmaktadır. IoT/IoS hizmetleri, gemi dinamik bilgi toplama, insansız gemiler, insansız sürüş, dijital liman ve nakliye inşaatı ve denizde acil durum komuta arama ve kurtarma gibi denizcilik alanında geniş uygulama beklentilerine sahiptir. Trafik unsuru algılama bilgilerinin gerçek zamanlı iletimini gerçekleştirmek için mevcut deniz özel ağı, internet, kablosuz iletişim ağı vb. temel alınarak daha rahat ve daha hızlı olacaktır. IoT/IoS hizmetleri denizcilik alanının dijital ve akıllı gelişimini desteklemeye devam etmektedir (Bucak vd., 2019).

2.2.5.4. Büyük veri

Son yıllarda büyük veri, Endüstri 4.0, bulut bilişim ve kişisel medya ile birlikte bir bilişim çılgınlığı yaratmıştır. Büyük veri internetin hızlı gelişmesiyle doğmuştur. Büyük veri terimi ilk olarak 1980 yılında Alvin Toffler tarafından yayınlanan "Üçüncü Dalga" kitabında karşımıza çıkmıştır (Wu, 2020). Bulut çağının gelişiyle birlikte büyük veri artık giderek daha fazla kullanılmaktadır. Büyük veri, içeriği belirli bir süre içerisinde yakalanamayan, yönetilemeyen ve geleneksel yazılım araçlarıyla işlenemeyen veri koleksiyonunu ifade etmektedir. Veri, yalnızca internetteki çeşitli faaliyetler tarafından üretilen bilgi ve verileri ifade etmekle kalmaz, aynı zamanda endüstriyel ekipmanlar, ölçüm cihazları ve çeşitli sensörler dahil olmak üzere dünyada kurulu çeşitli sensörler tarafından ölçülen ve iletilen konum, sıcaklık ve ışık yoğunluğunu da içermektedir. Büyük veri teknolojisi, çeşitli veri türlerinden değerli bilgileri hızlı bir şekilde elde etme yeteneğini ifade etmektedir. Büyük veri hacmi, çeşitli veri türleri, hızlı işlem hızı ve düşük değer yoğunluğu dahil olmak üzere dört temel özelliğe sahiptir. Büyük veriye uygulanabilir teknolojiler arasında büyük ölçüde paralel işleme veri tabanları, veri

madenciliği, dağıtılmış dosya sistemleri, dağıtılmış veri tabanları, bulut bilişim platformları, internet ve ölçeklenebilir depolama sistemleri yer almaktadır (Chang, 2020).

Denizcilik sektörü, büyük miktarda veri içeren tipik bir geleneksel sektördür. Örneğin, denizcilik piyasası verileri, liman terminali verileri, denizcilik yetenek verileri, gemi işlem fiyatı verileri, denizcilik hizmet verileri kullanılmaktadır. Büyük veri, denizcilik alanında güvenlik denetimi, iş uygulamaları, acil durum yönetimi, kamu hizmeti ve deniz güvenliği açısından geniş uygulama olanaklarına sahiptir. Örneğin, gemi dinamik izleme sistemi, denizcilik bulut verileri, denizcilik yönetimi departmanlar arası veri paylaşımı, AIS verileri, AIS sanal navigasyon işareti uygulaması, GPS konumlandırma sistemi, denizcilik büyük veri bulut hizmeti platformu, gemiler, konteynerler ve kargo platformları için tek noktadan gerçek zamanlı bilgi hizmetleri, liman operasyon yönetimi, otonom gemiler ve insansız dedektörlerin tümü büyük veri kullanılarak uygulanabilir durumdadır. Aynı zamanda görselleştirilmiş büyük veriler, nakliye şirketlerine tahmine dayalı analizler sağlayabilir ve ticari ihracat hacmini analiz ederek rota geliştirme planlamasına temel sağlayabilir (Ren, 2021).

En son denizcilik büyük veri uygulama konsepti, çok boyutlu ve çok tipli bir büyük veri rota görselleştirme sistemine, bir denizcilik kurumsal müşteri ilişkileri yönetim sistemine ve liman üretim operasyon zinciri için tam bilgi izlenebilirliğine ve yardımcı karar verme sistemine sahiptir (Chang, 2020).

2.2.5.5. Yapay zekâ

Alan Turing'in, bir makinenin insan-makine diyaloğu gibi yeteneğini test etmek için Turing testini önerdiği 1950 yılından bu yana, yapay zekâ (AI), bilgisayar bilimcilerin hayali haline gelmiştir. Yapay zekâ, sözde akıllı makinelerin ve akıllı sistemlerin temel sağlayıcısıdır. Yapay zekânın temel itici güçleri, giderek artan bilgisayar işlem gücü, bağlantı ve ses ve görüntü tanıma gibi teknolojilerdir. İnsan hızının çok ötesinde analiz etme ve karar verme yeteneği sağlamaktadır (Zhong, 2018).

Diğer dijital teknolojilerle karşılaştırıldığında, yapay zekâ daha ileri düzeydedir ve daha geniş bir gelişme beklentisine sahiptir. Limanın ve diğer nakliye departmanlarının verimliliğini büyük ölçüde artıracaktır. Denizcilik sektörünü teknolojik inovasyon yoluna yönlendirecektir. AI, toplumun tüm sektörleri, özellikle de işlerini daha hızlı, daha ucuz ve daha verimli bir şekilde yürütebilmekten faydalanacak olan denizcilik sektörü için büyük fırsatlar sunmaktadır. Gemiler, petrol kuleleri veya diğer platformlar kullanılırken, AI insanlı ve insansız seçenekleri destekleyebilir. İnsansız gemiler ve

otonom sürüş teknolojisi araştırmalarında, insansız gemiciliği daha da teşvik etmek için yapay zekâ uygulaması gemilere yerleştirilecektir (Qi, 2021).

2.2.5.6. Makine öğrenimi

Makine öğrenmesi yapay zekânın bir dalıdır. Büyük veri çağında çeşitli sektörlerde veri analizine olan talebin sürekli artmasıyla birlikte, makine öğrenmesi yoluyla bilginin verimli bir şekilde elde edilmesi, giderek günümüz makine öğrenmesi teknolojisinin gelişmesinin ana itici gücü haline gelmiştir (Akyuz vd., 2019). Makine öğrenimi, yapay zekânın özüdür ve bilgisayarları akıllı hale getirmenin temel yoludur. Yapay zekânın gelişim süreci açısından bakıldığında makine öğrenimi, yapay zekâ uygulamasının uzman sistemlerden sonra bir diğer önemli araştırma alanıdır ve aynı zamanda yapay zekâ ve sinirsel hesaplamanın temel araştırma konularından biridir. (Cai vd., 2016).

Makine öğreniminin gelişim süreci kabaca dört aşamaya ayrılabilir. İlk aşama 1950'lerin ortalarından 1960'ların ortalarına kadar olan dönem, heyecan dönemidir. 1960'ların ortalarından 1970'lerin ortalarına kadar olan ikinci aşamaya makine öğreniminin soğuma dönemi adı verilmiştir. 1970'lerin ortalarından 1980'lerin ortalarına kadar olan üçüncü aşamaya canlanma dönemi adı verilmektedir. Dördüncü aşama, makine öğreniminin 1980'lerin ortasındaki en son aşamasıdır. Makine öğreniminin son aşaması 1986'da başlamıştır. Bilgi keşfi ilk olarak Ağustos 1989'da önerilmiştir (Cai vd., 2016).

Makine öğrenmesi yalnızca bilgi tabanlı sistemlerde kullanılmamakta, aynı zamanda doğal dil anlama, monoton olmayan akıl yürütme, makine görüşü, örüntü tanıma gibi birçok alanda da yaygın olarak kullanılmaktadır. Denizcilikte dijitalleşmenin giderek artmasıyla birlikte makine öğrenimi de denizcilik alanına yavaş yavaş uygulanmaya başlanmıştır. Ancak diğer sektörlerle karşılaştırıldığında makine öğrenimi teknolojisinin deniz taşımacılığında uygulama kapsamı daha dardır. Makine öğrenmesi teknolojisi deniz ağı planlaması, sefer planlaması, kargo operasyonu optimizasyonu, bakım prosedürleri, sürdürülebilir ulaşım, yük kontrolü, takviyeli öğrenme, enerji verimliliği yönetimi, deniz güvenliğinin iyileştirilmesi ve diğer alanlarda kullanılabilir. Bunlar arasında sefer planlaması, yakıt verimliliğinin artırılması, mürettebat yükünün en aza indirilmesi, yolculuk tahmininin iyileştirilmesi, en iyi devir eğrisinin hesaplanması, gemi hız kontrolü, rota planlaması gibi konuları içermektedir. Bakım süreci, gövde ve motorun

bakım ve onarım çalışmalarının optimize edilmesine yardımcı olmayı içermektedir (Akyuz vd., 2019).

Ek olarak denizcilik alanı, çeşitli görevlerin düzenli bir şekilde ilerlemesine yardımcı olabilecek gemi akıllı çarpışmadan kaçınmaya karar verme, gemi planlama optimizasyonu, deniz güvenliği bilgileri otomatik sınıflandırma ve karar desteği, AIS iz analizi ve anormal yörünge tespiti, otonom insansız tekne çarpışmasından kaçınma, gemi trafik güvenliği uyarısı, gemi uyarlanabilir yörünge tahmini, denizcilik durumu istihbarat analizi, deniz dizel motorunun arıza teşhisi, deniz trafik işaretlerinin tanımlanması gibi çok sayıda veri içermektedir (Cai vd., 2016).

2.2.6. Dijital olgunluk

Olgunluk yapıları, etkili bir çerçevenin parçalarını ayırt etmenin yanı sıra dijital sistemlerin başlangıçtan yürütmeye ve ardından etkiye kadar nasıl geliştiğinin ilerlemesini yakalamaktadır (Khanbhai vd., 2019). Bir kuruluşun veya ulusun yaklaşan değişiklikleri yenmeye hazır olduğunu göstermektedir (Kutnjak vd., 2020). Dijital olgunluk, kuruluşun pazarda rekabetçi kalabilmek için kalıplara bağlı olarak yaratıcı teknolojileri değiştirme ve uygulama hazırlığını ve kapasitesini göstermektedir (Eremina vd., 2019). Teichert (2019) dijital olgunluğu, kuruluşun dijital dönüşüm açısından nerede olduğunun bir yansıması olarak tanımlamıştır. Ayrıca, halihazırda elde edilen dönüşüm çabalarının durumunu ve daha ileri dijital yeniliklere hazır olma durumunu tanımlamaktadır. Dijital olgunluk, hızla büyüyen bir dijital ortamda amansız ve kalıcı bir değişim sürecidir (Salviotti vd., 2019).

İşletmenin sistemini, çalışanlarını, kültürünü ve tasarımını müşteriler, temsilciler ve müşteriler için dijital varsayımlarla başa çıkacak şekilde ayarlayarak dijital yenilikler gerçekleştirmeyi gerektirir. Dolayısıyla dijital olgunluk, hızla ilerleyen dijital ortama yönelik kesintisiz ve sürekli bir dönüşüm sürecidir. Dijital dönüşümün amacı, kurumun çalıştığı alanın dijitalleşmesinin sunduğu ilerleme ve zorluklara göre kabul edilebilir bir dijital olgunluk seviyesine ulaşmak olduğundan, bir kurumun dijital olgunluğunun ölçümü dijitalleşme etkileşiminde kritik bir aşamadır. Dijital dönüşümün nitelikleri ve zorlukları her faaliyet alanına ve hatta her tür kuruluşa özgüdür ve bu nedenle her biri belirli bir dijital olgunluk modeli gerektirebilmektedir. (Nerima & Ralyté, 2021).

2.2.7. Dijital olgunluk modelleri

Dijital olgunluk modelleri, mevcut ve beklenen gelişim düzenlemelerini karakterize eden araçlardır, ancak hedefe ulaşmak için üstün bir yöntem önermedikleri için kuralcı değildirler (Menchini vd., 2021).

Ayrıca dijital olgunluk modelleri, dijital dönüşümle ilgili olarak mevcut durumun ve dijital olgunluk seviyesinin belirlenmesine hizmet etmekte ve mevcut olgunluk seviyesinden hareketle gelecekteki faaliyetler için önerilerde bulunulmasına olanak tanımaktadır (Schallmo vd., 2020).

Olgunluk modeli, çeşitli bölgelerin ana hatlarını verdiği ve kuruluşların değişime nasıl yaklaştıklarına dair düzenli yollara rehberlik ettiği için bu konuda bir yön vermektedir (Back & Berghaus, 2016).

Bu çalışmada oluşturulan kriterler ve alt kriterler literatür araştırmaları sonucunda 9 modele dayandırılmıştır.

2.2.7.1. Üretim işletmelerini değerlendirmek için olgunluk modeli

Schumacher vd. (2016) yaptıkları çalışma ile, ayrık üretim alanındaki endüstriyel işletmelerin Endüstri 4.0 olgunluğunu değerlendirmek için ampirik olarak temellendirilmiş yeni bir model ve bunun uygulamasını önermişlerdir. Genel olarak 9 boyut tanımlamışlardır ve Endüstri 4.0 olgunluğunu değerlendirmek için bunlara 62 madde atamışlardır. Ürünler, müşteriler, operasyonlar ve teknoloji boyutları temel kolaylaştırıcıları değerlendirmek üzere oluşturulmuştur. Buna ek olarak, strateji, liderlik, yönetişim, kültür ve insanlar boyutları, kurumsal yönlerin değerlendirmeye dahil edilmesine olanak tanımaktadır. Daha sonra, model pratik bir araca dönüştürülmüş ve birkaç şirkette test edilmiş olup, makalede bir vaka sunulmuştur. Modelin yapısı ve içeriğine ilişkin ilk doğrulamalar, modelin şeffaf ve kullanımının kolay olduğunu göstermiş ve gerçek üretim ortamlarında uygulanabilirliğini kanıtlamıştır. Kriterlerler likert ölçeği ile 5 seviyede değerlendirilmiştir. Geliştirmiş oldukları kriterler ve örnek olgunluk maddeleri Tablo 2.2'de gösterilmiştir.

Tablo 2.2 Üretim işletmeleri için olgunluk kriterleri ve örnek olgunluk maddeleri (Schumacher vd., 2016)

Olgunluk Kriterleri	Örnek Olgunluk Maddeleri
Strateji	Endüstri 4.0 yol haritası uygulanması, gerçekleştirilmesi için mevcut kaynaklar, iş modellerinin uyarlanması
Liderlik	Liderlerin istekliliği, yönetim yeterlilikleri ve yöntemleri, Endüstri 4.0 için merkezi koordinasyonun varlığı
Müşteriler	Müşteri verilerinin kullanılması, satışların/hizmetlerin dijitalleştirilmesi, müşterinin Dijital medya yetkinliği
Ürünler	Ürünlerin bireyselleştirilmesi, ürünlerin dijitalleştirilmesi, diğer sistemlere ürün entegrasyonu
Operasyonlar	Süreçlerin merkezden uzaklaştırılması, modelleme ve simülasyon, Disiplinler arası, departmanlar arası iş birliği
Kültür	Bilgi paylaşımı, açık inovasyon ve şirketler arası iş birliği, Şirkette BİT'in değeri
İnsanlar	Çalışanların BİT yeterlilikleri, çalışanların yeni teknolojiye açıklığı, çalışanların özerkliği
Yönetim	Endüstri 4.0 için çalışma düzenlemeleri, teknolojik standartların uygunluğu, fikri mülkiyetin korunması
Teknoloji	Modern BİT'in varlığı, mobil cihazların kullanımı, makineden makineye iletişimin kullanılması

2.2.7.2. Impuls endüstri 4.0 olgunluk modeli

Lichtblau vd. (2015) çalışmalarında, makine ve tesis mühendisliği alanlarındaki şirketlerin şu anda nerede durduklarını incelemiş, onları neyin motive ettiğine ve neyin geride tuttuğuna ve bir yandan küçük ve orta ölçekli işletmeler ile diğer yandan büyük işletmeler arasında ortaya çıkan farklılıklara odaklanmışlardır. Çalışmalarının sonuçları, mühendislik sektöründe Endüstri 4.0'a hazır olma durumunun ilk kez ayrıntılı ve sistematik bir resminin çizilmesini mümkün kılmaktadır.

Şirketlerin yapısal özelliklerini, endüstri 4.0 hakkında genel soruları, şirketlerin endüstri 4.0 boyutlarını karşılama derecesini, endüstri 4.0 yolundaki motive edici faktörler ve engelleri araştırmak için bir anket geliştirmişlerdir. Hazırlık modelinin olgunluk seviyeleri ise; Seviye 0: Yabancı, Seviye 1: Yeni Başlayan, Seviye 2: Orta Seviye, Seviye 3: Deneyimli, Seviye 4: Uzman, Seviye 5: En iyi performansı göstermektedir. Modelleri Tablo 2.3'teki gibi toplamda altı ana boyuttan ve 18 alt boyuttan oluşmaktadır.

Tablo 2.3 Impuls olgunluk modeli ana kriterler ve alt kriterler (Lichtblau vd., 2015)

Kriterler	Alt Kriterler
Strateji ve Organizasyon	Strateji
	Yatırımlar
	İnovasyon Yönetimi
Akıllı Fabrika	Dijital Modelleme
	Altyapı
	Veri Kullanımı
	BT Sistemleri
Akıllı Operasyonlar	Bilgi Paylaşımı
	Özerk Süreçler
	BT Güvenliği
	Bulut Kullanımı
Akıllı Ürünler	BİT Eklenti İşlevleri
	Veri Analizi
Veri Tabanlı Hizmetler	Veri Odaklı Hizmetler
	Gelir Payı
	Kullanılan Verilerin Seviyesi
Çalışanlar	Beceri Edinme
	Çalışan Beceri Setleri

2.2.7.3. Akıllı liman gelişimine yönelik dijital olgunluk modeli

Paulauskas ve Philipp (2020) limanların dijital hazır olma durumunu değerlendirmek için bir araç uygulamayı ve bunun üzerine inşa ederek sürdürülebilir bir akıllı liman gelişimine yönelik dijital dönüşüm için yol haritasını belirleyen somut bir stratejik mezuniyet elde etmeyi amaçlamışlardır. Büyüklükleri ve yük tercihleri ne olursa olsun limanların dijital performansının nasıl değerlendirilebileceğini, limanların akıllı limana dönüşebilmesi için hangi stratejik tavsiyelerin türetilebileceğini araştırmaya çalışmışlardır. Araştırmalarını, INTERREG Güney Baltık Programı 2014-2020 sınır ötesi iş birliği platformunda uygulanan "Connect2SmallPorts" isimli AB projesi çerçevesinde gerçekleştirmişlerdir.

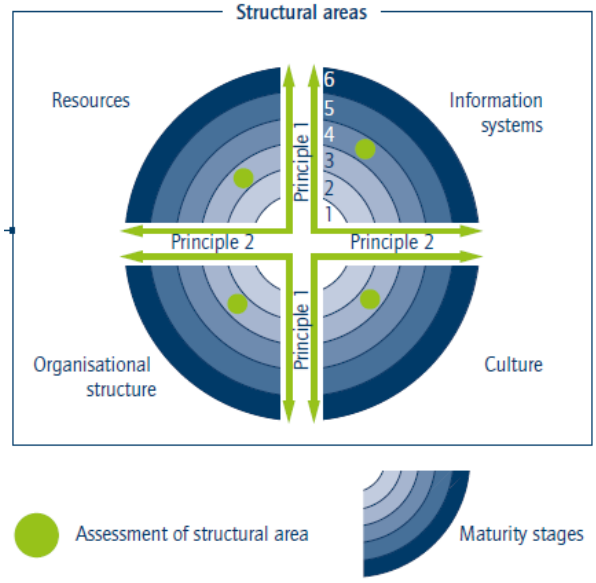
Ayrıca, literatür taraması makaleleri çerçevesinde limanlar için dijital hazırlık endeksini teorik bir temelde önermişler ve limanlar için eksik dijital performans araçlarına ilişkin tespit edilen ilgili araştırma boşluğunu kapatmışlardır. Limanlar için oluşturdukları bu dijital hazırlık endeksi DRIP olarak adlandırılmaktadır. Göstergeler, dijital hazırlık endeksleri, olgunluk modelleri ile analiz edilmiş literatür bulgularına dayanarak çalışmalarını meydana getirmişlerdir. Çalışmaları türünün ilk örneğidir ve örneğin potansiyel bir öz değerlendirme veya kıyaslama çerçevesinde limanların dijital performansının denetlenmesine olanak sağlamaktadır. DRIP dijital hazırlık endeksi beş

boyuttan, birbiriyle ilişkili 38 bölümden ve 6 seviyeden oluşmaktadır. Toplam boyutun yönetim %20 sini, insan etkisi %20 sini, işlevsellik (IT) %25 ini, teknoloji %30 unu, bilgi %5 ini, oluşturmaktadır.

2.2.7.4. Acatech endüstri 4.0 olgunluk modeli

Schuh vd. (2017), şirketlerin mevcut endüstri 4.0 olgunluk aşamasını oluşturmanın bir yolunu sağlamak ve endüstri 4.0 ve dijitalleşmenin ekonomik faydalarını en üst düzeye çıkarmak amacıyla daha yüksek bir olgunluk aşamasına ulaşmalarına yardımcı olacak somut önlemleri belirlemeye yönelik bir çalışma gerçekleştirmişlerdir. Mevcut süreçlerin değerlendirilmesi ve ardından eylem gerektiren alanların belirlenmesi, şirketlere dijital dönüşümlerini şekillendirmek için özel ve pratik rehberlik sağlamaktadır. Acatech Endüstri 4.0 Olgunluk Endeksi, bir şirketin yapısını kaynaklar, bilgi sistemleri, kültür ve organizasyonel yapı olmak üzere dört yapısal alana ayırmaktadır. Acatech Endüstri 4.0 Olgunluk Endeksi'nde "kaynaklar" somut, fiziksel kaynakları ifade etmektedir. Bunlar bir şirketin işgücünü (insan kaynakları), makine ve ekipmanlarını, araçlarını, malzemelerini ve nihai ürününü içermektedir.

Firma çalışmaları kaynak yapısal alanında dijital yetenek ve yapılandırılmış iletişim açılarından incelenmektedir. Bilgi sistemleri alanı, kendi kendine öğrenen bilgi işleme ve bilgi sistemi entegrasyonundan oluşur. Organizasyon yapısı, organik iç organizasyon ve değer ağı içerisinde dinamik iş birliğini kapsayan iki prensip tarafından oluşmaktadır. Kültür yapısı ise değişim isteği ve sosyal iş birliğini barındırmaktadır. Accatech Endüstri 4.0 Olgunluk Endeksi Şekil 2.4'te gösterilmiştir.



Şekil 2.4 Accatech endüstri 4.0 olgunluk endeksi

2.2.7.5. Tübitak dijital olgunluk modeli

TÜBİTAK ve BİLGEM Yazılım Teknolojileri Araştırma Enstitüsü (YTE) tarafından 2017 yılında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan kurumsal "Dijital Olgunluk Modeli" geliştirilmiş ve bu yönde kurumsal dijital kapasitenin arttırılması amacıyla model ile uyumlu "İşletim ve Bakım Rehberi" hazırlanmıştır. Model ile kamu kurumlarının dijitalleşme konusundaki yetkinliğinin ve kapasitesinin belirlenmesi amaçlanmıştır.

Model stratejik yönetişim, organizasyon, yazılım hizmetleri, yazılım yaşam döngüsü, işletme ve bakım, BT hizmetleri ve d-hizmetler adlı 7 ana kriterden oluşmaktadır. Model 5'li likert ölçeği ile değerlendirilmiştir.

2.2.7.6. Pwc dijital olgunluk modeli

PwC (Price Waterhouse Coopers) isimli danışmanlık firmasının 2016 yılındaki küresel Endüstri 4.0 araştırması, dokuz ana sanayi sektöründen ve 26 ülkeden 2.000'den fazla katılımcının yer aldığı, türünün dünya çapındaki en büyük araştırmasıdır. Çalışma, şirketlerin yatay ve dikey değer zincirlerini dijitalleştirmenin yanı sıra dijital ürün ve hizmet portföyü oluşturmanın faydalarını araştırmaktadır (Geissbauer vd., 2016).

Çalışmada şirketlerin dijital başarıya ulaşmaları için, endüstri 4.0 stratejilerini oluşturmaları, pilot projeler hazırlamaları, gerekli yetenekleri ifade etmeleri, veri analizinde uzman olmaları, dijital bir işletmeye dönüşmeleri ve firma-çevre uyumunu faal olarak planlamaları gerektiği bildirilmiştir.

Model 4 aşamadan oluşmaktadır. Bunlar;

- Dijital acemi
- Dikey bütünleştirici
- Yatay iş birlikçi
- Dijital şampiyondur.

Olgunluk modeli 7 boyut üzerine kurulmuştur. Bunlar;

- Dijital iş modeller ve müşteri erişimi,
- Ürün ve hizmet sunumlarının dijitalleştirilmesi
- Dikey ve yatay değer zincirlerinin dijitalleşmesi ve entegrasyonu
- Temel yetenek olarak veri ve analitik
- Çevik bilgi teknolojileri mimarisi
- Uyum, güvenlik, hukuk ve vergi

- Organizasyon, çalışanlar ve dijital kültürdür.

2.2.7.7. Dreamy dijital olgunluk modeli

De Carolis vd. (2017) çalışmalarında "imalat şirketleri dijitalleşmeye hazır mı?" sorusundan hareketle, imalat firmalarının dijital hazırlığını ölçmek için bir olgunluk değerlendirme yöntemi oluşturarak bu soruyu yanıtlamak için bir "araç" göstermeyi amaçlamışlardır. CMMI (Capability Maturity Model Integration) çerçevesinin ilham verici ilkelerine dayanarak, şirketin dijital olgunluğunun araştırılmasına zemin hazırlamak için DREAMY (Digital Readiness Assessment Maturity) modelini önermişlerdir. Temel üretim süreçlerinin gruplandırılabileceği 5 alanı değerlendirmek için farklı boyutlar kullanılmaktadır: 1) tasarım ve mühendislik, 2) üretim yönetimi, 3) kalite yönetimi, 4) bakım yönetimi ve 5) lojistik yönetimi. Böylece olgunluk modeli, her bir alan ve boyuttaki uygulamaların normatif bir tanımını sunmakta ve uygulamaların sıralı bir düzenini (yani düşük olgunluktan yüksek olgunluğa doğru) oluşturmaktadır. Başlangıç, yönetilen, tanımlı, entegre ve beraber çalışılabilirlik, dijital oryantasyonu içeren 5 olgunluk seviyesi belirlenmiştir. Dijital dönüşümün uygulanmasındaki kritik noktaları belirlemek ve ardından tüm sistemin iyileştirilmesini sağlamak amacıyla olgunluk değerlendirmesi için bir puanlama yöntemi tanımlanmıştır.

2.2.7.8. Endüstri 4.0 hazırlık değerlendirme olgunluk modeli

Agca vd. (2017), İngiltere Warwick Üniversitesi'ndeki (WMG) araştırmalarına dayanarak, endüstriyel işbirlikçileri Crimson & Co yönetim danışmanlığı firması ve Pinsent Masons hukuk firması ile birlikte bir Endüstri 4.0 hazırlık değerlendirme aracı geliştirmişlerdir. Amaçları, şirketlerin siber-fiziksel çağın potansiyelinden yararlanmaya yönelik hazırlıklarını ve gelecekteki hedeflerini değerlendirmeye başlamaları için basit ve sezgisel bir yol sağlamaktır.

Modelleri 6 ana kriter ve 37 alt kriterden oluşmaktadır. Bu kriterler 4 hazırlık seviyesi (başlangıç, orta, deneyimli ve uzman) etrafında tasarlanmıştır. Ana kriterler;

- Ürün ve servisler
- Üretim ve operasyonlar
- Strateji ve organizasyon
- Tedarik zinciri
- İş modeli
- Yasal hususlardır.

2.2.7.9. Accenture dijital olgunluk modeli

Accenture firmasının Vodafone Türkiye, ODTÜ, Boğaziçi Üniversitesi, Türkiye Bilişim Vakfı iş birliği ile 2015 yılında yapmış olduğu çalışmada bir dijitalleşme endeksi geliştirilmiştir. Şirketlerin, strateji, hizmet ve operasyonel yetkinlikleri dijital kapasiteleri kapsamında incelenmiştir. Sektör bazlı olgunluk düzeyleri belirlenmeye çalışılmıştır. Çalışmaya göre, Türkiye'deki 104 şirketin dijitalleşme ortalaması % 60 seviyesindedir ve finansal hizmetler dijitalleşme performansı en yüksek sektördür.

Endeks, dijital strateji, dijital hizmetler ve dijital operasyonel yetkinliği içeren 3 ana boyuttan oluşmaktadır. Dijital strateji; sektör trendleri ve şirket hedefleri alt boyutlarından oluşmaktadır. Dijital hizmetler; ürünler, servisler, etkileşim, satış fonksiyonları, servis fonksiyon alt boyutlarından oluşmaktadır. Dijital operasyonel yetkinlik ise; operasyon- süreçler, kaynaklar-organizasyon ve iş akışı alt boyutlarından oluşmaktadır.

2.2.7.10. Dijital olgunluk modelleri ile ilgili yapılan diğer çalışmalar

Leyh vd. (2016)'nın oluşturdukları model SIMMI 4.0 (System Integration Maturity Model Industry 4.0, Sistem Entegrasyon Olgunluk Modeli Endüstrisi 4.0), kuruluşların bilgi teknolojileri yeteneklerini değerlendirmesine olanak tanımaktadır. Dört boyuttan; dikey entegrasyon, yatay entegrasyon, dijital ürün geliştirme, kesitsel teknoloji ve beş aşamadan; temel dijitalleşme, bölümler arası dijitalleşme, yatay ve dikey dijitalleşme, tam dijitalleşme, optimize edilmiş tam dijitalleşmeden oluşmaktadır.

M2DDM (Maturity for Data-Driven Manufacturing, Veri Odaklı İmalat İçin Olgunluk Modeli), hizmet vermeye yönelik bir geliştirme yolu sağlamak için imalat şirketlerinin bilgi teknolojileri mimarisini analiz etmektedir. Weber vd. (2017) modellerinde beş aşama önermektedirler; var olmayan bilgi teknolojileri entegrasyonu, veri ve sistem entegrasyonu, yaşam döngüsü boyunca verilerin entegrasyonu, hizmet odaklılık, dijital ikiz, kendi kendini optimize eden bir fabrikaya kadar. Model tek boyuttan oluşmaktadır ve tamamen BT sistemlerine odaklanmaktadır.

Rakoma (2021) çalışmanda, deniz taşımacılığı şirketlerinin dijital olgunluğunu uygun şekilde ölçecek dijital olgunluk modelini araştırmaya çalışmıştır. Çalışmanın temel yönlerini belirlemek amacıyla CIMO (Context, Intervention, Mechanism and Outcome) (Bağlam, Müdahale, Mekanizma ve Sonuç) modelini benimsemiştir. Modeli İş kültürü, teknoloji kullanımı, müşteri ilişkileri, operasyonel süreçler, strateji, alt yapı, sermaye, yönetişim ve liderliği içeren 8 ana boyuttan ve 5 olgunluk seviyesinden oluşmaktadır.

Mittal vd. (2018) çalışmalarında küçük ve orta büyüklükte işletmeler için yeni bir akıllı üretim dijital olgunluk modeli tavsiye etmektedir. Önerilen modele göre SM3E (small and medium-sized enterprises) olgunluk modelini benimseyen bir KOBİ, beş temel kurumsal boyutunun her biri için kendisini beş olgunluk seviyesinden birinde değerlendirebilecek ve konumlandırabilecektir. Böylece KOBİ, bir organizasyon boyutunda bir sonraki olgunluk seviyesine ulaşmak için gereken girdiyi veya desteği belirleyebilecek ve bu da özel araç kutuları tarafından sağlanabilecektir. Bir araç kutusu KOBİ'nin ilgili boyutta daha sofistike faaliyetler gerçekleştirmesini sağlamaktadır. Model 2 kurumsal boyuttan oluşmaktadır. Organizasyonel boyutun alt kriterleri; finans, insan, strateji, süreç ve üründür. Araç kutuları boyutunun alt kriterleri; fabrikasyon, tasarım ve simülasyon, robotik ve otomasyon, sensörler ve bağlantı, veri analitik araç kutusu, bulut araç kutusu ve iş yönetimi araç kutusudur. Model, acemi, başlangıç seviyesi, öğrenci, orta seviye ve uzman olmak üzere 5 olgunluk seviyesinden oluşmaktadır.

Kaltenbach vd. (2018) makalelerinde, seçilen üç Alman kuruluşunun akıllı hizmetlere ilişkin olgunluk düzeyine ilişkin bir çalışmayı rapor etmektedir. Amaçları, devam eden dijital dönüşümün etkisini vurgulamak, dijitalleşme ve akıllı hizmetlere ilişkin olgunluk seviyelerini haritalandırmaktır. Bu olgunluk modeli altı boyuta bölünmüştür; ürün geliştirme süreci, yönlendirme ve kontrol, operasyon ve üretim, büyük veri entegrasyonu, organizasyon yapısı ve akıllı hizmetler. Ayrıca model 6 dijital olgunluk seviyesinden oluşmaktadır.

Gökalp ve Martinez (2021)' in oluşturdukları DX-CMM (The digital transformation capability maturity model) (Dijital dönüşüm kabiliyet olgunluk modeli) modeli, mevcut dijital dönüşüm kabiliyetin belirlenmesini, bir boşluk analizinin türetilmesini ve kapsamlı, yapılandırılmış, objektif, eksiksiz ve standartlaştırılmış bir şekilde iyileştirme için kapsamlı bir yol haritası oluşturulmasını sağlayarak kuruluşlara yardımcı olmak için geliştirilmiştir. Çalışmalarının amacı, kimya ve makine imalatı alanlarındaki iki kuruluşta dijital dönüşüm olgunluk seviyesinin değerlendirilmesi ve dijital dönüşüm olgunluk seviyesinin bir seviye daha ileriye taşınması için bir yol haritası türetilmesini içeren çoklu bir vaka çalışması gerçekleştirerek DX-CMM'in kullanılabilirliğini ve uygulanabilirliğini kontrol etmektir. DXCMM'nin süreç boyutu, stratejik yönetişim, bilgi ve teknoloji, dijital süreç dönüşümü ve işgücü yönetimi olmak üzere 4 süreç grubu altında tanımlanan 26 dijital dönüşüm sürecinden oluşmaktadır. Model 6 seviyeden oluşmuştur. Bunlar; tamamlanmamış, gerçekleştirilen, yönetilen, kurulmuş, ön görülebilir, yenilikçiliktir.

Baltacı (2020), lojistik sektörü için bir dijital olgunluk modeli önermiştir. Çalışmasında, çok kriterli karar verme yöntemlerinden analitik hiyerarşi prosesi (AHP) yöntemini kullanarak 5 ana boyut ve 24 alt boyut belirlemiştir. Ana boyutlar; dijital süreçlerin stratejisi ve yönetimi, organizasyon, dijital altyapı ve entegrasyonlar, dijital teknolojiler ve dijital faydalı modeller, dijital uygulamalardır. Modeli 6 olgunluk seviyesinden oluşmaktadır. Bunlar; hiç uygulanmayan, başlangıç, istekli, orta, kuvvetli ve en iyi performans gösterendir.

Serdar (2019) çalışmasında AHP ile Ağırlıklandırılmış Olgunluk Yaklaşımı ile lojistik sektörünün ve işletmelerin olgunluk düzeylerini belirlemiştir. IMPULS modelinin kriterlerini temel alarak modelini meydana getirmiştir. AHP-TOPSIS ve AHPVIKOR yöntemlerini beraber kullanarak işletmelerin sıralamasını gerçekleştirmiş, yeni bir çok kriterli olgunluk yaklaşımı önerisinde bulunmuştur.

Dutta ve Lanvin (2019), bilgi ve iletişim teknolojilerinin uygulanması ve kullanımına ilişkin önde gelen küresel endekslerden biri olarak ABD'de Portulans Enstitüsü ile Ağ Hazırlık Endeksi (NRI) oluşturmuşlardır. Sonuçta ortaya, politika yapıcılara, iş dünyası liderlerine, akademi dünyasına ve sivil topluma ilerlemeyi değerlendirmek ve dijital çağda daha kapsayıcı ve sürdürülebilir büyüme için eylem gündemini belirlemek üzere güvenilir ve değerli bir araç sunma geleneğini devam ettirecek, geleceğe hazır bir endeks çıkarmışlardır. NRI dört sütuna dayanmaktadır: Teknoloji, İnsan, Yönetişim ve Etki. Her sütun üç alt sütundan oluşmaktadır. Teknoloji kriteri erişim, içerik ve gelecek teknolojilerinden, insan kriteri bireyler, işletmeler ve hükümetlerden, yönetim kriteri güven, düzenleme, dahil etmeden, etki kriteri ise ekonomi, yaşam kalitesi ve sdg katkısı alt kriterlerinden oluşmaktadır. Dijital ekonominin kıyaslanmasında yirmi yıllık deneyime dayanan NRI, 62 göstergedeki performanslarına göre 121 ekonominin ağ tabanlı hazırlık durumunun haritasını çıkarmaktadır.

2.3. Denizcilik Sektörü ve Siber Güvenlik

Siber uzay olarak da bilinen bitlerin dünyası, günümüz dünyasının ayrılmaz bir parçasıdır. Küresel ekonomi, toplumun güvenliği, iş faaliyetleri ve günlük yaşam giderek siber uzaydaki başarılı ve güvenli operasyonlara bağlı hale gelmektedir. Dijitalleşme, coğrafi ve zamansal sınırların öneminin azaldığı durumlarda neredeyse sınırsız fırsatlar sunmaktadır. Aynı zamanda güvenlik açığı da artmaktadır. Bitlerin fiziksel atomlara göre anlamı arttıkça siber uzayın güvenliğinin de önemi artmaktadır. Siber güvenlik sadece teknolojik değil, herkesi ilgilendiren ve herkesin kendi payına düşeni üstlendiği stratejik

ve politik bir konudur. Denizcilik sektörü bu dönüşümün farkına varmıştır; önceden siber bağımlı olmayan endüstrinin artık kaçınılmaz olarak gelen değişikliklere uyum sağlaması gerekmektedir (Peura, 2017).

Sektör, deniz yolculuğundan liman altyapısına, gelen ve giden faaliyetlere kadar uzanan geniş bir tedarik zinciri olan uluslararası tedarik zincirinin ayrılmaz bir parçasıdır ve bu da sektörü çeşitli paydaşları olan karmaşık bir ekosistem haline getirmektedir. Böyle bir bağlamda sektör, küresel tedarik zincirindeki çok sayıda tarafı birbirine bağlayarak ekonomik büyümeyi, istihdam yaratmayı ve dünya genelindeki ulusların genel refah ve esenliğini teşvik eden bir temel yapı taşı görevi görmektedir. Dolayısıyla denizciliği etkileyen durumlar, dünyayı da etkilemektedir. Bu durumda, denizcilikte siber güvenlik küresel bir mesele haline gelmektedir (Meland vd., 2021).

Denizcilik sektörü, küresel ticaret ve taşımacılıkta hayati bir rol oynamakta ve dünya ticaretinin büyük bir kısmı için cankurtaran halatı görevi görmektedir. Sektör, ileri bilgi teknolojisine ve operasyonel teknoloji sistemlerine giderek daha fazla bağımlı hale geldikçe, siber tehditler için de potansiyel bir hedef haline gelmiştir. Dijital bağlantının yaygınlaşması ve sistemlerin ve ağların entegrasyonuyla denizcilik sektörü, ele alınması gereken önemli siber güvenlik sorunlarıyla karşı karşıyadır. (Peura, 2017).

2.3.1. Siber güvenlik açıklaması

Siber güvenliğin tek ve kapsamlı bir tanımı mevcut değildir. Siber güvenlik, kuruluşun kendisini siber saldırılardan ve sonuçlarından korumak için gerçekleştirdiği operasyonlar ve kuruluşun gerekli karşı önlemleri alması olarak değerlendirilebilmektedir. Risk ve tehdit analizi, siber güvenliğin temelini oluşturmaktadır. Kurumun siber stratejisinin ve siber programının yapısı ve unsurları, değerlendirilen bu risklere ve tehditlere dayanmaktadır. Siber güvenliğin artırılması, siber riskin azaltılmasıyla yapılabilmektedir. Kritik altyapılar gibi güvenlikle ilgili sistemlere önem verilmektedir. Risk temelli bir yaklaşım ve bütünsel risk yönetimi, bir kuruluşun bu hedefe ulaşmasının anahtarıdır. Siber risk yönetimi, “siberle ilgili bir riskin tanımlanması, analiz edilmesi, değerlendirilmesi ve iletilmesi ve paydaşlara yönelik eylemlerin maliyet ve faydalarını dikkate alarak bu riski kabul etme, önleme, aktarma veya kabul edilebilir bir düzeye indirme süreci” olarak tanımlanabilmektedir. Siber güvenliğin uygulanması yönetim seviyesinden başlamaktadır ve insan faktörünün siber güvenlik üzerindeki etkisi önemli olduğundan organizasyonun tüm seviyelerinde taahhüt

gerektirmektedir. Siber güvenliğin iyileştirilmesi, bilgi güvenliği yönetiminin geliştirilmesini gerektirmektedir. (Lehto & Kähkönen, 2015).

Denizcilik siber güvenliği, denizcilik endüstrisinde siber güvenliğe katkıda bulunan bir dizi siber güvenlik aracı, kılavuz, prosedür, politika, risk değerlendirmesi, değerlendirmeler, önerilen uygulamalar/standartlar, güvenlik kontrolleri, eğitim, yönetişim ve diğer faktörleri kullanarak deniz ortamlarının, gemilerin, kuruluşların ve varlıkların korunmasını içerir. Aynı zamanda denizcilikte siber güvenlik, bilgi teknolojisi (BT) sistemlerinin, gemilerdeki donanımın, sensörlerin ve veri sızıntısının yetkisiz erişime, manipülasyona ve kesintiye karşı korunması ile ilgilidir ve mürettebatın, geminin, kargonun ve limanların güvenliği üzerinde büyük bir etkiye sahiptir (Trent, 2023).

2.3.2. Siber riskler

Denizcilik endüstrisinin dayandığı sistemlerin artan karmaşıklığı, dijitalleşmesi, entegrasyonu ve otomasyonu, bütünsel bir siber risk yönetimi gerektirmektedir. Farklı sistemlerin birbirine ve internete bağlanması siber riski daha da artırmaktadır. Etkili siber risk yönetimi, yönetim seviyesinden başlar ve siber risk farkındalığı kültürünün her seviyede elde edilmesi gerekmektedir. Bu, etkili geri bildirim yoluyla bütünsel, sürekli çalışmayı ve değerlendirmeyi mümkün kılmaktadır. IMO, denizcilik siber riskini "bir teknoloji varlığının, bilgi veya sistemlerin bozulması sonucunda gemicilikle ilgili operasyonel, emniyet veya güvenlik arızalarıyla sonuçlanabilecek potansiyel bir durum veya olay tarafından ne ölçüde tehdit edilebileceğinin ölçüsü" olarak ifade etmektedir. Denizcilik siber riski, yalnızca siber saldırı olaylarını değil aynı zamanda BT veya OT sistemlerinin güvenlik özelliklerini doğrudan veya dolaylı olarak etkileyen her türlü olayı içermektedir (IMO, 2017).

BT ve OT güvenlik açıkları, saldırganlar tarafından gemi operasyonlarını veya denizcilik endüstrisindeki diğer ilgili operasyonları aksatmak için kullanılabilmektedir. Kesintiler, yükleme ve boşaltma operasyonlarında gecikmelere veya navigasyon, sevk sistemleri gibi hayati sistemlerin aksamasından kaynaklanan güvensiz gemi operasyonlarına neden olabilmektedir. Planlı bakım sistemine yapılacak bir saldırı, bakımın günlük yönetiminde aksamalara neden olabileceği gibi, emniyet yönetim sistemlerine yapılacak bir saldırı da gemideki günlük iş görevlerinde riskler yaratabilmektedir. Bu nedenle tüm bu sistemler gemilerin güvenli çalışması için hayati öneme sahiptir. Gelişmiş bilgi teknolojisine ve operasyonel teknoloji sistemlerine olan

bağımlılığın artmasıyla birlikte denizcilik sektörü siber tehditlere karşı savunmasız hale geldi. Bu tehditlerin sonuçları gemi operasyonlarının güvenliğini, verimliliğini ve sürekliliğini etkileyebilir. Bu nedenle gemi operasyonlarında siber güvenlik risklerinin azaltılmasına yönelik etkili stratejiler geliştirmek büyük önem taşımaktadır (Sørensen, 2023).

Yeni teknolojilerin kullanılması verimliliğin ve güvenliğin artmasını sağlayabilmektedir ancak aynı zamanda siber riski de artırmaktadır. Faydaları elde etmek ve tam olarak benimsemek için siber güvenliğin kuruluşun her düzeyinde dikkate alınması ve kuruluşların sağlam bir siber strateji oluşturması ve takip etmesi gerekmektedir. Güvenlik ihlallerinin büyük bir kısmı insanlardan ve kötü süreçlerden kaynaklanmaktadır; bu da siber risk değerlendirilirken teknolojik denizcilik sistemleriyle ilgili personel, fiziksel ve fiziksel hususların da dikkate alınması gerektiği anlamına gelmektedir (Boyes & Isbell, 2017).

Siber riskler, aşağıdaki olayları içerebilecek ancak bunlarla sınırlı olmamak üzere siber olaylardan kaynaklanmaktadır (Peura, 2017):

- Yazılım bakımı ve yama uygulaması sırasında meydana gelen istenmeyen sistem hatası
- Yazılım çökmeleri veya "hatalar" nedeniyle sistemin arızalanması
- Hassas verilerin kaybına veya gemi sistemlerine kötü amaçlı yazılım bulaşmasına yol açabilecek herhangi bir mürettebat etkileşimi
- Fidye yazılımı veya hizmet reddi olayı.
- Bir geminin çalışması için kritik olan harici sensör verilerinin kaybı veya manipülasyonu
- Elektronik navigasyon ekipmanının kullanılabilirliği kaybı veya navigasyonla ilgili verilerin bütünlüğünün kaybı
- Kıyıyla temel bağlantının kaybı
- Tahrik, yardımcı sistemler ve diğer kritik sistemler de dahil olmak üzere OT sistemlerinin kullanılabilirliğinin kaybedilmesinin yanı sıra veri yönetimi ve kontrolün bütünlüğünün kaybı

2.3.3. Siber saldırı ve tehditler

Siber tehdit, bir bilgi sistemi üzerinden yetkisiz erişim yoluyla bir kişiyi, mülkü (maddi veya gayri maddi), kuruluşu veya ülkeyi olumsuz etkileme potansiyeline sahip herhangi bir olaydır. Siber saldırılar, internete bağlı herhangi bir cihazı kötü niyetle

bozmak veya zarar vermek amacıyla hedef alabilir ve toplumun dijital teknolojiye olan bağımlılığı siber saldırılar için daha fazla fırsat yaratmaktadır. Siber tehditler günümüzde şirketlerin karşı karşıya olduğu başlıca risklerden biridir ve her yıl çoğu şirketi etkilemektedir. Bununla birlikte, en organik çözüm, bilgi kaynaklarının kendilerine, belirli çalışma koşullarını dikkate alırken korunmalarını sağlayacak uygun işlevsellik sağlamaktır. Bu sorunun çözümü, koruma sistemi tarafından karşı konulması gereken siber tehditlerin ve korunan bilgi kaynaklarının belirli özelliklerinin dikkate alınmasını içermektedir. Siber tehditler çok yönlüdür ve hızla gelişmektedir. Etki değerlendirmesi ve risk yönetimi, siber durumları değerlendirmenin ve bir hafifletme planının parçası olarak iyileştirme sunmanın önemli parçalarıdır. Siber tehditler, mevcut bilgisayar sistemlerine karşı saldırılar planlamak ve başlatmak için kritik altyapıdaki bağlantı ve karmaşıklığı sürekli olarak istismar etmektedir. Bu, çeşitli ticari kuruluşlar tarafından yaşanan büyük bir zorluktur. (Putra vd., 2023).

Denizcilik siber tehditleri açısından, denizcilik siber riski, bir teknoloji varlığının, hasar görmüş, kaybolmuş veya tehlikeye girmiş bilgi veya sistemlerin bir sonucu olarak operasyonel, emniyet veya nakliye ile ilgili güvenlik arızalarına neden olabilecek potansiyel koşullar veya olaylar tarafından ne ölçüde tehdit edildiğinin bir ölçüsü olarak tanımlanmıştır. Siber güvenlik sağlayıcıları genellikle denizcilik ortamının sadece teknolojik kısmını dikkate aldıklarından, sistemin bir parçasının tek başına görülemeyeceğini, ancak diğer parçalar hakkında görülmesi gerektiğini hatırlamak çok önemlidir. Dolayısıyla buradaki denizcilik siber tehditleri, denizcilik alanını etkileyen siber tehditler olarak anlaşılmaktadır. Denizcilik siber tehdit ortamı, kötü amaçlı yazılım bulaşmasının sistemleri tehlikeye atmanın yaygın bir yolu olduğunu, bir veya birkaç alt bileşenin enfekte olabileceği olumsuz olaylara ilişkin değerlendirmenin kapsamını ve ilişkili olasılıkları göstermektedir (Putra vd., 2023).

Birbirine bağlı kontrol sistemlerinin büyümesi, denizcilik sektöründeki kuruluşların dikkate alması gereken önemli bir faktördür. Gemilerin bilgi ve operasyonel teknoloji sistemleri sadece birbirleriyle değil, aynı zamanda internetle de giderek daha fazla bağlantılı hale gelmektedir. Tahrik tesisi ve gemi kontrolü ile balast ve kargo yönetimi gibi gemi veya platform sistemleri, örneğin web tabanlı sistemler ve uzaktan erişim yöntemleri gibi dijital erişimlerle birleştiğinde, kötü amaçlı yazılım, kimlik avı ve vishing (sesli kimlik avı) ve zehirli bağlantılar veya ekler gibi yeni tehditlerin ortaya çıkmasını sağlamaktadır.

Siber risk değerlendirmesi, harici veya dahili olabilen siber tehditlerin tanımlanmasıyla başlamaktadır. Geçmiş kanıtların mevcut olmaması ve olayların kaydedilmesinin gerekli olmaması, siber güvenliğin bir zorluğudur. Bununla birlikte, kuruluşun siber olaylara karşı savunmasızlığını artırabilecek faaliyetlerinin tüm yönlerini dikkate alması gerekmektedir. Bu güvenlik açıklarını araştıran aktörler, verileri yok ederek itibar zedelemeye çalışan aktivistler, çalınan verileri satarak maddi kazanç peşinde koşan suçlular, siber güvenlik savunmalarını aşmak isteyen fırsatçılar, ekonomileri ve kritik altyapıları sekteye uğratarak siyasi kazanç peşinde koşan devletler/devlet destekli örgütler ve teröristler gibi farklı güdülere sahip kuruluşlar veya bireyler olabilmektedir.

Siber saldırılar Tablo 2.4'te gösterildiği gibi hedefli ve hedefsiz saldırılar olmak üzere iki kategoriye ayrılabilmektedir. Hedefli saldırılarda, kuruluş veya geminin sistemleri ve verileri amaçlanan hedeftir. Hedefsiz saldırılarda ise birçok hedeften biridir. Bu saldırılar genellikle yaygındır ve potansiyel güvenlik açıklarından yararlanmak için internette bulunan araç ve teknikleri kullanmaktadırlar (BIMCO, 2016).

Tablo 2.4 Siber saldırıların araç ve teknikleri (BIMCO, 2016).

Hedeflenmemiş Saldırılar	**Hedefli Saldırılar**
Kötü amaçlı yazılım: sahibinin bilgisi olmadan bir bilgisayara erişmek veya zarar vermek için kötü amaçlı yazılım	Kaba kuvvet: Eninde sonunda doğru şifreyi bulmayı umarak mümkün olan tüm şifreleri sistematik olarak denemek
Sosyal mühendislik: örneğin sosyal medyadaki etkileşim yoluyla bir siber güvenlik prosedürünü frenlemek için kuruluşun personelini manipüle etmek için kullanılan teknik olmayan bir tekniktir.	Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS): meşru kullanıcıların bilgiye erişmesini önlemek için ağın veriyle doldurulması, DDoS'ta birden fazla sunucu/ bilgisayarın kontrol altına alınması
Kimlik avı: hassas veya gizli bilgiler talep eden veya sahte bir web sitesini ziyaret eden çok sayıda kişiyi hedef alan e postalar	Hedef odaklı kimlik avı: Belirli bir kişiyi hedef alan, genellikle kötü amaçlı yazılım veya bağlantılar içeren e-postalar
Water holing: sahte bir web sitesi veya ziyaretçileri istismar etmek için gerçek bir web sitesini tehlikeye atmak	Tedarik zincirini altüst etmek: hedeflenen kuruluş/gemi için gerekli olan yazılım, ekipman veya destek hizmetlerinden ödün verilmesi
Tarama: İnternetin büyük bir bölümünü rastgele hedef alan saldırı	

2.3.4. Denizcilik sektöründeki siber varlıklar

Denizcilik sektöründeki siber saldırılar literatürü incelendiğinde limanlar, gemiler ve şirketler bazlı konular olduğu görülmektedir.

Limanlarda IT tabanlı bina yönetim sistemlerine sahip gemi hareket ve izleme merkezleri, antrepo ve depolar, bilgi merkezleri, devlet hizmet binaları vb. yapılar bulunmaktadır. Bu yapılar ve kablolu ya da kablosuz ağ ile kuruludur. Kargo elleçleme sistemleri, boru devreleri otomatik bariyerler ve kapılar, pompalar, mobil vinçler ve araçlar, göstergeler, güvenlik ve erişim kontrolü gerektiren siber altyapıya sahip liman sistemleridir. Bunların bazılarının genel özelliği SCADA teknolojilerini kullanmasıdır. Kargo, konteyner izleme sistemleri, liman bilgi sistemi, otomatik plaka/etiket tanımlama sistemi, optik okuyucular, CCTV gibi sistemler, planlama, programlama, izleme, kayıt etme, bilgi verme gibi birçok süreçlerin yürütüldüğü sistemlerdir (Boyes vd., 2016).

Gemilerde kullanılan siber varlıklar ise;

- Köprü ve navigasyon sistemleri: Bu kategorideki sistemler; elektronik harita görüntüleme bilgi sistemleri (ECDIS), küresel konumlandırma sistemleri (GPS), dinamik konumlandırma sistemleri (DPS), küresel navigasyon uydu sistemleri (GNSS), otomatik tanımlama sistemleri (AIS), yolculuk veri kaydedicileri (VDR) ve Radar/Otomatik radar çizim yardımıdır (ARPA).
- Kargo yönetim sistemleri: Dijital kargo yönetimi ve kontrol sistemleri, karadaki birden fazla sistemle arayüzlere sahip olabilir. Örneğin internet bağlantısı üzerinden kullanılabilen gönderi takip araçları, kargo manifestoları ve kargo yönetim sistemlerindeki verileri siber risklere maruz bırakmaktadır.
- İletişim sistemleri: Uydu üzerinden internet bağlantısı ve radyo iletişimleri (geniş bant, IP Üzerinden Ses (VOIP) dahil olmak üzere diğer kablosuz iletişimler, gemideki güvenlik açıklarını potansiyel olarak artırabilmektedir.
- Kontrol sistemleri: Ana motor, jeneratörler, balast tankı, yaşam desteği, yakıt ve yağ pompaları, su geçirmez kapılar, yangın alarmları ve kontrolleri, kargo ambarı fanları, çevresel kontroller, geminin tahriki ve yönlendirilmesi dahil olmak üzere elektromekanik sistemler için dijital kontrol ve izleme sistemleri, siber saldırılara karşı savunmasızdır. Uzaktan durum bazlı izleme ve teşhis, riski artırmanın yanı sıra, bu sistemlerin entegre köprü sistemleri kullanan gemilerde navigasyon ve iletişimlere entegre edilmesiyle de mümkün olmaktadır.

- Erişim kontrol sistemleri: Bu tür sistemler, gözetleme, gemi güvenlik alarmı ve elektronik "gemideki personel" sistemleri de dahil olmak üzere, geminin ve yükünün fiziksel güvenliğini ve emniyetini sağlamak amacıyla erişim kontrolünü desteklemek için kullanılır.

Tablo 2.5 Denizcilik sektöründeki siber varlıklar (Yüksel, 2019)

Gemi Tabanlı Siber Uzayda Ekipman ve Sistemler	**Liman Tabanlı Siber Uzayda Ekipman ve Sistemler**	**Şirket Bazlı Siber Uzayda Sistemler**
Uydu İletişim Sistemleri (INMARSAT)	Liman Yönetimi ve Bilgi Sistemleri	Gemi ve Diğer Parçalarla İletişim Sistemleri
Konumlandırma Sistemleri (GPS)	Ortak İşletim Resmi (COP)	ISM Yazılım Sistemleri
Elektronik Harita Gösterim ve Bilgilendirme Sistemi (ECDIS)	Terminal İşletim Sistemleri	
Otomatik Tanımlama Sistemi (AIS)	Otomatik Terminal Sistemleri	
Yolculuk Veri Kayıt Sistemleri (VDR)	Mekik Taşıyıcılar (AGV)	
İç İletişim Sistemi	Otomatik İstifleme Vinçlerinin (ASC'ler) Değişimi (STS, MHC, RTG, RMG, SC)	
VoIP Ekipmanları	Süreç Kontrol Sistemi (PCS)	
Wi-Fi	Otomatik Kapı Tesisleri	
Alarm Sistemleri	Otomatik Bahçe Sistemleri	
Entegre Navigasyon Sistemleri	Elektronik Veri Değişimi (EDI)	
Radyo Algılama ve Uzaklık Ölçümü (RADAR)	Radyo Frekansı ile Tanımlama (RFID)	
GMDSS	Optik karakter tanıma (OCR)	
Diğer İzleme Sistemleri	Wireless Sensor Network (WSN)	
Dizel Kontrol Sistemleri	Gerçek Zamanlı Konumlandırma Sistemleri (RTLS)	
Yardımcı Kontrol Sistemleri	Liman Topluluğu Bilgi Sistemi	
Elektrik Dağıtım Sistemleri		

2.3.5. Denizcilik sektöründe yaşanmış siber güvenlik olayları

Denizcilik siber güvenlik saldırıları 2010'lardan bu yana görülmekte ve şekil ve davranış değiştirmektedir.

Denizcilik sektörünün siber saldırılara karşı kırılganlığı, Eylül 2020'den bu yana sektörün en büyük dört şirketinin saldırıya uğramış olmasıyla vurgulanmaktadır. Daha spesifik olarak, Maersk ve CMA CGM Group fidye yazılımı saldırılarına maruz kalırken, COSCO Shipping ve MSC'nin dijital ağları da vurulmuştur. Tüm saldırılar, 2017 yılında Maersk fidye yazılımı saldırısıyla başlayarak kısa bir süre içinde gerçekleşmiştir (Cimpanu, 2021).

Haziran 2017'de meydana gelen NotPetya siber olayının, denizcilik sektörü de dahil olmak üzere dünya çapındaki endüstriler üzerinde önemli etkileri olmuştur. Bu fidye yazılımı saldırısı, birçok işletme için BT sistemlerinin potansiyel güvenlik açığı konusunda bir uyandırma çağrısıydı. NotPetya olayı nedeniyle özellikle denizcilik sektörü ciddi sonuçlarla karşılaşmıştır. Nakliye ve lojistik alanında küresel bir lider olan Maersk, bu durumdan en ciddi şekilde etkilenen şirketlerden biriydi. Saldırının Maersk'e 250 ila 300 milyon dolar arasında bir maliyete mal olduğu tahmin edilmektedir Maersk'in operasyonları ciddi şekilde kesintiye uğramıştır. Fidye yazılımı şirketin 130 ülkedeki bilgisayar sistemlerine bulaştı ve onları kapatmıştır. Bu da şirketin 76 liman ve terminal operasyonunu yönetmesini imkânsız hale getirmiştir. Sonuç olarak şirket, siparişleri işleme koyamamıştır ve manuel süreçlere dönmek zorunda kalmıştır. Nakliye ve liman operasyonlarında önemli gecikmelere neden olmuştur. Maersk'in mali durumu üzerindeki etkisi önemliydi. Operasyonların aksaması nedeniyle şirket mali kayıp yaşamıştır. Kurtarmanın maliyeti ve önemli siber güvenlik yükseltmelerine duyulan ihtiyaç oldukça yüksekti. Tahmini 250 milyon ila 300 milyon dolar arasındaki maliyet aralığı bu unsurları içermektedir. Olay aynı zamanda Maersk'in itibarının da zarar görmesine yol açmıştır. Sevkiyat siparişlerinin zamanında yerine getirilememesi ve bunun sonucunda ortaya çıkan kaos, müşterilerin şirketin güvenilirliğine olan güvenini zedelemiştir. Ancak bazı müşteriler, şirketin performansına olan güveni korumak ve yeniden tesis etmek için bunun karşılığını hızla almışlardır. NotPetya olayının ardından Maersk ve denizcilik sektöründeki diğer şirketler gelecekte benzer olayları önlemek için siber güvenlik önlemlerine yoğun yatırım yapmak zorunda kalmıştır. Buna sistemlerin güncellenmesi ve yamalanması, personelin siber farkındalık konusunda eğitilmesi ve daha sağlam güvenlik protokollerinin uygulanması da dahildir. Geriye dönüp bakıldığında Maersk'in, NotPetya gibi kaçamak amaçlı bir siber saldırıyı azaltmak için gereken uygun siber güvenlik altyapısına sahip olmadığı tespit edilmiştir. Bazı sunucular artık desteklenmeyen veya güncellenmeyen eski Microsoft sistemlerinde çalışıyordu. Maersk'in tamamen normal operasyonel standartlara dönmesi 5 ay sürmüştür. Sonuç olarak, NotPetya siber olayının denizcilik sektörü için geniş kapsamlı etkileri olmuştur ve giderek dijitalleşen bu sektörde acil olarak sağlam siber güvenlik önlemlerine duyulan ihtiyacın altını çizmiştir (Greenberg, 2018).

Bununla birlikte, olaylar her zaman meydana gelirken, küçük veya büyük olayların nadiren rapor edilmektedir. Siber saldırılar, siber profesyonel olmayan herkesin inandırıldığından çok daha büyük bir oranda gerçekleşmektedir, ancak yalnızca birkaç

nakliye siber olayı kamuoyunun dikkatini çekmektedir. Yinede, siber saldırıların denizcilik sektörü üzerinde yarattığı tehdit, tablo 6'da görüldüğü gibi, son yıllarda meydana gelen olaylarla doğrulanmaktadır.

Tablo 2.6 Denizcilik sektörüne yönelik önemli siber saldırılar (Ben Farah vd., 2022).

Sıra	Siber Saldırı Türü	Yıl	Açıklama
1	Fidye yazılımı saldırısı	2021	Güney Kore'nin ulusal amiral gemisi HMM: Siber saldırı e-posta görünüm sistemine sınırlı erişimle sonuçlanmıştır.
2	Fidye yazılımı saldırısı	2020	Hürmüz Limanı: Siber saldırı girişimi bazı limanlardaki bazı iletişim sistemlerine zarar vermiştir.
3	Kötü amaçlı yazılım saldırısı	2020	Mediterranean Shipping Company (MSC): Güvenlik sorunları için MSC'nin sunucuları şirket verilerinin korunması amacıyla kapatılmış ve bunun sonucunda şirketin web sitesi ele geçirilmiştir.
4	Kötü amaçlı yazılım saldırısı	2019	Saldırı bir ABD gemisini hedef almış ve kritik kimlik bilgilerinin ele geçirilmesine neden olmuştur. FBI, gemideki güvenlik stratejilerinin eksikliğinin böyle bir saldırının ana nedeni olduğunu bildirmiştir. Gemideki tüm mürettebatın geminin bilgisayarında aynı kullanıcı adı ve şifreyi paylaştığı fark edilmiştir.
5	Kimlik avı saldırısı	2019	Bilgisayar korsanları James Fisher and Sons Pls (UK) şirketinin bilgisayar sistemlerine yetkisiz erişim sağlamıştır.
6	Fidye yazılımı saldırısı	2018	Çinli bilgisayar korsanları ABD Donanması yüklenicilerine saldırmıştır.
7	Petya Fidye Yazılımı	2017	Petya adlı saldırı Avrupa ve Hindistan'daki bilgisayar sunucularını etkilemiştir. Şifrelenmiş kötü amaçlı yazılım Maersk denizcilik şirketinin tüm hizmetlerini hedef almıştır. Sonuç olarak, 17 nakliye konteyner terminali etkilenmiş ve 200 milyon ABD Dolarından fazla para kaybedilmiştir.
8	GPS sahtekarlığı saldırısı	2017	Saldırı ABD denizcilik idaresi tarafından rapor edilmiştir. Rusya'nın Novorossiysk limanındaki bir geminin GPS'i yanlış bir lokalizasyon göstermiştir.
9	Navigasyon Sistemleri saldırısı	2017	USS Fitzgerald ile bir konteyner gemisi arasında Japonya kıyılarında meydana gelen ve 7 denizcinin ölümüne neden olan çarpışmadır.

Siber güvenlik tehditlerini ve risklerini engellemek için kuruluşların varlıklarının, ortamlarının ve personelinin güvenliğini koruyacak bir siber güvenlik altyapısı kurmaları gerekmektedir. Son dönemde gerçekleşen siber saldırılar, gemilerin, denizcilik

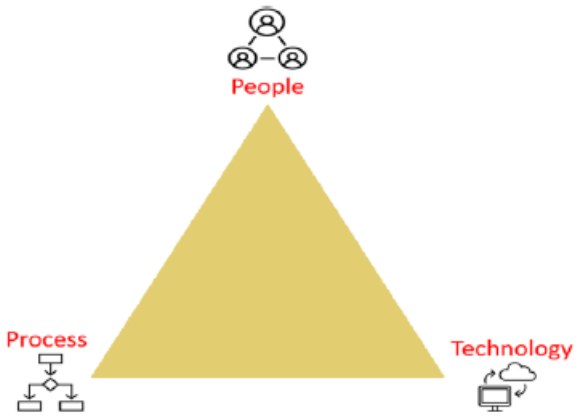
şirketlerinin, limanların ve denizcilik terminallerinin ortaya çıkan siber tehditlerden muaf olmadığını göstermiştir. Operasyonların güvenli ve verimli bir şekilde sürdürülebilmesi için siber riskin de fiziksel güvenlik, doğal afetler ve endüstriyel kazalar gibi diğer önemli tehditler gibi yönetilmesi gerekmektedir.

2.3.6. Siber güvenlik farkındalığı

Pek çok kuruluştaki personel, siber güvenlik olayı durumunda doğru tepki veremediği için farkındalık ve yeterlilik oluşturmak çok önemlidir. ENISA (European Network and Information Security Agency), siber güvenlik konusunda sektörün ilk zayıf noktası olarak düşük farkındalığı belirtmektedir (Cimpeanvd., 2011).

İnternet şu anda en dönüşümsel ve en hızlı büyüyen teknolojilerden biridir ve kullanıcıların bilgi teknolojisi sistemleri aracılığıyla zaman ve mekândan bağımsız olarak bilgi hizmetlerine rahatça erişmesine ve bunları kullanmasına olanak sağlamaktadır. Bu arada, sistemdeki büyük miktarda veri, güvenlik sisteminin yetersiz olması durumunda saldırılara, hırsızlığa ve tahribata karşı savunmasızdır. COVID-19 virüs salgını gibi durumlar nedeniyle, özellikle 2021'de, daha fazla insan eğitim, çalışma veya bir şeyler alıp satma ile ilgili günlük faaliyetleri için internete başvurduğundan, siber saldırıların sayısı artmıştır. Bu da suçluların çeşitli şekillerde saldırmasına olanak sağlamaktadır (Kate, 2021).

Şekil 2.5'te gösterildiği gibi siber güvenliği destekleyen 3 unsur vardır.



Şekil 2.5 Siber güvenliği destekleyen unsurlar (Ştefănescu & Papoi, 2020)

"İnsanlar" mantıksal olarak insan hatasından kaynaklanan en büyük riske sahip sütundur ve insan müdahalesini tahmin etmek ve kesinleştirmek yazılım ve sisteminden daha zordur. Bu nedenle, çalışanların eğitimi, bilgisi ve kaynakları, siber saldırılara karşı nihai savunma için işgücünü desteklemek açısından hayati önem taşımaktadır.

"Süreçler", ilgili teknoloji ve personel eğitimi gerektiren üç sütundan biridir. Denetim, çerçeveler, risk değerlendirmeleri ve en iyi yöntemi desteklemek için yönetim sistemleri yaklaşımlarının uygulanması kullanılabilecek süreçlerden bazılarıdır. Süreçler ancak onları takip eden insanlar ve eğitimli çalışanlar kadar etkilidir.

"Teknoloji", özellikle kayıtların ve potansiyel olarak hassas verilerin çok sayıda kişi ve sistem arasında paylaşıldığı sektörde, kurumlarda siber tehdit riskini yönetmek ve azaltmak için kritik öneme sahiptir. Kuruluşlar verilere erişim olmadan çalışamazlar, bu da bu süreçleri ve veri erişimini korumak için doğru yazılımı kullanmayı daha önemli hale getirmektedir.

Bununla birlikte, siber saldırılardan kaynaklanan etkileri en aza indirmek için siber güvenlik konusunda sağlam bir temel oluşturulmalı, siber tehditlere karşı başarılı bir savunma oluşturmak için her kuruluşta insanlar, prosedürler ve teknoloji birlikte çalışmalıdır. (Ungkap & Daengsi, 2022),

Farkındalık ve eğitimde, gemilerde siber güvenliği artırmak için belirli prosedürlerin uygulanmasına odaklanılmaktadır. Bu önlemler, güvenlik açıklarını ele almayı ve siber olay riskini azaltmayı amaçlamaktadır. Şirketler, gemi mürettebatı da dahil olmak üzere her seviyedeki personele siber güvenlik farkındalık eğitimi vermelidir. Eğitim, kimlik avı e-postalarının tanınması, uygun şifre hijyeni ve şüpheli faaliyetlerin bildirilmesi gibi konuları kapsayabilir. Uygulanması gereken bir siber hayati önlem de bir olay müdahale planına sahip olmaktır. İyi tanımlanmış bir olay müdahale planının yürürlükte olması hayati önem taşımaktadır. Bu plan, iletişim kanalları, roller ve sorumluluklar ve kontrol altına alma, soruşturma ve kurtarma adımları dahil olmak üzere bir siber olay durumunda atılacak adımları ana hatlarıyla belirtmelidir (Sørensen, 2023).

2.3.6.1. Siber güvenlik farkındalığı ile ilgili yapılan çalışmalar

Sørensen (2023), gemi sistemleri ve ağlarının artan birbirine bağlılığı ve dijitalleşmesi dikkate alınarak, denizcilik endüstrisinde siber güvenlik farkındalığı oluşturmaya ve siber güvenlik önlemlerinin yönlerini anlamaya çalışmıştır. Mevcut siber güvenlik önlemlerini değerlendirirken gemilerin karşı karşıya kaldığı potansiyel siber tehditler ve saldırı vektörlerinin anlaşılmasını sağlamayı ve gemi operasyonlarının özel ihtiyaçlarını ve gerekliliklerini karşılamak için oluşturulan bir çerçeve önermeyi amaçlamıştır. Çalışması, bu konuyu derinlemesine inceleyerek denizcilik endüstrisinde siber güvenlik bilgisine ve anlayışına katkıda bulunmayı istemiştir. Aynı zamanda gemilerdeki siber güvenlik uygulamalarını geliştirmeye yönelik pratik öneriler

belirlemeyi ve gemi operasyonlarındaki siber riskleri azaltmak için etkili siber güvenlik önlemlerinin benimsenmesini teşvik etmeyi de amaçlamıştır.

Bolat ve Kayışoğlu (2019) çalışmalarında denizcilik siber güvenliği literatürünü inceleyip, Türk Denizcilik Sektörünü örnek olay olarak ele alarak, denizcilik alanında siber güvenlik farkındalığının öncül faktörlerinin ve sonuçlarının anlaşılmasını amaçlamaya çalışmışlardır. Türkiye'de Deniz Ulaştırma İşletme Mühendisliği ve Gemi Mühendisliği bölümünden mezun 211 denizcilik çalışanından alınan anket verilerinin doğrulanmasıyla faktörlerin anlaşılması için yapısal eşitlik modellemesini kullanmışlar, AMOS programı ile verileri değerlendirmişlerdir. Çalışanların denizcilik siber güvenliği farkındalığının ve siber güvenliğe yönelik tutumlarının arttırılmasında eğitimin önemli bir faktör olduğunun ve denizcilik siber güvenliği farkındalığının, güvenli kullanıcı davranışını önemli ölçüde etkilediğinin sonucuna varmışlardır.

Ungkap ve Daengsi (2022), çalışmalarında internet kullanıcılarının siber güvenlik farkındalığını etkileyen faktörlerin belirlenmesi ve değerlendirilmesi için bir yöntem oluşturmuşlardır. Tayland'daki demiryolu kuruluşlarındaki çalışanlara odaklanarak, kullanıcıların siber güvenlik farkındalığı ile ilişkili faktörleri belirlemek ve ölçmek için tutum, bilişsel, deneyim, eğitim ve cinsiyet faktörleri kullanılmıştır. Her faktörün ağırlığını çıkarmak için Analitik Hiyerarşi Süreci (AHP) adı verilen bir karar verme tekniği uygulandıktan sonra, çalışma en önemli faktörün bilişsel olduğunu olduğunu göstermektedir.

Kovačević vd. (2020) siber güvenlik farkındalığını derinlemesine analiz etmek ve sosyodemografik özellikler, siber güvenlik algıları, önceki siber güvenlik ihlalleri, BT kullanımı ve bilgi birikimi gibi çeşitli faktörlerin tek tek veya birlikte siber güvenlik davranışını nasıl etkileyebileceğini keşfetmeye çalışmışlardır. Bunu kanıtlamak için araştırmalarını, toplumun teknolojik açıdan en aktif kesimi olan öğrenciler üzerinde gerçekleştirmişlerdir. Bilginin siber güvenlik farkındalığı için baskın faktör olduğunu ve öğrencilerin dijital yerliler olmalarına rağmen siber ortamda kendilerini güvende hissetmediklerini; güvenli davranmadıklarını ve siber alanda kendilerini korumak için yeterli bilgiye sahip olmadıklarını keşfetmişlerdir. Siber güvenlik algıları, siber güvenlik ihlali deneyimleri ve cep telefonu ve şifre davranışlarına yapı geçerliliği sağlamak için öncelikle ilgili sorulara temel bileşenler analizi ile faktör analizi uygulamışlardır.

Fatokun vd. (2019) yaş, cinsiyet ve eğitim düzeyinin, yükseköğretim öğrencilerinin siber güvenlik davranışlarını etkileyen faktörlere aracılık etmede ne ölçüde rol oynadığını araştırmışlardır. Anket 340 öğrenci arasında gerçekleştirilmiş ve etkileri

değerlendirmek için yapısal eşitlik modellemesi kullanılmıştır. Veri analizi SPSS (V.25) aracılığıyla gerçekleştirilmiştir. Sonuçlar, öğrencilerin siber güvenlik davranışlarının yaşa göre aşağıdaki faktörlere göre değiştiğini göstermektedir: Algılanan şiddet, akran davranışı, siber tehditlere aşinalık, müdahale yeterliliği ve algılanan savunmasızlık. Güvenlik öz yeterliliği, bilgisayar becerileri, siber güvenlik davranışları, algılanan önem derecesinde cinsiyet etkileri mevcutken, bilgisayar güvenliği uygulamaları ile ilgili önceki deneyimler konusunda çok az etki görülmüştür. Eğitim düzeyi farklılıkları ise harekete geçme ipuçları ve siber tehditlere aşinalık konularında ortaya çıkmıştır. Pratik olarak, bulguları yükseköğretim kurumlarındaki öğrenciler için özel/odaklı siber güvenlik eğitimi ve müdahalelerine duyulan ihtiyacı ortaya koyabilmektedir. Ayrıca, yükseköğretim kurumlarındaki siber güvenlik eğitim birimlerinin siber güvenlik davranış modelinin çok hayati bileşenlerini hedeflemesine ve dolayısıyla öğrencilerin siber güvenlik davranışlarını geliştirmesine yardımcı olabilmektedir.

Agustini ve Kencana (2016) araştırmalarını, sosyal medya araçlarından biri olan Path kullanıcılarının güvenlik farkındalığını demografik açıdan incelemek amacıyla gerçekleştirmişlerdir. Cinsiyet, yaş, gelir ve eğitim durumu gibi demografik unsurlar dahil edilerek güvenlik farkındalığı düzeyini anlamaya çalışmışlardır. Kullandıkları değişkenler güvenlik farkındalığı ve demografiktir. Araştırmalarında kullanılan yöntem, araştırma yapmanın temel dayanağı olarak nicel tanımlayıcı bir araştırmadır. Araştırmanın evrenini Path sosyal medya kullanıcıları oluşturmaktadır ve toplam örneklem 400 katılımcıdan oluşmaktadır; bu katılımcılar için örnekleme tekniği olarak olasılıklı olmayan örnekleme yöntemi kullanılmıştır. Bu araştırmada veri analiz tekniği olarak Crosstab tekniği ve Ki kare kullanılmıştır. Verilerin işlenmesinde Microsoft Excel yazılımı ve SPSS istatistik aracı versiyon 2.0 kullanılmıştır. Bu araştırmanın sonuçları, cinsiyet faktörüne göre erkeklerin bilgi güvenliği konusunda daha bilinçli olduğunu göstermektedir. Yaş faktörü ile ilgili olarak, 26-29 yaş aralığındaki katılımcılar daha bilinçlidir. Ayrıca, yüksek geliri olan ve lisansüstü eğitim geçmişi olan katılımcılar da güvenlik farkındalığı konusunda daha bilinçli olanlarla aynı sonucu göstermektedir. Bununla birlikte, gizlilik ayarı, bilgi erişiminin sınırlandırılması, gizlilik eğitimi, hassas konu bildirimi, bilgi paylaşımı ve tehditlere yanıt verme gibi bazı güvenlik farkındalığı öğelerinde cinsiyet, yaş, gelir ve eğitim durumuna göre belirgin farklılıklar bulunmaktadır.

Siber güvenlik farkındalığından yoksun olarak işgücüne katılan öğrenciler, kurumsal siber güvenliğin zaten bilinen en zayıf halkası olan kullanıcıya katkıda bulunma

riskiyle karşı karşıyadır. Muhirwe ve White (2016) çalışmalarında yeni nesil kurumsal teknoloji kullanıcıları için siber güvenlik farkındalığı ve uygulaması arasındaki ilişkiyi araştırmışlardır. Siber güvenlik eğitimi kişinin farkındalığını etkili bir şekilde tahmin etmese de siber güvenlik farkındalığıyla önemli bir ilişki göstermiştir. Anket 214 kişi ile yapılmış ve yapısal eşitlik modeli uygulanmıştır. Modellerinde yer alan yansıtıcı yapıların göstergeleri SmartPLS 2.0 ve SPSS kullanılarak değerlendirilmiştir. Bu çalışmadan elde edilen sonuçlar, siber güvenlik farkındalığının kişinin siber güvenlik uygulamalarını önemli ölçüde etkilediğini göstermektedir.

McCormac vd. (2017) bilgi güvenliği farkındalığını ölçmek için bilgi güvenliğinin insani yönleri anketini tasarlamışlardır. Çalışmaları, bireyin işyerinde bilgi güvenliğine ilişkin bilgi, tutum ve kendi bildirdiği davranışları ölçmektedir. Toplam 197 çalışan Avustralyalı, yaklaşık 4 hafta arayla anket sorularını cevaplamışlardır. Analiz sonuçları anket sonuçlarının dışsal olarak güvenilir ve içsel olarak tutarlı olduğunu göstermiştir. Bu bulguların sonuçları, kuruluşların oluşturdukları anketin yalnızca kuruluşlarındaki çalışan bilgi güvenliği farkındalığının mevcut durumunu ölçmek için değil, aynı zamanda eğitim müdahalelerinin, bilgi güvenliği farkındalık programlarının ve kampanyalarının etkinliğini ve etkilerini ölçmek için de güvenle kullanabilecekleri anlamına gelmektedir.

Genel olarak, insanlar siber tehditlere karşı zayıf bir şekilde korunmaktadır ve bunun temel nedeni kullanıcı davranışlarıdır. De Kok vd. (2020) makalelerinde, insanların hem siber tehditler hem de siber güvenlik kontrolleri hakkındaki bilgi ve tutumlarının siber güvenli davranışları benimseme niyetini nasıl etkilediğini anlamak amacıyla bir anket geliştirmişlerdir. Çalışma tutumu bilişsel ve duyuşsal bileşenlere ayırmaktadır. Genellikle tutumun sadece bilişsel bileşeni incelenmesine rağmen, 300 katılımcıyla yapılan bir anketten elde edilen sonuçlar, tutumun hem duyuşsal hem de bilişsel bileşenlerinin davranışsal niyet üzerinde değişen de olsa açıkça olumlu bir etkiye sahip olduğunu ve duyuşsal bileşenin tutum üzerinde bilişsel yönden daha da büyük bir etkiye sahip olduğunu göstermektedir. Bilgi ile davranışsal niyet arasında herhangi bir korelasyon bulunmamıştır. Sonuçlar, tutumun davranışsal müdahaleler geliştirilirken dahil edilmesi gereken önemli bir faktör olduğunu, ancak aynı zamanda farklı tutum türlerinin müdahalelerde farklı şekilde ele alınması gerektiğini göstermektedir.

Siber saldırılar bilgi güvenliğine yönelik potansiyel bir tehdit oluşturmaktadır. Veri kullanımı ve internet tüketimi oranları artmaya devam ettikçe siber farkındalık giderek daha acil hale gelmiştir. Zwilling vd. (2022) çalışmalarında genel olarak bireyler

arasında ve dört ülkede (özellikle İsrail, Slovenya, Polonya ve Türkiye) siber güvenlik farkındalığı, bilgisi ve davranışı ile koruma araçları arasındaki ilişkilere odaklanmışlardır. Teorik bir çerçeve sağlamak amacıyla, deneklerin siber güvenlik sorunlarına küresel aşinalığını ve özellikle siber güvenlik risklerine ilişkin farkındalık düzeyini test etmeyi amaçlayan çeşitli sorular içeren bir anket geliştirmişlerdir. Sonuçlar, internet kullanıcılarının yeterli siber tehdit farkındalığına sahip olduklarını, ancak genellikle nispeten yaygın ve basit olan minimum koruyucu önlemleri uyguladıklarını göstermektedir. Araştırma bulguları ayrıca, katılımcı ülke veya cinsiyet farklılıklarının ötesinde, daha yüksek siber bilginin siber farkındalık düzeyiyle bağlantılı olduğunu da göstermektedir. Ayrıca farkındalık, koruma araçlarıyla da bağlantılıdır ancak açıklamaya hazır oldukları bilgilerle bağlantılı değildir. Son olarak bulguları, araştırılan ülkeler arasında farkındalık, bilgi ve davranışlar arasındaki etkileşimi etkileyen farklılıklar ortaya koymaktadır. Etkili tabanlı siber güvenlik eğitim programlarına yönelik sonuçlar, çıkarımlar ve öneriler sunulmakta ve tartışılmaktadır.

Artan siber suç oranı, insanların siber savaştan, nükleer silah ve iklim değişikliğinden daha fazla korkmasına neden olan önemli bir endişeye dönüşmüştür. Ahmed vd. (2019) çalışmalarında tatmin edici olmayan endişe verici bir farkındalık düzeyi gözlemlemişlerdir Nüfusun önemli bir yüzdesi siber güvenlik politikaları ve uygulamalarından habersizdir. Hükümetin yanı sıra ilgili kuruluşlar bile siber suçlar konusunda endişe duymamaktadır. Siber güvenlik politikalarını ve uygulamalarını zenginleştirmek için önemli bir değişim gereklidir. Ayrıca, zamanın hızıyla birlikte izlenmesi ve yeniden yapılandırılması gerekmektedir. Bu pilot çalışma, Bangladeş halkı arasında siber suç farkındalık düzeyine ilişkin kapsamlı bir araştırmayı dikkate almak üzere tasarlanmıştır. Anket, iyi hazırlanmış bir soru formuna karşı hem çevrimiçi hem de çevrimdışı yanıtlar aracılığıyla gerçekleştirilmiştir. Ayrıca, detaylı analiz için T-testi, ortalama puan ve ANOVA testleri kullanılmıştır. Bu çalışmaya dayanarak, vatandaşları siber tehditlerden koruyacak büyük bir siber güvenlik farkındalık programının geliştirilmesi ve uygulanmasının acilen gerekli olduğu önerilmektedir.

Adebiaye ve Ajani (2018) çalışmalarında, Amerika Birleşik Devletleri'ndeki üniversite öğrencileri arasında akıllı telefon kullanımına ilişkin güvenlik önlemlerinin etkin olmayan bir şekilde uygulanmasının nedenlerini niceliksel olarak belirlemeyi amaçlamışlardır. Çalışmada ayrıca akıllı telefon güvenlik önlemlerinin düzeyi ile ilgili olarak gelecekteki sonuçların dikkate alınması düzeyi incelenmiş, kullanıcılar tarafından akıllı telefon üzerindeki güvenlik önlemlerinin düzeyleri belirlenmiş ve gelecekteki

sonuçların dikkate alınması düzeyi ile akıllı telefondaki güvenlik önlemleri arasındaki ilişki kurulmuştur. Amerika Birleşik Devletleri'ndeki lisans öğrencilerinde akıllı telefon güvenliği farkındalığı ve uygulamaları için niceliksel bir araştırma anketi ve basit rastgele örnekleme prosedürünü kullanan metodoloji, hipotezlerin test edilmesi yoluyla verilerin analiz edilmesine odaklanmıştır. Sonuçlar, üniversite öğrencilerinin %69,8'inin akıllı telefonlarına PIN, şifre ve ekran kilidi koyduğunu, %74,8'inin akıllı telefon uygulamalarında dikkatli olduğunu ve %6,2'sinin rooting hizmetleri de dahil olmak üzere güvenlik yazılımı ayarlama konusunda pratik yaptığını göstermiştir.

Li vd. (2016) makalelerinde, akran davranışı, eyleme geçirme ipucu ve çalışanların siber güvenlik eylem deneyimi, tehdit algısı, tepki algısı ve çalışanın siber güvenlik davranışı arasındaki ilişkileri doğrulamak için koruma motivasyonu teorisini genişleten bir model önermektedir. Kavramsal modelde yapılar arasındaki ilişkileri araştırmak için SPSS ile yapısal eşitlik modellemesi yöntemi uygulanmıştır. Çalışmanın bulguları, akran davranışının ve çalışanların siber güvenlik eylem deneyiminin etkisinin, kuruluşlarda siber güvenlik davranışını geliştirmek için önemli bir faktör olduğunu göstermektedir. Akran davranışı, harekete geçme ipucunu olumlu yönde etkilemekte, bu da çalışanların harekete geçme deneyimini olumlu yönde etkilemektedir. Çalışanların eylem deneyimi de tehdit algısı ve tepki algısı üzerinde olumlu etkilere sahip olacaktır. Sonuç olarak, çalışanların tehdit algısı ve tepki algısı siber güvenlik davranışlarıyla olumlu yönde ilişkilidir.

Çalışanların siber güvenlik davranışlarını birçok farklı psikolojik ve sosyal faktör etkilemektedir. Araştırılması gereken önemli bir araştırma sorusu, çalışanların siber güvenlik inanç ve davranışlarını etkileyen faktörlere aracılık etmede cinsiyetin ne ölçüde rol oynadığıdır. Bu doğrultuda Anwar vd. (2017) farklı kuruluşların çalışanları arasında kesitsel bir anket çalışması gerçekleştirmişlerdir. Psikososyal faktörler ile kişisel olarak bildirilen siber güvenlik davranışları arasındaki ilişkilerde cinsiyetin moderatör değişken olarak etkisini değerlendirmek için yapısal eşitlik modellemesini kullanmışlardır. Sonuçları cinsiyetin güvenlik öz-yeterliliği üzerinde bir etkisi olduğunu göstermektedir.

Venter vd. (2019) gelişmekte olan bir ülke olarak Güney Afrika'da yaptıkları çalışma ile iki soruya cevap vermek istemişlerdir: Soru 1: Bilgisayarla ilgili bir diploma alan öğrenciler ile farklı türde bir diploma alan öğrenciler arasında siber güvenlik farkındalığı açısından bir fark var mı? Soru 2: Soru 1'e göre cinsiyet farklılıkları var mı? 252 öğrenciye uygulanan anket soruları sonucunda incelemeleri, kadınların bilgisayarla ilgili lisans programları ve dersleri alma eğiliminde olmadıklarını göstermektedir. Siber

güvenlik farkındalığı eğitimlerinin çoğu bu lisans programlarında verildiğinden, üniversite eğitimlerinin bir parçası olarak bu ilkelere maruz kalmayacaklardır. Sonuç olarak, demografik olarak siber kadınların güvenlik konularında daha az farkındalık sahibi oldukları anlamına gelmektedir.

Garba vd. (2020) çalışmalarında öğrencilerin siber güvenliğe ilişkin temel bilgiler konusundaki farkındalıklarını araştırmayı amaçlamışlardır. Tasarlanmış bir dizi anket kullanılarak veri toplamak için nicel bir yaklaşım kullanılmıştır. Bu yöntem, öğrencilerin siber güvenlik bilgilerini araştırmak ve internet kullanımına yönelik davranışlarını gözlemlemek için kullanılmıştır. Anket, Nijerya'daki Yobe Eyalet Üniversitesi'nden toplam 201 bilgisayar bilimleri öğrencisiyle yapılmıştır. Araştırmada, COVİD 19 salgını nedeniyle bu dönemde tüm üniversitelerin kapalı olması nedeniyle öğrencilerden orta düzeyde tepkilerle karşılaşılmış, çalışmada yalnızca kentte yaşayan öğrencilere ulaşılabilmiştir. Deneyden elde edilen sonuçlar analiz edildiğinde, üniversite öğrencilerinin siber güvenlik farkındalıklarının tatmin edici düzeyde olduğu ve öğrencilerin ortalamanın üzerinde bir kısmının verilerini nasıl koruyacakları konusunda yeterince bilinçli olmadıkları ortaya çıkmıştır. Bunun yanı sıra anket, öğrencilerin siber güvenlik hakkında daha fazla bilgi edinme konusunda büyük bir istek duyduğunu da ortaya koymuştur.

Daengsi vd. (2022) Taylandlı çalışanların yaş ve cinsiyetinin kimlik avı saldırılarıyla ilişkili etkilerine ilişkin bir araştırma yapmışlardır. Tayland'daki büyük bir finans kuruluşunda ülke çapında yaklaşık 20.000 çalışanın siber güvenlik farkındalığına odaklanmışlardır. Çalışmaları, ilk phishing saldırısı, karma yaklaşımla bilgi aktarımı ve farklı içerikli ikinci phishing saldırısı olmak üzere üç aşamadan oluşmuştur. Verilerin doğrulanması ve sonuçların analizi sonrasında çalışanların siber güvenlik farkındalık düzeyinin önemli ölçüde arttığı tespit edildi. Kimlik avı e-postasını açan çalışan sayısı %71,5 azalmıştır. Ayrıca Taylandlı kadın çalışanların erkek çalışanlara göre daha yüksek düzeyde siber güvenlik farkındalığına sahip olduğu tespit edildiğinden, Tayland siber güvenlik ekosisteminde cinsiyetin siber güvenlik farkındalığında önemli bir rol oynadığı tespit edilmiştir.

Aljohani ve Elfadil, (2020) araştırma makalelerinde Fahad Bin Sultan Üniversitesi öğrencileri arasındaki mevcut siber güvenlik farkındalığı düzeyini ölçmek için bir anket aracı tasarlamışlardır ve öğrencilerinin siber güvenlik farkındalık düzeyini değerlendirmeyi amaçlamışlardır. Ankete toplam 212 öğrenci katılmıştır. Araştırma bulguları öğrencilerin farkındalıklarının ortalama düzeyde olduğunu ve erkek ve kız

öğrenciler arasında siber güvenlik farkındalık düzeyinde bir fark olmadığını göstermektedir. Ayrıca anket aracının sonuçları, modülün öğrencilerin farkındalığını ölçmede etkili olduğunu göstermektedir.

Siber güvenlik, COVID-19 salgınının yaşandığı bu dönemde interneti genellikle amaçları doğrultusunda (örneğin e-ticaret) kullanan kişiler için önemli bir konudur. Siber tehditler için, e-posta yoluyla gönderilebilen kimlik avı, kuruluştaki bilgi sistemlerine zarar verebilir. Ancak, çalışanların siber güvenlik farkındalığına sahip olması halinde bu tür tehditlerden kaynaklanan riskler azaltılabilir. Bu hipotezi Taylandlı çalışanlarla kanıtlamak için Daengsi vd. (2021), yazdıkları makale ile Bangkok, Tayland'da aynı kuruluş içinde farklı departmanlarda çalışan çalışanlarla ilgili siber güvenlik farkındalığının artırılmasına ilişkin karşılaştırmalı bir çalışma sunmaktadır. Bu çalışmada, çalışanlara siber güvenlik konusunda bilgi ve eğitim verilmeden önce ilk oltalama saldırısı simülasyonu gerçekleştirilmiş ve ikinci simülasyon ile saldırı yapılmıştır. Sonuçların toplanması ve analiz edilmesinin ardından, aynı kurumdaki teknoloji tabanlı departmanlarda (örneğin BT departmanı) ve sosyal tabanlı departmanlarda (örneğin İK departmanı) çalışan Taylandlı personel arasında siber güvenlik farkındalık düzeyi açısından önemli farklılıklar olduğu tespit edilmiştir. Ayrıca, sosyal tabanlı departmandaki Taylandlı çalışanların diğerine kıyasla zayıf olan siber güvenlik farkındalık düzeylerinin, siber güvenlik farkındalığı geliştirme süreçlerine dahil olduktan sonra belirgin bir şekilde iyileştiği tespit edilmiştir.

2.4. Çok Kriterli Karar Verme Yöntemleri

Çok sayıda ve çok çeşitli kriter söz konusu olduğunda, doğrudan karşılaştırma yapmak zor hale gelecektir ve genel bir değerlendirme yapmak birçok sorunla karşılaşacaktır. Bununla birlikte, değerlendirme kriterlerinin sayısını azaltmaya çalışmak yanlış olacaktır çünkü böyle sınırlı bir değerlendirme güvenilir olmayabilmektedir. Bu nedenle, bu tür sorunlarla başa çıkmada en iyisi olan çok kriterli analitik yöntemlerin uygulanması tavsiye edilmektedir. Çok kriterli yöntemler kullanıcının ölçülebilir ve ölçülebilir olmayan kriterleri değerlendirmesini sağlamaktadır. (Marques vd., 2011).

2.4.1. AHP (Analitik Hiyerarşi Prosesi) yöntemi

Karar verme sürecinde en az iki kriterin dikkate alındığı ve değerlendirildiği durumları kolaylaştırmak için çok kriterli karar verme temelli birçok yöntem uygulanmıştır. Bu yöntemlerden AHP (Analytic Hierarchy Process), kararla ilgili

kriterleri değerlendirmek için kolay bir tekniktir (Stocker vd., 2018). Kriterlerle ilgili ikili karşılaştırmalar, uzmanların göz önünde bulundurulan olgular hakkındaki bilgilerini yakalayarak her bir faktöre normalleştirilmiş ağırlıklar oluşturmadan önce AHP sürecinde 9 seviyeli ölçeğe dayalı olarak gerçekleştirilir (Sadik vd., 2018).

Tablo 2.7 AHP'de iki parametre arasındaki tercih ölçeği (Saaty, 1994).

Ölçekler	Tercih Derecesi	Açıklama
1	Eşit seviyede önemli	İki faaliyet hedefe eşit derecede katkıda bulunmaktadır.
3	Orta derecede önemli	Deneyim ve muhakeme, bir faaliyeti diğerine göre biraz veya orta derecede tercih eder.
5	Kesinlikle önemli	Deneyim ve muhakeme, bir faaliyeti diğerine güçlü bir şekilde veya esasen tercih eder.
7	Çok kuvvetli derecede önemli	Bir faaliyet diğerine göre güçlü bir şekilde tercih edilir ve uygulamada baskınlığı gösterilir.
9	Aşırı derecede önemli	Bir faaliyeti diğerine tercih etmenin kanıtı, bir olumlama için mümkün olan en yüksek derecededir.
2,4,6,8	Ara değerler	Ağırlık 1, 3, 5, 7 ve 9'daki tercihler arasındaki uzlaşmaları temsil etmek için kullanılır.

AHP, Saaty (1994) tarafından karar problemlerini çözmek için bir model olarak geliştirilmiştir. AHP, karar vericilerin önceliklerini dikkate alarak nicel ve nitel değişkenlerin birlikte değerlendirilebilmesini sağlamaktadır. AHP sürecindeki aşamalar aşağıdaki gibi özetlenebilir:

- Problemin amacı tanımlanır.
- Alternatiflere göre karar hiyerarşisi çerçevesi çizilir.
- Kriterlerin ikili karşılaştırmaları yapılır ve ikili karşılaştırma matrisleri geliştirilir.
- İkili karşılaştırma matrisinden kriter ağırlıkları elde edilir.
- Belirlenen kriter ağırlıklarının tutarlılığı dikkate alınır.

Yöntemin adımları aşağıdaki gibi verilebilir:

- Karar durumlarını hedefler, karar kriterleri ve alternatifler olarak düzenlemek.
- Anket oluşturma ve veri toplama. Her kriter için karşılaştırmalar yapılır ve dilbilimsel terimler kullanılarak nicel rakamlara dönüştürülür.
- Çeşitli kriterler için ikili karşılaştırmalar oluşturma.
- Her bir kriterin ağırlığını belirleme.
- Tutarlılık analizinin yapılması. Tutarlılık oranı aşağıdaki adımlara göre hesaplanır:

Tutarlılık endeksi (CI) Eşitlik 2.1 ile belirlenir:

$$CI = \frac{\lambda max - n}{n} \tag{2.1}$$

Burada λmax, karar matrisinin maksimum öz değeri, n ise matris boyutudur. Ardından, nihai tutarlılık oranı (CR) Eşitlik 2.2 ile elde edilir:

$$CR = \frac{CI}{RI} \tag{2.2}$$

CR oranı ≤ 0,10 (yani %10) ise matrisin tutarlı olduğu söylenebilmektedir.

Tablo 2.8 Rassal gösterge değerleri (Saaty, 1980).

N	1	2	3	4	5	6	7	8	9	10	11	12
RI	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48

2.4.2. Ağırlıklandırılmış olgunluk yaklaşımı

Yapılan literatür araştırmasıyla endüstri 4.0'da olgunluk analizini kolaylaştırmak ve söz konusu modelleri bir değerlendirme aracına dönüştürmek için ilk olarak Schumacher (2016) tarafından önerilen Eşitlik 2.3 kullanılmaktadır. (Kaltenbach vd., 2018).

$$M = \frac{\sum_{i=1}^{n} f_i x\, g_i}{\sum_{i=1}^{n} f_i} \tag{2.3}$$

Yukarıdaki Eşitlik 2.3'te, bir olgunluk puanı oluşturmak için, olgunluk öğelerinin ağırlıklı ortalaması her bir kategorinin puanlamasıyla çarpılır ve tüm kategorilerin toplamı ağırlıklandırma faktörüne bölünür. (Kaltenbach vd., 2018). Eşitlik 2.3'te, gi değeri ağırlık değerini gösterirken, fi değeri her bir olgunluk kriterinin ağırlıklı ortalaması için puanlama değerini göstermektedir. Bu eşitlik yardımıyla firmaların Endüstri 4.0 hazırlık seviyeleri belirlenmektedir.

3.YÖNTEM

3.1. Araştırmanın Amacı ve Önemi

Literatür araştırmaları sonucunda denizcilik sektörünün ve firmaların dijital olgunluk seviyesinin ölçülmesi ile ilgili yapılan bir çalışma ile karşılaşılmamıştır. Literatürdeki olgunluk modelleri, raporlar detaylı olarak incelenerek, denizcilik sektöründe faaliyet gösteren firmaları kapsayacak şekilde kriter ve alt kriterlerden oluşan sorular ile model oluşturulmuştur. AHP ve ağırlıklandırılmış olgunluk yaklaşımı ile denizcilik sektörünün ve firmaların dijital olgunluk seviyelerinin ölçülerek değerlendirilmesi amaçlanmıştır.

Ayrıca denizcilik sektöründe siber güvenlik farkındalığını etkileyen faktörlerin belirlenmesi ve değerlendirilmesi ile ilgili yapılan bir çalışmaya da rastlanmamıştır. Bu çalışma ile denizcilik sektöründe internet kullanıcılarının siber güvenlik farkındalığını etkileyen faktörlerin belirlenmesi ve AHP yöntemi ile değerlendirilmesi amaçlanmıştır.

Bu çalışma hem denizlik sektörünün ve firmaların dijital olgunluğunun ölçülmesinin, hem de denizcilik sektöründe siber güvenlik farkındalığını etkileyen faktörlerin belirlenmesi ve değerlendirilmesinin bir arada yapıldığı ilk çalışma olması açısından önemlidir.

3.2. Araştırmanın Örneklemi ve Evreni

Firmaların olgunluk seviyelerinin ölçülebilmesi için Türkiye'de denizlik sektöründe faaliyet gösteren firmalarda çalışan, ortalama 20 yıldan fazla deneyime sahip 4 yönetici ile görüşülerek ana ve alt kriterler belirlenmiştir. Siber farkındalığı etkileyen faktörlerin değerlendirilmesi için de bu 4 yönetici ile görüşülmüştür. Yöneticilerin ortak özellikleri, firmalarında dijitalleşme ve siber güvenlik ile ilgili konularda öncü olmaları, dijital dönüşüme ve siber güvenlik farkındalığına önem vermeleridir.

- Yönetici 1: Genel müdür. Limancılık ve dijital teknolojiler konularında 24 yıl tecrübeye sahip.
- Yönetici 2: Operasyon müdürü. Deniz taşımacılığı, siber güvenlik alanında 20 yıl tecrübeye sahip.
- Yönetici 3: Tedarik zinciri müdürü. Gemi, yat inşaatı, tedarik zinciri, lojistik konularında 16 yıllık deneyime sahip.
- Yönetici 4: Genel müdür. Limancılık, operasyon, teknoloji yönetimi konularında 23 yıllık tecrübeye sahip.

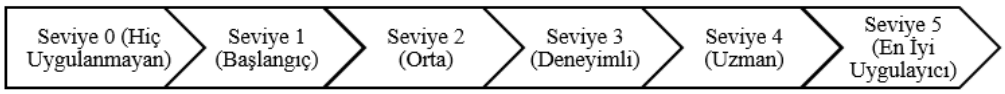
Olgunluk modelinin denizcilik sektöründe faaliyet gösteren tüm firmaları ele alacak şekilde olmasına önem verilmiştir. Bu sebeple önerilen olgunluk modelinin evrenini denizcilik sektöründe faaliyet gösteren tüm firmalar olarak ifade edebiliriz.

3.3. Araştırmanın Yöntem ve Modeli

3.3.1. Önerilen dijital olgunluk modeli

Dijital olgunluk modeli için denizcilik sektöründe faaliyet gösteren firmalarda çalışan uzmanlar ile birlikte belirlenen ana ve alt kriterlerde, AHP yöntemi ve ağırlıklandırılmış olgunluk yaklaşımı kullanılmıştır. AHP yöntemi ile tutarlılık analizi yapılmıştır. Sonuçların tutarlı olmasının ardından kriterlerin ağırlık puanları hesaplanmış, ağırlıklandırılmış olgunluk yaklaşımı ile de denizcilik sektörünün ve firmaların dijital olgunluk düzeyleri hesaplanarak değerlendirilmiştir.

Sektörün ve firmaların dijital olgunluk seviyelerinin değerlendirilebilmesi için Şekil 3.1 de gösterilen, 0 ile 5 puan arasında değişen aşamalar oluşturulmuştur.



Şekil 3.1 Oluşturulan dijital olgunluk modelinin seviyeleri

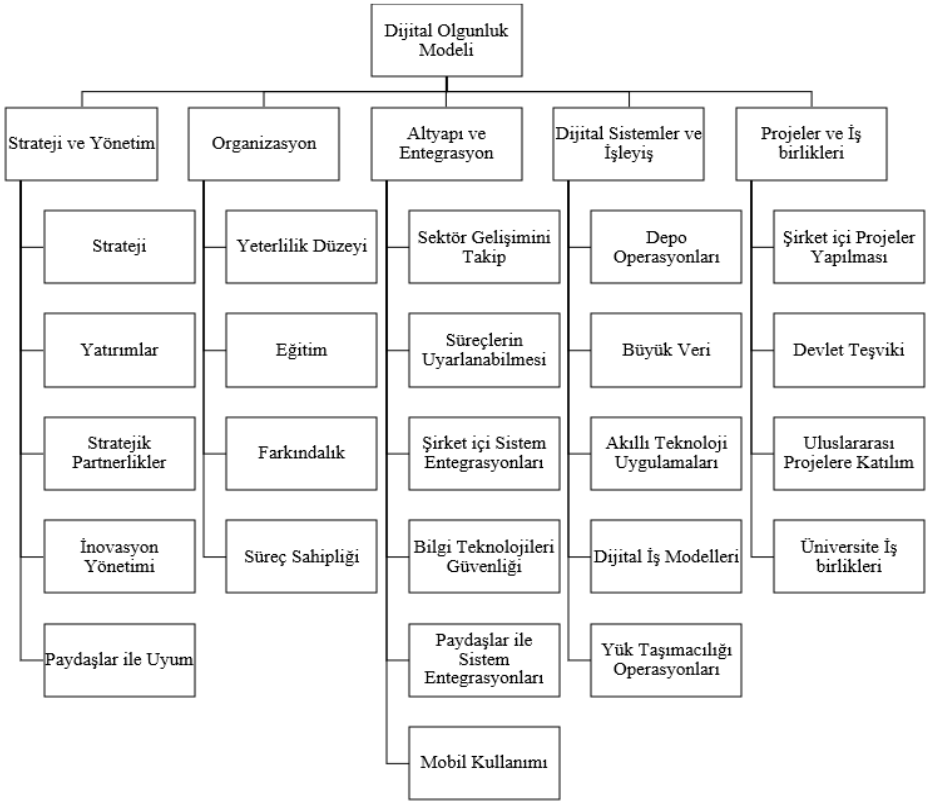
Seviyelerin açıklamaları ise;

- Hiç uygulanmayan: Endüstri 4.0 gerekliliklerinden hiçbirini karşılamayan bir şirket seviyesini tanımlamaktadır. Gereksinimlerin bazıları hiç olmayacak kadar düşük seviyededir. Farkındalık oluşmamıştır.
- Başlangıç: Dijital dönüşüm ile ilgili çalışmalar az veya yetersizdir. Düşük düzeyde ilgi vardır. Strateji ve yatırım konuları başlangıç seviyesindedir.
- Orta: Çalışmaların varlığı görülmekte ve ilgi artmaktadır. Şirketin fonksiyonel departmanlarında bazı pilot girişimlerinin olduğu bir olgunluk seviyesidir. Şirket bazı dijital dönüşümler sunmaktadır, ancak bu ürünler tamamen akıllı olma kapasitesine sahip değildir. Entegrasyon ve otomasyon seviyeleri düşüktür ve veri toplama/kullanma seviyeleri Endüstri 4.0 dönüşümünü gerçekleştirmek için yeterli değildir. Dijital teknolojiler ve bulut tüm operasyonlara uygulanmamıştır. Ekipman altyapısı hazırlığı da düşük seviyededir. Üst yönetim, Endüstri 4.0 stratejisini birkaç alana yatırım yaparak uygulamayı düşünmektedir. İş modelleri

oluşturmak veya mevcut modelleri dönüştürmek için pilot girişimler bulunmaktadır. Organizasyon yapısı yeterince uygun değildir.

- Deneyimli: Şirketin ürünlerinin gerçek zamanlı veri yönetimi yapabildiği ve farklı siteler üzerinden takip edilebildiği bir olgunluk seviyesidir. Şirket iş süreçleri entegrasyon, veri paylaşımı/toplanması/kullanımı ve çeviklik açısından deneyim sahibidir. Yönetim, Endüstri 4.0 için planlar geliştirmektedir ve birkaç alanda yatırım yapmıştır. Organizasyon yapısı ilk Endüstri 4.0 projeleri için uygundur ve yeni iş modelleri oluşturulmaktadır.
- Uzman: Stratejiler oluşturulmuş, iş birlikleri arttırılmış ve dijital dönüşüm konusunda yatırımlar ileri seviyededir. Şirket yeni iş fırsatlarını değerlendirmekte ve diğer şirketlerle veya üniversiteler ile ortaklıklar kurmakta uzmanlaşmıştır.
- En iyi performans gösteren: Bilgi birikimi benimsenmiş ve kabul edilmiştir. Olgunluk, şirketin ürünlerinin akıllı olarak tanımlandığı ve veri odaklı hizmetlerin üst düzeyde sağlandığı bir olgunluk seviyesidir. Şirketin iş süreçleri entegrasyon, veri paylaşımı, toplanması, kullanımı ve çeviklik açısından en üst düzeydedir. Neredeyse tüm süreçler merkezi olmadan yürütülebilmekte ve birlikte çalışabilirlik ilkesi ileri dijital teknolojilerin de desteğiyle şirkette pek çok alanda uygulanmaktadır. Yönetim, Endüstri 4.0 için yaygın destek sağlamakta ve neredeyse tüm departmanlar için yatırımlar yapmaktadır. Organizasyon yapısı şirket genelinde dönüşümü yönetmek için uygundur. Şirketler, akademisyenler, tedarikçiler ve teknoloji sağlayıcıları ile çok sayıda ortaklık kurmaktadır. Dijital iş modelleri şirketin mevcut iş modellerine entegre edilmiştir ve şirket bu modellerden gelir elde etmektedir.

Geniş literatür araştırmaları sonucunda denizcilik sektörünün ve firmaların dijital olgunluk seviyesinin ölçülebilmesi için 5 ana kriter ve 25 alt kriterden oluşan Şekil 3.2' de gösterilen hiyerarşik yapı meydana getirilmiştir.



Şekil 3.2 Hiyerarşik yapı

Modeldeki ana ve alt kriterler literatür araştırması sonucunda Tablo 3.1'de gösterilen 9 modele dayandırılarak oluşturulmuştur. Model oluşturulurken literatürde kabul görmüş modeller seçilmiştir.

Çalışmanın ana ve alt kriterlerinin açıklamaları bir sonraki alt başlıklarda belirtilmiştir. Dijital olgunluk seviyesinin belirlenebilmesi için oluşturulan tüm anket soruları Ek 1 ve 2'de verilmiştir.

Tablo 3.1 Kriterler ve ilişkilendirilen modeller

Sıra	Ana Kriterler	Alt Kriter No.su	Alt Kriterler	Açıklama	Schumacher vd. (2016)	Lichtblau vd. (2015)	Paulauskas ve Philipp (2020)	Schuh vd. (2017)	Tübitak (2017)	Pwc (2016)	De Carolis vd. (2017)	Agca vd. (2017)	Accenture (2015)
1	Strateji ve Yönetim	1.1	Strateji	Dijital dönüşüm için yönetim stratejisinin uygulanma durumu		•	•	•				•	•
		1.2	Yatırımlar	Dijitalleşme alanında yatırım faaliyetleri	•	•	•	•					•
		1.3	Stratejik Partnerlikler	Dijital dönüşüm için stratejik partnerlikler sağlanması	•								
		1.4	İnovasyon Yönetimi	İnovasyona yönelik iş birliği oluşturulması ve strateji geliştirilmesi			•					•	
		1.5	Paydaşlar ile Uyum	Stratejik uygulamaların paydaşlar ile paylaşılması	•	•		•				•	•
2	Organizasyon	2.1	Yeterlilik Düzeyi	Çalışanların bilgi teknolojileriyle ilgili alanlarda sahip olduğu eğitim geçmişi	•	•	•	•	•			•	
		2.2	Eğitim	Çalışanlara dijital teknolojiler ile ilgili eğitimlerin verilmesi	•	•	•	•	•	•			
		2.3	Farkındalık	Dijitalleşme farkındalığı	•	•		•	•			•	
		2.4	Süreç Sahipliği	Dijitalleşme süreçlerinin gözetilmesi	•			•					
3	Altyapı ve Entegrasyon	3.1	Sektör Gelişimini Takip	Dijital sektör ilerlemesinin izlenmesi		•		•	•			•	
		3.2	Süreçlerin Uyarlanabilmesi	Müşterilere göre süreçlerin uyarlanabilmesi			•					•	
		3.3	Şirket içi Sistem Entegrasyonları	Şirket içi dijital sistemlerin uyumu	•					•		•	
		3.4	Bilgi Teknolojileri Güvenliği	Sistem emniyetini sağlama ve acil müdahale yolları	•	•							•
		3.5	Paydaşlar ile Sistem Entegrasyonları	Paydaşlar ile sistem entegrasyonları	•								•
		3.6	Mobil Kullanımı	Mobil kullanımı									•
4	Dijital Sistemler ve İşleyiş	4.1	Depo Operasyonları	Depo operasyonlarında dijital uygulama kullanımı				•		•	•	•	•
		4.2	Büyük Veri	Büyük veri kullanımı		•		•		•			•
		4.3	Akıllı Teknoloji Uygulamaları	Son teknoloji dijital uygulamalar	•	•	•			•		•	
		4.4	Dijital iş modelleri	Karar verme safhasında faydalı örneklerden yararlanma		•	•		•			•	
		4.5	Yük Taşımacılığı Operasyonları	Yük taşımacılığı operasyonlarında dijital ürün kullanımı				•		•	•	•	•
		4.6	Ürün Takip Edilebilirliği	Ürün takip edilebilirliği						•	•	•	•
5	Projeler ve İş Birlikleri	5.1	Şirket İçi Projeler Yapılması	Şirket içerisinde dijitalleşmeye yönelik projeler uygulanması				•	•				
		5.2	Devlet Teşviki	Dijital projeler için devlet teşviki sağlanması					•				
		5.3	Uluslararası Projelere Katılım	Uluslararası projelere iştirak edilmesi				•	•				
		5.4	Üniversite İş Birlikleri	Dijitalleşme projeleri için üniversiteler ile iş birlikleri yapılması	•				•				

3.3.1.1. Strateji ve yönetim

1. ana kriter strateji ve yönetimdir. 5 alt kritere sahiptir. Bunlar; dijital dönüşüm için yönetim stratejisinin uygulanma durumu, dijitalleşme alanında yatırım faaliyetleri, dijital dönüşüm için stratejik partnerlikler sağlanması, inovasyona yönelik iş birliği oluşturulması ve strateji geliştirilmesi, stratejik uygulamaların paydaşlar ile paylaşılmasıdır.

- Dijital dönüşüm için yönetim stratejisinin uygulanma durumu: Şirketlerin dijital araçlarla yeni rekabet avantajı oluşturmak için izleyeceği yönü ve bu ilerlemeleri gerçekleştirmek için benimseyeceği stratejilerin uygulanma durumu belirlenmeye çalışılmıştır.
- Dijitalleşme alanında yatırım faaliyetleri: Şirketlerin yıllık bütçeleri içerisinde dijital dönüşüm için ne kadar bir bütçe ayırarak, dijitalleşmeye ne derecede hazır olduğunun ölçülmeye çalışıldığı sorudur.
- Dijital dönüşüm için stratejik partnerlikler sağlanması: Şirketlerin dijital dönüşümleri için teknoloji firmaları ile ilişkileri araştırılmıştır.
- İnovasyona yönelik iş birliği oluşturulması ve strateji geliştirilmesi: Şirketlerin inovasyon yolu ile dijitalleşme durumu, inovasyon yönetimi, hangi seviyede strateji ve iş birliği geliştirdiği sorulmuştur.
- Stratejik uygulamaların paydaşlar ile paylaşılması: Şirketlerin paydaşlar ile ne derecede uyumlu çalışılabildiği ve strateji olarak belirlenen aksiyonların paydaşlar ile paylaşılmasının, aksiyonların yayılımının sağlanmasının ne durumda olduğunun araştırıldığı alt kriterdir.

3.3.1.2. Organizasyon

2. ana kriter organizasyondur. 4 alt kritere sahiptir. Bunlar; çalışanların bilgi teknolojileriyle ilgili alanlarda sahip olduğu eğitim geçmişi, çalışanlara dijital teknolojiler ile ilgili eğitimlerin verilmesi, dijitalleşme farkındalığı, dijitalleşme süreçlerinin gözetilmesidir.

- Çalışanların bilgi teknolojileriyle ilgili alanlarda sahip olduğu eğitim geçmişi: Firmada, acil durumlara müdahale için bilgi teknolojileriyle ilgili alanlarda eğitim geçmişine sahip çalışan sayısının sorulduğu alt kriterdir.
- Çalışanlara dijital teknolojiler ile ilgili eğitimlerin verilmesi: Dijital işyerindeki değişimlerden en çok etkilenenler çalışanlardır. Doğrudan çalışma ortamları

değiştirilmektedir ve yeni beceriler ile nitelikler kazanmaları gerekmektedir. Uzmanlar bu durumun, şirketlerin çalışanlarını uygun eğitim ve sürekli eğitim yoluyla bu değişikliklere hazırlamasının giderek daha kritik hale getirdiğini vurgulamaktadırlar.

- Dijitalleşme farkındalığı: Dijitalleşmenin firmalara sağladığı ekonomik faydanın farkındalığı konusunda alınan aksiyonlar araştırılmıştır. Şirketlerin etkili bir strateji tanımlayabilmeleri ve diğer uygun tedbirleri alabilmeleri için öncelikle bu konunun öneminin farkına varmaları gerekmektedir. Olası veri sızıntıları ve bunların nedenleri konusunda farkındalık yaratmak için çalışan eğitiminin önemli bir parçasıdır.
- Dijitalleşme süreçlerinin gözetilmesi: Bilgi ve iletişim teknolojilerinin ürün ve süreçlerde kullanımının giderek yaygınlaşması nedeniyle, yöneticilerin çalışanlarının düşünce ve davranış biçimlerinde disiplinler arası bir yaklaşıma teşvik etmesi önem taşıdığından, şirketlerin mevcut süreçlerini yeni teknolojilere uygun olarak yeniden şekillendirmek için net bir yol oluşturma konusunda C seviye yöneticiler büyük rol oynamaktadırlar.

3.3.1.3. Altyapı ve entegrasyon

3. ana kriter altyapı ve entegrasyondur. 6 alt kritere sahiptir. Bunlar; dijital sektör ilerlemesinin izlenmesi, müşterilere göre süreçlerin uyarlanabilmesi, şirket içi dijital sistemlerin uyumu, sistem emniyetini sağlama ve acil müdahale yolları, paydaşlar ile sistem bütünleşmeleri ve mobil kullanımıdır.

- Dijital sektör ilerlemesinin izlenmesi: Firma içerisinde kullanılan dijital altyapının güncelliğinin hangi seviyede takip edildiği ve yeniliklerin kullanılan uygulamalara ne derecede eklendiğinin araştırıldığı alt kriterdir.
- Müşterilere göre süreçlerin uyarlanabilmesi: Müşteri arayüzünün dijital entegrasyonuna ve şirketin ürün ve hizmetleri aracılığıyla hangi seviyede bütünleştirildiğine odaklanılmıştır.
- Şirket içi dijital sistemlerin uyumu: Müşteri deneyimini geliştirmek için birlikte çalışabilirliğe ve veri paylaşımına olanak tanıyan sistemlerin birbiriyle uyum durumu irdelenmiştir.
- Sistem emniyetini sağlama ve acil müdahale yolları: Yapılacak saldırı veya teknik problemler sonucunda oluşabilecek sistem çökmelerine karşı sistemin stabil duruma ne kadar sürede hızlı şekilde getirildiği araştırılmıştır.

- Paydaşlar ile sistem bütünleşmeleri: Firmaların hedeflerine ulaşabilmeleri için paydaşları (acente, müşteri, tedarikçi vs.) ile birlikte yapmış oldukları iş birliklerinde sistem entegrasyonlarının durumunun ölçülmeye çalışıldığı alt kriterdir.
- Mobil kullanımı: Şirket içerisinde kullanılan dijital programların, yazılımların mobil kullanım seçeneklerinin olup olmadığına bakılan sorudur.

3.3.1.4. Dijital sistemler ve işleyiş

4. ana kriter dijital sistemler ve işleyiştir. 6 alt kritere sahiptir. Bunlar; depo operasyonlarında dijital uygulama kullanımı, büyük veri kullanımı, son teknoloji dijital uygulamalar, karar alma safhasında faydalı örneklerden yararlanma, yük taşımacılığı operasyonlarında dijital uygulama kullanımı ve ürün takip edilebilirliğidir.

- Depo operasyonlarında dijital uygulama kullanımı: Yüksek düzeyde uygulama standardını karşılamak ve kaliteyi, müşteri ve son kullanıcı deneyimini geliştirmek amacıyla, depo operasyonlarında hangi seviyede dijital teknoloji kullanıldığına yönelik sorudur.
- Büyük veri kullanımı: Veri analitiği kullanılarak, bilgilendirme amaçlı olarak büyük hacimli verilerin analizini destekleyen yeni teknolojilerin hangi seviyede kullanıldığını değerlendiren alt kriter sorusudur.
- Son teknoloji dijital uygulamalar: Akıllı Sensörler, drone, 3d yazıcı, akıllı robotlar, arttırılmış gerçeklik, gelişmiş arayüzler, yapay zekâ, sanal ticaret, akıllı şebekeler gibi son teknoloji dijital ürünlerin firmalar içerisinde kullanımının ne durumda olduğu araştırılmıştır.
- Karar alma safhasında faydalı örneklerden yararlanma: Müşteriler, kamu memurları gibi paydaşlar tarafından işlerin dijital ortamlardan (web sitesi, mobil uygulama) izlenmesi ve dijital sipariş yönetimi gibi konularda dijital iş modellerinden faydalanıp faydalanılmadığının incelendiği ilgili alt kriterdir.
- Yük taşımacılığı operasyonlarında dijital uygulama kullanımı: Yük taşımacılığı operasyonlarının dijital teknolojilerden hangi seviyede faydalanılarak yapıldığına dair alt kriterdir.
- Ürün takip edilebilirliği: Firmaların müşterilerin beklentilerini karşılamak adına tüm iş süreçleri sırasında ürünlere hangi durumlarda gerçek zamanlı izlemenin yapılabildiğine yönelik yapılan alt kriterdir.

3.3.1.5. Projeler ve iş birlikleri

5. ana kriter projeler ve iş birlikleridir. 4 alt kritere sahiptir. Bunlar; şirket içerisinde dijitalleşmeye yönelik projeler uygulanması, dijital projeler için devlet teşviki sağlanması, uluslararası projelere iştirak edilmesi, dijitalleşme projeleri için üniversiteler ile iş birliği yapılmasıdır.

- Şirket içerisinde dijitalleşmeye yönelik projeler uygulanması: Firma içerisinde dijital dönüşüm ile ilgili yapılan projelerin hangi düzeyde olduğu araştırılmıştır.
- Dijital projeler için devlet teşviki sağlanması: Şirketlerin yaptıkları dijital projeler için devlet tarafından katkı alıp almadıklarını inceleyen alt kriter sorusudur.
- Uluslararası projelere iştirak edilmesi: Firmaların alanlarında uluslararası düzeyde projelere katılıp katılmadığı ile ilgili alt kriterdir.
- Dijitalleşme projeleri için üniversiteler ile iş birliği yapılması: Şirketlerin dijital projeler için üniversiteler ile hangi seviyede iş birliği yaptığı görülmek istenmiştir.

3.3.2 Önerilen etkileyici faktörlerle ilgili siber güvenlik farkındalığı modeli

Literatür bölümünde de bahsedildiği gibi, kullanıcıların siber güvenlik farkındalık düzeyini etkileyen faktörlere dayanan birçok ilginç çalışma bulunmaktadır. Bunların çoğunda nicel istatistiksel yöntemler kullanılmıştır. Tablo 3.2 de bu çalışmalar gösterilmektedir.

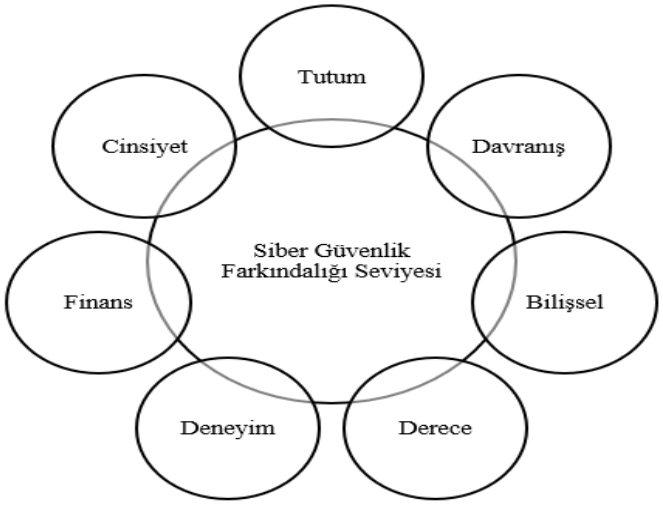
Tablo 3.2 Önerilen model ile ilişkili çalışmalar

Kaynaklar	Tutum	Davranış	Bilişsel	Derece	Deneyim	Finans	Cinsiyet	Yaş	Metodoloji
Kovačević vd. (2020)	•	•	•		•		•		Nicel İstatistik
Fatokun vd. (2019)		•		•	•		•		Yapısal Eşitlik Modeli
Agustini ve Kencana (2016)				•		•	•	•	Nicel İstatistik
Muhirwe ve White (2016)				•	•		•	•	Yapısal Eşitlik Modeli
McCormac vd. (2017)	•	•	•						Nicel İstatistik
De Kok vd. (2020)	•	•	•						Nicel İstatistik
Zwilling vd. (2022)		•	•				•		Nicel İstatistik
Ahmed vd. (2019)					•		•	•	Nicel İstatistik
Adebiaye ve Ajani (2018)		•	•						Nicel İstatistik
Li vd. (2016)		•			•				Yapısal Eşitlik Modeli
Anwar vd. (2017)		•					•		Nicel İstatistik
Venter vd. (2019)				•			•		Nicel İstatistik
Garba vd. (2020)				•			•		Nicel İstatistik

Tablo 3.2 Önerilen model ile ilişkili çalışmalar (Devam)

Kaynaklar	Tutum	Davranış	Bilişsel	Derece	Deneyim	Finans	Cinsiyet	Yaş	Metodoloji
Daengsi vd. (2022)							•	•	Nicel İstatistik
Aljohani ve Elfadil, (2020)							•		Nicel İstatistik
Daengsi vd. (2021)				•					Nicel İstatistik
Ungkap ve Daengsi (2022)	•		•	•	•		•		Nicel İstatistik

Önerilen etkileyici faktörlerle ilgili siber güvenlik farkındalığı modellemesi, bireysel farklılıklara dayalı insan faktörlerine odaklanmaktadır. Oluşturulan bu model, siber güvenlik farkındalığı seviyesini etkileyen faktörlerin önemini veya etkisini incelemek için önerilmiş ve geliştirilmiştir. Bu faktörler tutum, davranış, bilişsel (bilgi), derece, deneyim, finans ve cinsiyetten oluşmaktadır. Şekil 3.3'de oluşturulan model verilmiştir. Uzmanlardan 9 puanlık bir ölçek kullanarak her bir çift içindeki belirli bireysel farklılık faktörlerinin önemini belirlemek için bir dizi ikili karşılaştırmayı değerlendirmeleri istenmiştir. Daha sonra, her bir katılımcıdan elde edilen veriler toplanmış, AHP yöntemi ile yapılan tutarlılık analizlerinin olumlu olmasının ardından ağırlık puanları üzerinden değerlendirilmiştir.



Şekil 3.3 Etkileyici faktörlerle ilgili siber güvenlik farkındalığı modellemesi

4.BULGULAR

4.1. Dijital Olgunluk Modeli Uygulaması

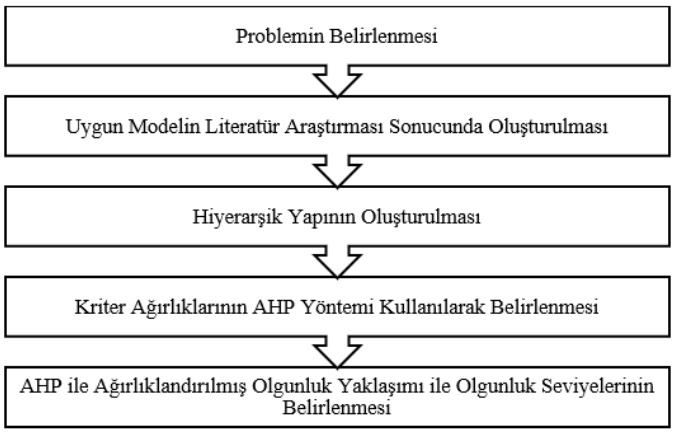
Bu çalışma ile, denizcilik sektörünün ve firmaların dijital olgunluk seviyesinin ne durumda olduğuna cevap aranarak, sektörün ve firmaların genel durumları hakkında bilgi sahibi olunmasına yönelik bir dijital olgunluk modeli önerilmiştir.

Yapılan literatür araştırmaları sonucunda bulunan modellere dayandırılarak, denizcilik sektörü ve firmaların dijital olgunluk seviyesinin belirlenebilmesi için yeni olgunluk modeli oluşturulmuştur. Modelin tüm denizcilik sektörünü kapsayacak şekilde oluşturulmasına önem verilmiştir.

Önerilen model 3. bölümde Tablo 3.1' de gösterildiği gibi 5 ana kriter ve 25 alt kriterden meydana gelmiştir. 3. Bölüm Şekil 3.2'de gösterildiği gibi ise hiyerarşik yapı oluşturulmuştur.

4 farklı firma yöneticisine, hazırlanan 2 ayrı anket soruları yöneltilmiştir. Seçilen firmaların sektör içindeki tüm alanlardan olmasına dikkat gösterilmiştir. İlk anket, modelin kriter ağırlıklarının belirlenmesi için oluşturulan AHP anketidir. İkinci anket, firmaların dijitalleşme seviyelerini belirlemek amacıyla oluşturulan olgunluk düzeyi anketidir.

Uygulanması kolay, ikili karşılaştırmalara önem veren AHP yöntemi ile kriterlerin ağırlıkları hesaplanmıştır. AHP ile Ağırlıklandırılmış Olgunluk Yaklaşımı ile de sektörün ve firmaların olgunluk seviyeleri belirlenmiştir. Uygulama sürecinin akış diyagramı Şekil 4.1'de gösterilmiştir.



Şekil 4.1 Uygulama süreci akış diyagramı

Kriterlerin ağırlıklarının hesaplanabilmesi için;

- 5x5 ikili karşılaştırma matrisi hazırlanmıştır. Bu matrisler yöneticiler tarafından 1'den 9'a kadar olan önem dereceleri ile doldurulmuştur. Bir kriterin diğer kriterden ne kadar daha önemli olduğu bulunmaya çalışılmıştır.
- İkili karşılaştırma matrisi hazırlandıktan sonra her bir sütunun toplamı alınmıştır. Her bir sütun değeri sütun toplamına bölünerek normalize edilmiştir.
- Normalize edilen değer, normalize edilmiş sütun toplamına bölünerek her bir kriterin ağırlığı hesaplanmıştır.
- Ana ve alt kriterlerin, ikili karşılaştırmaların belirlenmesinde verilen kararların tutarlı olması gerekmektedir. Eşitlik 2.1 ile CI, yani tutarlılık endeks değeri hesaplanmıştır.
- Bulunan tutarlılık endeks değerlerinin Tablo 2.8'deki rassal göstergede uygun matris boyutunun değerine bölünerek CR, yani tutarlılık oranı bulunmuştur.
- CR oranı ≤ 0,10 (yani %10) ise matrisin tutarlı ve kabul edilebilir olduğu söylenebilmektedir.
- Sonuçların tutarlı çıkmasının ardından normalize edilen değerin, normalize edilmiş sütun toplamına bölünerek elde edilen kriter ağırlıkları, analiz için kullanılabilmektedir.

Aşağıda yönetici 1'e ait hesaplamalardan örnekler verilmiştir. Diğer yöneticilerin cevapları da aynı yöntemler ile çalışma içerisinde hesaplanmıştır.

Ana kriterler değerlendirilmesi için yönetici 1 tarafından verilen cevaplar, tutarlılık analizi ve kriter ağırlıklarını gösteren sonuçlar Tablo 4.1'de verilmiştir.

Tablo 4.1 Yönetici 1'e ait ana kriterlerin AHP değerlendirme tablosu

	Strateji ve Yönetim	Organizasyon	Altyapı ve Entegrasyon	Dijital Sistemler ve İşleyiş	Projeler ve İş Birlikleri	Normalize	Sonuç	Tutarlılık	Alfamax	N	5,00
Strateji ve Yönetim	1,00	3,00	5,00	5,00	5,00	2,37	0,47	2,65	5,59	Rassallık	1,12
Organizasyon	0,33	1,00	3,00	3,00	3,00	1,13	0,23	1,28	5,70	CI	0,10
Altyapı ve Entegrasyon	0,20	0,33	1,00	3,00	3,00	0,72	0,14	0,78	5,47	CR	0,09
Dijital Sistemler ve İşleyiş	0,20	0,33	0,33	1,00	3,00	0,49	0,10	0,49	5,08		
Projeler ve İş Birlikleri	0,20	0,33	0,33	0,33	1,00	0,30	0,06	0,31	5,19		
Sütun Toplamı	1,93	5,00	9,67	12,33	15,00	5,00	1,00	Ortalama	5,41		

Birinci yönetici ile yapılan anketin AHP ile değerlendirilmesi sonucunda %47 ile strateji ve yönetimin en önemli kriter olduğu görülmektedir. %23 ile organizasyon 2.

sırada, %14 ile altyapı ve entegrasyon 3. sırada, %10 ile dijital sistemler ve işleyiş 4. sırada, %6 ile projeler ve iş birlikleri 5. sırada yer almaktadır.

Anket sorularına verilen cevaplar neticesinde ana kriterlerin ikili karşılaştırmaları için Microsoft Excel'de 5x5 boyutunda matris meydana getirilerek, sonuçların elde edilebilmesi için ilgili hücrelerde formüller oluşturulmuştur. Değerler girilerek her bir sütunun toplamı alınmıştır. Her bir sütun değerinin sütun toplamına bölünerek normalize edilmiş değerler bulunmuştur. Normalize edilmiş değerlerin sütun toplamına bölünmesi ile de kriterlerin ağırlık sonuçları elde edilmiştir. Sonuçların tutarlı olduğunun ispatlanması için ise alfamax ve tutarlılık endeks değeri (CI) değerleri hesaplanmıştır. Tutarlılık endeks değerinin rassal gösterge tablosundan alınan uygun değere bölünmesiyle de tutarlılık oranı (CR) bulunmuştur. Tutarlılık oranının 0,10'dan küçük bir değer yani 0,09 olması ile yönetici 1'in ana kriterler için AHP ile değerlendirilmesinin tutarlı olduğu söylenebilmektedir.

4 farklı yöneticinin vermiş olduğu cevaplar ile ana kriterler ve alt kriterler ikili karşılaştırma yapılarak tüm sonuçların 0,10 ve altında çıktığı, yani tutarlı olduğu görülmüştür. Tüm tutarlılık oranları Tablo 4.2'de verilmiştir.

Tablo 4.2 AHP tutarlılık sonuçları

	Yönetici 1	Yönetici 2	Yönetici 3	Yönetici 4
Ana Kriterler	0,09	0,10	0,04	0,06
1. Ana Kriter	0,08	0,10	0,08	0,10
2. Ana Kriter	0,07	0,10	0,10	0,07
3. Ana Kriter	0,09	0,08	0,09	0,09
4. Ana Kriter	0,09	0,10	0,09	0,10
5. Ana Kriter	0,07	0,01	0,04	0,06

Ardından 4 farklı yöneticinin verdiği cevapların geometrik ortalamaları alınarak, ana kriterler ve alt kriterlerin ağırlık puanları hesaplanmıştır. Ana kriterlerin hesaplamaları Tablo 4.3'de, 1. ana kriterin alt kriterlerinin hesaplamaları Tablo 4.4'de, 2. ana kriterin alt kriterlerinin hesaplamaları Tablo 4.5'de, 3. ana kriterin alt kriterlerinin hesaplamaları Tablo 4.6'de, 4. ana kriterin alt kriterlerinin hesaplamaları Tablo 4.7'de, 5. ana kriterin alt kriterlerinin hesaplamaları Tablo 4.8'de verilmiştir.

Tablo 4.3 Ana kriterlerin ağırlık hesap tablosu

	Strateji ve Yönetim	Organizasyon	Altyapı ve Entegrasyon	Dijital Sistemler ve İşleyiş	Projeler ve İş Birlikleri	Normalize	Sonuç
Strateji ve Yönetim	1,00	3,71	5,00	4,79	6,30	2,68	53,54%
Organizasyon	0,27	1,00	1,32	1,16	1,52	0,69	13,80%
Altyapı ve Entegrasyon	0,20	0,76	1,00	1,32	3,00	0,71	14,15%
Dijital Sistemler ve İşleyiş	0,21	0,86	0,76	1,00	1,73	0,57	11,38%
Projeler ve İş Birlikleri	0,16	0,66	0,44	0,44	1,00	0,36	7,12%
Sütun Toplamı	1,84	6,99	8,51	8,70	13,56	5,00	100,00%

Tablo 4.4 Birinci ana kriterin alt kriterlerinin ağırlık hesap tablosu

	Strateji	Yatırımlar	Stratejik Partnerlikler	İnovasyon Yönetimi	Paydaşlar ile Uyum	Normalize	Sonuç
Strateji	1,00	0,88	1,97	2,14	3,95	1,57	31,35%
Yatırımlar	1,14	1,00	1,50	1,32	1,63	1,21	24,18%
Stratejik Partnerlikler	0,51	0,67	1,00	0,76	1,73	0,77	15,39%
İnovasyon Yönetimi	0,47	0,76	1,32	1,00	2,94	0,98	19,62%
Paydaşlar ile Uyum	0,25	0,61	0,58	0,34	1,00	0,47	9,46%
Sütun Toplamı	3,36	3,92	6,36	5,56	11,25	5,00	100,00%

Tablo 4.5 İkinci ana kriterin alt kriterlerinin ağırlık hesap tablosu

	Yeterlilik Düzeyi	Eğitim	Farkındalık	Süreç Sahipliği	Normalize	Sonuç
Yeterlilik Düzeyi	1,00	1,14	0,61	0,81	0,87	21,69%
Eğitim	0,88	1,00	1,32	1,32	1,11	27,74%
Farkındalık	1,63	0,76	1,00	1,50	1,15	28,81%
Süreç Sahipliği	1,24	0,76	0,67	1,00	0,87	21,77%
Sütun Toplamı	4,74	3,66	3,60	4,62	4,00	100,00%

Tablo 4.6 Üçüncü ana kriterin alt kriterlerinin ağırlık hesap tablosu

	Sektör Gelişimini Takip	Süreçlerin Uyarlanabilmesi	Şirket içi Sistem Entegrasyonları	Bilgi Teknolojileri Güvenliği	Paydaşlar ile Sistem Entegrasyonları	Mobil Kullanımı	Normalize	Sonuç
Sektör Gelişimini Takip	1,00	1,00	0,51	0,31	1,00	3,00	0,71	11,80%
Süreçlerin Uyarlanabilmesi	1,00	1,00	0,59	0,18	1,14	1,97	0,62	10,26%
Şirket içi Sistem Entegrasyonları	1,97	1,70	1,00	0,33	1,50	2,94	1,03	17,10%
Bilgi Teknolojileri Güvenliği	3,26	5,66	3,00	1,00	4,88	6,42	2,72	45,39%
Paydaşlar ile Sistem Entegrasyonları	1,00	0,88	0,59	0,20	1,00	1,97	0,60	10,07%
Mobil Kullanımı	0,33	0,51	0,34	0,16	0,51	1,00	0,32	5,38%
Sütun Toplamı	8,56	10,75	6,03	2,18	10,02	17,30	6,00	100,00 %

Tablo 4.7 Dördüncü ana kriterin alt kriterlerinin ağırlık hesap tablosu

	Depo Operasyonları	Büyük Veri	Akıllı Teknoloji Uygulamaları	Dijital iş modelleri	Yük Taşımacılığı Operasyonları	Ürün Takip Edilebilirliği	Normalize	Sonuç
Depo Operasyonları	1,00	0,81	0,81	0,16	0,65	0,17	0,35	5,80%
Büyük Veri	1,24	1,00	0,76	0,18	0,76	0,23	0,40	6,71%
Akıllı Teknoloji Uygulamaları	1,24	1,32	1,00	0,26	0,92	0,23	0,49	8,24%
Dijital iş modelleri	6,30	5,54	3,87	1,00	5,00	2,59	2,53	42,24%
Yük Taşımacılığı Operasyonları	1,53	1,32	1,09	0,20	1,00	0,29	0,51	8,56%
Ürün Takip Edilebilirliği	5,90	4,40	4,40	0,39	3,41	1,00	1,71	28,45%
Sütun Toplamı	17,20	14,39	11,93	2,18	11,74	4,51	6,00	100,00%

Tablo 4.8 Beşinci ana kriterin alt kriterlerinin ağırlık hesap tablosu

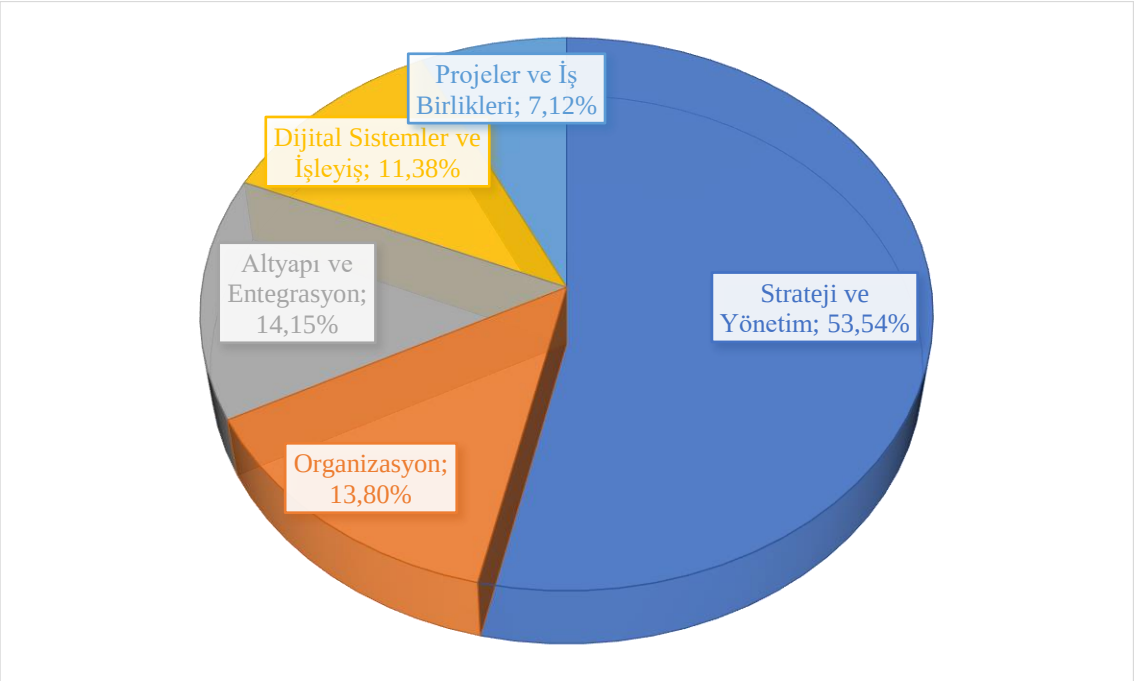
	Şirket İçi Projeler Yapılması	Devlet Teşviki	Uluslararası Projelere Katılım	Üniversite İş Birlikleri	Normalize	Sonuç
Şirket İçi Projeler Yapılması	1,00	1,00	1,24	1,73	1,14	28,55%
Devlet Teşviki	1,00	1,00	2,59	2,59	1,51	37,76%
Uluslararası Projelere Katılım	0,81	0,39	1,00	1,00	0,71	17,70%
Üniversite İş Birlikleri	0,58	0,39	1,00	1,00	0,64	15,99%
Sütun Toplamı	3,39	2,77	5,83	6,32	4,00	100,00%

Alt kriterlerin de ağırlıkları hesaplandıktan sonra ana kriterlerin ağırlıkları ile çarpılarak her bir alt kriter için genel ağırlık derecesi hesaplanmıştır. Tüm kriterlerin tüm ağırlıkları Tablo 4.9' da bir arada gösterilmiştir.

Tablo 4.9 Tüm kriterlere ait ağırlık hesap tablosu

Ana Kriterler	Ana Kriter Ağırlıkları	Alt Kriterler	Alt Kriter Ağırlıkları	Genel Ağırlık
Strateji ve Yönetim	53,54%	Strateji	31,35%	16,78%
		Yatırımlar	24,18%	12,95%
		Stratejik Partnerlikler	15,39%	8,24%
		İnovasyon Yönetimi	19,62%	10,51%
		Paydaşlar ile Uyum	9,46%	5,06%
Organizasyon	13,80%	Yeterlilik Düzeyi	21,69%	2,99%
		Eğitim	27,74%	3,83%
		Farkındalık	28,81%	3,98%
		Süreç Sahipliği	21,77%	3,00%
Altyapı ve Entegrasyon	14,15%	Sektör Gelişimini Takip	11,80%	1,67%
		Süreçlerin Uyarlanabilmesi	10,26%	1,45%
		Şirket içi Sistem Entegrasyonları	17,10%	2,42%
		Bilgi Teknolojileri Güvenliği	45,39%	6,42%
		Paydaşlar ile Sistem Entegrasyonları	10,07%	1,42%
		Mobil Kullanımı	5,38%	0,76%
Dijital Sistemler ve İşleyiş	11,38%	Depo Operasyonları	5,80%	0,66%
		Büyük Veri	6,71%	0,76%
		Akıllı Teknoloji Uygulamaları	8,24%	0,94%
		Dijital iş modelleri	42,24%	4,81%
		Yük Taşımacılığı Operasyonları	8,56%	0,97%
		Ürün Takip Edilebilirliği	28,45%	3,24%
Projeler ve İş Birlikleri	7,12%	Şirket İçi Projeler Yapılması	28,55%	2,03%
		Devlet Teşviki	37,76%	2,69%
		Uluslararası Projelere Katılım	17,70%	1,26%
		Üniversite İş Birlikleri	15,99%	1,14%

Tablo 4.9 incelendiğinde, ana kriterler içerisinde en önemli kriterin açık ara fark ile %53,54 ile strateji ve yönetimin geldiği görülmektedir. 2. sırada %13.80 ile organizasyon, 3. %14.15 sırada altyapı ve entegrasyon, 4. sırada ise %11.38 ile dijital sistemler ve işleyiş gelmektedir. %7.12 ile projeler ve iş birlikleri ise ana kriterler arasında son sırada gelmektedir. Ana kriterlerin ağırlıklarının sonuçları Şekil 4.2'deki grafikte verilmiştir.



Şekil 4.2 Ana kriterlerin ağırlık sonuçları

Strateji ve yönetim ana kriteri içerisinde ise strateji alt kriteri %31,35 ile ilk sıradadır. 2. sırada %24,18 ile yatırımlar, 3. sırada %19,62 inovasyon yönetimi, 4.sırada %15,39 stratejik partnerlikler yer almaktadır. Paydaşlar ve uyum alt kriteri ise % 9,46 ile 5. Sıradadır.

Organizasyon ana kriterinde ise sonuçlar hemen hemen birbirine yakın çıkmıştır. %28.81 ile farkındalık ilk sırada yerini alırken, eğitim alt kriteri %27,74 ile ikinci sıradadır. %21,77 ile süreç sahipliği 3., %21,69 ile yeterlilik düzeyi 4. Sıradadır.

Altyapı ve entegrasyonda ise bilgi teknolojileri ve güvenliği %45.39 ile en öndedir. Şirket içi sistem entegrasyonları %17,10, sektör gelişimini takip %11,80, süreçlerin uyarlanabilmesi %10,26, paydaşlar ile sistem entegrasyonları %10,07, mobil kullanımı %5,38 puan almıştır.

Dijital sistemler ve işleyiş ana kriterinde dijital iş modelleri %42,24, ürün takip edilebilirliği %28,45, yük taşımacılığı operasyonları %8,56, akıllı teknoloji uygulamaları %8,24, büyük veri %6,71, depo operasyonları %5,80 puan almıştır.

Ana kriterler içerisinde en düşük puana sahip projeler ve iş birliklerinde ise devlet teşviki %37,76, şirket içi projeler yapılması %28,55, uluslararası projelere katılım %17,70, üniversite iş birlikleri %15,99 ile sıralamada yer almıştır.

Ek 1'de verilen anket soruları AHP yöntemi ile değerlendirilip, kriterlerin ağırlıkları hesaplandıktan sonra, Ek 2'deki olgunluk düzeylerinin belirlenmesi için oluşturulan anket yöneticilere yöneltilmiştir. Firmaların olgunluk düzeyi değerlendirme

puanları Tablo 4.10'da verilmiştir. Verilen puanlamalara göre, 2. bölümdeki Eşitlik 2.3 ile denizcilik sektörünün ve firmaların dijital olgunluk seviyeleri belirlenmiştir. Her bir kriterin genel ağırlık puanı ile kriterlerin ağırlıklandırılmış ortalamaları çarpılarak toplanmış, sonuç toplam değerine bölünerek olgunluk seviyesi sonucuna ulaşılmıştır. Eşitlik 4.1'de olgunluk düzeyinin hesaplanması verilmiştir.

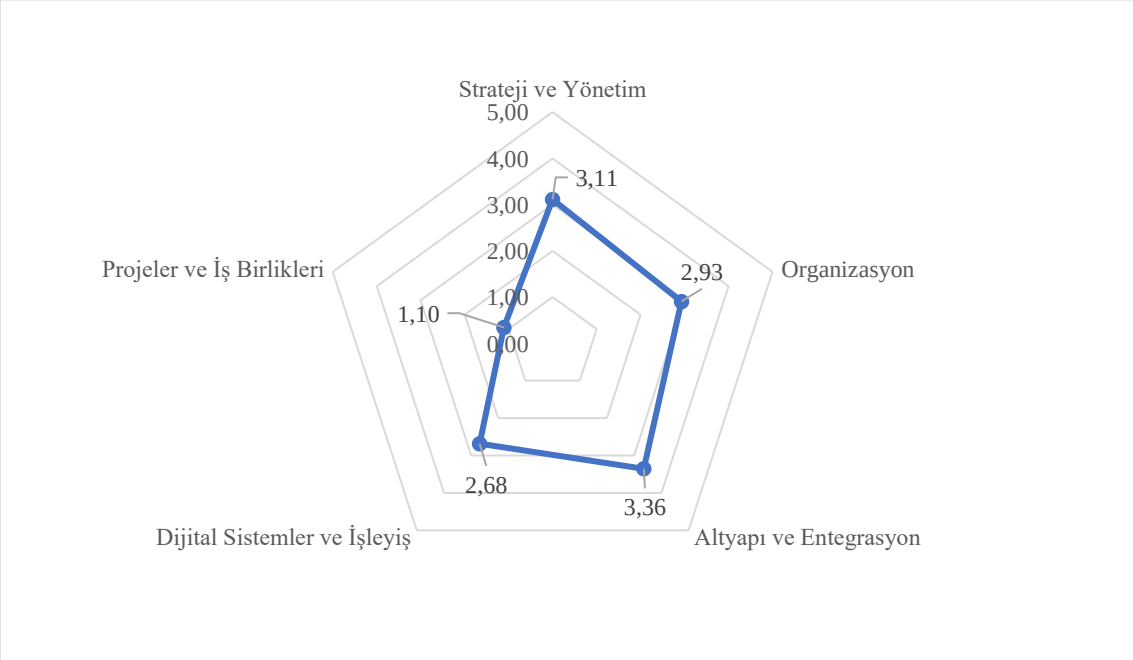
Tablo 4.10 Firmaların olgunluk düzeyi değerlendirme puanları

Ana Kriterler	Alt Kriterler	Firma 1	Firma 2	Firma 3	Firma 4	Ortalama
Strateji ve Yönetim	Strateji	1,00	5,00	2,00	5,00	3,25
	Yatırımlar	3,00	5,00	2,00	5,00	3,75
	Stratejik Partnerlikler	2,00	5,00	1,00	2,00	2,50
	İnovasyon Yönetimi	0,00	5,00	2,00	5,00	3,00
	Paydaşlar ile Uyum	0,00	5,00	2,00	2,00	2,25
Organizasyon	Yeterlilik Düzeyi	0,00	5,00	0,00	2,00	1,75
	Eğitim	2,00	5,00	2,00	2,00	2,75
	Farkındalık	4,00	5,00	2,00	4,00	3,75
	Süreç Sahipliği	3,00	5,00	1,00	4,00	3,25
Altyapı ve Entegrasyon	Sektör Gelişimini Takip	2,00	5,00	2,00	4,00	3,25
	Süreçlerin Uyarlanabilmesi	1,00	5,00	3,00	2,00	2,75
	Şirket içi Sistem Entegrasyonları	1,00	5,00	3,00	3,00	3,00
	Bilgi Teknolojileri Güvenliği	3,00	4,00	4,00	5,00	4,00
	Paydaşlar ile Sistem Entegrasyonları	0,00	5,00	1,00	3,00	2,25
	Mobil Kullanımı	1,00	4,00	2,00	3,00	2,50
Dijital Sistemler ve İşleyiş	Depo Operasyonları	0,00	4,00	2,00	3,00	2,25
	Büyük Veri	0,00	3,00	1,00	3,00	1,75
	Akıllı Teknoloji Uygulamaları	0,00	2,00	1,00	3,00	1,50
	Dijital iş modelleri	2,00	5,00	2,00	3,00	3,00
	Yük Taşımacılığı Operasyonları	2,00	2,00	2,00	3,00	2,25
	Ürün Takip Edilebilirliği	3,00	5,00	1,00	3,00	3,00
Projeler ve İş Birlikleri	Şirket İçi Projeler Yapılması	3,00	5,00	2,00	3,00	3,25
	Devlet Teşviki	0,00	0,00	0,00	0,00	0,00
	Uluslararası Projelere Katılım	0,00	0,00	0,00	4,00	1,00
	Üniversite İş Birlikleri	0,00	0,00	0,00	0,00	0,00

$$M = \frac{\begin{array}{c}(0{,}16 * 3{,}25) + (12{,}95 * 3.75) + (8{,}24 * 2{,}50) + (10{,}51 * 3{,}00) + (5{,}06 * 2{,}25) + (2{,}99 * 1{,}75) + (3{,}83 * 2{,}75) + \\ (3{,}98 * 3{,}75) + (3{,}00 * 3{,}25) + (1{,}67 * 3{,}25) + (1{,}45 * 2{,}75) + (2{,}42 * 3{,}00) + (6{,}42 * 4{,}00) + (1{,}42 * 2{,}25) + \\ (0{,}76 * 2{,}50) + (0{,}66 * 2{,}25) + (0{,}76 * 1{,}75) + (0{,}94 * 1{,}50) + (4{,}81 * 3{,}00) + (0{,}97 * 2{,}25) + (3{,}24 * 3{,}00) + \\ (2{,}03 * 3{,}25) + (0 * 2{,}69) + (1 * 1{,}26) + (1{,}14 * 0)\end{array}}{1} \quad (4.1)$$

$$= 2{,}93$$

Denizcilik sektörünün dijital olgunluk seviyesi, AHP ile ağırlıklandırılmış olgunluk yaklaşımı ile değerlendirilmesi sonucunda 5 üzerinden 2,93 olarak ortaya çıkmıştır. Şekil 4.3'de denizcilik sektöründe ana kriterlerin dijital olgunluk düzeylerinin sonuçları verilmiştir.



Şekil 4.3 Denizcilik sektöründe ana kriterlerin dijital olgunlukları

Firmaların dijital olgunluk seviyeleri Tablo 4.11'de gösterilmiştir. Firma 2, 5 üzerinden 4,59 ile en üst seviyede dijital olgunluğa sahip olan firmadır.

Tablo 4.11 Firmaların dijital olgunlukları

Firmalar	Olgunluk Seviyeleri
Firma 1	1,59
Firma 2	4,59
Firma 3	1,83
Firma 4	3,70

4.2. Etkileyici Faktörlerle İlgili Siber Güvenlik Farkındalığı Modeli Uygulaması

Bu çalışmada, denizcilik sektörünün ve firmaların dijital olgunluk seviyesinin belirlenmesi için geliştirilen modelin yanında, geniş literatür araştırmaları sonucunda bulunan, siber güvenlik farkındalığını etkileyen 7 faktör (tutum, davranış, bilişsel (bilgi), derece, deneyim, finans ve cinsiyet) ile bir model daha geliştirilmiştir. Ek 3'te verilen 9 puanlık ölçekten oluşan ikili karşılaştırmalar ile, 4 farklı yöneticinin faktörlerin birbirlerine göre önem derecelerini belirlemeleri istenmiştir.

Puanlamalar sonucunda Microsoft Excel'de 7x7 boyutunda bir matris oluşturulmuştur. Olgunluk modelinin AHP ile analizi sırasındaki aşamaların aynısı uygulanmıştır. Değerler matrise işlendikten sonra normalize edilmiş, faktörlerin ağırlıkları belirlenmiştir. Tutarlılık analizi sonuçlarının 0,10 ve altında çıkması ile değerler kabul edilerek hesaplamalarda kullanılmıştır. Tablo 4.12'de tutarlılık analizi sonuçları verilmiştir.

Tablo 4.12 AHP 2. Model tutarlılık sonuçları

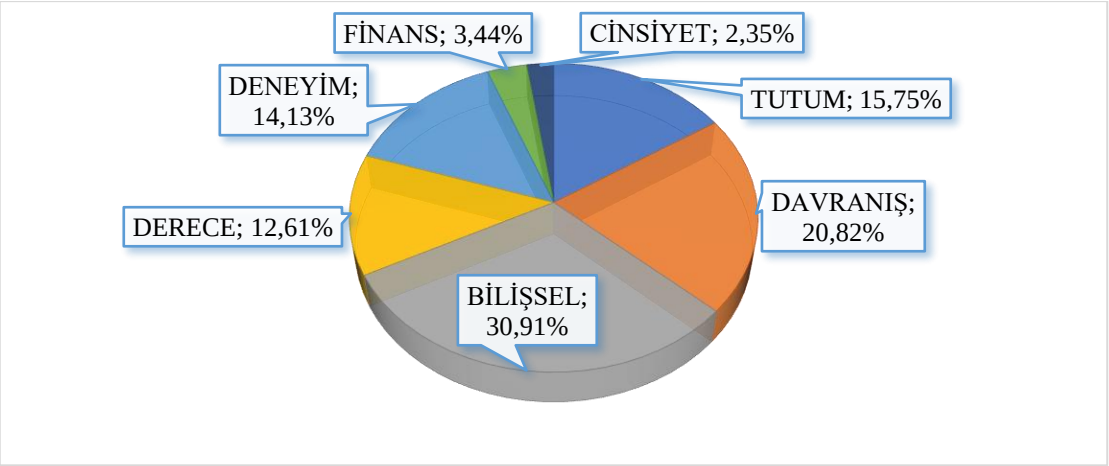
	Tutarlılık Oranı (CR)	Sonuç
Yönetici 1	0,10	Tutarlı
Yönetici 2	0,07	Tutarlı
Yönetici 3	0,10	Tutarlı
Yönetici 4	0,08	Tutarlı

4 yöneticinin verdiği cevapların geometrik ortalamaları alınarak yeni bir matris oluşturulmuş, AHP yöntemi ile de faktörlerin ağırlık puanları bulunmuştur. Tablo 4.13'de faktörlerin ağırlık hesaplamaları gösterilmiştir.

Tablo 4.13 Faktörlerin ağırlıklarının hesap tablosu

	TUTUM	DAVRANIŞ	BİLİŞSEL	DERECE	DENEYİM	FİNANS	CİNSİYET	NORMALİZE	SONUÇ
TUTUM	1,00	0,76	0,47	1,32	1,06	4,79	7,94	1,10	15,75%
DAVRANIŞ	1,32	1,00	0,76	1,73	1,73	5,79	7,94	1,46	20,82%
BİLİŞSEL	2,14	1,32	1,00	3,41	3,71	6,30	7,94	2,16	30,91%
DERECE	0,76	0,58	0,29	1,00	0,76	4,79	7,30	0,88	12,61%
DENEYİM	0,94	0,58	0,27	1,32	1,00	5,79	6,85	0,99	14,13%
FİNANS	0,21	0,17	0,16	0,20	0,17	1,00	1,73	0,24	3,44%
CİNSİYET	0,13	0,13	0,13	0,14	0,15	0,58	1,00	0,16	2,35%
SÜTUN TOPLAMI	6,49	4,53	3,07	9,11	8,58	29,03	40,69	7,00	100,00%

Şekil 4.4'te ise faktörlerin ağırlık sonuçları grafik üzerinde verilmiştir.



Şekil 4.4 Faktörlerin ağırlık sonuçları

Şekil 4.4 incelendiğinde siber güvenlik farkındalığını etkileyen önemli faktörün %30,91 ile bilişsel yani bilginin olduğu görülmektedir. Bilgiyi ise sırasıyla %20,82 ile davranış, %15,75 ile tutum, %14,13 ile deneyim, %12.61 ile derece, %3,44 ile finans ve %2,35 ile cinsiyet izlemektedir.

5. TARTIŞMA, SONUÇ VE ÖNERİLER

Denizcilik sektörünün dijital olgunluk seviyesinin ölçülmesi amacıyla oluşturulan model, sektörde uzun yıllar çalışmış 4 yöneticiye sunulmuş, sonuçlar AHP yöntemi ile değerlendirilerek en önemli ana kriterin %53,54 ile strateji ve yönetim olduğu bulunmuştur. Sektörün dijitalleşme yolunda ilk sırada bir strateji belirlemesi gerektiği ve bu stratejilerin doğru bir yönetim ile daha ileriye götürülebileceği bu sonuç ile ortaya çıkmaktadır.

AHP ile kriterlerin ağırlıklarının belirlenmesinin ardından, sektörün dijital olgunluk seviyesinin bulunabilmesi için AHP ile ağırlıklandırılmış olgunluk yaklaşımı kullanılmış, denizcilik sektörünün dijital olgunluk seviyesi en yüksek 5 seviye üzerinden 2,93 olarak bulunmuştur. Denizcilik sektörünün dijital dönüşüm konusunda deneyimli olduğu, genel olarak yönetim stratejilerinin tanımlandığı, yıllık belirli oranlarda dijitalleşme için bütçe ayrıldığı ve inovasyona yönelik iş birliklerinin yapıldığı söylenebilmektedir. Denizcilik sektörünün küresel pazarı güçlendirmedeki hayati konumu göz önüne alındığında, sektörün dijital ekosisteme adaptasyonu için dünya çapındaki diğer sektörlere göre daha da yol alması gerektiği görülmektedir.

Tablo 4.9'de genel ağırlıklar incelendiğinde en önemli ilk 3 alt kriterin sırası ile %16.78 ile strateji, %12.95 ile yatırım, %10.51 ile inovasyon yönetimi olduğu görülmektedir. Sektör dijitalleşme için strateji ve yönetim konusuna öncelik vermektedir. Son 3 kriter ise %0.66 ile depo operasyonları, %0.76 ile büyük veri, %0.94 ile akıllı teknoloji uygulamaları gelmektedir.

Şekil 4.3 incelendiğinde denizcilik sektörünün strateji ve yönetim ana kriteri açısından olgunluk düzeyinin 3,11, organizasyon açısından 2,93, altyapı ve entegrasyon açısından 3,36, dijital sistemler ve işleyiş açısından 2,68, projeler ve iş birlikleri açısından ise 1,10 olduğu görülmektedir. Firmalar bilgi teknolojilerinin güvenliği, şirket içerisinde kullanılan sistemlerin birbiri ile entegre olması, altyapının güncel gelişmeler ile birlikte sürekli yeni kalabilmesi konusunda genel olarak deneyim sahibi olmuşlardır. Sektör kamu kuruluşları, üniversiteler ile iş birliği konusunda ise başlangıç seviyesindedir. Dijitalleşmeye yönelik devlet teşviklerinin arttırılması, üniversitelerin dijital dönüşüm ile ilgili firmalar ile projeler yapması, firmaların gelişimi açısından önemli olacaktır.

Firma 1, 1.59 olgunluk puanı ile 4 firma arasında son sırada gelmektedir. Firmanın dijitalleşme konusunda daha başlangıç aşamasında olduğu söylenebilmektedir. Strateji geliştirilip yol haritası oluşturmalıdır. İnovasyona yönelik iş birliklerini arttırmalı, bilgi

teknolojileri konusunda çalışanlarına düzenli olarak eğitim vermelidir. Akıllı teknoloji ürünlerin kullanımını sağlayıp, kullanılan yazılımların şirket içi entegrasyonlarını oluşturmalıdırlar.

Firma 2, 4.59 olgunluk puanı ile dijitalleşme konusunda uzmanlaşmış, en iyi performans gösteren olma yolunda emin adımlarla ilerlemektedir. Deniz taşımacılığı alanında uluslararası düzeyde faaliyet gösterdiklerinden, dijital yenilikleri bünyelerinde uygulamaya devam etmelidirler. Akıllı teknoloji uygulamalarının şirket içerisinde daha da yaygın kullanılmasıyla daha da ileri seviye gidebilecek durumdadırlar.

Firma 3, 1.83 olgunluk puanı ile dijital dönüşüme başlamış, ortalama bir seviyeye gelmişlerdir. Sektörel gelişimleri daha fazla takip etmeli, dijitalleşme stratejilerinin geliştirme aşamalarını bitirmeleri gerekmektedir. Şirket çalışanlarının dijitalleşme konusunda eğitimlerine önem vermeli, iş süreçlerinin müşteri isteklerine göre uyarlanabilmesi için yol arayışlarına girmelidirler.

Firma 4, 3.70 olgunluk puanı ile sektör ortalamasının üzerinde yer alarak, dijitalleşme konusunda deneyim sahibi konumundadır. Dijitalleşmeye yönelik stratejik partner sayısını arttırarak, stratejik aksiyonlarının paydaşlar ile uyum içinde yayılım gösterilmesi için çaba sarf etmelidirler. Şirket içi projelerin sayısının arttırmalıdırlar ve dijital iş modellerinin uygulanabilirliği için yol haritası belirlemelidirler.

Çalışmanın devamında ise, etkili faktörlerin (tutum, davranış, bilişsel, derece, deneyim, finans ve cinsiyet) ağırlıklarını elde etmek için AHP karar verme tekniği kullanıldıktan sonra, önerilen siber güvenlik farkındalık modeli oluşturulmuştur. Analiz sonucunda bilişsel faktörün ağırlığının %30.91 olması nedeniyle en yüksek etkiye sahip olduğu görülmektedir. Davranış, tutum, deneyim, derece, finans ve cinsiyet için ağırlıklar Şekil 4.4'te gösterildiği gibi sırasıyla %20.82, %15.75, %14.13, %12.61, %3,44, %2,35'tir. Çalışma sonucunda, denizcilik sektöründe çalışan personellerin siber güvenlik farkındalığı üzerinde en etkili faktörün bilişsel (bilgi) olduğu ortaya çıkmaktadır. Bu nedenle, denizcilik sektöründe faaliyet gösteren firmaların, çalışanlarının siber güvenlik farkındalık düzeyini artırmak için siber güvenlik konuları ile ilgili eğitimine öncelik vermelidirler.

İşletmeler, Endüstri 4.0'ın tüm alanlarında olgunluk seviyelerini değerlendirmek için zaman ayırmalıdırlar. Böylece hangi güçlü yönlerini geliştirebileceklerini ve gelecekteki çözümlere hangi sistemleri, süreçleri entegre etmeleri gerekebileceğini anlayabilirler. Önerilen olgunluk modeli bu süreci hızlandırmaya yardımcı olabilecek bir araçtır. Modelin amacı, denizcilik sektöründeki şirketlerin süreçlerini değerlendirerek

dijital dönüşüme ne kadar hazır olduklarını anlamalarına yardımcı olmak olsa da dönüşüm yol haritalarını geliştirmelerine de yardımcı olduğunun altını çizmek gerekmektedir. Bu nedenle olgunluk değerlendirmesi genel bir yaklaşımın yalnızca ilk adımı olarak görülmelidir.

Dijital teknolojiler iş yapma şekillerinin geleceğini yeniden yapılandıracaktır. İşletmelerin ve müşterilerin değişen ihtiyaçlarına en iyi şekilde cevap verebilmek için bilgi ve iletişim alanındaki modern teknolojilerin sunduğu fırsatların değerlendirilmesi gerekmektedir. Dijital teknolojilerin desteğiyle iş süreçlerinin dönüştürülmesinin yanı sıra, daha etkili organizasyonlar oluşacak, müşterilere daha etkin hizmet verilebilecek ve şirketler büyüme hedeflerine daha hızlı ulaşabileceklerdir. Ayrıca, dünyanın artan entegrasyonu ve dijital dönüşüm, teknoloji ve iş dünyası için hayal bile edilemeyecek bir potansiyel yaratmaktadır. Bu nedenle dijital dönüşüm en alt seviyede olsa bile, zayıf ve güçlü yönlerin tanımlanması tüm şirketler için çok önemli bir konudur.

Dijital dönüşümün gerçekleşebilmesi için yönetimin, öncelikli olarak Endüstri 4.0'ı üst düzey yöneticilerinin gündeminin merkezine yerleştirmesi ve onu birinci öncelik haline getirmesi gerekmektedir. Şirketlerin süreçleri, münferit sistemler arasında bilgi paylaşımını kademeli olarak genişletecek şekilde uyarlanmalıdır. Hem standartlaştırılmış ara yüzlere hem de uygun ara yazılımların kullanımına odaklanılmalıdır. Endüstri 4.0'a giden yolda ilerlemeye başlamadan önce şirket içinde bilgi teknolojileri altyapısı, otomasyon teknolojisi ve veri analitiği konularında temel becerilerin oluşturulması kritik önem taşımaktadır. Şirket hangi spesifik becerilerin gerekli olduğunu belirlemek için genellikle önce kendi yaklaşımını tanımlamalıdır. Şirketler öncelikle çalışanlarının neye ihtiyaç duyduğuna dair sistematik bir değerlendirme yapmalı, ardından eğitim ve mesleki gelişim programlarını bu ihtiyaçlara göre uyarlamalıdır. Finansal engellerin aşılması için yatırım dostu koşullar yaratılmalıdır. Devlet, Endüstri 4.0 için hedefe yönelik teşvik programları oluşturabilir. Şirketler, müşteri ihtiyaçlarına göre uyarlanmış veri odaklı hizmetlerin kapsamını genişletmeli ve iş modellerini buna göre uyarlamalıdır. Bu da müşteriyle entegrasyonu gerektirmektedir. Departmanların, iyileştirmeleri teşvik etmek için şirketler arası iş birliğine açık olması gerekecektir. İşletmeler stratejiyi eyleme dönüştürmek için doğru dijital bilgi ve becerilere sahip çalışanlara ihtiyaç duyacaktır ve becerilere yatırım gündemin bir parçası olmalıdır. İşletmelerin Endüstri 4.0'ın faydalarını görmeyi bekledikleri açıktır, bu nedenle yatırımın geri dönüşünün yanı sıra dönüşümün etkinliğini izlemek için uygun ölçümlerin yapılmasını sağlamak önemlidir. İşletmeler, Endüstri 4.0 kavramını işletme fonksiyonları ve seviyeleri arasında yerleştirmeli, daha iyi

benimseme ve finansal getiri sağlamak için dahili KPI'lar ve çapraz fonksiyonel iş birliklerinin tutarlı olmasını sağlamalıdır.

Şirketler, denizcilik alanındaki dijital trendle yüzleşirken, deneme, yenilik yapma ve iyileştirme cesaretine sahip olmalıdırlar. Denizcilik sektörü Endüstri 4.0 fırsatını değerlendirmeli ve dijital havacılık gibi dijital çağdaki diğer sektörlerin dijital dönüşüm deneyimlerinden ders çıkaracak kadar cesur olmalıdır. Özetle, dijitalleşme ve dijital teknoloji denizcilik alanında büyük etkiye ve uygulama olanaklarına sahiptir. Denizcilik alanının gelişmesine ve yeni ufuklar açmasına yardımcı olacaktır.

Öte yandan, dijital güvenlik denizcilik sektöründeki temel zorluk olarak görünmektedir. Son zamanlarda denizcilik sektöründe siber güvenliğin yeni bir konu olarak ortaya çıkmasıyla birlikte artan sayıda çalışma yapılmaktadır. Bu da doğal olarak meselenin henüz ele alınmayı bekleyen pek çok yönünün olduğunu ortaya koymaktadır.

Denizcilik sektörünün gelecekteki siber destekli çözümlere ve otonom gemilere yönelik yönelimi, firmaların endüstrinin en yeni siber güvenlik gereklilikleri ve kuralları konusunda güncel kalmasını gerektirmektedir. Yeni ürünlerin başarılı bir şekilde pazara sunulabilmesi için bu gerekliliklerin yerine getirilmesi ve bunun müşterilere ve diğer paydaşlara gösterilmesi gerekmektedir.

Denizcilik sektöründeki pek çok çalışan, siber güvenlikle ilgili en iyi uygulamalar konusunda yeterli farkındalık ve eğitimden yoksundur. Bu, şirketi ve gemileri siber risklere maruz bırakacak kasıtsız eylemlere yol açabilir. Pek çok şirket, siber olaylara etkili bir şekilde müdahale etmek için kapsamlı acil durum planlarına ve prosedürlerine sahip değildir. Bu, tehditlerin tanımlanmasında ve kontrol altına alınmasında gecikmelere yol açarak zararların artmasına neden olabilir. Bu bulgulara dayanarak denizcilik kuruluşlarının siber güvenliğe yatırımlarını artırmaları, eğitim ve farkındalık programlarını geliştirmeleri, iş birliği ve bilgi paylaşımını geliştirmeleri gerekmektedir. Denizcilik sektörü, bu kilit alanları ele alarak siber güvenlik duruşunu geliştirebilir ve siber olaylarla ilişkili riskleri azaltabilir.

Bu çalışma, denizcilik şirketlerinin çalışanlar arasında siber güvenlik farkındalığını artırmanın önemini anlamalarına yardımcı olabilir ve denizcilik sektörünün siber olaylara karşı direncini artırmak için daha fazla araştırma ve yeniliği teşvik edebilir. Anket sonuçlarına göre denizcilerin siber güvenlik farkındalığını etkileyen en önemli faktörün konusunda bilgi olduğu göz önünde bulundurulduğunda, özellikle potansiyel siber tehditlerin belirlenmesi ve bunlara müdahale edilmesi konusunda daha fazla eğitim ve öğretime ihtiyaç duyulmaktadır. Denizcilik kuruluşları, farkındalığı artırarak, iş

birliğini teşvik ederek, risk değerlendirme ve azaltma stratejilerini uygulayarak, teknolojiden yararlanarak ve gelişen tehdit ortamı hakkında bilgi sahibi olarak siber tehditlere karşı dayanıklılıklarını önemli ölçüde artırabilir. İnsanlar siber güvenlik konusundaki güvenlik açıkları hakkında önceden bilgi sahibi olursa, kendilerini savunmanın yollarını bulacaklardır. Bununla birlikte denizcilik paydaşlarının sektörün dijitalleşmesini ve otomasyonunu bir fırsat olarak görmesi gerekmektedir. Siber güvenlik esnekliği, dijital sevkiyatın avantajlarını güvenli bir şekilde gerçekleştirmenin ve operasyonları daha iyi yapmanın anahtarıdır. Çoğu şirket uzaktan çalışmayı, operasyon maliyetlerini azaltmayı, performansı optimize etmeyi, daha iyi bir lojistik zincirinden yararlanmayı, bakımı azaltmayı ve daha iyi ve daha verimli hizmetler sağlamanın yollarını aramaktadır. Dijital evrime direnen şirketler rekabetin gerisinde kalacaktır. Bunu benimseyenler ise rekabet avantajı elde edebilecektir.

Denizcilik sektöründe, taşımacılık işletmeleri, tersaneler ve liman paydaşları dijital dönüşüm yolculuğunun farklı aşamalarındadır. Yüksek oranda dijitalleşen işletmeler olduğu gibi, bazı firmalar da geride kalmaktadır. Bu çalışma ile denizcilik sektöründeki dijitalleşme, dijital dönüşüm ve siber güvenlik farkındalığı alanındaki bilgi birikimi zenginleştirilerek literatüre katkı sağlanmaktadır.

Günümüz denizcilik endüstrisinin Endüstri 4.0'ın ulaşmayı hedeflediği son derece dijitalleşmiş endüstriyel paradigmaya geçiş yapmakta olduğu görülmektedir. Bununla birlikte, denizcilik sektöründe Endüstri 4.0 üzerine artan araştırmalara rağmen, Denizcilik 4.0 kapsamlı araştırma gerektiren az gelişmiş bir konuyu temsil etmektedir. Özellikle, sektöre yönelik dijital olgunluk modellerinin geliştirilmesi yetersiz kalmaktadır. Gelecekteki çalışmalar için, bu çalışmayla karşılaştırmak amacıyla sonuçların tutarlılığını kontrol etmek için diğer sektörlerde veya endüstrilerde de benzer bir çalışma yapılabilir. Farklı çok kriterli karar verme yöntemleri kullanılarak değerlendirme yapılabilir. Yeni model oluşturularak, örneklem sayısı arttırılabilir. Ayrıca, benzer bir çalışmanın farklı kültürlere sahip diğer ülkelerde de yapılması düşünülmelidir.

6. KAYNAKLAR

Accenture Dijitalleşme Endeksi Türkiye Sonuçları (2015). *Türkiye'nin En Dijital Şirketleri.* http://www.tbv.org.tr/core/uploads/page/document/1100_18031611540.pdf

Adebiaye, R., & Ajani, T. (2018). Information technology usage: quantitative analysis of smartphone security awareness and practices among undergraduate students in the United States. *Int J Eng Tech Mgmt Res*, *5*(3), 270-84.

Agca, O., Gibson, J., Godsell, J., Ignatius, J., Wyn Davies, C., & Xu, O. (2017). An Industry 4 Readiness Assessment Tool. *International Institute for Product and Service Innovation*, 1–19.

Ahmed, N., Islam, M. R., Kulsum, U., Islam, M. R., Haque, M. E., & Rahman, M. S. (2019). Demographic factors of cybersecurity awareness in Bangladesh. *In 2019 5th International Conference on Advances in Electrical Engineering (ICAEE)* (pp. 685-690). IEEE.

Agustini, I., & Kencana Sari, P. (2016). Measurement of information security awareness among social media path users in Indonesia. *Asia Pacific Journal of Contemporary Education and Communication Technology*, *2*(2), 114-123.

Akyuz, E., Cicek, K., & Celik, M. (2019). A comparative research of machine learning impact to future of maritime transportation. *Procedia Computer Science*, *158*, 275-280.

Aljohani, W., & Elfadil, N. (2020). Measuring cyber security awareness of students: A case study at Fahad Bin Sultan University. *International Journal of Computer Science and Mobile Computing*, *9*(6), 141-155.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Atkeson, A., & Kehoe, P. J. (2001). The transition to a new economy after the second industrial revolution. *National Bureau of Economic Research Cambridge: Cambridge, MA*, USA.

Back, A., & Berghaus, S. (2016). Digital maturity & transformation studie: über das digital maturity model. *Universität St Gallen*, *2*, 1-19.

Baltacı, İ. (2020). *Lojistik sektöründe djital olgunluk seviyesinin ölçülmesi ve bir uygulama.* (Yüksek lisans tezi). Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Banalieva, E. R., & Dhanaraj, C. (2019). Internalization theory for the digital economy. *Journal of International Business Studies*, *50*(8), 1372–1387. https://doi.org/10.1057/s41267-019-00243-7

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), 22.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly*, *37*(2), 471–482. https://doi.org/10.25300/MISQ/2013/37:2.3

BIMCO. (2016). The guidelines on cyber security onboard ships. https://www.bimco.org/About-us-and-our-members/Publications/The-Guidelines-on-Cyber-Security-Onboard-Ships

Bloomberg, J. (2018). Digitization, Digitalization, And Digital Transformation: Confuse Them At Your Peril. *Forbes*, 1–6. https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization56 digitalization-and-digital-transformation-confuse-them-at-yourperil/# 78e677fd2f2c

Bolat, P., & Kayişoğlu, G. (2019). Antecedents and consequences of cybersecurity awareness: a case study for Turkish maritime sector. *Journal of ETA Maritime Science*, *7*(4).

Boyes, H., & Isbell, R. (2017). Code of practice: Cyber security for ships. Institution of Engineering and Technology.

Boyes, H., Isbell, R., & Luck, A. (2016). Code of practice: Cyber security for ports and port systems. Institution of Engineering and Technology, 28, 2016.

Bucak, U., Dinçer, M. F., & Demirel, H. (2019). Evaluation of the maritime 4.0 using the AHP method. In *Global Conference on Innovation in Marine Technology and the Future of Maritime Transportation* (pp. 123-137).

Cai, Z., Liu, L., Cai, J., & Chen, B. (2016). *Artificial Intelligence* : *Principles & Applications (5th ed.).* Beijing: Qinghua University Press.

Chang, J. (2020). *Research on the application of big data in ship navigation safety assessment*. (Unpublished master's thesis) Dalian Maritime University, Dalian, China.

Chesbrough, H. (2010). Business Model Innovation: Opportunities and Barriers. *Long Range Planning*, *43*(2), 354–363. https://doi.org/10.1016/j.lrp.2009.07.010

Cil, I., Arisoy, F., Kilinc, H., & Cil, A. Y. (2022). A comparative analysis of indoor positioning technologies in shipyard digitalization context. *J Mar Technol Environ*, *1*, 15-25.

Cil, I., Arisoy, F., & Kilinc, H. (2021). An analysis on industrial internet of things in digital transformation of shipyard industry in Turkey. *Global Journal of Computer Sciences: Theory and Research*, *11*(2), 67-87.

Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A., & Hellebooge, L. (2011). Analysis of cyber security aspects in the maritime sector.

Cimpanu, C. (2021). All four of the world's largest shipping companies have now been hit by cyber-attacks | ZDNet. https://www.zdnet.com/article/allfour-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, 1-24.

Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021). A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 102-106). IEEE.

De Carolis, A., Macchi, M., Negri, E., Terzi, S. (2017). A Maturity Model for Assessing the Digital Readiness of Manufacturing Companies. In Proceedings of the IFIP

International Conference on Advances in Production Management Systems, (s. 13- 20). Hamburg, Germany.

Dehning, B., Richardson, V. J., & Zmud, R. W. (2003). The value relevance of announcements of transformational information technology investments. *MIS quarterly*, 637-656. https://doi.org/10.2307/30036551

De Kok, L. C., Oosting, D., & Spruit, M. (2020). The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security*, *46*(3), 251-266.

Dong, F., & Liu, Z. (2010). Digital navigation. Dalian: Dalian Maritime University press.

Du, J., & Pang, X. (2015). Digital port and shipping construction and development. Beijing: Science Press.

Dutta, S., & Lanvin, B. (2019). The network readiness index 2019. *Washington: Portulans Institute*.

Ellingsen, O., & Aasland, K. E. (2019). Digitalizing the maritime industry: A case study of technology acquisition and enabling advanced manufacturing technology. *Journal of Engineering and Technology Management*, *54*, 12-27.

Emad, G., Enshaei, H., & Ghosh, S. (2021). Identifying seafarer training needs for operating future autonomous ships: a systematic literature review. *Aus. J. Marit. Ocean Aff.* 1–22. https://doi.org/10.1080/18366503.2021.1941725

Eremina, Y., Lace, N., & Bistrova, J. (2019). Digital maturity and corporate performance: The case of the Baltic states. *Journal of open innovation: technology, market, and complexity*, *5*(3), 54.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012098). IOP Publishing.

Feibert, D. C., Hansen, M. S., & Jacobsen, P. (2018). An integrated process and digitalization perspective on the shipping supply chain. A literature review. *IEEE International Conference on Industrial Engineering and Engineering Management*, *2017-Decem*, 1352–1356. https://doi.org/10.1109/IEEM.2017.8290113

Gavalas, D., Syriopoulos, T., & Roumpis, E. (2022). Digital adoption and efficiency in the maritime industry. *Journal of Shipping and Trade*, *7*(1), 11.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *Int. J. Emerg. Technol*, *11*(5), 41-49.

Geissbauer, R., Vedso, V., Schrauf, S. (2016). Industry 4.0: Building the Digital Enterprise; Munich, Germany: PriceWaterhouseCoopers. https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

González-Cancelas, N., Molina Serrano, B., Soler-Flores, F., & Camarero-Orive, A. (2020). Using the SWOT Methodology to Know the Scope of the Digitalization of the Spanish Ports. *Logistics*, *4*(3), 20.

Gökalp, E., & Martinez, V. (2021). Digital transformation capability maturity model enabling the assessment of industrial manufacturers. *Computers in Industry*, *132*, 103522.

Grzelakowski, A. S. (2019). Global container shipping market development and its impact on mega logistics system. *TransNav*, *13*(3), 529–535. https://doi.org/10.12716/1001.13.03.06

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired, August*, *22*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russiacode-crashed-the-world/

Gu, Y., Goez, J. C., Guajardo, M., & Wallace, S. W. (2021). Autonomous vessels: state of the art and potential opportunities in logistics. *Int. Trans. Op. Res. 28*(4), 1706–1739. https://doi.org/10.1111/itor.12785

Guo, N., & Jia, C. (2017). Survey on Research and Application of Cyber-Physical Systems at Home and Abroad. *Information Technology and Standardization, 06*, 47-50.

Heilig, L., Lalla-Ruiz, E., & Voß, S. (2017). Digital transformation in maritime ports: analysis and a game theoretic framework. *Netnomics: Economic research and electronic networking*, *18*(2), 227-254. https://doi.org/10.1007/s11066-017-9122-x

https://www.uab.gov.tr (Erişim tarihi: 02.04.2024)

https://www.kiyiemniyeti.gov.tr/hakkimizda (Erişim tarihi: 02.04.2024)

https://denizcilik.uab.gov.tr/gorevler (Erişim tarihi: 02.04.2024)

https://tkygm.uab.gov.tr/gorevler (Erişim tarihi: 02.04.2024)

https://manavgatliman.uab.gov.tr/baskanligin-gorev-ve-yetkileri (Erişim tarihi: 02.04.2024)

IMEAK Maritime Sector Report (2023). İstanbul ve Marmara, Ege, Akdeniz, Karadeniz Bölgeleri Ticaret Odası Denizcilik Sektörü Raporu. https://www.denizticaretodasi.org.tr/media/SharedDocuments/sektorraporu/2023/Denizcilik_Sektor_Raporu_12.06.2023_v2.pdf

IMO. (2017). Guidelines on Maritime Cyber Risk Management. Maritime Cyber Risk, International Maritime Organization. (2017). https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

Kaltenbach, F., Marber, P., Gosemann, C., Bölts, T., & Kühn, A. (2018). Smart services maturity level in Germany. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1-7). IEEE.

Kamaruzaman, M., Hamid, R., Mutalib, A., & Rasul, M. (2019). Comparison of engineering skills with IR 4.0 skills.

Kate, P. T. (2021). Cyberattacks more than double since COVID-19. *PwC Thailand says*. https://www.pwc.com/th/en/press-room/press-release/2021/press-release-18-08-21-en.html

Kaufman, B. E. (2020). Employee voice before Hirschman: its early history, conceptualization and practice. In *Handbook of research on employee voice* (pp. 19-37). Edward Elgar Publishing.

Khanbhai, M., Flott, K., Darzi, A., & Mayer, E. (2019). Evaluating digital maturity and patient acceptability of real-time patient experience feedback systems: systematic review. *Journal of medical Internet research*, *21*(1), e9076.

Klein, M., & Spychalska-Wojtkiewicz, M. (2023). Digitalization of small ports as a step in achieving sustainable goals. *Procedia Computer Science*, *225*, 3381-3387.

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, *8*, 125140-125148.

Kutnjak, A., Pihir, I., & Furjan, M. T. (2020). Assessing Digital Transformation Readiness Using Digital Maturity Indices. In *Central European Conference on Information and Intelligent Systems* (pp. 307-314). Faculty of Organization and Informatics Varazdin.

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee's behavior. In *Research and Practical Issues of Enterprise Information Systems: 10th IFIP WG 8.9 Working Conference, CONFENIS 2016, Vienna, Austria, December 13–14, 2016, Proceedings 10* (pp. 103-111). Springer International Publishing.

Li, H., Wei, M., Huang, J., Qiu, B., Zhao, Y., Luo, W., He, X. (2019). Overview of Cyber-Physical System Technology. *Acta Automatica Sinica, 45*(01), 37-50.

Lehto, M., & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. Informaatioteknologian tiedekunnan julkaisuja, (20/2015).

Lei, L. (2020). The application and legal regulation of blockchain in the shipping field. *J. China Ocean Shipping*, *12*, 78-80.

Leyh, C., Bley, K., Schäffer, T., & Forstenhäusler, S. (2016). SIMMI 4.0-a maturity model for classifying the enterprise-wide it and software landscape focusing on Industry 4.0. In *2016 federated conference on computer science and information systems (fedcsis)* (pp. 1297-1302). IEEE.

Lichtblau, K., Stich, V., Bertenrath, R., Blum, M., Bleider, M., Millack, A., & Schröter, M. (2015). Industrie 4.0-Readiness.

Lind, M., Watson, R. T., Ward, R., Bergmann, M., Bjorn-Andersen, N., Rosemann, M., & Andersen, T. (2018). Digital data sharing: The ignored opportunity for making global maritime transport chains more efficient. *Unctad Transport and Trade Facilitation Newsletter*.

Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & information systems engineering*, *57*, 339-343. https://doi.org/10.1007/s12599-015-0401-5

Marques, G., Gourc, D., & Lauras, M. (2011). Multi-criteria performance analysis for decision making in project management. *International Journal of Project Management*, *29*(8), 1057-1069.

Maydanova, S., & Ilin, I. (2019). Strategic approach to global company digital transformation. In *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020* (pp. 8818-8833).

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, *21*.

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents.

Menchini, F., Russo, P. T., Slavov, T. N. B., & Souza, R. P. (2021). Strategic capabilities for business model digitalization. *Revista de Gestão*, *29*(1), 2-16.

Mi, W., & Liu, Y. (2022). Smart port and digital monitoring and diagnosis. In *Smart Ports* (pp. 171-188). Singapore: Springer Singapore.

Mittal, S., Romero, D., & Wuest, T. (2018). Towards a smart manufacturing maturity model for SMEs (SM 3 E). In *Advances in Production Management Systems. Smart Manufacturing for Industry 4.0: IFIP WG 5.7 International Conference, APMS 2018, Seoul, Korea, August 26-30, 2018, Proceedings, Part II* (pp. 155-163). Springer International Publishing.

Mohd Salleh, N. H., Selvaduray, M., Jeevan, J., Ngah, A. H., & Zailani, S. (2021). Adaptation of industrial revolution 4.0 in a seaport system. *Sustainability*, *13*(19), 10667.

Muhammad, B., Kumar, A., Cianca, E., & Lindgren, P. (2018). Improving Port Operations through the Application of Robotics and Automation within the Framework of Shipping 4.0. *2018 21st International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 387–392. https://doi.org/10.1109/WPMC.2018.8712998

Muhirwe, J., & White, N. (2016). Cyberscurity Awareness and Practice of Next Generation Corperate Technology Users. *Issues in Information Systems,* 17(2).

Munim, Z. H. (2019). Autonomous ships: a review, innovative applications and future maritime business models. In *Supply Chain Forum: An International Journal* (Vol. 20, No. 4, pp. 266-279). Taylor & Francis.

Munín-Doce, A., Díaz-Casás, V., Trueba, P., Ferreno-González, S., & Vilar-Montesinos, M. (2020). Industrial Internet of Things in the production environment of a Shipyard 4.0. *The International Journal of Advanced Manufacturing Technology*, *108*(1), 47-59.

Nerima, M., & Ralyté, J. (2021). Towards a digital maturity balance model for public organizations. In *International Conference on Research Challenges in Information Science* (pp. 295-310). Cham: Springer International Publishing.

Nikitakos, N., & Thoetokas, I. (2001). Network Centric Organisations in Shipping'. *Management Sciences and Regional Development (MSRD)*, (3), 183-96.

Nwankpa, J. K., & Datta, P. (2017). Balancing exploration and exploitation of IT resources: The influence of Digital Business Intensity on perceived organizational performance. *European Journal of Information Systems*, *26*, 469-488.

Pacchini, A. P. T., Lucato, W. C., Facchini, F., & Mummolo, G. (2019). The degree of readiness for the implementation of Industry 4.0. *Computers in industry*, *113*, 103125.

Paulauskas, V., Philipp, R. (2020). Connect2SmallPorts within the frame of the South Baltic Programme. *Digital Auditing Benchmarking.* South Baltic Sea Region: Europe.

Peura, R. (2017). Maritime Cybersecurity and Improvement of Project Execution Process (Master's thesis). Automation Technology Programme. Tampere University of Technology, Tampere, Finland.

Philipp, R. (2020). Digital readiness index assessment towards smart port development. In *Sustainability Management Forum| NachhaltigkeitsManagementForum* (Vol. 28, No. 1, pp. 49-60). Berlin/Heidelberg: Springer Berlin Heidelberg.

Putra, I. N., Octavian, A., Heikhmakhtiar, A. K., Tjahjadi, H., & Susilo, A. K. (2023). Cyber Threat Analysis of Maritime Cybersecurity Using AHP-Topsis. *Journal of Maritime Research*, *20*(2), 13-24.

Qi, J. (2021). The review of implication and development of digital technologies in maritime sector. (Master's thesis). Marıtıme safety and envıronmental management. World Maritime University, Malmö, Sweden.

Qureshi, A.H., Alaloul, W.S., Manzoor, B., Musarat, M.A., Saad, S.A., & Ammad, S. (2020). Implications of Machine Learning Integrated Technologies for Construction Progress Detection Under Industry 4.0 (IR 4.0). *2020 Second International Sustainability and Resilience Conference: Technology and Innovation in Building Designs (51154)*, 1-6.

Rakoma, S. K. (2021). A review of digital maturity models for shipping companies. (Master's thesis). World Maritime University. Malmö, Sweden.

Ren, J. (2021). On maritime management in the era of big data. *Navigation, 3*, 56-58

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston consulting group*, *9*(1), 54-89.

Saaty, T. L. (1994). How to make a decision: the analytic hierarchy process. *Interfaces*, *24*(6), 19-43.

Saaty, T.L. (1980) "The Analytic Hierarchy Process", McGraw-Hill, New York.

Sadik, M., Akkari, N., & Aldabbagh, G. (2018). QoS/QoE based handover decision in Multi-Tier LTE networks. *International Journal of Digital Information and Wireless Communications (IJDIWC)*, *8*(2), 133-138.

Salah, B. (2021). Real-time implementation of a fully automated industrial system based on ir 4.0 concept. In *Actuators* (Vol. 10, No. 12, p. 318). MDPI.

Salviotti, G., Gaur, A., & Pennarola, F. (2019). Strategic factors enabling digital maturity: An extended survey.

Sanchez-Gonzalez, P. L., Díaz-Gutiérrez, D., Leo, T. J., & Núñez-Rivas, L. R. (2019). Toward digitalization of maritime transport? *Sensors*, *19*(4), 926. https://doi.org/10.3390/s19040926

Sanders, A., Elangeswaran, C., & Wulfsberg, J. P. (2016). Industry 4.0 implies lean manufacturing: Research activities in industry 4.0 function as enablers for lean manufacturing. *Journal of Industrial Engineering and Management (JIEM)*, *9*(3), 811-833.

Schallmo, D. R., Lang, K., Hasler, D., Ehmig-Klassen, K., & Williams, C. A. (2021). An approach for a digital maturity model for SMEs based on their requirements. In *Digitalization: Approaches, case studies, and tools for strategy, transformation and implementation* (pp. 87-101). Cham: Springer International Publishing.

Schuh, G., Anderl, R., Gausemeier, J., ten Hompel, M., & Wahlster, W. (2017). Industrie 4.0 maturity index. *Managing the digital transformation of companies*, *61*.

Schumacher, A., Erol, S., & Sihn, W. (2016). A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises. *Procedia Cirp*, 52, 161-166.

Serdar, D. (2019). *İşletmelerin sanayi 4.0 olgunluk düzeylerinin belirlenmesine yönelik çok kriterli bir yaklaşım: Lojistik sektörü uygulaması*. (Yüksek lisans tezi). KATÜ, Sosyal Bilimler Enstitüsü, Trabzon.

Song, Q. (2020). Application and thinking of blockchain technology in the maritime field. *China Maritime, 10*, 53-55.

Sørensen, R. (2023). How to Improve the Cyber Security Awareness in The Shipping Industry. (Master's thesis). Maritime Management Program. Satakunta University, Pori, Finland.

Stocker, F., Villar, E. G., Roglio, K. D. D., & Abib, G. (2018). Dismissal: Important criteria in managerial decision-making. *Revista de Administração de Empresas*, *58*, 116-129.

Struck, E. L. (2020). *Digital transformation in the shipping industry: how Industry 4.0 is shaping the shipping industry?* (Doctoral dissertation). Universidade Católica Portuguesa.

Ştefănescu, D. C., & Papoi, A. (2020). New threats to the national security of states–cyber threat. *Zeszyty Naukowe. Transport/Politechnika Śląska*, (107).

Taalbi, J. (2019). Origins and pathways of innovation in the third industrial revolution. *Industrial and corporate change*, *28*(5), 1125-1148.

Teichert, R. (2019). Digital transformation maturity: A systematic review of literature. *Acta universitatis agriculturae et silviculturae mendelianae brunensis*.

Tijan, E., Jović, M., Aksentijević, S., & Pucihar, A. (2021). Digital transformation in the maritime transport sector. *Technological Forecasting and Social Change*, *170*, 120879.

Trent, A. (2023). Compliance analysis for cyber security marine standards.

UNCTAD. (2019). Digitalization in Maritime Transport: Ensuring Opportunities for Development. *UNCTAD Policy Brief No. 75 (UNCTAD/PRESS/PB/2019/4)*.

UNCTAD. (2022). Review of Maritime Transport 2021. United Nations.

Ungkap, P., & Daengsi, T. (2022). Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand. In *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 1359-1362). IEEE.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". *Heliyon*, *5*(12).

Weber, C., Königsberger, J., Kassner, L., & Mitschang, B. (2017). M2DDM–a maturity model for data-driven manufacturing. *Procedia Cirp*, *63*, 173-178.

Westerman, G., Calméjane, C., Bonnet, D., Ferraris, P., & McAfee, A. (2011). Digital Transformation: A roadmap for billion-dollar organizations. *MIT Center for Digital Business and Capgemini Consulting*, *1*, 1–68.

World Bank. (2020). *Accelerating Digitalization: Critical Actions to Strengthen the Resilience of the Maritime Supply Chain*. World Bank.

Wu, Y. (2020). Navigation industry development in the era of big data. *Electronic world*, *03*, 48-49.

Yorulmaz, M. & Derici, M. (2023). Akıllı Limanlar ve Türkiye'deki Limanların Dijital Teknoloji Uygulamaları. *Asya Studies-Academic Social Studies / Akademik Sosyal Araştırmalar*, 7(26), 291-308.

Yüksel, G. (2019). Antecedents and consequences of cyber security awareness: A case study for maritime sector (Master's thesis). Fen Bilimleri Enstitüsü, İTÜ, İstanbul.

Zaman, I., Pazouki, K., Norman, R., Younessi, S., & Coleman, S. (2017). Challenges and opportunities of big data analytics for upcoming regulations and future transformation of the shipping industry. *Proc. Eng. 194*, 537–544. https://doi.org/10.1016/j.proeng.2017.08.182

Zhen, H. (2017). Thoughts on China's Shipping Development Strategy under the Influence of the Third Industrial Revolution. *China Navigation, 40*(01), 119-123+128.

Zhong, W. (2018). The application prospects of artificial intelligence in maritime management. *China Water Transport, 12*, 19-20.

Zou, J. (2020). Research on the development of shipping industry based on blockchain technology. *Pearl River Water Transport, 01*, 111-113.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.

7. EKLER

Sayın katılımcı,

Bu anketler Alanya Alaaddin Keykubat Üniversitesi (ALKÜ) Lisansüstü Eğitim Enstitüsü İşletme Mühendisliği Anabilim Dalı İşletme Mühendisliği Programında yapılan Yüksek Lisans Tezi için hazırlanmıştır. İlk ankette denizcilik sektörünün ve firmaların dijital olgunluk seviyelerinin ölçülebilmesi için oluşturulan 5 ana kriter ve 25 alt kriterin başlıkları verilmiştir. Sizden her bir kriterin birbirine göre önem derecesini 1'den 9'a kadar değerlendirmeniz istenmektedir. İkinci ankette, firmanızın dijital olgunluk seviyesini ölçmeye yönelik sorular yöneltilmiştir. Üçüncü ankette ise 9 puanlık ölçekten oluşan ikili karşılaştırmalar ile siber güvenlik farkındalığını etkileyen faktörlerin birbirlerine göre önem derecelerini belirlemeniz istenmektedir. Analizlerin sağlıklı yapılabilmesi için sorulara gerçekçi cevaplar vermeniz önem arz etmektedir. Verdiğiniz cevaplar sadece bilimsel çalışma için kullanılacağında, firma ve isim bilgileriniz 3. şahıslar ile paylaşılmayacaktır. Değerli zamanınızı ayırdığınız için ve desteklerinizden ötürü sizlere teşekkürlerimi sunarım.

Ek 1: 1. Anket

Sıra	Ana Kriterler	Alt Kriter No.su	Alt Kriterler	Açıklama
1	Strateji ve Yönetim	1.1	Strateji	Dijital dönüşüm için yönetim stratejisinin uygulanma durumu
		1.2	Yatırımlar	Dijitalleşme alanında yatırım faaliyetleri
		1.3	Stratejik Partnerlikler	Dijital dönüşüm için stratejik partnerlikler sağlanması
		1.4	İnovasyon Yönetimi	İnovasyona yönelik iş birliği oluşturulması ve strateji geliştirilmesi
		1.5	Paydaşlar ile Uyum	Stratejik uygulamaların paydaşlar ile paylaşılması
2	Organizasyon	2.1	Yeterlilik Düzeyi	Çalışanların bilgi teknolojileriyle ilgili alanlarda sahip olduğu eğitim geçmişi
		2.2	Eğitim	Çalışanlara dijital teknolojiler ile ilgili eğitimlerin verilmesi
		2.3	Farkındalık	Dijitalleşme farkındalığı
		2.4	Süreç Sahipliği	Dijitalleşme süreçlerinin gözetilmesi
3	Altyapı ve Entegrasyon	3.1	Sektör Gelişimini Takip	Dijital sektör ilerlemesinin izlenmesi
		3.2	Süreçlerin Uyarlanabilmesi	Müşterilere göre süreçlerin uyarlanabilmesi
		3.3	Şirket içi Sistem Entegrasyonları	Şirket içi dijital sistemlerin uyumu
		3.4	Bilgi Teknolojileri Güvenliği	Sistem emniyetini sağlama ve acil müdahale yolları
		3.5	Paydaşlar ile Sistem Entegrasyonları	Paydaşlar ile sistem entegrasyonları
		3.6	Mobil Kullanımı	Mobil kullanımı
4	Dijital Sistemler ve İşleyiş	4.1	Depo Operasyonları	Depo operasyonlarında dijital uygulama kullanımı
		4.2	Büyük Veri	Büyük veri kullanımı
		4.3	Akıllı Teknoloji Uygulamaları	Son teknoloji dijital uygulamalar
		4.4	Dijital iş modelleri	Karar verme safhasında faydalı örneklerden yararlanma
		4.5	Yük Taşımacılığı Operasyonları	Yük taşımacılığı operasyonlarında dijital ürün kullanımı
		4.6	Ürün Takip Edilebilirliği	Ürün takip edilebilirliği
5	Projeler ve İş Birlikleri	5.1	Şirket İçi Projeler Yapılması	Şirket içerisinde dijitalleşmeye yönelik projeler uygulanması
		5.2	Devlet Teşviki	Dijital projeler için devlet teşviki sağlanması
		5.3	Uluslararası Projelere Katılım	Uluslararası projelere iştirak edilmesi
		5.4	Üniversite İş Birlikleri	Dijitalleşme projeleri için üniversiteler ile iş birlikleri yapılması

Ölçekler	Tercih Derecesi	Açıklama
1	Eşit seviyede önemli	İki faaliyet hedefe eşit derecede katkıda bulunmaktadır.
3	Orta derecede önemli	Deneyim ve muhakeme, bir faaliyeti diğerine göre biraz veya orta derecede tercih eder.
5	Kesinlikle önemli	Deneyim ve muhakeme, bir faaliyeti diğerine güçlü bir şekilde veya esasen tercih eder.
7	Çok kuvvetli derecede önemli	Bir faaliyet diğerine göre güçlü bir şekilde tercih edilir ve uygulamada baskınlığı gösterilir.
9	Aşırı derecede önemli	Bir faaliyeti diğerine tercih etmenin kanıtı, bir olumlama için mümkün olan en yüksek derecededir.
2,4,6,8	Ara değerler	Ağırlık 1, 3, 5, 7 ve 9'daki tercihler arasındaki uzlaşmaları temsil etmek için kullanılır.

		9	7	5	3	1	3	5	7	9	
1	Strateji ve Yönetim										Organizasyon
2	Strateji ve Yönetim										Altyapı ve Entegrasyon
3	Strateji ve Yönetim										Dijital Sistemler ve İşleyiş
4	Strateji ve Yönetim										Projeler ve İş Birlikleri
5	Organizasyon										Altyapı ve Entegrasyon
6	Organizasyon										Dijital Sistemler ve İşleyiş
7	Organizasyon										Projeler ve İş Birlikleri
8	Altyapı ve Entegrasyon										Dijital Sistemler ve İşleyiş
9	Altyapı ve Entegrasyon										Projeler ve İş Birlikleri
10	Dijital Sistemler ve İşleyiş										Projeler ve İş Birlikleri

		9	7	5	3	1	3	5	7	9	
1	Strateji										Yatırımlar
2	Strateji										Stratejik Partnerlikler
3	Strateji										İnovasyon Yönetimi
4	Strateji										Paydaşlar ile Uyum
5	Yatırımlar										Stratejik Partnerlikler
6	Yatırımlar										İnovasyon Yönetimi
7	Yatırımlar										Paydaşlar ile Uyum
8	Stratejik Partnerlikler										İnovasyon Yönetimi
9	Stratejik Partnerlikler										Paydaşlar ile Uyum
10	İnovasyon Yönetimi										Paydaşlar ile Uyum

		9	7	5	3	1	3	5	7	9	
1	Yeterlilik Düzeyi										Eğitim
2	Yeterlilik Düzeyi										Farkındalık
3	Yeterlilik Düzeyi										Süreç Sahipliği
4	Eğitim										Farkındalık
5	Eğitim										Süreç Sahipliği
6	Farkındalık										Süreç Sahipliği

		9	7	5	3	1	3	5	7	9	
1	Sektör Gelişimini Takip										Süreçlerin Uyarlanabilmesi
2	Sektör Gelişimini Takip										Şirket içi Sistem Entegrasyonları
3	Sektör Gelişimini Takip										Bilgi Teknolojileri Güvenliği
4	Sektör Gelişimini Takip										Paydaşlar ile Sistem Entegrasyonları
5	Sektör Gelişimini Takip										Mobil Kullanımı
6	Süreçlerin Uyarlanabilmesi										Şirket içi Sistem Entegrasyonları
7	Süreçlerin Uyarlanabilmesi										Bilgi Teknolojileri Güvenliği
8	Süreçlerin Uyarlanabilmesi										Paydaşlar ile Sistem Entegrasyonları
9	Süreçlerin Uyarlanabilmesi										Mobil Kullanımı
10	Şirket içi Sistem Entegrasyonları										Bilgi Teknolojileri Güvenliği
11	Şirket içi Sistem Entegrasyonları										Paydaşlar ile Sistem Entegrasyonları
12	Şirket içi Sistem Entegrasyonları										Mobil Kullanımı
13	Bilgi Teknolojileri Güvenliği										Paydaşlar ile Sistem Entegrasyonları
14	Bilgi Teknolojileri Güvenliği										Mobil Kullanımı
15	Paydaşlar ile Sistem Entegrasyonları										Mobil Kullanımı

		9	7	5	3	1	3	5	7	9	
1	Depo Operasyonları										Büyük Veri
2	Depo Operasyonları										Akıllı Teknoloji Uygulamaları
3	Depo Operasyonları										Dijital iş modelleri
4	Depo Operasyonları										Yük Taşımacılığı Operasyonları
5	Depo Operasyonları										Ürün Takip Edilebilirliği
6	Büyük Veri										Akıllı Teknoloji Uygulamaları
7	Büyük Veri										Dijital iş modelleri
8	Büyük Veri										Yük Taşımacılığı Operasyonları
9	Büyük Veri										Ürün Takip Edilebilirliği
10	Akıllı Teknoloji Uygulamaları										Dijital iş modelleri
11	Akıllı Teknoloji Uygulamaları										Yük Taşımacılığı Operasyonları
12	Akıllı Teknoloji Uygulamaları										Ürün Takip Edilebilirliği
13	Dijital iş modelleri										Yük Taşımacılığı Operasyonları
14	Dijital iş modelleri										Ürün Takip Edilebilirliği
15	Yük Taşımacılığı Operasyonları										Ürün Takip Edilebilirliği

		9	7	5	3	1	3	5	7	9	
1	Şirket İçi Projeler Yapılması										Devlet Teşviki
2	Şirket İçi Projeler Yapılması										Uluslararası Projelere Katılım
3	Şirket İçi Projeler Yapılması										Üniversite İş Birlikleri
4	Devlet Teşviki										Uluslararası Projelere Katılım
5	Devlet Teşviki										Üniversite İş Birlikleri
6	Uluslararası Projelere Katılım										Üniversite İş Birlikleri

Ek 2: 2. Anket

DENİZCİLİK SEKTÖRÜNÜN VE FİRMALARIN DİJİTAL OLGUNLUK SEVİYESİNİN ÖLÇÜLMESİ	0 (HİÇ UYGULANMAYAN)	1 (BAŞLANGIÇ)	2 (ORTA)	3 (DENEYİMLİ)	4 (UZMAN)	5 (EN İYİ PERFORMANS GÖSTEREN)
1. STRATEJİ VE YÖNETİM						
1.1. Dijitalleşmeye yönelik firmanın yönetim stratejisi bulunmaktadır.	Strateji oluşturulmamıştır.	Pilot çalışmalar planlanmıştır.	Geliştirilme aşamasındadır.	Genel olarak tanımlanmış ve yol haritası oluşturulmaktadır.	Strateji oluşturulmuş ancak uygulamaya geçilmemiştir.	Strateji hayata geçirilerek uygulamaya alınmıştır.
1.2. Dijitalleşme alanında yatırım faaliyetleri mevcuttur.	Dijitalleşme için bütçe oluşturulmamıştır	Yılda yaklaşık 50.000 Euro bütçe oluşturulmaktadır	Yılda 50.000-100.000 Euro aralığında bütçe oluşturulmuştur	Yılda 101.000-250.000 Euro aralığında bütçe oluşturulmuştur	Yılda 251.000-500.000 Euro aralığında bütçe oluşturulmuştur	Dijitalleşme için yılda 501.000 Euro 'dan fazla bütçe oluşturulmaktadır.
1.3. Dijital dönüşüm için stratejik ortaklıklar sağlanmaktadır.	Partnerlik mevcut değildir	Bir partnerlik sağlanmıştır	İki ya da üç partnerlik sağlanmıştır	4 ya da 5 partnerlik sağlanmıştır	6-9 arasında partnerlik sağlanmıştır	Dijital dönüşüm için 10 ve üzeri partnerlik sağlanmıştır
1.4. İnovasyona yönelik iş birlikleri oluşturulmaktadır.	İş birliği yoktur	1 iş birliği vardır	2 ya da 3 iş birliği vardır	4 ya da 5 iş birliği vardır	6-9 arasında iş birliği vardır	10 ve üzeri iş birliği vardır
1.5. Stratejik uygulamalar ortaklar ile paylaşılarak aksiyonların yaygın hale gelmesi sağlanmaktadır.	Stratejik uygulamalar yoktur	Temel seviyededir	Kısmen paylaşılmaktadır	Önemli düzeyde paylaşılmaktadır	Büyük ölçüde paylaşılmaktadır	Tüm stratejik uygulamalar paylaşılmaktadır
2. ORGANİZASYON						

2.1. Acil durumlara müdahale için bilgi teknolojileriyle ilgili alanlarda eğitim geçmişine sahip çalışanlar bulunmaktadır.	%10 dan az çalışanın ilgili alanlarda eğitim geçmişi vardır	%10-%20 arası çalışanın ilgili alanlarda eğitim geçmişi vardır	%20-%30 arası çalışanın ilgili alanlarda eğitim geçmişi vardır	%30-%40 arası çalışanın ilgili alanlarda eğitim geçmişi vardır	%40-%50 arası çalışanın ilgili alanlarda eğitim geçmişi vardır	%50 den fazla çalışanın ilgili alanlarda eğitim geçmişi vardır
2.2. Çalışanların dijital teknolojiler ile ilgili eğitimler verilerek programların kullanımı yaygınlaştırılmaya çalışılmaktadır.	Çalışanlara eğitim sunulmamaktadır	Çalışanlara iki yılda bir eğitim sunulmaktadır	Çalışanlara yılda bir eğitim sunulmaktadır	Çalışanlara yılda iki eğitim sunulmaktadır	Çalışanlara yılda üç eğitim sunulmaktadır	Çalışanlara yılda dört eğitim sunulmaktadır
2.3. Firma içerisinde dijital dönüşüm farkındalığının yükselmesi için eylem planı vardır.	Plan yoktur	Pilot çalışmalar planlanmıştır.	Geliştirilme aşamasındadır.	Genel olarak tanımlanmış ve yol haritası oluşturulmaktadır.	Plan oluşturulmuş yalnız uygulamaya geçilmemiştir	Plan düzenli olarak uygulanmaktadır
2.4. Dijital dönüşüm için firmada bir yönetici ve ekibi mevcuttur.	Dijital dönüşüm için birim mevcut değildir	Dışarıdan destek alınmaktadır	Bilgi işlem sorumluları mevcuttur	Bilgi işlem müdürü ve ekibi mevcuttur	Firma bünyesinde CIO ya da CTO vardır	Firma bünyesinde CIO ve CTO vardır
3. ALTYAPI VE ENTEGRASYON						
3.1. Firmadaki mevcut dijital altyapı sürekli yenilenmekte ve güncellemelerin yazılımlarla uyumlu olması sağlanmaktadır.	Dijital yenilikler izlenmemektedir	Başlangıç düzeydedir	Orta düzeydedir	Deneyim sahibi olunmuştur.	Konuda uzmanlaşılmıştır.	Dijital yeniliklerin takip edilmesi ve uygulanması sürekli hale getirilmiştir.
3.2. Şirketin çalışma süreçleri müşteri gereksinimlerine göre uyarlanabilir durumdadır.	Uyarlanamaz durumdadır	Müşterilerin %10 una uyarlanabilir	Müşterilerin %25 ine uyarlanabilir	Müşterilerin %50 sine uyarlanabilir	Müşterilerin %75 ine uyarlanabilir	Müşterilerin %100 üne uyarlanabilir
3.3.Firmadaki mevcut tüm dijital sistemler kendi aralarında uyum içerisinde çalışmaktadırlar.	Dijital sistemler birbirleri ile uyumlu çalışmamaktadır	Tüm dijital sistemler birbirleriyle %10 uyumlu durumdadır	Tüm dijital sistemler birbirleriyle %25 uyumlu durumdadır	Tüm dijital sistemler birbirleriyle %50 uyumlu durumdadır	Tüm dijital sistemler birbirleriyle %75 entegre durumdadır	Tüm dijital sistemler birbirleriyle %100 entegre durumdadır
3.4. Teknik arızalar ya da siber saldırılar neticesinde acil müdahale yolları ile sistem emniyeti sağlanmaktadır.	Sistem emniyeti 3 günden sonra alınabilmektedir	Sistem emniyeti 3 gün içerisinde alınabilmektedir	Sistem emniyeti 2 gün içerisinde alınabilmektedir	Sistem emniyeti 1 gün içerisinde alınabilmektedir	Sistem emniyeti 6 saat içerisinde alınabilmektedir	Sistem emniyeti 2 saat içerisinde alınabilmektedir

3.5. Şirket dışı çalışılan ortaklar ile (müşteri, tedarikçi vs.) dijital sistem uyumu oluşturulmuştur.	Ortaklar ile dijital sistem uyumu yoktur	Ortakların %10'u ile dijital uyum içerisinde çalışılmaktadır	Ortakların %25'i ile dijital uyum içerisinde çalışılmaktadır	Ortakların %50'si ile dijital uyum içerisinde çalışılmaktadır	Ortakların %75'i ile dijital uyum içerisinde çalışılmaktadır	Ortakların tamamı ile dijital uyum içerisinde çalışılmaktadır.
3.6. Şirket içerisinde kullanılan dijital sistemlerin mobil kullanım seçenekleri de vardır.	Mobil kullanım seçeneği yoktur	Dijital sistemlerin %10'unda mobil kullanım seçeneği vardır	Dijital sistemlerin %25'inde mobil kullanım seçeneği vardır	Dijital sistemlerin %50'sinde mobil kullanım seçeneği vardır	Dijital sistemlerin %75'inde mobil kullanım seçeneği vardır	Kullanılan tüm dijital sistemlerin mobil kullanım seçeneği vardır
4. DİJİTAL SİSTEMLER VE İŞLEYİŞ	4.3. Kullanılan akıllı teknolojiler: Yapay Zekâ, Akıllı Şebekeler, Drone, Akıllı Sensörler, Arttırılmış Gerçeklik (AR), Akıllı Robotlar, Gelişmiş Arayüzler, 3D Yazıcı, Sanal Ticaret. 4.4. Dijital iş modeli örneği: Liman müşterileri, gümrük bakanlığı memurları gibi paydaşlar tarafından liman yüklerinin dijital ortamlardan (web sitesi, mobil uygulama) izlenmesi, dijital sipariş yönetimi, liman içindeki envanterinin takibi, müşteri ve gümrük bakanlığı entegrasyonları vb. dijital iş modeli ortaklıkları.					
4.1. Depolama saha ve operasyonlarında yük elleçlemeleri ve alan kullanımı dijital teknolojiler ve sanayi 4.0 uygulamalarından yararlanılarak gerçekleştirilmektedir.	Depo çalışmalarında dijital teknolojiler kullanılmamaktadır	1 depo operasyonunda yararlanılmaktadır	Sınırlı sayıda operasyonda yararlanılmaktadır	Bazı operasyonlarda yararlanılmaktadır	Operasyonların genelinde dijital teknolojilerden yararlanılmaktadır	Tüm depo operasyonlarında dijital teknolojilerden yararlanılmaktadır
4.2. Şirket içerisinde büyük veri (big data) kullanılmakta ve veri analitiği yapılmaktadır.	Kullanılmamaktadır	İş takibi yapılmakta, KPI'lar izlenebilmektedir	İş öngörüleri çıkarılmaktadır.	Optimizasyon yapılmaktadır.	Veri üzerinden para kazanabilmektedir.	Şirketin ana faaliyeti veriden para kazanmaya yönelik olarak değişmektedir.
4.3. Akıllı dijital teknoloji ve uygulamaları kullanılmaktadır. (Örnekler 4. bölüm başlığında verilmiştir.)	Şirkette akıllı dijital teknoloji ve uygulamaları kullanılmamaktadır	Teknolojik araçların 1'i kullanılmaktadır	Teknolojik araçların 2'si kullanılmaktadır	Teknolojik araçların 4'ü kullanılmaktadır	Teknolojik araçların 6'sı kullanılmaktadır	Teknolojik araçların 9'u da kullanılmaktadır
4.4. Dijital iş modeli-modelleri uygulanmaktadır. (Açıklama yukarıdadır)	İş modeli-modelleri uygulanmamaktadır	Pilot çalışmalar planlanmıştır	Geliştirilme aşamasındadır	Genel olarak tanımlanmış ve yol haritası oluşturulmaktadır	Model oluşturulmuş ancak uygulamaya geçilmemiştir	Model hayata geçirilerek uygulamaya alınmıştır
4.5. Yük taşımacılığı operasyonlarında dijital ürünler kullanılmaktadır.	Dijital ürünler kullanılmamaktadır	1 yük taşımacılığı operasyonunda yararlanılmaktadır	Sınırlı sayıda operasyonda yararlanılmaktadır	Bazı operasyonlarda yararlanılmaktadır	Operasyonların genelinde dijital teknolojilerden yararlanılmaktadır	Tüm yük taşımacılığı operasyonlarında dijital teknolojilerden yararlanılmaktadır
4.6. Kullanılan tüm ürünler dijital olarak uzaktan izlenebilmektedir.	Uzaktan takip sistemi mevcut değildir	Depo içerisinde bulunmaktadır.	Taşıma sürecinde izlenebilirlik sağlanmaktadır	Depo ve taşımacılık süreçlerinde izlenebilirlik sağlanmaktadır	Depo, taşımacılık ve gümrük süreçlerinde izlenebilirlik sağlanmaktadır.	Üretim, gümrük, taşımacılık, depo işlemleri sırasında ürünlerin tamamı takip edilebilmektedir

5. PROJELER VE İŞ BİRLİKLERİ						
5.1.Firma içerisinde dijitalleşmeye ait projeler gerçekleştirilmektedir.	Dijital projeler gerçekleştirilmemektedir	Son 5 yılda bir dijital proje gerçekleştirilmiştir	Son 4 yılda bir dijital proje gerçekleştirilmiştir	Son 3 yılda bir dijital proje gerçekleştirilmiştir	Son 1 yılda iki dijital proje gerçekleştirilmiştir	Son 1 yılda ikiden fazla dijital proje gerçekleştirilmiştir
5.2 Devlet teşviklerinden, firma içerisinde gerçekleştirilen dijital projeler için yararlanılmaktadır.	Devlet teşviklerinden yararlanılmamaktadır	Son 4 yılda 50.000 Dolar devlet yardımından yararlanılmıştır	Son 3 yılda 50.000 Dolar devlet yardımından yararlanılmıştır	Son 2 yılda 75.000 Dolar devlet yardımından yararlanılmıştır	Son 1 yılda 100.000 Dolar devlet yardımından yararlanılmıştır	Son 1 yılda 100.000 Dolardan fazla devlet yardımından yararlanılmıştır
5.3. Firma uluslararası düzeyde dijitalleşme ile ilgili gerçekleştirilen projelere iştirak etmektedir.	Uluslararası projeler yapılmamaktadır	Son 4 yılda 1 uluslararası proje yapılmıştır	Son 3 yılda 1 uluslararası proje yapılmıştır	Son 2 yılda 1 uluslararası proje yapılmıştır	Son 1 yılda 1 uluslararası proje yapılmıştır	Son 1 yılda 1 den fazla uluslararası proje yapılmıştır
5.4. Üniversiteler ile birlikte dijital dönüşüm projeleri için çalışılmaktadır.	Üniversiteler ile çalışılmamaktadır	Son 4 yılda 1 projede üniversiteler ile çalışılmıştır	Son 3 yılda 1 projede üniversiteler ile çalışılmıştır	Son 2 yılda 1 projede üniversiteler ile çalışılmıştır	Son 1 yılda 1 projede üniversiteler ile çalışılmıştır	Son 1 yılda 1'den fazla projede üniversiteler ile çalışılmıştır

Ek 3: 3. Anket

Sıra	Kriterler	Açıklama
1	Tutum	Çalışanların siber güvenlik konusunu ele alış biçimi
2	Davranış	Çalışanların siber güvenlik konusundaki davranışları
3	Bilişsel	Çalışanların siber güvenlik konusunda bilgi edinme, anlama, kavrama durumu
4	Derece	Çalışanların siber güvenlik konusunda eğitim düzeyi
5	Deneyim	Çalışanların siber güvenlik, saldırı konusunda deneyimi
6	Finans	Çalışanların gelir düzeyi
7	Cinsiyet	Çalışanların cinsiyeti

	9	7	5	3	1	3	5	7	9	
Tutum										Davranış
Tutum										Bilişsel
Tutum										Derece
Tutum										Deneyim
Tutum										Finans
Tutum										Cinsiyet
Davranış										Bilişsel
Davranış										Derece
Davranış										Deneyim
Davranış										Finans
Davranış										Cinsiyet
Bilişsel										Derece
Bilişsel										Deneyim
Bilişsel										Finans
Bilişsel										Cinsiyet
Derece										Deneyim
Derece										Finans
Derece										Cinsiyet
Deneyim										Finans
Deneyim										Cinsiyet
Finans										Cinsiyet

ÖZGEÇMİŞ

Adı Soyadı: Lemi Kaya

Eğitim ve Mesleki Geçmişi:

- 2023-Devam Ediyor, Ortadoğu Antalya Liman İşletmesi A.Ş., QTerminals Antalya, Teknik Uzman
- 2020-2023, Antalya Büyükşehir Belediyesi, Ulaşım Daire Başkanlığı, Bakım Onarım Mühendisi
- 2018-2020, Akça Makina Otomotiv A.Ş., Servis Mühendisi
- 2016-2017, Türk Silahlı Kuvvetleri, Yedek Subay
- 2011-2016, Karabük Üniversitesi Mühendislik Fakültesi Otomotiv Mühendisliği

Yabancı Dil Bilgisi: İngilizce