Araştırma Makalesi / Research Article

DOI: 10.29064/ijma.1519040

Denizcilikte Dijitalleşme ve Siber Güvenlik

Murat Yorulmaz[1], Nejla Arıca[2]

[1]Kocaeli Üniversitesi, Denizcilik Fakültesi, Kocaeli, Türkiye/murat.yorulmaz@kocaeli.edu.tr

[2]Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü, Kocaeli, Türkiye/ nejlarc44@gmail.com

Özet

Bu çalışmanın amacı, denizcilikte dijitalleşmenin etkilerini ve dijitalleşme ile birlikte denizcilik faaliyetlerini sürdürülebilir kılmak için zorunluluk olan siber güvenlik uygulamalarını açıklamak ve denizcilik sektör profesyonellerinin siber güvenliğe karşı görüşlerini ortaya çıkartmaktır. Araştırmada, nitel araştırma yöntemlerinden olgu bilim modeli kullanılmış, veri toplama tekniği olarak görüşme tekniği, verilerin analizinde de betimsel ve içerik analizi teknikleri uygulanmıştır. Araştırmanın amacına yönelik olarak denizcilik sektöründe çalışan 14 kişiden elde edilen verilerin analizi sonucunda katılımcıların tamamı siber güvenlik hakkında bilgi sahibi olduğunu ifade etmiştir. Katılımcıların çoğu siber güvenlik ile ilgili profesyonel bir eğitim almadığını, eğitim alanlar ise aldıkları eğitimleri yeterli bulmadığını ifade etmiştir. Çoğu katılımcı dijitalleşmeyi tehdit olarak gördüklerini belirtmiştir. Dijitalleşmenin deniz ulaştırma faaliyetlerini kolaylaştırdığı, tehdit olarak görülmesinin yanı sıra olumlu etkilerinin de olduğu sonucuna varılmıştır.

Anahtar Kelimeler: Denizcilik, Dijitalleşme, Siber Güvenlik, Nitel Araştırma, Olgu Bilimi.

JEL Sınıflandırması: M10, M19

ORCID[1]: 0000-0002-5736-9146/ **ORCID[2]:** 0009-0006-5561-8600

Digitalization and Cyber Security in Maritime

Abstract

The aim of this study is to explain the effects of digitalization in maritime and cyber security practices that are a necessity to make maritime activities sustainable with digitalization and to reveal the views of maritime sector professionals on cyber security. In the study, the phenomenology model, one of the qualitative research methods, was used, interview technique was used as the data collection technique, and descriptive and content analysis techniques were applied to analyze the data. As a result of the analysis of the data obtained from 14 people working in the maritime sector for the purpose of the research, all of the participants stated that they had knowledge about cyber security. Most of the participants stated that they did not receive professional training on cyber security, and those who received training stated that they did not find the training they received sufficient. Most participants stated that they see digitalization as a threat. It was concluded that digitalization facilitates maritime transportation activities and has positive effects as well as being seen as a threat.

Keywords: Maritime, Digitalization, Cybersecurity, Qualitative Research, Phenomenology.

JEL Classification: M10, M19

ORCID[1]: 0000-0002-5736-9146/ **ORCID[2]:** 0009-0006-5561-8600

GİRİŞ

Denizyolu taşımacılığı, taşınacak malların gemilere yüklenmesi, elleçlenmesi ve gideceği yere kadar güvenle taşınması süreçlerini kapsayan bir taşımacılık türüdür (Yangal, 2022). Denizcilik faaliyetleri, ülkelerin milli gücüne maddi ve manevi katkı sağlayan karmaşık bir güç sistemi olarak tanımlanmaktadır. Denizler ve limanlar, siyasi, askeri ve iktisadi anlamda devletlerin gücünü ortaya koymaktadır. Bu gücün kaybı devletlerin bağımsızlığını tehlikeye sokmaktadır. Bunu engellemek için eldeki kaynakların en iyi şekilde kullanılması denizlerdeki etkinliğimizi artıracaktır. Geçmişten günümüze denizler hem bilim hem de kültürlerin yayılışında rol oynadığından, bu ticaret yollarını korumak devletler için önemli bir yere sahiptir. Yaşanan olaylar devletlerin denizcilikten beklentilerini ve bakış açılarını etkileyerek günümüzdeki denizciliğin yapısını şekillendirmiştir. Çağdaş, güvenilir ve ekonomik açıdan güçlü bir devlet olmak için denizlerimize ve denizcilik sektörüne uygun stratejileri geliştirmek hedefimiz olmalıdır (Özdemir, 2015: 422).

Uluslararası ticaretin ve küreselleşmenin gelişmesiyle birlikte deniz taşımacılığı dünyada giderek önem kazanmıştır. Ekonomik kalkınmanın bir göstergesi haline gelen denizyolu taşımacılığı, düşük maliyetli olması ve çok sayıda yükü etkin nakliye hizmetiyle tek seferde taşıması nedeniyle günümüzde sıklıkla kullanılmaktadır (Yurdakul, 2023:23). Önemli bir ihracat kaynağı olan gemi hizmetleri, ülkelerin dış ticaretinin oluşturulmasında da rol oynamaktadır. Tonaj bazında Dünya ticaretinin %85'inin denizyolu taşımacılığı ile yapıldığı Deniz Ticaret Odası tarafından bildirilmektedir (Germir, 2022). Türkiye 8.350 km olan kıyı şeridi ile denizyolu taşımacılığında önemli bir konuma sahiptir. Gelişmiş ekonomiye sahip olan ülkelerin siyasi alanda da güçlü olmasının sebebi, denizcilik faaliyetlerinde gösterdikleri performans ve başarı ile dünya denizlerinde söz sahibi olmalarından kaynaklanmaktadır. Limanların kombine taşımacılığa uygun hale getirilmesi için yapılacak çalışmalar, Türkiye'nin uluslararası ticarette rekabet gücünü giderek artırmaktadır (Cesur, 2020).

Dünya ticaret hacminde meydana gelen artış, denizyolu taşımacılığının önemini bir kez daha ortaya koymuştur. Denizyolu taşımacılığının önemli halkalarından biri olan limanlarda gün geçtikçe rekabet ve yük hacmi de artmaktadır. Artan bu yük hacmi nedeniyle limanlarda verilen hizmetlerde aksamalar olmakta, kimi zaman durma noktasına gelmektedir. Bu bağlamda dijitalleşme kavramını benimseyen limanların hizmet kalitesi artmakta, diğerlerine göre üstünlük sağladığı görülmektedir (Yorulmaz ve Partuna, 2021: 118). Her ne kadar denizcilik sektörü dijitalleşme konusunda çok yol katetmemiş olsa da bazı limanlar sektörün dijital öncüsü haline gelmiştir (Balık vd., 2021:267). Dijitalleşme limanlar için verimlilik fırsatı sunmakla birlikte beraberinde siber kaygıları da meydana getirmiştir. Bu nedenle denizcilik sektörünün dijital teknolojileri benimsemesi yeniliklere açık olması gerekmektedir (Yorulmaz ve Patruna, 2021: 118-131).

Bu çalışmanın amacı, denizcilikte dijitalleşmenin etkilerini ve dijitalleşme ile birlikte denizcilik faaliyetlerini sürdürülebilir kılmak için zorunluluk olan siber güvenlik uygulamalarını açıklamak ve sektör profesyonellerinin siber güvenliğe karşı görüşlerini ortaya çıkartmaktır.

1. Dijitalleşme ve Siber Güvenlik

Küreselleşen dünyada meydana gelen teknolojik gelişmeler neticesinde dijitalleşmeye olan ihtiyaç gün geçtikçe artmaktadır. Denizcilik sektörü, bünyesinde çok taraf barındırması nedeniyle karmaşık bir süreç yönetimi gerektirmektedir. Bu sebeple teknolojide meydana gelen yenilikleri takip etmek ve ona ayak uydurmak sektör

açısından önemlidir. Yük taşımanın yanı sıra, liman otoriteleri tarafından yapılan kontroller, elleçleme, gümrük ve kargo gibi süreçlerin yürütülmesinde kolaylık sağlaması açısından denizcilik sektörünün yenilikçi teknolojilere açık olması gerekmektedir. Denizcilikte dijitalleşme süreçlerinden hangi alanlarda yararlanılabileceğini görmek için, bilgi paylaşımının doğru, güvenilir ve hızlı olması önem taşımaktadır. Verilerin paylaşımının açık ve şeffaf olması dijitalleşmenin avantajlarındandır (Özen, 2021).

Dijitalleşmenin uygulanması; gerçek zamanlı kontrol, blok zinciri ve büyük veri, otonom araçlar ve robotik, yapay zekâ, sanal gerçeklik, iletişim, ağ bağlantısı ve IoT gibi teknolojilere dayanmaktadır Bazı deniz kazalarının, dijital teknolojilerin eksikliğinden de kaynaklandığını söylemek mümkündür. Bu teknolojilerin kombine kullanılması ile doğabilecek risklerin en aza indirilebileceği düşünülmektedir (Yanık, 2022).

1.1. Endüstri 4.0 Bileşenleri

Endüstri 4.0 ilk kez 2011 yılında Almanya'da bir teknoloji fuarında ortaya çıkmıştır. Dijital teknolojileri kullanarak gerçekliği sanallaştırmayı, verimliliği ve üretkenliği artırmayı amaçlayan sanayi devrimi kavramıdır (Napolitano ve Pedrazzoli, 2019).

1.1.1. Nesnelerin İnterneti (IOT)

İnternet üzerinden diğer sistemlere ve cihazlara bağlanmayı, alışveriş yapmayı amaçlayan nesnelerin interneti, yazılımlar, sensörler ve diğer teknolojilerle fiziksel nesnelerin ağını ifade etmektedir. Bilgi işlem cihazları ve makinelerden oluşan, akıllı cihazlarla veri toplayarak insana gerek kalmadan başka cihazlarla paylaşmaya olanak sağlayan bir teknolojidir. Nesnelerin interneti sayesinde dijital dünya ile gerçek dünya iş birliği yapmaktadır. Bunun dışında gerçek zamanlı verilere istenildiğinde ulaşılması, süreçle ilgili karar vermeyi kolaylaştırması, müşteri deneyimlerini iyileştiriyor olması ve maliyetleri azaltması avantajları olarak sayılabilir (Özen, 2021).

1.1.2. Blok Zincir Teknolojisi

Dağıtılmış Defter Teknolojisi, blok zincir olarak adlandırılmış olup, verilerin güvenli bir şekilde aktarılmasında, depolanmasında ve üçüncü tarafa ihtiyaç duyulmadan işlem yapılabilen bir teknolojidir. Habersiz işlem değişikliğine izin vermeyen blok zincir teknolojisinde bilgiler bir bloğa eklenmekte olup, aynı verilerin birden çok kopyası farklı konumlarda depolanarak zincire yeni bloklar eklenerek işlem yapılır. Sonuçta karmaşık bir sistem oluşacağından kullanıcılar için güvenilir bir ortam oluşturacaktır (Özen, 2021).

Avantajları arasında dijital belgelerin paylaşımı, maliyet ve zamandan tasarruf, hırsızlık ve dolandırıcılığı azaltması yer almaktadır. Uygulamada zorluk yaşanmasının nedenleri arasında paydaşlardan yeterli destek görememe, bilgi eksikliği ve hükümetlerin bu konudaki düzenlemelerinin eksikliği sayılabilir (Yanık, 2022).

1.1.3. Yapay Zekâ

Yapay Zekâ (AI), makinelerin sergilediği zekâ olarak tanımlanabilir (Özen, 2021). Bilgisayar biliminde ise, "çevresini tanımlayan ve hedefe ulaşmada başarı şansını azami seviyeye çıkarmak için harekete geçen her cihaz" olarak ifade edilmektedir (Kara, 2020:20). Yapay zekâ teknolojileri denizcilik sektöründe çoğunlukla limanlarda konteyner istifleme problemini yönetmek için kullanılmaktadır. Bunun dışında zaman ve maliyet tasarrufu sağlayarak gemi tasarımlarında da kullanılmaktadır (Özen, 2021). Yapay zekâyı gemilerde kullanarak ülke ekonomisine fayda

sağlamak da istenmektedir. Bu bağlamda gemi seferdeyken hava durumu veya deniz şartlarını gösteren bilgilerden yola çıkarak kısa sürede, güvenilir bir şekilde ve yüksek yakıt verimliliği ile rotaları düzenleyen sistemler geliştirilmeye çalışılmaktadır (Kara, 2020:21).

1.1.4. Büyük Veri Analizi

Büyük veri, geleneksel yazılımlar tarafından düzenlenemeyecek kadar komplike olan, yüksek hızda gelen, çeşitlilik içeren verileri analiz etme ve bilgiyi açığa çıkarmayı sağlayan bir alandır. Geleneksel verilerin kullanımı kolay ve anlaşılırdır ancak büyük verileri kullanılır hale getirmek ve bu verileri işlemek için iş analitiği kullanılmalıdır. Denizcilik sektöründe kullanılan navigasyon sayesinde çok sayıda veri üretilmektedir. Li ve arkadaşları yapmış oldukları çalışmada, bu veriler sayesinde gemilerin birbiri ile çarpışmasını önlemek için kaçış rotalarını optimize edebilmelerine olanak sağladılar (Özen, 2021).

1.1.5. Bulut Bilişim

Bulut bilişim, esnek olması ve pek çok avantajlarından dolayı endüstri 4.0'ın en önemli bileşenlerinden biridir. Bulut bilişim uygulama, servis ve altyapıların internette yer alan sunucular üzerinde bulundurularak internete bağlı bir cihazla uygulama ve servislerin çalıştırılmasıdır. Bulut bilişim sayesinde kullanıcılar, şirket için gerekli uygulamaları veri merkezlerinde veya kurum içi bilgisayarlarda depolamak yerine, servis sağlayıcılara ait bilgisayarlar yardımıyla internet üzerinden istedikleri zaman kullanabilmektedirler. Bu şekilde daha esnek ve ekonomik veri yönetimi elde edilmektedir (Tonga ve Tonga, 2022:50-51).

1.1.6. Simülasyon Yazılımlar

Gerçekliği yeniden üretmek ve test etmek olarak tanımlanan simülasyon yazılımlar, özellikle eğitim, imalat ve tasarım sektöründe sıkça karşımıza çıkmaktadır. Gemi inşa sürecinde simülasyon yazılımların kullanılması pratik çözümler üretmektedir (Özen, 2021).

Denizcilik sektöründe görev alan personellerin, sorumlu olduğu alanlarda yetkinlik kazanabilmesi için verilen eğitimin, düşük risk ve maksimum gerçeklikle organize edilmesi önemlidir. Bu amaçla personele risksiz bir ortamda beceri kazandırılarak, herhangi olumsuz bir durumdan kaçınmak için avantaj sağlamaktadır (Bolat, 2021:2).

1.2. Siber Güvenlik

Siber saldırılar, yetki dışı bırakarak sistemlere zarar veren, bilgi alışverişini kısıtlayan veya engelleyen tüm saldırılar olarak nitelendirilebilir. Siber güvenlik ise bu tür durumlara karşı alınacak önlemleri ifade etmektedir (Topal, 2020). Denizcilik sektöründe siber güvenlik kavramı gemi, liman ve operasyonlarında kullanılan tüm iletişim ve uygulama ağlarını korumak için alınan önlemler olarak tanımlanabilir. Günümüzde dijital sistemlerin yaygınlaşmasıyla limanlarda ve gemilerde yazılımların kullanımında artış görülmüştür. Özellikle yolcu gemileri yüzen bilgisayar olarak nitelendirilebilir. Çünkü bu gemilerde okyanuslarda bile kablosuz internet hizmeti sunulmaktadır (Şakar vd., 2019:6).

Denizcilik sektöründe yaşanan teknolojik gelişmeler beraberinde siber saldırıları da getirdiğinden, denizcilikte güvenlik önemli bir unsur haline gelmiştir. Güvelik önlemleri alınmadığında maddi ve manevi zararlar doğmaktadır. Bu yüzden siber saldırıları bilmek ve gereken önlemleri önceden almak oldukça önemlidir. İnsan faktörü bu noktada en zayıf faktör olarak karşımıza çıkmaktadır. Siber saldırılara karşı eğitimli ve farkındalık sahibi personeller yetiştirmek en basit önlemlerdendir (Topal, 2020).

Dijitalleşmenin artmasıyla beraber verilerin kolayca depolanıp paylaşıldığı bulut yazılımların ortaya çıkmasıyla siber güvenlik sorunu da bunu takip etmiştir. Denizcilikte günlük olarak liman, gemi ve acenteler arasında bilgi alışverişleri yapılmaktadır. Sistemlerin çalışması sırasında dijital hatalar meydana gelebileceğinden casus yazılımlara da fırsat doğmaktadır (Özen, 2021).

Siber saldırılar ulusal güvenliği yönelik üst düzey tehdit olarak nitelendirilmektedir. Bu nedenle denizcilik sektöründe öncelikli hale gelmeye başlamıştır. Bilgiye erişimin engellenmesi, gizliliğin sağlanması ve sistem bütünlüğünün korunması iş sürekliliği bakımından da önemlidir. Maersk firmasının siber güvenlik ile ilgili yaşadığı sorun nedeniyle 49.000 bilgisayarın yok edildiği, 3500 sunucunun imha edildiği, gemiler ile iletişimde gecikmeler yaşandığı ve şirkete ait faaliyetlerin durma noktasına geldiği belirtilmiştir (Lagouvardou, 2018).

Gemilerde siber güvenlik zafiyetine neden olan faktörler arasında; bilgisayar, cep telefonu, kişisel dijital ekipmanlar ve bunların gemideki cihazlarla alışverişi yer almaktadır. Güvenlik konusunda eğitimli ve yetkin personel yetiştirmek öncelik haline gelmelidir. Bu nedenle personellere belli periyotlarda eğitimler verilerek siber güvelik konusunda bilinçlendirme ve farkındalık oluşturulabilir. Kullanılmakta olan dijital teknolojilerin sürekli güncel tutulması gerekmektedir. Bu nedenle herhangi bir siber saldırı sonrası şirket politikaları gözden geçirilip güncellenmelidir. Gelecek yıllarda teknolojinin gelişmesiyle birlikte siber güvenlik konusu daha da önemli hale gelecektir (Topal, 2020).

1.2.1. Denizcilik Sektöründe Yaşanan Başlıca Siber Saldırı Olayları

Antwerp Limanı olayında yıllarca süren ve fark edilmesi zaman alan bir siber saldırı gerçekleşmiştir. Olay uyuşturucu kaçakçılığı yapan bir suç örgütü tarafından 2011 Haziran ayında e-mail aracılığıyla casus yazılım bulaştırılarak gerçekleştirilmiştir. Bu siber saldırıyla konteynerlerde taşınan yüklerin bilgileri değiştirilerek, alıcı bilgileri ve varış limanı gibi verilere müdahalede bulunulmuştur. Neticede 2013 yılının sonlarında yüklerin kaçırıldığı ve izlerinin silindiği fark edilerek gereken önlemler alınmıştır (Gürler, 2022).

Nisan 2012'de Danimarka' da acentede çalışan bir kullanıcıya gönderilen mailin ekinde bulunan virüs bulaştırılmış pdf ile önce denizcilik otoritesinin tüm bilgisayarlarına sonra diğer devlet kurumlarına siber saldırı düzenlenmiştir. Bu durumu düzeltmek için sistem günlerce kapatılmış ve anti- virüs programlarıyla sistem desteklenmiştir (Topal, 2020).

Güney Kore 2016 Nisan ayında 280 geminin seyir sistemlerinde sorun olduğunu rapor etmiştir. Sinyalleri yok eden GPS hackerler yanlış bilgi verilmesine sebep olmuştur. GPS sinyallerinin kaybolması seyirsel hataya neden olarak hava koşullarının ağır olduğu yerlerde trafiğin sıkışık olmasıyla birlikte ciddi kazalara sebebiyet verebilmektedir (Topal, 2020).

2017 Mayıs ayında gerçekleşen WannaCry fidye yazılımı olarak bilinen siber saldırı, verileri şifreleyip fidye talep ederek birçok organizasyonu etkileyerek küresel ekonomiye 6 milyar İngiliz Sterlini zarar vermiştir (Gürler,

2022). 2017 Ekim ayında gerçekleşen Badrabbit siber saldırısı kötü niyetli yazılım olarak ortaya çıkmıştır. Ukrayna, Doğu Avrupa ve Rusya'nın yanı sıra bu saldırıdan Türkiye'de etkilenmiştir. Kurbanlardan, 0.05 Bitcoin istenmiştir. Saldırıda sistem kilidinin açılması için süre verilmiş, süre geçtikçe bedelin yükseleceğinin bilgisayar ekranlarında gözüktüğü ifade edilmiştir (Gürler, 2022).

Temmuz 2018'de Çin' de gerçekleşen COSCO (China Ocean Shipping Company) saldırısında, şirketin internet bağlantısı kesilip, şirket içi iletişim ağında aksaklık yaşanmıştır. Konteyner taşımacılık şirketi olan COSCO firması aldığı önlemler sayesinde bu saldırıdan zarar görmediğini açıklamıştır (Gürler, 2022).

2019 Eylül ayında XHunter isimli siber saldırıyla Kuveyt deniz taşımacılık organizasyonunun bilgileri ifşa edilmiştir. 2019 Aralık ayında Ryuk Ransomware siber saldırısıyla bir denizcilik tesisi işlem göremez hale gelmiştir. 2020 yılında Mediterranean Shipping Company (MSC), gerçekleşen siber saldırının veri merkezi kesintisine sebep olduğunu buna bağlı olarak da web sitelerinin birkaç gün boyunca kapalı kaldığını doğrulamıştır. 2021 yılında Güney Kore'nin ulusal amiral gemisi taşıyıcısı HMM'e e-posta ile oltalama saldırısı gerçekleştirilerek, sisteme sınırlı erişim sağlanmıştır (Siber Tehdit Durum Raporu, 2022).

2022 yılında Birleşik Krallıkta Wightlink isimli feribot şirketi, bilişim teknolojisi alt yapılarına siber saldırı düzenlendiğini ve bazı müşterilerinin kişisel verilerinin ve banka bilgilerinin ele geçirildiğini duyurmuştur (Yanık, 2022).

1.2.2. Siber Saldırılara Karşı Alınacak Önlemler

Denizcilik sektöründe dijitalleşme beraberinde zorlukları da getirmektedir. Limanlarda bilgi teknolojilerinde oluşacak her türlü sorun, işlerin zamanında yapılmamasına ve sonuçta ekonomik kayıplara sebebiyet verecektir. Dünya'da hızla artan siber saldırılar karşısında, şirketler gereken önlemleri alma konusunda ciddi bütçe ayırmaktadır. Son yıllarda milyonlarca dolarlık kayba sebep olan ve seksenden fazla ülkeyi etkileyen fidye yazılımlar büyük sorun oluşturmuştur. Sadece fidye yazılımlar bile denizcilik sektörünü çökertebilecek kapasiteye sahiptir. Gemiler, casus yazılımlar nedeniyle rotalarından saptırılarak kötü niyetli kişilerin eline geçebilme tehlikesiyle karşı karşıya kalmaktadır. Son zamanlarda yazılımcılar, bu konuyla ilgili çeşitli güvenlik çalışmaları yapmaktadır. Gemi çalışanlarının siber güvenlik farkındalığına sahip olmaması, geminin güvenliği açısından büyük risk oluşturmaktadır. Bu nedenle eğitim programlarının düzenlenmesi önemlidir (Koldemir, Yapıcı ve Keleştemur, 2017: 1-3). Bunun dışında bilgi teknolojilerine yönelik saldırılara karşı antivirüs ve casus yazılımları önleyebilecek sistemler geliştirilerek, izinsiz girişlerin tespit edilmesi, bu girişlere karşı koruma sistemlerinin devreye girmesi ve kimlik doğrulama sisteminin aktif olması diğer önlemler olarak sayılabilir (Yanık, 2022).

2. YÖNTEM

Bu çalışmada dijitalleşme ile birlikte denizcilik faaliyetlerini sürdürülebilir kılmak için zorunluluk olan siber güvenliğe yönelik sektör profesyonellerinin düşünlerini ortaya çıkartmak amacıyla nitel araştırma yöntemlerinden olgu bilim (fenomoloji) modeli kullanılmıştır. Veri toplama tekniği olarak görüşme tekniği ve veri analiz yöntemi olarak da betimsel ve içerik analizi teknikleri uygulanmıştır. Olgubilim bireylerin deneyimlerini ve yaşamlarını nasıl anlamlandırdıklarını inceleyen, belli bir olgunun özünün nasıl keşfedileceğini ortaya koyan, bireyler arasındaki ortak noktaları bulan nitel bir araştırma desenidir. Fenomenoloji olarak da bilinen olgubilim deseni, bireylerin yaşamış

olduğu deneyimlere ve bu deneyimlerin kişiler için ne anlama geldiğine odaklanmaktadır (Çapar ve Ceylan, 2022:299).

Betimsel içerik analizi ise belirli bir konuda veya alanda nitel ve nicel araştırmaların birbirinden bağımsız olarak yapılarak derinlemesine incelenip düzenlenmesi anlamına gelir. Bu şekilde genel eğilimler belirlenmektedir. Bu yöntemin amacı; elde edilen sonuçların, hedeflenen konulara yönelik olarak gelecekte yapılacak araştırmalara yol göstermesidir (Ültay ve Akyurt 2021:189).

Araştırmada katılımcılara yöneltilen sorular şunlardır;

S.1. Siber güvenlik hakkında bilginiz var mıdır?

S.2. Siber güvenlik seviyelerinin artırılması hususunda görüş ve önerileriniz nelerdir?

S.3. Gemilerde siber saldırıya karşı alınması gereken önlemler ve koruma programları hakkındaki düşünceniz nedir?

S.4. Gemilerde siber saldırıya karşı eğitim programları düzenleniyor mu? Düzenleniyorsa bu eğitimlerin çalışanlara etkileri nedir?

S.5. Çalıştığınız süre boyunca geminiz/işletmeniz herhangi bir siber saldırıya maruz kaldı mı?

S.6. Denizcilik sektöründe kullanılan dijital teknolojiler ve uygulamaların etkileri hakkındaki düşüncelerinizi belirtiniz?

S.7. Denizcilik sektöründe dijitalleşmeyi tehdit olarak görüyor musunuz?

S.8.Dijitalleşmenin deniz ulaştırma faaliyetlerini kolaylaştırıp kolaylaştırmadığı ile ilgili düşünceniz nedir?

3. BULGULAR

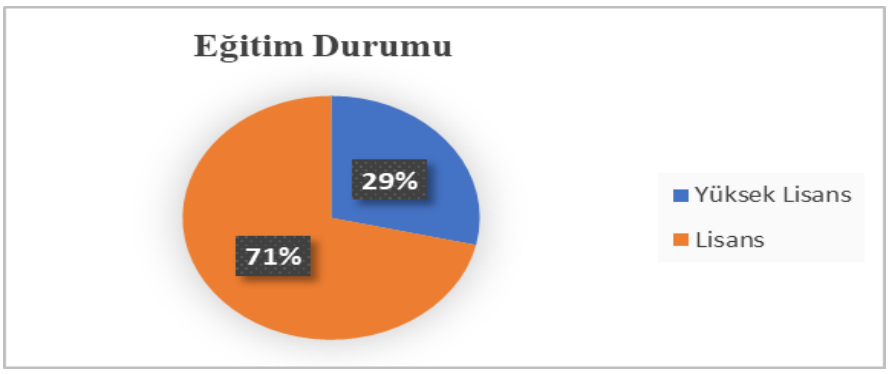
Anket çalışması denizcilik sektöründe çalışan 15 katılımcı ile yapılmıştır. 1 katılımcı sorulara eksik yanıt vermesi nedeniyle çalışma dışı bırakılmıştır. Katılımcıların %57,1'i erkek, %42,9' u kadındır ve yaş ortalamaları 32,5' tir. Katılımcıların demografik özellikleri Tablo 1' de gösterilmiştir.

Tablo 1: Katılımcıların Özellikleri

Katılımcı	Eğitim Durumu	Görev Tanımı	Sektördeki Deneyim Süresi
K1	Yüksek Lisans	Uzakyol Kaptanı	11 yıl
K2	Lisans	Uzakyol Kaptanı	20 yıl
K3	Lisans	Uzakyol Kaptanı	30 yıl
K4	Lisans	Uzakyol Vardiya Zabiti	1 yıl
K5	Yüksek Lisans	Uzakyol Makine Zabiti	3 yıl
K6	Lisans	Uzakyol Vardiya Zabiti	4 yıl
K7	Lisans	Uzakyol Kaptanı	30 yıl
K8	Yüksek Lisans	Uzakyol Kaptanı	2 yıl
K9	Lisans	Uzakyol Kaptanı	9 yıl
K10	Lisans	Uzakyol Vardiya Zabiti	2 yıl
K11	Lisans	Uzakyol Kaptanı	10 yıl
K12	Yüksek Lisans	Uzakyol Kaptanı	1 yıl

K13	Lisans	Uzakyol Kaptanı	11 yıl
K14	Lisans	Uzakyol Kaptanı	17 yıl

Tablo 1'de görüldüğü gibi katılımcılar, uzakyol grubu yönetim düzeyindeki gemi insanlarıdır. Katılımcı gemi insanlarının 4'ü yüksek lisans 10'u ise yüksek lisans mezunudur.



Grafik 1: Katılımcıların Eğitim Durumu

Katılımcıların %71'i lisans mezunuyken, %29' u yüksek lisans mezunudur.

Grafik 2: Siber Güvenlik Hakkındaki Bilgi Düzeyi

Katılımcıların tamamı siber güvenlik hakkında bilgi sahibi olduğunu belirtmiştir.

Grafik 3: Siber Saldırıya Maruz Kalma Durumu

Katılımcıların %93'ü siber saldırıya maruz kalmadığını ifade ederken, 1 katılımcı maruz kaldığını belirtmiştir.

Tablo 2: Siber güvenlik seviyelerinin artırılması hususunda görüş ve önerileriniz nelerdir?

Tema	Kodlar	f	%
Siber güvenliğin artırılması	Eğitim verilmeli (K5, K6, K13)	3	%22
	Siber güvenlik uzmanı istihdamı (K2, K10, K11)	3	%22
	Güvenlik seviyelerinin artırılması (K1, K3, K4, K7, K8, K9, K12)	7	%50
	Devlet kontrolü altında olmalı (K14)	1	%6

Tablo 2' de görüldüğü gibi 14 katılımcının S.2' ye verdiği yanıtlar 4 farklı kategoride kodlanmıştır. K6 ve K13'ün yanıtları aşağıda yer almaktadır.

"Siber güvenlik konusunda eğitimlerin artırılması gerektiğini düşünüyorum." (K6). "Siber güvenlik dijitalleşen dünyanın karşısındaki en büyük tehditlerden birisi olmasına rağmen konu hakkında insanların bilinç seviyesi maalesef düşüktür. Özellikle dijital ortam yürütülen faaliyetlerin kullanıcılarına bu konuda bilgilendirici brifingler verilmesinin faydalı olacağı değerlendirilmektedir." (K13).

Tablo 3: Gemilerde siber saldırıya karşı alınması gereken önlemler ve koruma programları hakkındaki düşünceniz nedir?

Tema	Kodlar	f	%
Siber güvenlik önlemleri	Şifreleme, ağ yönetimi ve güvenli yazılım kullanımı (K7, K1, K6, K9)	4	%29
	İşletme uygulamaları ve kişisel uygulamaların birbirinden ayrılması (K3)	1	%7
	Nitelikli personel yetiştirilmesi (K2, K13, K12, K10, K11)	5	%36
	Önlem alınmadığını düşünme (K4, K8)	2	%14
	Siber güvenlik uzmanı istihdamı (K5, K14)	2	%14

Tablo 3 incelendiğinde S.3' e verilen yanıtlar 5 kategoriye ayrılmıştır. Katılımcıların %29'u alınması gereken önlemlerin, şifreleme, ağ yönetimi ve güvenli yazılım kullanımı olduğunu belirmiştir. %36'sı ise nitelikli personel yetiştirilmesi gerektiğimi belirtmiştir. K5 ve K14'ün verdiği yanıtlar aşağıda yer almaktadır.

"Her gemiye siber güvenlik uzmanları atanabilir." (K5). *"Gemilerde siber saldırı makine dairesi hariç güverte cihazlarını etkileyebilir. (radar telsiz gibi) Devlet veri tabanlı sistemlerin kullanılması ve gemi kaptanlarına özel uydu telefonları tahsis edilerek böyle bir durum yaşandığı zaman direkt bakanlık ile irtibata geçilmesi bu tarz durumların hızlı çözülmesini sağlayabilir. (Uluslararası yardım geminin konumuna göre bir operasyon yardım vs.*

durumu) Ayrıca, gemi firmaları bilgisayar ve bilişim sistemleri konusunda bilgili siber saldırı alanında uzman kişileri kadrosuna katarak, karada ve gemilerde (firma büyüklüğüne göre) personeli aktif şekilde kullanmadır." (K14).

Tablo 4: Gemilerde siber saldırıya karşı eğitim programları düzenleniyor mu? Düzenleniyorsa bu eğitimlerin çalışanlara etkileri nedir?

Tema	Kodlar	f	%
Eğitim düzenlenme durumu	Düzenleniyor. (K3, K7, K9, K13)	4	%28
	Düzenlenmiyor. (K2, K4, K5, K6, K12, K14)	6	%44
	Yetersiz bulunuyor. (K8, K10, K11, K1)	4	%28

Tablo 4 incelendiğinde katılımcıların %44'ü eğitim düzenlenmediğini, %28'i ise düzenlenen eğitimleri yeterli bulmadığını ifade etmiştir.

Tablo 5: Denizcilik sektöründe kullanılan dijital teknolojiler ve uygulamaların etkileri hakkındaki düşüncelerinizi belirtiniz?

Tema	Kodlar	f	%
Dijital teknolojilerin uygulanabilirliği	Verimli, hızlı, takibi kolay, olumlu etki (K1, K2, K3, K4, K5, K6, K7, K10, K11, K12, K13)	11	%79
	Veri güvenliği sorunu (K8)	1	%7
	Yetersiz bulma (K9, K14)	2	%14

Tablo 5 incelendiğinde katılımcıların %79'u dijital teknolojilerin, verimli, hızlı ve takibinin kolay olduğunu, %14'ü yetersiz bulduğunu %7' si ise veri güvenliği konusunda sorun oluşturabileceğini ifade etmiştir. K7, K11 ve K12'nin vermiş olduğu yanıtlar aşağıda yer almaktadır:

"Gemimizde harita ve publication olarak dijital kullanıyoruz, kullanımı takibi ve pratiği kolay verimli çalışma olanağı sunuyor." (K7). *"Dijitalleşme ile birlikte birçok şeyin kontrolü ve takibi daha rahat yapılmaktadır."* (K11). *"Artarak devam etmelidir. Zamanı ve verimliliği artırdığını, uzun vadede maliyeti de azalttığını düşünüyorum."* (K12).

Tablo 6: Denizcilik sektöründe dijitalleşmeyi tehdit olarak görüyor musunuz?

Tema	Kodlar	f	%
Dijitalleşmeyi tehdit olarak algılama	Tehdit olarak görüyorum (K5, K6, K8, K14)	4	%29
	Tehdit olarak görmüyorum (K1, K2, K3, K4, K7, K9, K10, K11, K12, K13)	10	%71

Tablo 6 incelendiğinde katılımcıların %71' i dijitalleşmeyi tehdit olarak görmediğini, %29'u ise tehdit olarak gördüğünü ifade etmiştir. K2, K6 ve K8' in vermiş olduğu yanıtlar aşağıda yer almaktadır.

"Evet. Örnek verirsek gemilere gelen şüpheli mailler şüpheli bağlantılara yanlışlıkla da olsa tıklamak ve bu siber saldırının var olduğunun bilincinde olmamak şirkete ve belki de en kötüsü gemiye zarar verebilir. Duymuş olduğuma göre bazı güvenlik seviyesi düşük ülkelerde korsanların gemilere mail atıp gerekli olan pilot çarmıhı yüksekliğini, gemi hızını ve kılavuz pilot alma konumunu belirttiği mailler attıklarına dair bir söylenti duydum ne kadar doğru ne kadar yanlış bilemem ama çok ciddi bir durum." (K8). *"Dijital teknolojilerin artırılması tehdit olarak siber güvenliği önemli bir sorun haline getirmiştir. Dijital korsanlık faaliyetleri her iş kolunda olduğu gibi denizcilikte de önemli bir tehdittir."* (K6). *"Hayır kesinlikle tehdit olarak görmüyorum. Bilakis dijitalleşmenin mesleğimizi kolaylaştıracağını daha emniyetli seyirler icra etmemizi sağlayacağını düşünüyorum*." (K2).

Tablo 7: Dijitalleşmenin deniz ulaştırma faaliyetlerini kolaylaştırıp kolaylaştırmadığı ile ilgili düşünceniz nedir?

Tema	Kodlar	f	%
Denizcilik faaliyetlerine etkisi	Zaman tasarrufu ve iş kolaylığı sağlar. (K1, K2, K3, K4, K5, K6, K7, K9, K10, K12, K13)	11	%79
	Avantaj ve dezavantajları vardır. (K8, K11, K14)	3	%21

Tablo 7 incelendiğinde, katılımcıların %79'u dijitalleşmenin zaman tasarrufu ve iş kolaylığı sağladığını, %21' i ise avantaj ve dezavantajlarının olduğunu ifade etmiştir. K6, K12 ve K14' ün verdiği yanıtlar aşağıda yer almaktadır.

"Dijitalleşme deniz ulaştırma faaliyetlerinin yerine getirilmesinde büyük kolaylık sağlamaktadır. Personel, yük ve operasyonel faaliyetlerin takip edilmesinde zaman ve maaliyet girdilerini azaltmakta, bilgilerin erişiminde kolaylıklar sağlamaktadır." (K6). *"Elbette ciddi kolaylık oluşturuyor: En basitinden ECDİS kullanımı gemide kağıt harita kullanımını neredeyse kaldırdı. Liman operasyonlarında dijitalleşmeden, otonom gemilere, limanların robotik altyapı donanımlarının hazırlanması gibi gelişmelerin denizciliğin her sektöründe kolaylık sağlayacağını düşünüyorum."* (K12). *"Gemide ve yatta bulunan güverte, belli başlı elektrik elektronik ile çalışan aletlerin kullanımında, personeli daha az yoran çalışma yükünü azaltan sistemler bu yönde olumlu etkiye sahiptir. Ayrıca ilerleyen yıllarda tamamen gemileri bir komuta kontrol sistemi ile uzaktan kumanda ile yönetilebileceği konuşuluyor. Bu teknolojinin olumlu yönleri olsa da iş gücü, denizde güvenli seyir ve taşınan yükün güvenliği açısından büyük sorunlar yaratacaktır."* (K14).

SONUÇ VE DEĞERLENDİRME

Dijitalleşme her sektörde olduğu gibi, dünya ticareti için vazgeçilmez olan denizcilik sektöründe de önemli bir yere sahiptir. Büyük veri analizi, yapay zekâ, nesnelerin interneti, simülasyon yazılımlar denizcilik sektöründe sıklıkla kullanılmaya başlanmıştır. Bu bağlamda dijitalleşme denizcilik sektörü için birçok yeniliği de beraberinde getirmiştir. Nesnelerin interneti ve sensörler, gemilerin bakım ve onarım süreçlerini yönetebilmekte ve bu şekilde maliyeti düşürerek maksimum verimlilik sağlamaktadır. Bunun dışında insan iş gücüne duyulan ihtiyacın azalması, yapılan

hataların en aza indirilmesi de dijitalleşmenin sonucu olarak karşımıza çıkmaktadır. Dijitalleşme ile birlikte gemilerin takibi ve güvenilir haberleşme ağı sayesinde lojistik ve tedarik süreçlerinin yönetimi daha kolay hale gelmiştir. Böylece zamandan tasarruf sağlanarak, maliyette en aza indirilebilmiştir.

Dijitalleşme siber saldırı girişimlerini de beraberinde getirmektedir. Kötü amaçlı yazılımlar ile gemiye ait tüm verilere ulaşılarak fidye talep edilebilir, gemi seyir sistemleri devre dışı bırakılarak rotası değiştirilerek korsanların hedefi haline gelebilir. Bu durum hem gemi hem de içindeki personel için risk oluşturmaktadır. Sonuç olarak denizcilik sektörü yeniliklere açık olmalı ve dijitalleşme süreçlerini yakından takip etmelidir. Dijitalleşmenin sonucu olarak karşımıza çıkan siber saldırı sorununu çözebilmek adına, personellere bu konuda belli periyotlarda eğitimler düzenlenmesi, siber güvenlik uzmanlarının sektörde istihdamının artırılması ve güvenilir yazılımların kullanılması önem arz etmektedir.

Bu çalışma; denizcilik sektöründe çalışan gemi insanlarının dijitalleşme ve siber güvenlik algılarını ölçmeyi hedeflemiştir. Araştırmada elde edilen bulgular göstermektedir ki, denizcilik sektöründe çalışmakta olan katılımcıların büyük çoğunluğu dijitalleşme süreçlerini desteklemektedir. Katılımcılar, dijitalleşmenin zaman tasarrufu ve iş kolaylığı sağlamasının yanı sıra verimliliği artırdığı ve maliyetleri azalttığı konusunda da görüş bildirmişlerdir. Dijitalleşme ile ilgili olumlu görüş bildiren katılımcılar, siber güvenlik konusunda gerekli önlemlerin alınması ve personellere bu konuda verilen veya verilecek olan eğitimlerin nitelikli ve denetlenebilir olması gerektiğini ifade etmişlerdir.

Araştırmanın kısıtları ise denizcilik sektöründe çalışmakta olan gemi insanlarına ulaşmakta yaşanan zorluk nedeniyle katılımcı sayısının az olmasıdır. Konu ile ilgili literatür tarandığında denizcilik sektöründe dijitalleşme ve siber güvenlik ile ilgili az sayıda çalışma yapılmıştır. Bu bağlamda daha büyük örneklemlerde, geniş kapsamlı çalışmaların yapılması denizcilik sektörüne ışık tutacaktır.

ARAŞTIRMACI KATKI ORANI BEYANI

Yazarların çalışmaya katkı oranları eşittir.

DESTEK VE TEŞEKKÜR BEYANI

Çalışma herhangi bir destek almamıştır. Teşekkür edilecek kurum veya kişi yoktur.

ÇIKAR ÇATIŞMASI BEYANI

Çalışma kapsamında herhangi bir kurum veya kişi ile çıkar çatışması bulunmamaktadır.

KAYNAKLAR

Balık, İ., Aydın, S. Z., Bitiktaş, F. (2021). Liman hizmetleri markalarının dijitalleşme gündemi: Çevrim İçi Medya İçerik Analizi. Dokuz Eylül Üniversitesi Denizcilik Fakültesi Dergisi, 13(2), 267-298. https://doi.org/10.18613/deudfd.787013

Bolat, F. (2021). Denizcilik eğitiminde kullanılan simülatörlerin dünya çapında dağılımı. Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi, 4(1), 1-15. https://doi.org/10.51513/jitsa.871903

Bahçe Özen, T. (2021). Türkiye'de denizcilik şirketlerinin dijitalleşme sürecindeki eğilimlerinin analizi. Doktora Tezi. İstanbul Üniversitesi Cerrahpaşa Lisansüstü Eğitim Enstitüsü Deniz Ulaştırma ve İşletme Mühendisliği Anabilim Dalı, İstanbul.

Cesur, H. (2020). Denizyolu taşımacılığında ve liman hizmetlerinde ilgili pazarın tanımlanması. Uzmanlık Tezleri Serisi No: 167, Rekabet Kurumu, Ankara.

Ceylan Çapar, M., Ceylan, M. (2022). Durum çalışması ve olgubilim desenlerinin karşılaştırılması. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 22 (Özel Sayı 2), 295-312. https://doi.org/10.18037/ausbd.1227359

Germir, H.N. (2022). Denizyolu taşımacılığının önemi ve sektöre yönelik kullandırılan banka kredileri: Türkiye örneği. https://tasam.org/tr-tr/ıcerik/70131/denizyolu_tasimaciliginin_onemi_ve_sektore_yonelik_kullandirilan_banka_kredileri_turkiye_ornegi. Erişim Tarihi: 6.11.2023

Gürler, H,E. (2022). Denizde siber güvenliğe ilişkin gelişmeler: Türkiye ve Yabancı Devletler açısından https://tasam.org/tr-tr/ıcerik/70130/denizde_siber_guvenlige_iliskin_gelismeler_turkiye_ve_yabanci_devletler_acisindan. Erişim Tarihi: 15.11.2023

Lagouvardou, S. (2018). Maritime cyber security: concepts, problems and models [Technical University İn Denmark]. in Master Thesis (Issue July). https://backend.orbit.dtu.dk/ws/portalfiles/portal/156025857/lagouvardou_mscthesis_final.pdf

Kara, H. (2020). Gemilerde yapay zekâ kullanımı ve buna dair hukuki sorunlar. Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, 10(1), 17-51.

Koldemir, B., Yapıcı, M., Keleştemur, A. (2017). Deniz taşımacılığında siber güvenliği tehdit eden unsurlar ve koruma önlemleri üzerine bir çalışma. III. Ulusal Liman Kongresi Doi: 10.18872/deu.df.ulk.2017.017 (Tam Metin)

Napolitano, A., Pedrazzoli, A. (2019). Skills development model towards maritime ındustry. School of Industrial Engineering.

Özdemir, Ü. (2015). Tarihte Türk denizcilik faaliyetleri ve günümüz limanlarının gelişim sürecine olan etkisinin incelenmesi. Ordu Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Araştırmaları Dergisi, 5(12), 421-441.

Şakar C., Köseoğlu. B., Büber M. ve Töz A. (2019). Are the ships fully secured against the cyber-attacks?. Dokuz Eylul University Maritime Faculty: 6.

Topal, O. (2020). Denizcilikte siber güvenlik: Türk gemi işletmecileri üzerine bir inceleme. Yüksek Lisans Tezi. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Deniz Ulaştırma İşletme Mühendisliği Anabilim Dalı, İzmir

Ültay, E., Akyurt, H. & Ültay, N. (2021). Sosyal Bilimlerde Betimsel İçerik Analizi. IBAD Sosyal Bilimler Dergisi, (10), 188-201. Doı: 10.21733/ibad.871703

Yangal, Y. (2022). Türkiye'de 2017 – 2021 Yılları Arasında Uluslararası Denizyolu Taşımacılığının Uluslararası Ticaretteki Yeri ve Önemi, Yüksek Lisans Tezi, Yaşar Üniversitesi Lisansüstü Eğitim Enstitüsü, İzmir.

Yanık, D.A. (2022). Denizcilikte siber risklerin değerlendirilmesi ve yönetimi. Yüksek Lisans Tezi. Kocaeli Üniversitesi Denizcilik İşletmeleri Yönetimi Anabilim Dalı. Kocaeli

Yıldız Tonga, M.,Tonga, M. (2022). Endüstri 4.0'a genel bir bakış: Sanayinin geleceği. G.Ü. İslâhiye İİBF Uluslararası E-Dergi, 6(6), 40-60.

Yorulmaz, M., Patruna, E. (2021). Liman işletmelerinde dijitalleşmeden beklentiler ve yöneticilerin bakış açısı. International Journal of Management and Administration, 5(9), 118-131.

Yurdakul, E. M. (2023). Türkiye'nin Deniz Yoluyla Uluslararası Ticareti ve Ekonomik Büyüme İlişkisi. Turkish Journal of Maritime and Marine Sciences, 9(1), 22-29. https://doi.org/10.52998/trjmms.1205937