

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

**DENİZCİLİK SEKTÖRÜNDE GERÇEKLEŞEN SİBER SALDIRILARDAN
TAŞIYANIN SORUMLULUĞU**

YÜKSEK LİSANS TEZİ

Melis GEDİKOĞLU

Denizcilik Çalışmaları Anabilim Dalı

Denizcilik Çalışmaları Programı

Tez Danışmanı: Doç. Dr. Pelin BOLAT

ŞUBAT 2023

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

**DENİZCİLİK SEKTÖRÜNDE GERÇEKLEŞEN SİBER SALDIRILARDAN
TAŞIYANIN SORUMLULUĞU**

YÜKSEK LİSANS TEZİ

**Melis GEDİKOĞLU
(423201004)**

Denizcilik Çalışmaları Anabilim Dalı

Denizcilik Çalışmaları Programı

**Tez Danışmanı: Doç. Dr. Pelin BOLAT
Eş Danışman: Dr. Belma BULUT**

ŞUBAT 2023

İTÜ, Lisansüstü Eğitim Enstitüsü'nün 423201004 numaralı Yüksek Lisans Öğrencisi Melis GEDİKOĞLU, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı “DENİZCİLİK SEKTÖRÜNDE GERÇEKLEŞEN SİBER SALDIRILARDAN TAŞIYANIN SORUMLULUĞU” başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Doç. Dr. Pelin BOLAT**
İstanbul Teknik Üniversitesi

Eş Danışman : **Dr. Belma BULUT**
Essex University

Jüri Üyeleri : **Dr. Öğr. Elif BAL BEŞİKÇİ**
İstanbul Teknik Üniversitesi

Jüri Üyeleri : **Dr. Öğr. Dinçer BAYER**
Piri Reis Üniversitesi

Jüri Üyeleri : **Dr. Öğr. Melek ERTÖĞAN**
İstanbul Teknik Üniversitesi

Teslim Tarihi : **30 Aralık 2022**
Savunma Tarihi : **10 Şubat 2023**



ÖNSÖZ

Deniz güvenliğinin siber tehditler kapsamında değerlendirilmesi bahsi, denizcilik endüstrisinde gerçekleşen teknolojik dönüşümün sonucu olarak büyük önem kazanmıştır. Bu durum, denizcilik sektöründe gerçekleşen siber saldırılardan sektördeki büyük ticari aktörlerin etkisi deniz alanlarının da dışına yayılan büyük maddi kayıplara uğramasına sebep olmuştur.

Bu çalışmada multidisipliner bir bakış açısıyla sorunlar tespit edilmeye çalışılmış ve henüz kapsamı çizilmemiş bir alan olan denizcilik sektöründe gerçekleşen siber saldırılardan taşıyanın sorumluluğu bahsinin önemli olduğu düşünülmüştür.

Hem akademik eğitim sürecimde hem tez yazımı sürecimde, farklı bakış açısıyla denizcilik sektörüne bakış açımı genişleten ve geliştiren, kıymetli vaktini ayırarak bana yardımcı olan Sayın Hocam Doç. Dr. Pelin BOLAT'a ne kadar teşekkür etsem az.

Tüm tez yazım sürecinde nazımı çeken, bana destek olan değerli Ailem'e, Zelal'e ve strese girdiğim anlarda beni rahatlatan tüylü dostum Pan'a sonsuz teşekkürlerimi sunarım.

Aralık 2022

Melis Gedikoğlu
Avukat



İÇİNDEKİLER

Sayfa

ÖNSÖZ.....	v
İÇİNDEKİLER	vii
KISALTMALAR	ix
ÇİZELGE LİSTESİ.....	xiii
ŞEKİL LİSTESİ.....	xv
ÖZET	xvii
SUMMARY	xix
1. GİRİŞ	1
1.1 Tezin Amacı	2
1.2 Denizcilik Ekonomisi, Deniz Güvenliği ve Siber Güvenlik	2
1.2.1 Dünya denizcilik ekonomisi.....	2
1.2.2 Deniz güvenliği	5
1.2.3 Siber güvenlik ve siber saldırı kavramı.....	9
2. BİLİŞİM SUÇLARI VE DENİZCİLİK BİLİŞİM SİSTEMLERİ.....	15
2.1 Bilişim Suçları	15
2.1.1 Denizcilik Bilişim Sistemleri	17
2.1.1.1 Denizcilik sektöründe kullanılan temel sistemler	19
2.1.1.2 Sistemleri yönelik gerçekleştirilebilecek siber saldırılara ilişkin güvenlik zaafiyetler ve oluşabilecek sonuçlar.....	24
2.1.1.3 Denizel alanda siber haydutluğun uluslararası niteliği	27
3. LİTERATÜR TARAMASI.....	29
3.1 Mevzuatın Tarihsel Gelişim	29
3.2 Taşıyanın Sorumluluğu Değerlendirmesi.....	35
3.2.1 Taşıyan kavramı	35
3.2.2 Taşıyanın sorumluluğunun uluslararası konvansiyonlar ve Türk hukuku kapsamında değerlendirilmesi.....	36
3.2.3 Mutlak sorumsuzluk sebepleri	42
4. METODOLOJİ	45
4.1 AHP Metodu.....	45
4.2 AHP Yapısının Oluşturulması.....	46
4.3 AHP Değerlendirme Formu ve Datalar	47
4.4 Bulgular	49
4.4.1 A faktörü için AHP analizi.....	49
4.4.2 B faktörü için AHP analizi	50
4.4.3 C faktörü için AHP analizi	50
4.4.4 E faktörü için AHP analizi	52
4.4.5 F faktörü için AHP analizi	53
4.4.6 Main factors	54
4.7 Benzer Vakalar	56
5. SONUÇ VE DEĞERLENDİRMELER.....	59
KAYNAKLAR	63
ÖZGEÇMİŞ.....	70



KISALTMALAR

AB	: Avrupa Birliđi
ACM	: Yetersiz Endüstriyel İndeksleme Sistemleri Analog Kontrolör
AFS	: Gemilerdeki (Zarar Verici) Zehirli Boya Sistemlerinin Kontrolüne İlişkin Uluslararası Sözleşme
AHP	: Analitik Hiyerarşı Prosesi
AIS	: Otomatik Tanımlama Sistemi
BM	: Birleşmiş Milletler
BIMCO	: Baltık ve Uluslararası Denizcilik Konseyi
BMDHS	: Birleşmiş Milletler Deniz Hukuku Sözleşmesi
BT	: Bilgi Teknolojisi
BWM	: Gemi Balast Suyu ve Sedimanlarının Kontrolü ve Yönetimi Hakkında Uluslararası Sözleşme
CI	: Tutarlılık Göstergesi (Consistency Index)
CLC	: Petrol Kirliliğinden Dođan Zararın Hukuki Sorumluluđu ile İlgili Uluslararası Sözleşme
CLIA	: Uluslararası Yolcu Gemileri Birliđi
COLREG	: Denizde Çatmanın Önlenmesine İlişkin Uluslararası Kurallar Hakkında Sözleşme
CR	: Tutarlılık Oranı (Consistency Rate)
CSC	: Emniyetli Konteynerler Hakkında Uluslararası Sözleşme
CTOC	: Uluslararası Örgütlü Suça Karşı Sözleşme (Countering Transnational Organized Crime)
DDoS	: Dağıtılmış Hizmet Reddi
DOC	: Uyumluluk Belgeleri
ECDIS	: Elektronik Harita Görüntüleme ve Bilgi Sistemi
FAL	: Uluslararası Deniz Trafiğinin Kolaylaştırılması Sözleşmesi
FAO	: Birleşmiş Milletler Gıda ve Tarım Örgütü (Food and Agriculture Organization of the United Nations)
FUND	: Petrol Kirliliği Zararlarının Tazmini İçin Uluslararası Bir Fonun Kurulmasına İlişkin Uluslararası Sözleşme
GDPR	: Genel Veri Koruma Yönetmeliđi
GMDSS	: Küresel Deniz Tehlike ve Güvenlik Sistemi

GNSS	: Küresel Navigasyon Uydu Sistemi
GPS	: Küresel Konumlandırma Sistemi
HK	: Hamburg Kuralları
HNS	: Tehlikeli ve Zararlı Maddelerin Deniz Yoluyla Taşınmasından Doğan Kirlilik Zararlarının Tazmini ve Sorumluluğa İlişkin Uluslararası Sözleşme
ICS	: Küresel Endüstriyel Kontrol Sistemleri
ICS	: Bilgi ve Haberleşme Sistemleri
IEC	: Uluslararası Elektroteknik Komisyonu
ILO	: Uluslararası Çalışma Örgütü
IMO	: Uluslararası Denizcilik Örgütü
ISM	: Uluslararası Emniyet Yönetim Kodu
IoT	: Nesnelerin İnterneti
IP	: İnternet Protokolü
ISPS	: Uluslararası Gemi ve Liman Tesisi Güvenlik Kodu
IT	: Enformasyon Teknolojileri
ISO	: Uluslararası Standardizasyon Örgütü
MARPOL	: Gemilerden Kaynaklanan Kirliliğin Önlenmesine İlişkin Uluslararası Sözleşme
MSC	: Deniz Emniyeti Komitesi
NATO	: Kuzey Atlantik Antlaşması Örgütü
NIST	: Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü'nün Kritik Altyapı Siber Güvenliğini Geliştirme Çerçevesi
OT	: Operasyonel Teknoloji
PAL	: Yolcuların ve Bagajların Deniz Yoluyla Taşınmasında Hakkında Atina Sözleşmesi
SATCOM	: Uydu Haberleşme Sistemleri
SALVAGE	: Uluslararası Kurtarma Sözleşmesi
SAR	: Denizde Arama ve Kurtarma Uluslararası Sözleşmesi
SDR	: Özel Çekme Hakkı
SOLAS	: Uluslararası Denizde Can Güvenliği Sözleşmesi (International Convention for the Safety of Life at Sea)
SUA	: Deniz Seyrinin Güvenliğine Karşı Hukuk Dışı Eylemlerin Önlenmesi Sözleşmesi (Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation)
STCW	: Gemiadamları için Eğitim, Belgelendirme ve Vardiya Tutma Standartları Hakkında Uluslararası Sözleşme
TBK	: Türk Borçlar Kanunu

TCP/IP	: Transmission Control/Internet Protocol
TTK	: Türk Ticaret Kanunu
UGYK	: Uluslararası Güvenlik Yönetim Kodu
UNCLOS	: Deniz Hukuku Üzerine Birleşmiş Milletler Sözleşmesi (United Nations Convention on the Law of the Sea)
VSAT	: Küçük Çaplı Uydu İstasyonu
VSS	: Video Gözetim Sistemleri
VMS	: Gemi İzleme Sistemi
W	: Ağırlık Vektörü (Weight)
WRC	: Enkaz Kaldırma Sözleşmesi





ÇİZELGE LİSTESİ

Sayfa

Çizelge 2.1: Siber tehdit çeşitleri.....	16
Çizelge 2.2: Siber suçların sınıflandırılması ve siber suç işleme yöntemleri.	16
Çizelge 2.3: AIS.	19
Çizelge 2.4: ECDIS.	19
Çizelge 2.5: GPS ve GNSS.....	20
Çizelge 2.6: RADAR.....	21
Çizelge 2.7: GMDSS.	21
Çizelge 2.8: ICS'ler.	21
Çizelge 2.9: VSAT.	21
Çizelge 2.10: Sevk ve makine yönetimi ve güç kontrol sistemleri.....	22
Çizelge 2.11: Video gözetim sistemi.	23
Çizelge 2.12: BT ağ sistemleri.	23
Çizelge 2.13: Sistemler/zaafiyetler/sonuçlar.	25
Çizelge 3.1: IMO düzenlemeleri.....	33
Çizelge 4.1: AHP alt ve ana boyutlar.	47
Çizelge 4.2: Faktörü için AHP analizi (1).	49
Çizelge 4.3: A faktörü için AHP analizi (2).	49
Çizelge 4.4: A faktörü için AHP analizi (3).	49
Çizelge 4.5: B faktörü için AHP analizi (1).	50
Çizelge 4.6: B faktörü için AHP analizi (2).	50
Çizelge 4.7: B faktörü için AHP analizi (3).	50
Çizelge 4.8: C faktörü için AHP analizi (1).	50
Çizelge 4.9: C faktörü için AHP analizi (2).	51
Çizelge 4.10: D faktörü için AHP analizi (2).	51
Çizelge 4.11: D faktörü için AHP analizi (3).	51
Çizelge 4.12: E faktörü için AHP analizi (1).....	52
Çizelge 4.13: E faktörü için AHP analizi (2).....	52
Çizelge 4.14: E faktörü için AHP analizi (3).....	52
Çizelge 4.15: F faktörü için AHP analizi (1).....	53
Çizelge 4.16: F faktörü için AHP analizi (2).....	53
Çizelge 4.17: F faktörü için AHP analizi (3).....	53
Çizelge 4.18: Main factors (1).....	54
Çizelge 4.19: Main factors (2).....	54
Çizelge 4.20: Main factors (3).....	54



ŞEKİL LİSTESİ

	<u>Sayfa</u>
Şekil 1.1: Ele alınan konular.....	2
Şekil 1.2: Denizcilik riskleri matrisi.....	8
Şekil 4.1: AHP karar verme süreci.	47





DENİZCİLİK SEKTÖRÜNDE GERÇEKLEŞEN SİBER SALDIRILARDAN TAŞIYANIN SORUMLULUĞU

ÖZET

İnsanlık yüzyıllardan beri denizlerden iki amaçla yararlanmaktadır. Birincisi ulaşım ve iletişim, diğeri deniz doğal kaynaklarının ve zenginliklerinin kullanılması ve işletilmesi. Bu amaçlar doğrultusunda deniz ticaretinde verimliliği arttırmak adına pek çok teknolojik gelişme yaşanmış ve denizcilik sektöründe yaşanan bu teknolojik dönüşüm, deniz ticaretinin gelişmesine sunduğu katkının yanı sıra pek çok siber riski de ortaya çıkarmıştır. Yeryüzünün dörtte üçünün deniz alanları ile kaplı olması bu alanların hukuki rejiminin tespit edilmesi ve bu alanlardaki faaliyetleri düzenleyen kuralların gerekliliğini de ortaya çıkarmıştır. Siber güvenlik, tüm denizcilik sektörü için en güncel ve potansiyeli yüksek sorunlardan birisidir. Küresel salgın sırasında tüm sektörlerle birlikte denizcilik endüstrisinin artan dijitalleşmesiyle son zamanlarda denizcilik sektöründe gerçekleşen siber saldırıların sayısı da artış göstermiştir. Bu çalışmada, denizel alanda gerçekleşen siber saldırılardan taşıyanın sorumluluğu cezai ve ticari yönden ayrı ayrı incelenecek ve denizcilik siber altyapılarının ortaya çıkardığı potansiyel riskler tartışılacaktır.

Denizcilik sektörünün uluslararası niteliği gereği uluslararası mevzuat düzenlemelerine ihtiyaç duyulmakta iken 1982 tarihli Birleşmiş Milletler Deniz Hukuku Sözleşmesi halen deniz hukukuna ilişkin hususları en ayrıntılı şekilde düzenleyen sözleşmedir. Ancak sözleşme güncel gelişmelere ve ihtiyaçlara cevap vermekten oldukça uzaktır. International Maritime Organization ise, Birleşmiş Milletler'in deniz taşımacılığını düzenlemekten sorumlu özel bir kuruluştur. Çalışma kapsamında deniz siber güvenliğine ilişkin yapılan uluslararası düzenlemeler ve International Maritime Organization düzenlemeleri kapsamında “Denizcilik Sektöründe Gerçekleşen Siber Saldırılarından Taşıyanın Sorumluluğu” bahsi değerlendirilmiştir. Çalışmada Analitik Hiyerarşi Süreci metodu uygulanmıştır. Analitik Hiyerarşi Süreci ikili karşılaştırmalar sunarak karar vermede etkili kriterlerin önem derecelerinin ve karar alternatiflerinin kendi aralarındaki hiyerarşiyi sıralamaktadır. Denizcilik Sektöründeki Dijital Dönüşümün Deniz Ticaretine Etkileri başlığı altında teknolojik gelişmeler, siber saldırı, siber saldırılardan taşıyanın ticari sorumluluğu, siber saldırılardan taşıyanın cezai sorumluluğu ve IMO düzenlemeleri olmak üzere 5 ana kriter olarak belirlenmiştir.

Anahtar Kelimeler: Deniz Güvenliği, Siber Güvenlik, Taşıyanın Sorumluluğu, Gemilerde Teknolojik Dönüşüm, Bilişim Sistemleri



CARRIER'S LIABILITY FOR CYBER ATTACKS IN THE SHIPPING SECTOR

SUMMARY

Humanity has been benefiting from the seas for two purposes for centuries. The first is transportation and communication, the other is the use and operation of marine natural resources and riches. In line with these purposes, many technological developments have been experienced in order to increase efficiency in maritime trade, and this technological transformation in the maritime sector has revealed many cyber risks as well as its contribution to the development of maritime trade. The fact that three quarters of the earth is covered by sea areas has also revealed the necessity of determining the legal regime of these areas and the rules regulating the activities in these areas. Cyber security is one of the most current and potential problems for the entire maritime industry. With the increasing digitalization of the maritime industry along with all sectors during the global epidemic, the number of cyber attacks in the maritime sector has increased recently. This study aims to identify the different dimensions and risks regarding the carrier's liability for cyber-attacks at sea and to provide new solutions to address them. The current national and international cyber security regulations are far from providing solutions for the maritime sector. The fact that cybercrimes are borderless in nature and can be carried out even with a simple tool increases the size and impact of the threat. In this study, the responsibility of the carrier for cyber attacks in the maritime sector will be examined separately from criminal and commercial aspects, and the potential risks posed by maritime cyber infrastructures will be discussed. The technology needed to conduct a cyber-attack on a ship is becoming more and more widespread, and access to this information is becoming easier. Cyber-attacks, according to one definition, are "activities carried out in cyberspace with the aim of exploiting, disrupting, changing information in cyberspace, preventing access to systems or causing damage". According to another definition, cyber-attack is defined as "rendering information systems inoperable by attackers, compromising the security or reliability of information systems, corrupting or stealing them". Nowadays, there are many examples of cyber-attacks on maritime transportation. Examples of attacks that can be exposed include hackers interfering with the navigation system or GPS system of a ship carrying chemical cargo, causing a collision, and the many safety and security consequences that result. The hazards that may arise as a result of this collision may arise as environmental pollution, loss of profit due to interruption of activities, discontinuation of port activities, total loss or damage to the ship, bodily injury or death of seamen or passengers, loss or damage to cargo. From my personal stand point, the carrier is liable for the damages suffered as a result of cyber-attacks in two ways. The first one is the commercial liability of the carrier arising from the contract and the other one is the criminal liability of the carrier against third parties. The liability of the carrier to the cargo owner under the freight contract between them is regulated in many international conventions and our domestic law; in which cases liability will arise, and in which cases absolute

irresponsibility will exist, are outlined. The Turkish Commercial Code regulates the carrier's liability for damages arising from loss or damage to the goods or late delivery of the goods due to certain reasons such as failure to keep the ship in a seaworthy, seaworthy and loadable condition at the outset, loading and transferring the goods to another ship without authorization, unauthorized carriage of goods on deck and departure from the route without a justifiable reason. It could be argued that, the voyage of the ship with cyber security vulnerabilities should be evaluated within the scope of the carrier's responsibility to keep the ship initially seaworthy. While international legislation is needed due to the international nature of the maritime sector, the 1982 United Nations Convention on the Law of the Sea is still the convention that regulates matters related to the law of the sea in the most detailed way. However, the contract is far from responding to current developments and needs. The International Maritime Organization is a private agency of the United Nations responsible for regulating maritime transport. Within the scope of the study, the issue of "The Responsibility of the Carrier for Cyber Attacks in the Maritime Industry" has been evaluated within the scope of the international regulations on maritime cyber security and the International Maritime Organization regulations. The Analytical Hierarchy Process method has been used in the study. Analytical Hierarchy Process presents pairwise comparisons and ranks the hierarchy among the importance levels of effective criteria and decision alternatives in decision making. Under the title of Effects of Digital Transformation on Maritime Trade in the Maritime Sector, 5 main criteria have been determined as technological developments, cyber attacks, commercial liability of the carrier for cyber attacks, criminal liability of the carrier for cyber attacks and IMO regulations. The prioritization of the sub-dimensions of the main dimension of Technological Developments is as follows; 1. Transfer of documents related to maritime trade to the interactive environment (0.24), 2. Continuous and fast data flow as a result of faster operation and mechanization of ships (0.19), 3. Powerful data solutions enabled by the cloud revolution in data storage and hardware (0.10), 4. Real information about the performance of a ship hundreds of miles from shore, thanks to improved ship-to-shore connectivity (0.10). Due to the international nature of maritime areas and the nature of cyber-attack crimes, which are transnational crimes, it is obvious that an international legal regulation is necessary. The increasing impact of globalization in the 90s laid the foundations for transnational crime to take on a more international character in the years to come. From this point of view, it is necessary to regulate who will be penalized for cyber-attacks in the maritime area and how, or what kind of liability will arise in case of defective performance in the contracts between the parties, through an international regulation. Otherwise, the actor of a cyber-attack on the carrier may be very large competitors, but due to the difficulty of identifying the source of the cyber-attacks due to the nature of the cyber-attacks, the perpetrators cannot be identified and the carrier will be left with many criminal and commercial problems.

Keywords: Maritime Security, Cyber Security, Carrier's Liability, Technological Transformation on Ships, Information Systems



1. GİRİŞ

1870-1913 dönemi, ticaretin küreselleşmesine adım atılan dönemdir. 1820 ve 1913 yılları arasında dünya ticaretinde, 1870'de başlayan belirgin bir ivme ile eş görülmemiş bir artış yaşanmıştır. Bu küreselleşme dalgası, 19. Yüzyılda dünya ticareti modelini şekillendiren buharlı gemilerin ortaya çıkması ile yayılmaya başlamıştır. Ekonomik anlamda bu ilişkilerin istatistiksel olarak değerlendirilmesinde; 1970 yılında deniz yoluyla 2.605 milyar ton yük taşındığı görölmekteyken bu sayının 2019 yılında 11.076 milyar tona yükseldiği görölmektedir[1].

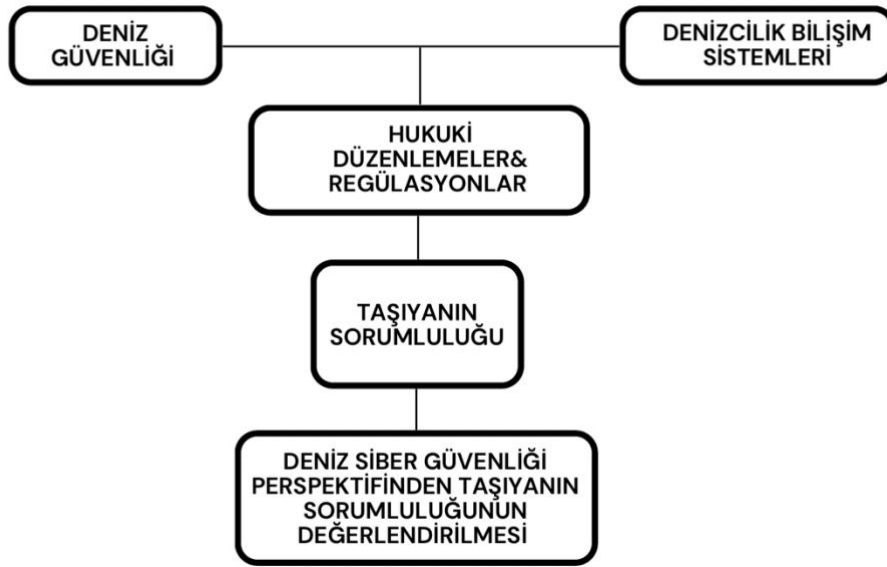
Günümüzün küresel denizcilik sektörü, dijitalleşme, operasyonel entegrasyon ve otomasyona giderek daha fazla bağımlı hale gelmektedir. Önde gelen gemi imalatçıları ve gemi işletmecileri, gelişmiş uzaktan kumanda, iletişim ve bağlantı yeteneklerine sahip gemiler ortaya çıkarmak için geleneksel tasarımların ötesine geçen son teknolojileri ve sistemleri kullanarak yenilikler yapmaya çalışmaktadır.

Özellikle son yıllarda gerçekleşen dijitalleşme, deniz taşımacılığı kapasitelerinde bir artış meydana getirirken gemilerin de daha iyi kontrol edilmesine olanak sağlamış ve sektöre kar optimizasyonu vaadi vermiştir. 2022 yılına gelindiğinde denizcilik sektöründe ciddi bir dijital yatırım ve dönüşüm gerçekleştiği ortadadır. Pandemi ile birlikte yeni sorunlar ve bunların karşılığında dijital çözümler denizcilik sektörünün gündemini fazlasıyla meşgul etmektedir. Karantina sonrası artan kargoların oluşturduğu liman yoğunlukları, yapay zekaya bağı elleçleme faaliyetlerinin önemini ortaya çıkarmıştır. Yapay zekaların liman yönetimi ve gümrük faaliyetlerine de büyük katkı sağlaması beklenmektedir. Aynı zamanda pandemi teknolojik dönüşümü hızlandırmış ve denizcilik sektörü de konişmento ve diğer kıymetli evraklar ve ödeme sistemleri ile ilgili dijital çözümlere yönelme ihtiyacı içinde olmuştur. Bunun sonucunda önümüzdeki yıllarda blockchain teknolojilerinin hem ticari işlemlerde hem de denizcilik sigortası endüstrisi tarafından yoğun bir şekilde benimsenmesi mümkün görönmektedir.

Dijital iletişime, otomasyona ve küresel ekonominin gelişmesine ilişkin oluşan güven algısı, siber güvenliği yalnızca bir ulusal güvenlik sorunu değil, aynı zamanda küresel bir endişe kaynağı haline getirmektedir. Kötü amaçlı yazılımlar, siber suçlar ve veri sızıntıları dahil olmak üzere ortaya çıkan tüm siber tehditler, devletleri ve denizcilik endüstrisini benzer şekilde etkileme potansiyeli taşımaktadır.

1.1 Tezin Amacı

Bu çalışma ile amaçlanan, deniz güvenliği ve denizcilik bilişim sistemlerinin zayıf noktalarının tespit edilerek, olası siber saldırı durumunda taşıyanın sorumluluğu bahsine ilişkin güncel düzenlemelerin saptanması, henüz düzenlenmemiş hukuki alanlar ile ilgili çözüm önerileri ve değerlendirmelerin sunulmasıdır.



Şekil 1.1: Ele alınan konular.

1.2 Denizcilik Ekonomisi, Deniz Güvenliği ve Siber Güvenlik

1.2.1 Dünya denizcilik ekonomisi

1870-1913 dönemi, ticaretin küreselleşmesine adım atılan dönemdir. 1820 ve 1913 yılları arasında dünya ticaretinde, 1870'de başlayan belirgin bir ivme ile eş görülmemiş bir artış yaşanmıştır. Bu küreselleşme dalgası, 19. Yüzyılda dünya ticareti modelini şekillendiren buharlı gemilerin ortaya çıkması ile yayılmaya başlamıştır. Maritime Transport 2020 raporuna göre, ekonomik anlamda bu ilişkilerin istatistiksel

olarak değerlendirilmesinde açıklanan verilerde, 1970 yılında deniz yoluyla 2.605 milyar ton yük taşındığı görülmekteyken bu sayının 2019 yılında 11.076 milyar tona yükseldiği görülmektedir[2].

Global ticaretin 1990lı yıllardan itibaren ivme kazanması ile firmaların ülkeler arası ticari faaliyetleri artış göstermiş böylece taşımacılık büyük önem kazanmıştır. Global dünya ticaretinin büyük bir kısmı deniz taşımacılığı yoluyla gerçekleştirilmekte ve deniz taşımacılığının diğer ulaşım modlarına göre büyük avantajları bulunmaktadır. Deniz taşımacılığı, düşük maliyetlerin yanı sıra büyük hacimli yüklerin tek seferde taşınabilmesi ve diğer ulaşım modlarına göre daha emniyetli olması sebebiyle tercih edilmektedir. Tüm denizcilik faaliyetlerinin aşağı yukarı üçte biri ticari denizcilikten kaynaklanmaktadır. Stopford'a göre denizcilik sektörü beş ana gruba ayrılmaktadır. Bunlar gemi işletmeciliği faaliyetiyle gemilerle doğrudan faaliyet gösterenler, gemi inşa ve deniz mühendisliği, açık deniz petrol ve gaz platformları, yenilenebilir enerji ve mineralleri içine alan deniz kaynakları, su kültürü ve deniz mahsüllerini içine alan su ürünleri ile balıkçılık ve turizm vb. hizmetleri içine alan diğer faaliyetler olarak sıralanır[3].

Gelişmiş ekonomiler politika faizi oranlarını yükselttikçe, finansal istikrara ve yükselen piyasa ve gelişmekte olan ekonomilerin sermaye akışlarına, para birimlerine ve mali pozisyonlarına yönelik riskler – özellikle son iki yılda önemli ölçüde artan borç seviyeleri ile ortaya çıkabilecektir. Diğer küresel riskler, jeopolitik gerilimler yüksek kalmaya devam ettikçe belirginleşebilir ve devam eden iklim acil durumu, büyük doğal afet olasılığının yüksek kalmaya devam ettiği anlamına gelmektedir.

2021 yılı, ülkelerin deniz yolu taşımacılığına dair birçok yeni politika, fikir ve yaklaşım geliştirmesine imkan sağlamıştır. Pandeminin etkisiyle denizcilik şirketleri daha yalın, daha çevre dostu sistemler için filolarını yenilemeye ve geniş çaplı dönüşüm planları yapmaya başlamıştır. Deniz taşımacılığındaki dönüşüm büyük gemi şirketlerinin filolarına henüz geniş çapta yansımaya da uzun vadeli planlarında büyük yer tutmaktadır. Denizcilik sektörü yeni önlemleri benimseme konusundaki muhafazakar eğilimleri sebebiyle sektördeki dev şirketler çoğunlukla finansal sonuçlara odaklanarak politikalar üretmektedir.

Günümüzün küresel denizcilik sektörü, dijitalleşme, operasyonel entegrasyon ve otomasyona giderek daha fazla bağımlı hale gelmektedir. Önde gelen gemi imalatçıları

ve gemi işletmecileri, gelişmiş uzaktan kumanda, iletişim ve bağlantı yeteneklerine sahip gemiler ortaya çıkarmak için geleneksel tasarımların ötesine geçen son teknolojileri ve sistemleri kullanarak yenilikler yapmaya çalışmaktadır.

Özellikle son yıllarda gerçekleşen dijitalleşme, deniz taşımacılığı kapasitelerinde bir artış meydana getirirken gemilerin de daha iyi kontrol edilmesine olanak sağlamış ve sektöre kar optimizasyonu vaadi vermiştir. 2022 yılına gelindiğinde denizcilik sektöründe ciddi bir dijital yatırım ve dönüşüm gerçekleştiği ortadadır. Pandemi ile birlikte yeni sorunlar ve bunların karşılığında dijital çözümler denizcilik sektörünün gündemini fazlasıyla meşgul etmektedir. Karantina sonrası artan kargoların oluşturduğu liman yoğunlukları, yapay zekaya bağlı elleçleme faaliyetlerinin önemini ortaya çıkarmıştır. Yapay zekaların liman yönetimi ve gümrük faaliyetlerine de büyük katkı sağlaması beklenmektedir. Aynı zamanda pandemi teknolojik dönüşümü hızlandırmış ve denizcilik sektörü de konişmento ve diğer kıymetli evraklar ve ödeme sistemleri ile ilgili dijital çözümlere yönelme ihtiyacı içinde olmuştur. Bunun sonucunda önümüzdeki yıllarda blockchain teknolojilerinin hem ticari işlemlerde hem de denizcilik sigortası endüstrisi tarafından yoğun bir şekilde benimsenmesi mümkün görünmektedir.

Nesnelerin İnterneti'nin (IoT) giderek yaygınlaşması, özel şartlarda taşınması gereken yüklerin taşıma sırasındaki risk yönetiminin usulünü de değiştirecektir. Konteynerlerin içindeki kargonun gerçek zamanlı olarak izlenebilmesi, yalnızca özel şartlarda taşınması gereken yüklerin zarar görmesini azaltmakla kalmayacak, gemilerde tehlikeyi ve yangın riskini de azaltacaktır.

Dijital iletişime, otomasyona ve küresel ekonominin gelişmesine ilişkin oluşan güven algısı, siber güvenliği yalnızca bir ulusal güvenlik sorunu değil, aynı zamanda küresel bir endişe kaynağı haline getirmektedir. Kötü amaçlı yazılımlar, siber suçlar ve veri sızıntıları dahil olmak üzere ortaya çıkan tüm siber tehditler, devletleri ve denizcilik endüstrisini benzer şekilde etkileme potansiyeli taşımaktadır.

Küresel deniz ticaretini etkileyen ekonomik, siyasi ve sektörel parametrelere bir yenisi olarak deniz güvenliği eklenmiştir. Ülkelerin dış ticaretinin ana etmenini deniz taşımacılığı oluşturmaktadır. Deniz taşımacılığı ve deniz ticareti arasındaki doğrusal orantı, deniz taşımacılığındaki güvenlik sorununun önemini vurgulamaktadır. Dünya

ticaretinin sağlıklı büyümesi için deniz güvenliği çok büyük öneme haizdir. Deniz ticaretini etkileyen etmenler çok çeşitli olmakla birlikte başlıca;

1. Küresel deniz ticareti ve taşımacılığındaki yeni oluşumlar,
2. Enerji güvenliği,
3. Petrol fiyatları ve taşımacılık maliyetleri,
4. Uluslararası taşımacılıktan kaynaklanan karbon emisyonlarının azaltılması,
5. İklim değişikliği,
6. Sürdürülebilir çevre güvenliği,
7. Sosyal sorumluluk konusundaki iş birlikleri, Deniz haydutluğu ve buna ilişkin maliyetlerdir.

1.2.2 Deniz güvenliği

Dünya ticaretinin büyük bir kısmının diğer taşıma modlarına göre daha avantajlı olan deniz yoluyla taşınması sonucu denizlerde emniyet ve güvenlik kavramları büyük önem kazanmıştır. Dünyadaki nüfus artışına paralel olarak üretimin artması ve üretilen malların dünya çapında pazarlanması ile birlikte gemi trafiği artmaktadır. Bu bağlamda denizciler için önemli olan 2 temel soru vardır: 1) Gemiler ve yükler seyrüseferi güvenli bir şekilde nasıl tamamlar? 2) Gemi adamlarının güvenliği nasıl sağlanabilir?

Günümüz dünyasında güvenlik kaygıları, güvenliğin yalnızca fiziksel boyutuyla sınırlanmaktan çok uzaktır. Geçmişte gemiler limandan ayrıldıktan sonra yalnızca gemi insanı hatası, mekanik arızalar yahut doğal koşullar sebebiyle emniyet riski taşımaktaydı. Ancak kıyı tesisleriyle iletişimi sağlayan altyapıların devreye girmesi ve kullanımının yaygınlaşması ile birlikte gemiler için dijital çağ başlamıştır.

Dijitalleşme denizcilik sektörünü tamamen dönüştürmüş ve gemilerin kıyı ile iletişimleri büyük önem kazanmıştır. Ancak bu durum da deniz ortamında siber tehditlerin ortaya çıkmasına sebep olmuştur. İlerleyen bölümlerde siber güvenlik risklerine değinmeden önce deniz emniyeti ve güvenliği kavramlarının açıklanmasında fayda vardır.

Deniz emniyeti ve güvenliği, geçtiğimiz yıllarda Uluslararası Denizcilik Örgütü'nün (IMO) ana hedeflerinden biri olmuştur. Uluslararası Emniyet Yönetimi Kodu (ISM) ve Uluslararası Gemi ve Liman Tesisi Güvenlik Kodu (ISPS), gemi ve liman operasyonlarının yanı sıra kıyıdaki ve gemilerdeki personeli içeren çalışma ortamının

güvenliğini sağlamak için oluşturulmuştur. Her iki kod da gemilerin denizde can kaybı ve çevre felaketi gibi önemli sonuçları olan tehlikeli durumlarla karşılaşmasını önlemeyi amaçlayan risk tanımlama, kaza önleme ve acil durumlara odaklanmaktadır.

Deniz yolu taşımacılığında ticari faaliyetlerin aksamadan devam edebilmesi için taşınacak yükün niteliğine ve taşınma ihtiyacına uygun nitelikte gemilerin olması deniz ticaret piyasalarının etkinliğini ve yükün güvenli olarak bir limandan diğerine ulaşabilmesini sağlayacaktır[4].

Denizcilik faaliyetlerinin uluslararası niteliği ve aksamaların yarattığı kümülatif zararların büyüklüğü sebebiyle deniz güvenliğinin önemi artmıştır. Deniz güvenliği, denizcilik alanının güvenliğine atıfta bulunan bir kavram veya denizcilik alanını güvenceye almak için bir dizi politika, düzenleme, önlem ve operasyon olarak anlaşılabilir.

Kraska, James ve Pedrozo'nun deniz güvenliğine dair bakış açılarında hukuki ve siyasi perspektif farklılıklar göstermektedir. Kraska, James ve Pedrozo'nun hukuki bakış açısını odağına alan çalışmalarda deniz güvenliğinin tek bir tanımı olmadığı vurgulanırken denizde “özen” vurgusu öne çıkmaktadır[5].

Araştırmacılara göre “Deniz Güvenliği” geniş kapsamlı ve bazen belirsiz bir kavram gibi görülmektedir. Aslında bu, uluslararası kamu ve özel sektör kuruluşlarını içeren büyük bir araştırma konusudur. Araştırmacılara göre deniz güvenliğinin deniz ticaretine katkıları şu şekildedir;

- Denizlerin özgürlüğünü korumak,
- Ticareti kolaylaştırmak ve savunmak ve
- Denizde iyi yönetimi sürdürmek.

“Deniz Güvenliği”, Deniz Güvenlik Operasyonları söz konusu olduğunda net bir tanımı olmayan bir sorumluluktur. Denizel güvenlik geniş çaplı politikaları kapsayan evrensel bir alandır ve bu niteliği sebebiyle üzerinde uzlaşmış herhangi bir yasal tanımı yoktur. Deniz güvenliğinin parçası olan unsurlar ise şu şekilde sıralanabilir;

- Uluslararası/ulusal barış ve güvenlik
- Egemenlik, toprak bütünlüğü ve siyasi bağımsızlık
- Deniz Haberleşme Hatlarının Güvenliği
- Denizdeki suçlara karşı güvenlik koruması
- Kaynak güvenliği, denizdeki kaynaklara ve deniz tabanına erişim

- Çevresel koruma
- Tüm denizcilerin ve balıkçıların güvenliği.

Natalie Klein'a göre kullanan kişiye ya da kullanılan bağlama göre farklı anlamlara sahip olduğu düşünülen deniz güvenliği, devletlerin menfaatleri ve savunma stratejileriyle geleneksel deniz gücü kavramından daha geniş bir alanı kapsamaktadır[6]. Bu açıdan Klein'a göre deniz güvenliği, bir devletin topraklarıyla birlikte deniz alanlarını, alt yapısını, ekonomisini, çevresini ve en önemlisi toplumun denizden kaynaklanan zararlı fiillerden korunmasını kapsamaktadır[7].

Deniz güvenliğinin tanımları arasında deniz emniyeti ile arasındaki farka dayanılarak yapılan bir takım kavramsal açıklamalar da mevcuttur. Del Pozo'nun çalışmasına göre tehditler ile kasıtlı gerçekleştirilen yasa dışı fiillere karşı alınan önleyici tedbirlerin birleşimi olan deniz güvenliği(security) kavramı ile; deniz alanının kasıtlı olmayan kazalara ve doğal tehlikelere, çevreye verilen zararlara, risklere veya kayıplara karşı korunup sınırlandırmasını ilişkin deniz emniyeti(safety) kavramı farklıdır[8].

Deniz emniyeti, tesadüfi ve doğal tehlike, zarar veya hasar anlamına gelirken, deniz güvenliği kasıtlı olayları ifade eder. Deniz ortamında sivil havacılık sektörü kadar kanlı olaylarla dolu terör saldırıları olmasa da özellikle 11 Eylül saldırılarında sonra Dünya genelinde artan güvenlik endişeleri denizcilik sektöründe de yer bulmuştur. Deniz güvenliği dönemini başlatan şey aslında 11 Eylül saldırılarından çok daha önce 1961'de Santa Maria gemisinin kaçırılması ile dikkat çekmiş ancak Ekim 1985'te İtalyan yolcu gemisi Achille Lauro'nun Mısır kıyılarında "Filistin Kurtuluş Cephesi" tarafından ele geçirilmesiyle deniz güvenliği sorunu kendisini açıkça göstermeye başlamıştır. Filistin Kurtuluş Cephesi'nin 450 yolcuyla rehin alması ve rehinelere biri olan Bay Klinghoffer'ı idam edip ve denize atması ile sonuçlanan bu olayın temel unsuru, teröristlerin bu gemiyi bir yıkım aracı olarak kullanmak için kaçırmış olmalarıdır.

Genellikle deniz güvenliği, emniyet ve emniyetle ilgili hususların bir kombinasyonu olarak tanımlanmıştır. Önleme faktörleri göz önüne alındığında, öncelikle deniz güvenliğinin ana faktörleri ile birlikte tanımlanması gerekir. Başka bir tanıma göre deniz güvenliği, denizde can ve mal güvenliğinin çevresel ve operasyonel tehditlere karşı korunması ve deniz çevresinin gemilerden kaynaklanan kirlilikten korunmasıdır (Urbański, Morgaś & Mięsikowski, 2009). Akademik çalışmalara göre "Deniz

güvenliği” kavramı, ilk kez 11 Eylül terör saldırılarından sonra deniz terörizminin yayılmasından kaynaklı olarak kamuoyunun dikkati çekmiştir. Murphy ve Bueger’e göre deniz terörizmi veya deniz terörizmi tehdidinin uzun bir süre gerçekleşmeyecek, sanal bir tehdit olarak kalacağı algısı ise 2008 ve 2011 yılları arasında Somali kıyılarında korsanlığın artmasıyla yıkılmıştır[9].

Akademide deniz güvenliği kavramı, 2000’li yılların başına kadar denizcilik alanının güvenliği ile ilgili tartışmalarda neredeyse hiç yoktur. 2002 yılından bu yana, deniz güvenliği ile ilgili akademik literatürde deniz güvenliğine yapılan atıfların sayısı, aşağıdaki üç faktörün birleşimi ile açıklanabilir:

1. 11 Eylül terör saldırılarının etkileri (özellikle denizde terörle mücadele operasyonlarının başlatılması)
2. Gemilere karşı yüksek görünürlüklü üç terör eyleminin gerçekleşmesi (2001’de USS Cole, 2002’de Fransız tanker Limburg ve 2004’te Filipin yolcu gemisi SuperFerry 14)
3. Malakka Boğazı’ndaki korsan saldırılarının 21.yüzyılın başında artması[10].



Şekil 1.2: Denizcilik riskleri matrisi.

Gelişen dünya ticareti sonucu deniz ticaret filolarının kapasite yükseltmesi, gemilerin kapasitelerini ve verimliliklerini arttırmak adına teknolojik bağımlılıklarının artması, bilgi teknolojilerine bağımlılıklarının yüksek olması gibi sebepler denizcilik sektörünü siber risklere açık hale getirmiştir. Deniz taşımacılığında kullanılan OT ve IT sistemleri hedef alan saldırılar denizlerde güvenlik ve emniyet açısından büyük bir risk ve tehdit oluşturma potansiyeline haizdir. Bu saldırılar sonucu gemi, gemi insanları, yük, denizcilik ve liman altyapısı büyük zararlar görme riski altındadır.

Diğer taraftan siber saldırılar, iş prosedürlerinde aksamalara, finansal kayıplara ve denizcilik şirketleri ile devletlerin itibarının zedelenmesine de sebep olabilmektedir. Denizcilik sektöründeki tüm gelişmelere rağmen sektör para hırsızlığı, hassas veri hırsızlığı, aktivizm/terör eylemlerine yönelik tedbirler alma konusunda da hazır değildir[11].

Sonuç olarak, “Big Data”, akıllı gemiler ve 'Nesnelerin İnterneti'nin artan kullanımı, siber saldırganlar için mevcut bilgi miktarını ve siber suçlulara yönelik potansiyel saldırı alanını arttırmaktadır. Bu durum, siber güvenliğe ilişkin sağlam adımlar atılmasını ve hukuki düzenleme ihtiyacını önemli hale getirmektedir.

1.2.3 Siber güvenlik ve siber saldırı kavramı

Siber” terimi, basit olarak Bilgi Teknolojisi((BT) ve Operasyonel Teknoloji(OT) sistemlerinin birbirine bağlı ağlarını ifade etmektedir[12]. “Siber alan”, siber uzayda var olan bilgi, hizmetler, sosyal ve ticari işlevler olmak üzere elektronik, bilgisayar tabanlı ve kablosuz sistemleri kullanan hem BT hem de siber-fiziksel sistemlerin birbirine bağlı ağlarının içerir[13].

Siber güvenlik, Uluslararası Telekomünikasyon Birliği'nin raporuna göre siber çevreyi, organizasyonu ve kullanıcının bilgilerini korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, kılavuzlar, risk yönetimi yaklaşımları, eylemler, eğitim, optimum uygulamalar, güvence ve teknolojilerin toplamı olarak tanımlanabilecektir[14].

Bu tanım dahilinde, siber ortam, Bilgi Teknolojisi (BT) ile elektronik ve bilgisayar altyapısına sahip kablosuz sistemleri kullanan ağları içerir. Dünyadaki tüm bilgisayar ağları ile onların bağlı olduğu ve kontrol ettiği ortamdır.

Siber saldırı, bir tanıma göre “Siber alanda yer alan bilgileri istismar etmek, bozmak, değiştirmek, sistemlere erişimi engellemek ya da zarar vermek amacıyla siber alanda gerçekleştirilen faaliyetlerdir”[15]. Başka bir tanıma göre ise siber saldırı, “saldırganlar tarafından bilgi sistemlerinin çalışamaz hale getirilmesi, bilgi sistemlerinin güvenliğinin veya güvenilirliğinin riske atılması, bozulması ve çalınması”[16] şeklinde ifade edilmektedir.

Siber saldırılarda saldırı aracı olarak dijital araçlar kullanılır. Bu da aynı anda bir çok yerde siber saldırı eyleminin ışık hızında bir çok hedefi vurarak gerçekleştirilmesini mümkün kılmaktadır. Siber saldırının amaçlanan sonucu fiziksel bir hasar vermek olsa dahi hasar ilk olarak dijital ortamdaki bir eylemden ortaya çıkmaktadır[17].

Siber güvenlik, tüm denizcilik sektörü için en güncel ve potansiyeli yüksek sorunlardan birisidir. Küresel salgın sırasında tüm sektörlerle birlikte denizcilik endüstrisinin artan dijitalleşmesiyle son zamanlarda denizcilik sektöründe gerçekleşen siber saldırıların sayısı da artış göstermiştir[18]. Halihazırda işlemekte olan 15 Asya Limanına yönelik planlı bir siber saldırının ekonomik maliyeti yaklaşık 110 milyar dolar olarak belirlenmiştir[19]. Deniz siber güvenliği, denizcilik endüstrisinin benzersiz doğası nedeniyle tehditler ve sonuçların özellikleri bakımından belirgin farklılıklar göstermektedir. Denizel alanda gerçekleşen siber güvenlik tehditleri hem devlet hem devlet dışı aktörlerden kaynaklanabilmektedir[20].

Birleşmiş Milletler siber saldırıları "deniz emniyeti ve güvenliğine yönelik yeni bir tehdit" olarak değerlendirmektedir[21]. Kanada ve Amerika Birleşik Devletleri tarafından IMO'ya yapılan bir sunumda ise[22]:

"Modern denizcilik endüstrisi operasyonları ve yönetimleri siber sistemlere güveniyor. Küresel Konumlandırma Sistemi (GPS), otomatik ekipman, fiziksel güvenlik sensörleri, elektronik sertifikalar, kargo takibi, elektronik seyrüsefer, Otomatik Tanımlama Sistemi (AIS), kayıt tutma ve ön-varış işlemleri, güvenilir ve güvenli siber sistemlere bağlı olan süreçlerden bazılarıdır. Bilgisayarlara ve bilgisayar ağlarına, özellikle internete bağlı olanlara olan bu güven, zayıf siber güvenlik uygulamaları ve siber saldırılar nedeniyle kayıplara, hasarlara ve kesintilere karşı potansiyel olarak güvenlik açıkları oluşturur." denilerek siber tehditlerin ne kadar göz ardı edildiğini ortaya koymaktadır.

IMO Siber Risk Yönergelerine göre ise[23]:

"Deniz siber riski, bir teknoloji varlığının, bilgi veya sistemlerin bozulması, kaybolması veya kaybolması sonucunda gemicilikle ilgili operasyonel, emniyet veya güvenlik arızalarıyla sonuçlanabilecek potansiyel bir durum veya olay tarafından ne ölçüde tehdit edildiğini ifade eder."

Görüldüğü üzere IMO'nun denizcilik siber riskleri tanımı emniyet ve güvenliği içermektedir. Deniz siber güvenliği, limanların, gemilerin ve açık deniz tesislerinin (örneğin petrol ve gaz tesisleri) siber saldırılara karşı emniyet ve emniyetinin sağlanmasını içerir. Denizcilik sektöründe gerçekleşen teknolojik gelişmeler sonucunda uluslararası ticari deniz taşımacılığı için otonom/uzaktan kumandalı gemilerin kullanılması, deniz siber güvenliği konusunda pek çok sorunu da beraberinde getirmektedir. Yine teknolojik gelişmelere ve araçlara duyulan bağımlılık sebebiyle limanların ve terminallerin siber güvenliği de ciddi bir sorun haline gelmiştir[24].

Siber saldırıların bir diğer boyutu ise 11 Eylül 2001 saldırıları sonrası ortaya çıkan güvenlik kavramına paralel olarak gelişen "siber terörizm" kavramıdır. Teröristlerin kritik altyapı sistemlerine, bilgisayar sistemlerini kullanarak gerçekleştirebilecekleri siber saldırılar neticesinde, klasik terör eylemlerindekine benzer şekilde toplumda korku ve dehşet ortamı oluşturabilecekleri öngörülmektedir. Bu doğrultuda teröristlerin, devletlerin ve şirketlerin kritik altyapılarına müdahale ederek örneğin nükleer enerji santrallerinde sızıntılara sebep olabilecekleri, kritik liman altyapılarına müdahale ederek can ve mal kayıplarına yol açabilecekleri öngörülen senaryolar arasındadır.

Denizcilik endstrisinin yapısı gereği teknolojik sistemlerin; geminin işletilmesinde, iletişimde, yükleme ve boşaltılmasında, navigasyonunda ve limanlarda vazgeçilemez yeri vardır. Tüm denizcilik sistemleri bir bilgisayar sistemi yahut IT sistemi üzerinden yürütülmektedir. Bunun sonucu olarak da sektör, siber saldırılara karşı yüksek duyarlı hale gelmektedir. Tüm bu teknolojik sistemlerin sorunsuz çalışması, geminin faaliyetlerini sorunsuz yürütmesi ve dünya ticaretinin dolaylı olarak sorunsuz işlemesi için önemlidir. Denizcilik sektörü, ufak aksamaların zincirleme tepkiler doğurduğu devasa büyüklükte bir sektördür. Örneğin Süveyş Kanalı'ndan geçmekte olan bir gemiye karşı gerçekleştirilecek siber saldırı neticesinde, söz konusu geminin kanalı tıkanması halinde dünya ticareti büyük darbe alacaktır.

Araştırma kuruluşlarınca yapılan pek çok test, siber saldırılarda geminin yakıt sistemi, navigasyon sistemi, dümen donanımı ve makine sisteminin kolayca ele geçirilebileceğini ortaya koymuştur. Tüm bu hususlar birlikte değerlendirildiğinde denizcilik siber güvenlik risklerine özel düzenlemelerin yetersizliği ortadadır.

Uluslararası deniz taşımacılığın uluslararası düzenleyici organı olan IMO, 2017 yılında siber riskler ile ilgili çeşitli farklı kuruluşları da kapsayan “Gemilerde Siber Güvenlik Rehberi” kılavuzu yayınlamıştır. Yanısıra, Baltık ve Uluslararası Denizcilik Konseyi(BIMCO)’ne ait “Gemilerde Siber Güvenlik Rehberi”, “Denizde Siber Farkındalık” ve “CyberSail” de bu alanda yapılmış çalışmalara örnektir.

Bu değişim dünya ticaretinin ana damarı olan denizcilik endüstrisini de derinden etkilemiş ve bunun sonucu olarak da denizcilik endüstrisinde kullanılmakta olan operasyonel teknoloji (OT) sistemlerine yönelik siber saldırılar son üç yılda %900 artarak; rapor edilen vakaların sayısı kadar rekor hacimlere ulaşmıştır.

Liman ve terminal operatörlerine hizmet veren Naval Dome şirketinin Boston merkezli Kuzey Amerika Operasyonları Başkanı Robert Rizika, 2017'de rapor edilen 50 önemli OT hack'inin 2018 yılında 120 olduğunu ve 2019 yılında 310'dan fazla olduğunu açıklamıştır. Amerikan Liman Yetkilileri Birliği tarafından düzenlenen 2020 Liman Güvenliği Semineri ve Fuarı sırasında konuşan Rizika, Maersk için 300 milyon ABD doları zarara neden olan virüs NotPetya'dan bu yana saldırıların artmakta olduğuna dikkat çekmiştir[25].

Elektromanyetik sinyaller ve siber iletişimin denizcilik sektöründe yaygınlaşmasından önce gemiler ve diğer denizcilik platformları çoğunlukla izole şekilde çalışmakta; gemi kaptanları yalnızca doğrudan gözlemlerine, haritalara ve geçmiş deneyimlere dayalı kararlar vermek zorundaydı. Günümüzde ise geminin sevk ve idaresine dair kararlar hala geçmiş deneyimlerden faydalansa da esas olarak alınan harici verilerin akışına bağlı şekilde işlemektedir. Tüm denizcilik altyapıları, esas olarak dijital bilgi alışverişi yapan IP tabanlı sistemler aracılığıyla denizde veya karada bulunan diğer gemilere, limanlara ve gemi sahibi yahut donatanlara ağ üzerinden bağlanarak gemi kaptanlarının ve ISTAR operatörlerinin ortak bir operasyon resminden yararlanmasına olanak tanımaktadır. Bu sistem iletişim ve bilgi bağımlılığı riskini artırırken aynı zamanda daha iyi ve detaylı bilgilendirilmiş; dolayısıyla daha iyi çalışan bir operasyon sistemiyle sonuçlanmaktadır.

Deniz siber güvenliğine ilişkin olaylar ile ilgili küresel bilgi alışverişi gerçekleştirilmesi siber risklerle başarılı şekilde mücadele edebilmek adına oldukça önemlidir. Diğer birçok kritik altyapı gibi, deniz taşımacılığı da Bilgi ve İletişim Teknolojilerine bağlıdır. Bilgi ve İletişim Teknolojileri olmadan limanlar, otomatik tanımlama sistemleri, navigasyon, lojistik sistemler ve gemiler çalışamayacaktır. Denizcilik siber riskleri için ana zorluk, günümüzde denizcilik siber güvenliğine ilişkin en önemli başvuru kaynağı olan Uluslararası Denizcilik ve Liman Güvenlik Kodu'nun (ISPS Kodu) dijital güvenlik risklerinden ziyade fiziksel risklere odaklanmasından kaynaklanmaktadır. Devletler ve bölgesel örgütler, ancak uluslararası hukuki düzenlemeler geliştirerek kritik denizcilik altyapıları için küresel güvenliğin geliştirilmesine yardımcı olabileceklerdir.





2. BİLİŞİM SUÇLARI VE DENİZCİLİK BİLİŞİM SİSTEMLERİ

2.1 Bilişim Suçları

Bilişim suçunun tanımı farklı hukuk doktrinlerinde farklı karşılıklar bulmuştur. Bilgisayarın anavatanı olan Amerika Birleşik Devletleri'nde, yaygın kullanım "computer crime" (bilgisayar suçu) iken Fransız Hukuku'nda bilişim suçları anlamına gelen "la fraude informatique" kullanılmaktadır[26].

Türk hukukunda ise bilişim suçlarının her biri farklı şekilde tanımlanarak ciddi bir kavram karmaşası oluşmuştur. "Siber suç", "sanal suç", "bilişim suçları", "bilişim sistemleri aracılığıyla işlenen suç" bu alanı karşılamak için kullanılan tanımlardan bazılarıdır.

Bilişim suçlarının ve bunun hukuki alanındaki etkilerinin ortaya çıkmasıyla birlikte bu konuda yapılan ilk tanımlarda bilgisayarla ilgili gerçekleştirilen her türlü eylem bilişim suçu olarak değerlendirilmiştir[27]. Ancak bu konuda yasalaştırma yoluna gidildiğinde "suçla korunan hukuksal değer" ölçütü esas alınmış ve her türlü eylemin bilişim suçu olarak kabul edilemeyeceğine karar verilmiştir.

Dülger, geniş anlamda bilişim suçunu bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her türlü suç olarak tanımlamıştır[28]. Dülger'e göre dar anlamda bilişim suçu ise, verilere ve/veya bilişim sistemlerine veya sistemlerin/verilerin düzgün ve işlevsel çalışmasına, güvenliğine ya da bütünselliğine karşı işlenen suçlardır.

Erkan ve Songur'un tanımına göre dünya üzerinde mevcut bulunan milyonlarca sayıdaki bilgisayarın birbirine entegre olması ile oluşan ağların yine birbirine entegrasi ile oluşan çok geniş özellikteki ağ ise internettir[29]. İnternetin teknik altyapısı, üzerinde veri iletiminin gerçekleştirildiği ve omurga olarak tanımlanan ağlar sistemi ile verilerin iletimini gerçekleştiren bir çok araç ve yazılımdan meydana gelmektedir[30].

İnsanların teknolojik araçları suç işlemek için kullanması ise çok eski tarihlere uzanır. Günümüzde asıl önemli olan nokta, kişisel kullanıma tabi sistemlerin küresel ağa

kolayca bağlanabilmesinin mümkün olmasıdır. Bir bilişim suçunun işlenmesi için gereken zaman saatler ve hatta dakikalarla sınırlanır olmuştur. Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihinde Minneapolis Tribune gazetesinin haberini yaptığı bir bankada çalışan bilgisayar uzmanının hesaplarda tahrifat yaptığına dair suçlamalarla topluma yansımıştır(31).

Bilgisayar yazılımlarının hukuka aykırı kullanımı, ATM'lerin kötüye kullanımı ve iletişim hatlarında ve şirketlerinde yapılan yolsuzluklar gibi olaylar bilgi toplumunun zayıflıklarını göz önüne sermiştir[32]. Günümüzde siber tehditler ciddi bir sorun haline gelmiştir. Bu kapsamda yaygın olarak kullanılan siber tehdit şekilde Çizelge 1.'de görülebilecektir.

Çizelge 2.1: Siber tehdit çeşitleri.

Siber Tehdit Çeşitleri	- Malware - Waterholing - Scanning - Typosquatting - Targeted Attacks vd.
------------------------	---

Siber suçlar ve siber suç işleme yöntemleri ise genel anlamıyla şu şekilde sınıflandırılabilir;

Çizelge 2.2: Siber suçların sınıflandırılması ve siber suç işleme yöntemleri.

Siber Suçların Sınıflandırılması	1- Bilgisayar Yoluyla Dolandırıcılık ve Sahtekarlık 2- Yetkisiz Erişim ve Dinleme 3- Bilgisayar Sabotajı 4- Ortam Dinlemesi 5- Bilgisayar Yazılımının İzinsiz Kullanılması 6- Verilere Yönelik Suçlar 7- Yasadışı Yayınlar 8- Siber Terörizm 9- Çocuk Pornografisi 10- Ödeme Sistemleri Sahtekarlığı ve Dolandırıcılığı 11- Haktivizm
----------------------------------	---

Çizelge 2.2 (devam): Siber suçların sınıflandırılması ve siber suç işleme yöntemleri.

Siber Suç İşleme Yöntemleri	1- Bilgi ve Veri Aldatmacası(Data Diddling) 2- Salam Tekniği(Salami Techniques) 3- Süper Darbe(Super Zapping) 4- Eşzamansız Saldırılar(Asynchronous Attacks) 5- Truva Atı(Casus Yazılımlar) 6- Zararlı Yazılımlar(Kötücül Yazılımlar) 7- Mantık Bombaları(Logic Bombs) 8- Oltaya Gelme(Phishing) 9- Tarama(Scanning) 10- Bukalemun(Chamelon) 11- İstem Dışı Alınan Elektronik Postalar(Spam) 12- Çöpe Dalma(Scavenging) 13- Gizli Kapılar(Trap Doors) 14- Sırtlama(Piggybacking) 15- Yerine Geçme(Masquerading) 16- Sistem Güvenliğini Kırıp İçeri Sızma(Hacking) 17- Hukuka Aykırı İçerik Sunma 18- Web Sayfası Hırsızlığı ve Yönlendirme 19- Sosyal Mühendislik
-----------------------------	---

2.1.1 Denizcilik Bilişim Sistemleri

Dijital dönüşüm her sektörde olduğu gibi denizcilik sektörü için de pek çok fırsat sunmaktadır. “Big Data” teknolojisiyle filoların kontrolleri geliştirilebilecek, maliyetler düşürülebilecek ve dijital evraklar ile ticaret hızlandırılabilir. Yine deniz ve liman trafik kontrollerinin dijitalleşmesiyle veriler optimize edilerek kaza riski minimize edilerek trafiğin hızı ve verimliliği artırılabilir.

Ancak gemilerdeki dijital dönüşümün olumlu tarafları olduğu gibi olumsuz tarafları da vardır. Teknolojik dönüşümün hızı ve internet ile teknolojinin hayatımızın merkezi haline gelmesi güncel bazı sorunları da ortaya çıkarmıştır. Özellikle elektronik ticaretin artması ve mevcut hukuk sistemlerinin elektronik ortamda gerçekleşen ticari işlemlere karşı yetersiz olması geniş kapsamlı hukuki düzenleme yapılmasını zorunlu kılmaktadır. Dijital dönüşüm gerçekleşmeden önce yalnızca insanlara özgü olarak kabul edilen bir çok fiil ve yöntem, günümüzde insanlar için mümkün olmayan bir hız ve doğruluk oranıyla bilgisayarlar tarafından gerçekleştirilmektedir[33]. Bilişim devrimi olarak adlandırılan bu sürecin en önemli nesneleri, bilişim sistemleri ve bilginin sınır tanımaksızın en hızlı şekilde aktarıldığı veri iletim ağlarıdır. Bu ağlar içerisinde kullanımı en kolay, en ucuz ve en yaygın olanı ise internettir. Bu sürecin en

önemli ve temel niteliği ise bilginin sınırsızca paylaşılmasıdır[34]. Günümüzde bilgiye sahip olmak en değerli varlık olarak kabul edilmeye başlanmıştır. Bu değişime ayak uyduran bireyler ve toplumlar dünya siyasetinin geleceğinde rol almaya devam ederken değişime kafa tutan toplumların ise çağın gerisinde kalması kaçınılmazdır.

Maliyet ve işlevsellik açısından denizcilik sektöründe teknoloji kullanımının artan popülaritesinin nedenleri ise şunlardır:

- Bilgi işlem gücü – Makinelerin daha hızlı çalışması ve komutları daha hızlı gerçekleştirmesi; matematiksel hesaplamalar ve algoritmalar sayesinde çok kısa zaman içinde gerçekleştirilir. Bu sayede sürekli ve hızlı bir bilgi akışı gerçekleştirilir.
- Veri depolama – Veri depolama ve donanımda gerçekleşen bulut devrimi, şirketlere veri toplama konusunda yüksek fayda sağlayan, uygun maliyetli ve güçlü veri depolama çözümlerinin geliştirilmesine katkıda bulunmuştur.
- Bağlantı – Gemi operasyonunun yeni ve hala gelişmekte olan bir yönü olan bağlantının iyileştirilmesi, kıyıda yüzlerce mil uzakta geminin performansı hakkında gerçek zamanlı bilgi sağlayarak endüstriye fayda sağlamaktadır.
- Sensörler – Gaz emisyonları ve kargo sıcaklığı gibi gemilerdeki bileşenlerle ilgili gerçek zamanlı verilerin toplanması, bakım ve güvenliğin verimliliğini artırırken işletme maliyetlerini ve ihmalden kaynaklanan arıza riskini azaltmaktadır.

Denizcilik sektörü dijitalleşme çağına hızla girerken “Büyük Veri Analitiği”, “Nesnelerin İnterneti”, “Bulut Bilişim”, “Makine Öğrenimi”, “Yapay Zeka” gibi kavramlar gemilerin çalışma şeklini değiştirecek yönlerden sadece birkaçı olarak ortaya çıkmaktadır.

“We Are Social” ve “Hootsuite” tarafından yayınlanan Digital 2020: Global Digital Overview raporuna göre[35]:

“Günümüzde 4,5 milyardan fazla insan interneti kullanmaktadır. Sosyal medya kullanıcı sayısı ise 3,8 milyarı geçmiş durumdadır. Ortalama bir internet kullanıcısı her gün çevrimiçi olarak 6 saat 43 dakika geçirmektedir. GlobalWebIndex, çevrimiçi harcadığımız sürenin yarısından fazlasını cep telefonları ile gerçekleştirdiğimizi ve mobil bağlantının tüm internet bağlantı zamanının 50,1%’ini oluşturduğunu tespit etmiştir. Dünyadaki internet kullanıcılarının yüzde 92’si mobil cihazlar üzerinden bağlantı sağlamaktadır”.

2.1.1.1 Denizcilik sektöründe kullanılan temel sistemler

Çizelge 2.3: AIS.

Otomatik Tanımlama Sistemi (AIS)	- Gemi trafiği izleme ve yardım - Çarpışmalardan kaçınmayı sağlar. - Geminin yerini limanlara ve denizcilik yetkililerine bildirir. - Gemi ile diğer gemiler arasındaki mesafeyi hesaplar. - Deniz trafiğini izleyerek deniz güvenliğini sağlar. - Kaza araştırma ve arama kurtarma çalışmaları yapar.
----------------------------------	--

AIS aktarıcıları, herhangi bir kimlik doğrulama veya bütünlük kontrolü olmaksızın kablosuz iletişim kurar, bu da bilgisayar korsanlarının sahte mesajları yaymak için sisteme sızma olanağı tanır[36]. Saldırganlar, sahte sinyaller başlatmak, gemiyi sistem üzerinde görünmez yapmak ve sahte hava raporları iletmek için bu sistemi kullanırlar. Saldırganların sızdığı sistem üzerinden gönderilen yanlış verilere güvenmek ciddi güvenlik zaafiyetlerine yol açacaktır. AIS verilerine, Vessel Finder Limited (<https://www.vesselfinder.com/>) ve Marine Traffic[37] gibi web siteleri aracılığıyla da kolayca erişilebilecektir. IMO, gemiler ve güzergahları hakkındaki bilgilerin açıklanmasını bu bilgilerin hedefli saldırılarda çok faydalı olabileceği düşüncesiyle eleştirmektedir.

Çizelge 2.4: ECDIS.

Elektronik Harita Görüntüleme Bilgi Sistemi (ECDIS)	- Elektronik navigasyon sensörlerinden veri toplar ve birleştirir. -Geminin konumunu gerçek zamanlı olarak gösterir.
---	--

ECDIS ile ilgili güvenlik konuları pek çok akademik çalışmaya konu olmuştur. Aslında, ECDIS yazılım uygulamalarında pek çok açık vardır. Sistem, güvenlik güncellemesi olmayan eski bilgisayarlarda da yoğun olarak kullanılmaktadır. Sistemde haritalar internetten indirilir veya USB üzerinden manuel olarak sisteme yüklenirler.

Bu durum haritaların güncellenmesi sırasında sistemin tehlikeye girmesine neden olabilir. Bu güncellemeler, olası saldırılar için fırsat yaratabilir[38]. “Assessing ship cyber risks: A framework and case study of ECDIS security” isimli makaledeki yazarlar, ECDIS’in siber riskleri üzerine yoğunlaşmış ve bir saldırının sistem

dosyalarını silmesi yeniden yüklemesi ve kötü amaçlı içerik implement etmesine olanak sağlayan güvenlik açıkları keşfetmiştir. Sonuç olarak, navigasyon kararlarını etkileme amacıyla değiştirilmiş sensör verileri ECDIS'e gönderilebilecek böylece çatismalar ya da başka güvenlik ihlalleri ortaya çıkabilecektir[39].

Çizelge 2.5: GPS ve GNSS.

GPS ve GNSS	- Geminin konumunu görüntüler - Geminin hızını görüntüler - Rotayı ve zamanı gösterir
-------------	---

Denizcilik sektöründe aktif olarak kullanılan GPS ve navigasyon teknolojileri, bu teknolojilere bağlı hizmetleri aksatmak amaçlı çeşitli siber saldırıların hedefi olmaktadır[40]. Bu tür saldırıların, veri ve hizmet protokolü ihlallerinin yanı sıra fiziksel zarar verme riski de bulunduğundan önemli bir risk faktörü olarak değerlendirilmelidirler. Bu teknolojik araçlara gerçekleştirilmiş bildirilmiş saldırılar mevcuttur[41]. Örneğin, sahte GPS sinyalleri, saldırganların sistem yönetiminden gelen bir alarmı veya uyarıyı tetiklemeden bir gemiyi yeniden yönlendirmesini sağlamıştır. Benzer bir olayda, Güney Kore'deki GPS sinyal sıkışması, bir haftadan fazla bir süre boyunca 1000'den fazla uçak ve 700 geminin sinyal alımını etkilemiştir. Bu tür siber saldırılar, orta ila yüksek risk derecesinde sınıflandırılabilir; GPS ve navigasyon sistemlerinin yazılım açıklarının sonucudur. A retrospective analysis of maritime cybersecurity incidents makalesine[42] göre, gemileri internet üzerinden birbirine ve anakaraya bağlayanlar da dahil olmak üzere Uydu Haberleşme Sistemleri (SATCOM'lar), güvenli olmayan ve hatta belgesiz protokoller kullanan cihazlar; kurulum hesapları, parola sıfırlama işlevinden yararlanma yeteneği ve arka kapılar gibi çok sayıda kritik güvenlik açıkları içerir.

En birbirine bağlı sistemlerden biri Küresel Navigasyon Uydu Sistemidir (GNSS). Sonuç olarak, operasyonel komutları ve sensör verilerini iletmek için gelişmiş uydu iletişimine dayanan otonom gemiler, hizmet reddi saldırıları, paket değişiklikleri ve ortadaki adam saldırıları gibi siber saldırılar[43] riski altında olabilir. Ayrıca, düşük güçlü uydu sinyalleri, basit tıkanıklık nedeniyle önemli bir teknik dezavantaja sahiptir. Sonuç olarak, sahtekarlık ve karıştırma, yüksek maliyetli ve düşük çaba gerektiren saldırıları temsil edebilen önemli kusurlardır. Ek olarak, birçok gemi sistemi büyük ölçüde uydu konumuna bağlı olduğundan, GNSS arızası diğer gemi sistemlerinin (örneğin AIS) bozulmasına neden olabilir. Otonom ulaşım sistemleri, yer ekiplerinden

operasyonel ekiplerle iletişim kurabilmeli, siber saldırıların kritik ulaşım operasyonlarının tam kontrolünü ele geçirmesine izin vermeli ve davetsiz misafirler için daha geniş bir saldırı ve teşvik yelpazesine izin vermelidir[44].

Çizelge 2.6: RADAR.

RADAR	- Geminin çevresi hakkında bilgi sağlar. - Nesnelerin konumunu ve hızını tespit eder.
-------	--

Radar sinyallerini kesmek uydulardan daha zor olsa da, siber saldırılardan kaynaklanan parazit ve DDoS saldırılarına karşı hala hassastırlar. Bir siber saldırı durumunda, radar, harici radar dalgalarının neden olduğu yanlış yankılar nedeniyle yakındaki nesneler hakkında yanlış bilgi verebilir. Bu yanlış bilgi gemi çarpışma kazalarına neden olabilir.

Bu yanlış bilgi, geminin bir cisimle çarpışmasına neden olabilir. Elektromanyetik spektrumdaki radar ve diğer frekanslar, gürültüye dayalı girişime veya daha gelişmiş yanıltma saldırılarına karşı hassas olsa da, aynı etkiyi elde etmek için mekanizmalar sistemler arasında önemli ölçüde farklılık gösterir[45].

Çizelge 2.7: GMDSS.

Küresel Deniz Tehlike Sistemi (GMDSS)	- Güvenlik sorunlarıyla ilgili tehlike mesajlarını yayınlar. - Kritik güvenlik uyarılarını gönderir ve alır.
---------------------------------------	---

Çizelge 2.8: ICS'ler.

Küresel Endüstriyel Kontrol Sistemleri (ICS'ler)	- İnsan hatalarının azaltılmasına yardımcı olur. - Kaynak verimliliğini artırır. - Ekipmanın ömrünü uzatır. - Bir gemideki parametreleri kontrol ve takip eder.
--	--

Çizelge 2.9: VSAT.

Küçük Çaplı Uydu İstasyonu (VSAT)	- Veri göndermek ve almak için bir uydu ağı kullanır. - Çeşitli iletişim ve güvenlik hizmetleri sunar.
-----------------------------------	---

Modern denizcilik endüstrisinde VSAT'ın yaygın olarak kullanılmasıyla, VSAT ağının şeffaf iletim ve açıklık gibi bazı yönlerinin, özellikle yetkisiz erişim ve müdahale saldırıları gibi güvenlik tehditlerine karşı geliştirilmesi gerekmektedir[46].

2014 yılında, IOActive[47] farklı satıcılardan birkaç VSAT'ı test etti ve doğrulama, şifreleme, güvenlik veya kişisel bilgilerin doğrulanması olmadan düz metin iletimi kullandıkları için test edilen tüm cihazların uygulama seviyelerinde savunmasız olduğu sonucuna vardı. Zayıf korumanın bir sonucu olarak, saldırganlar, cihazı devre dışı bırakmak veya sistemi tehlikeye atmak için cihaza yanlış sinyaller veya kötü amaçlı kodlar göndererek geminin güvenli bir şekilde seyretmesini engelleyebilir. Yukarıda da açıklandığı gibi, AIS toplayıcıları tipik olarak gemi konumu verileri sağlar. Gerçek risk, VSAT ağ arayüzlerinin İnternette Shodan Ship Tracker gibi araçlar kullanılarak bulunabilmesidir. Bu, marka adları, ürün kodları ve siber saldırılarda kullanılabilecek diğer veriler gibi değerli ve hassas bilgileri ortaya çıkarabilir. Standart bilgiler genellikle satıcıların web sitelerinde bulunur ve birçok terminal, kullanıcı adı ve sunucu parolası dahil aynı fabrika ayarlarını kullanmaya devam eder. Saldırgan, açık bir VSAT arayüzü bulursa, GPS koordinatlarını ve ayarlarını değiştirebilir ve kötü amaçlı yazılım indirebilir ve bu, daha fazla ağ korsanlığı sağlar ve kritik yönetim sistemlerine erişim sağlar.

Çizelge 2.10: Sevk ve makine yönetimi ve güç kontrol sistemleri.

Sevk ve makine yönetimi ve güç kontrol sistemleri	- Teknedeki makineleri izler ve düzenler
	- Tahrik gücünü izler ve düzenler
	- Direksiyonu izler ve düzenler

Çoğu endüstriyel kontrol sistemi, güvenlik gereksinimlerinden bağımsız olarak tasarlanmış ve programlanmıştır ve veriler düz metin olarak iletilir[48]. Bileşen güvenliği, güvenli geliştirme yapılarını sürdüren satıcılar ve bileşenleri endüstri standartlarına ve en iyi uygulamalara göre yapılandıran operatörler tarafından paylaşılmalıdır. Her iki durumda da, genellikle rakibin hatasını üstlenir ve herhangi bir işlem yapmaz, saldırganların yararlanabileceği birçok kritik kusuru ortaya çıkarır[49]. ICS tasarımcıları ve operatörleri, geminin güvenliği için kritik öneme sahip olduklarından, sistemin sınırlamalarını ve bileşenlerinin ve protokollerinin zayıflıklarını anlamalıdır. Geminin dağıtılmış bilgi teknolojisi ağı, bu kontrol sistemlerinin birbirleriyle iletişim kurmasını sağlar. BT ağı ve web sitesi arasındaki sürekli iletişim, uzaktan izleme, sorun giderme ve hata ayıklamayı sağlarken aynı zamanda saha seyahat maliyetlerini düşürür ve veri toplama ve değerlendirmeyi basitleştirir. Başlıca endişelerden biri, operatörlerin ve mühendislerin, tüm denizcilik endüstrisinde geniş kapsamlı sonuçlara yol açabilecek kolaylık ve verimlilik adına

güvenliği sıklıkla göz ardı etmesidir[50]. Bu davranış, zamandan tasarruf etmeye ve güvenlik politikalarını atlatmaya yönelik ticari baskıdan kaynaklanmaktadır[51].

Çizelge 2.11: Video gözetim sistemi.

Video Gözetim Sistemi	- Geniş depolama alanlarındaki nakliye operasyonlarını izler. - Büyük gemilerde nakliye operasyonlarını izler.
-----------------------	--

Video Gözetim Sistemleri (VSS'ler), her tür modern gemide gemilerin, kargoların ve mürettebatın güvenliği ve emniyetinde çok önemli bir rol oynamaktadır[52]. Bu sistemler esas olarak geminin kritik operasyonlarını izlemek ve takip etmek ve terörist ve korsan saldırılarına karşı korunmak için kullanılır. Bununla birlikte, VSS'lerin son zamanlarda çeşitli siber saldırılara karşı savunmasız olduğu bulunmuştur ve bir dizi güvenlik sorunu ortaya çıkmıştır[53]. Örneğin, Bitdefender araştırmacıları, modern gemilerde kullanılan iki CCTV kamera modelinin arabellek taşması kusurlarına karşı savunmasız olduğunu buldu. Bu güvenlik açığından yararlanan araştırmacılar, saldırıya uğramış kameranın etkinliklerini izleyebildi ve parolaların üzerine yazabildi[54]. Ayrıca, bu güvenlik açığı bir VSS sistem çökmesine neden olabilir veya daha da kötüsü, diğer siber saldırılar için bir giriş noktası oluşturabilir

Çizelge 2.12: BT ağ sistemleri.

BT Ağ Sistemleri	- Veri göndermek, almak ve depolamak için dahili/harici süreçler için kullanılır. - Mürettebatın refahı için kullanılır. - Mürettebatın kişisel cihazları için kullanılır.
------------------	--

Denizcilik endüstrisinde, ağ bağlantılı bilgi sistemleri tarafından toplanan ve işlenen verilerin iletimi için çeşitli ağ türleri kullanılmaktadır. Bu teknolojilerin örnekleri arasında SHIPNET, SAFENET, C3I sistemi, RICE 10, SHIP sistemi 2000, Smart Ship ve TSCE sayılabilir[55]. Bu teknolojilerin birçok güvenlik açığı vardır, çünkü BT ağları arasındaki iletişim bağlantılarının tasarımı ve yapılandırılması, kimlik doğrulama ve şifreleme yöntemlerine çok az dikkat eder ve bu da potansiyel olarak savunmasız ve güncel olmayan sistemlerin İnternet'te kullanılabilir olmasına neden olur. Aslında, gemi bilgi teknolojisi sistemleri sıklıkla karadaki tesislerle bağlantılıdır ve sistematik ve sürekli tehdit riskini artırır[56]. Mali baskılar, yasal gereksinimler ve uzaktan izleme ve yönetim gereksinimleri, modern denizcilik endüstrisinde BT sistemlerine ve ağ bağlantısına olan ihtiyacı artırıyor; ancak bu sistemler, güvenlik

ekiplerinin savunması gereken saldırı yüzeyinin boyutunu artıracak ve korsanların gemi sistemine girmek için kullanabilecekleri ek erişim noktaları oluşturacaktır. Bu nedenle, bu otomatik sistemlerdeki güvenlik açıkları dikkatlice araştırılmalıdır. Ayrıca, kritik kontrol ağları, geminin BT ve İnternet ağlarından güvenli bir alanda izole edilmelidir.

Gemi sistemlerinin tehlikeye girmesi, özet olarak aşağıdaki gibi istenmeyen sorunlara yol açabilir[57]:

- Sisteme veya gemi personeline veya kargoya fiziksel zarar – en kötü senaryoda can ve/veya geminin kaybolması riski
- Geminin artık amaçlandığı gibi çalışmaması veya seyir halinde olmamasından kaynaklanan aksaklıklar
- Ticari olarak hassas veya kişisel veriler dahil olmak üzere hassas bilgilerin kaybı
- Adam kaçırmak, korsanlık, dolandırıcılık, kargo hırsızlığı, fidye yazılımı yükleme dahil olmak üzere suç faaliyetlerinin gerçekleşmesi.

2.1.1.2 Sistemleri yönelik gerçekleştirilebilecek siber saldırılara ilişkin güvenlik zaafiyetler ve oluşabilecek sonuçlar

Son yıllarda denizcilik sektörü, siber güvenliğe yatırım yapmanın önemini algılayamaması ve önemli operasyonel kesintilerin yaşanması potansiyeli nedeniyle fidye yazılımı saldırıları için çekici ve yüksek kazançlı bir hedef haline gelmiştir [58]. Modern gemiler, seyir halindeyken, seyrin izlenmesine ve takip edilmesine olanak sağlayan birbirine bağlı sistemler kullanmaktadır. Bu sistemler, ortak bir ağ üzerinde faaliyet gösterdikleri için siber saldırılara oldukça açık sistemlerdir. Dolayısıyla zaafiyetleri, olası sonuçları ve saldırıların arkasındaki motivasyonları anlamak siber güvenliği sağlamak ve siber saldırılarla etkin bir şekilde mücadele edebilmek için önemlidir.

Siber saldırı bir tanıma göre, siber ortamda yer alan bilgileri kötü amaçlı kullanmak, bozmak, değiştirmek, sistemlere erişimin gerçekleşmesini engellemek ya da zarar vermek kastıyla siber alanda gerçekleştirilen faaliyetler[59] olarak tanımlanmaktadır. Başka bir tanıma göre ise siber saldırı, “kötü amaçlı fiilleri yerine getirenler tarafından bilgi sistemlerinin çalışamaz hale getirilmesi, bilgi sistemlerinin güvenliğinin veya güvenilirliğinin riske atılması, bozulması ve çalınması”[60] şeklinde de ifade edilmektedir.

Siber saldırılarda saldırı aracı olarak dijital araçlar kullanılır. Bu da aynı anda bir çok yerde siber saldırı eyleminin ışık hızında bir çok hedefi vurarak gerçekleştirilmesini mümkün kılmaktadır. Siber saldırının amaçlanan sonucu fiziksel bir şeye hasar vermek olabilir ancak hasar ilk olarak dijital alemdeki bir olaydan doğar[61].

Siber saldırının gerçekleştirilmesi için belli siber araçlar kullanılmaktadır. Siber silahın tanımı konusunda farklı görüşler olmakla birlikte, siber silahın neden olabileceği zarara göre bir sınıflandırma yapmak yerinde ve işlevsel bir yöntem olacaktır. Bu yaklaşım siber saldırıları etki spektrumları üzerinden düşük potansiyele sahip ve yüksek potansiyele sahip olarak sınıflandırmaktadır. Düşük potansiyelli siber silahlar, bir sistemi dışarıdan etkileyebilen ancak bu sistemin içine girmek ve onu içerden yönetmek gibi eylemleri gerçekleştiremeyen zararlı yazılımlardır. Ancak yüksek potansiyele sahip siber silahlar, sistemlere dışarıdan girilmek suretiyle “akıllı unsur” şeklinde faaliyet gösteren ve otonom şekilde fiillerde bulunarak sistemin normal faaliyet süreçlerine zarar veren yazılımlardır [62].

Yapısı ve uygulanış şekli gereğince fiziki güç kullanımı içermeye ancak silahlı saldırılar ile aynı derecede somut zararlara sebep olabilen siber saldırılar da silahlı saldırı olarak değerlendirilebilir. Siber saldırılar neticesinde doğalgaz hatlarının sabotaj edilmesi, nükleer gemilerin imha edilmesi, deniz trafiğinin felç edilerek binlerce insanın tedarik zincirinin sekteye uğratılması, gemilere yapılan siber saldırılar sonucu çatmalara sebep olunması gibi olaylarda siber saldırıyı silah gibi değerlendirip saldırı metodunu uluslararası hukuk kuralları bağlamında incelemek gerekmektedir. Tabloda denizcilik sistemlerinin muhtemel zaafiyetleri ve siber saldırıya uğramaları sonucu maruz kalabilecekleri sonuçlar açıklanmaya çalışılmıştır;

Çizelge 2.13: Sistemler/zaafiyetler/sonuçlar.

Sistemler	Tanımlama	Zaafiyetler	Sonuçlar
Otomatik Sistemi (AIS)		Sinyal ara girişimi/karışma Hatalı bilgi paylaşımı Kötücül yazılım Sahtecilik Şifreleme eksikliği Sinyal bozma	Geminin kaçırılması Veri tahribatı Değerli verilerin çalınması

Çizelge 2.13 (devam): Sistemler/zaafiyetler/sonuçlar.

Sistemler	Zaafiyetler	Sonuçlar
Elektronik Harita Görüntüleme ve Bilgi Sistemi (ECDIS)	Eski işletim sistemi Güvenli olmayan güncelleme araçları	Ağ sistemleri ile haberleşme kaybı Geminin kaçırılması Hassas verilerin çalınması İşletim sistemi ve bilgisayarın bozulması
GNSS ve GPS	Sinyal bozma saldırıları Zayıf sinyal gücü Sinyal karışması Sahtecilik saldırıları Hizmet reddi saldırıları Paket üzerinde oynama	Geminin kaçırılması Ağ sistemleri ile ilgili sorunlar GPS'in hatalı bilgi aktarımı Gemi operasyonlarının kesintiye uğraması Hizmetlerde gecikme
Radar	Sinyal bozma saldırıları Sahtecilik saldırıları Hizmet reddi saldırıları	Ağ sistemleri ile haberleşme kaybı Can ve mal kaybı Kargo operasyon yönetiminde gecikmeler
Küresel Denizcilik Tehlike ve Güvenlik Sistemi (GMDSS)	Kötücül yazılım Sahtecilik saldırıları Hizmet reddi saldırıları	Hatalı gemi pozisyonu ECDIS üzerinden ileri saldırıları
Endüstriyel Kontrol Sistemleri (ICS)	Yetersiz Endüstriyel İndeksleme Sistemleri Analog Kontrolör (ACM) Siber güvenlik üçgeninin faktörlerinden olan bütünlük(Integrity) kontrolünün olmaması Bilgi maruziyeti Zayıf yama yöntemi Donanımsal hatalar Uygunsuz güvenlik kurulumu Ağ bölütleme eksikliği Zayıf şifre politikası Güvenlik duvarı eksikliği Şifreleme eksikliği Zayıf uzaktan erişim politikası	Geminin kaçırılması Bilgi ve Haberleşme Sistemlerine(ICS) erişimin engellenmesi Veri sızması Tesislere fiziki zarar Emniyet sistemlerine müdahale Planlı olmayan operasyon kesintileri Ekipmanların zarar uğraması

Kaynak: Hugh Boyes and Roy Isbell, Code of Practice: Cyber Security for Ships. United Kingdom: IET Standards, Department for Transport, and Defence Science&Technology Laboratory (UK), 2017.

2.1.1.3 Denizel alanda siber haydutluğun uluslararası niteliği

Uluslararası toplumunun huzur ve düzenini bozmak amacıyla toplumu mağdur eden kötü niyetli eylemler uluslararası suç olarak görülmektedir. Ancak doktrinde uluslararası suç kavramının tanımı konusunda bir uzlaşma henüz söz konusu değildir. Bu belirsizlik suç işleyenlerin yargılanması ve cezalandırılması konusunda da eksiklikler ortaya çıkarmaktadır.

Uluslararası hukuku ihlal eden kötü niyetli uluslararası suçların cezalandırılabilmesi için devletlerin iç hukukunda düzenlenmiş olmalarına gerek olmaksızın doğrudan uluslararası hukukun uygulanması ile suçluların yargılanması mümkündür[63].

Sınıraşan suçlar da denilen başta deniz haydutluğu olmak üzere uyuşturucu ticareti, insan ticareti ve göçmen kaçakçılığı gibi suçlar birden çok devletin menfaatini de ihlal eden diğer uluslararası suçlardır. Bu suçlar, esasen devletlerin ulusal hukuklarında suç olarak düzenlenen ama ulusal sınırları aşan, bir çok devletin ulusal hukukunu çiğneyen ve başka ülkeler üzerinde de etki doğuran suçlardır. Bunlar, sözleşme ile yasaklanan fakat cezalandırılması devletlerin iç hukukuna bırakılan suçlardır. Bireysel ceza sorumluluğu doğurmayan bu suçların kovuşturulması ulusal hukuka dahil edilmesine ve suç olarak düzenlenmesine bağlıdır.

Yeni operasyonel teknolojilerin denizcilik sektöründe hızla benimsenmesi ve ağ bağlantılı siber yapılara artan bağımlılık sonucunda ekonomiyi, mürettebat emniyet ve güvenliğini, çevreyi veya ulusal güvenliği tehdit edebilecek siber saldırı olasılığı artış göstermiştir. Siber güvenliğe yönelik sorunların artış göstermesi ve sektörün ilgisi denizcilik alanındaki artan sorunları ele alan düzenleyici bir çerçevenin çıkarılması ihtiyacını artırmıştır. IMO, Avrupa Birliği (AB) ve büyük petrol şirketleri olası kayıpların önüne geçmek siber güvenlik riskini azaltmak için yasal çerçeve çizilmesini önermektedir.



3. LİTERATÜR TARAMASI

3.1 Mevzuatın Tarihsel Gelişim

Yeryüzünün dörtte üçünün deniz alanlarıyla kaplı olması sonucu insanlık denizlerden pek çok amaçla yararlanmaktadır. Denizlerin kapladığı alanın genişliği ve insanlığın faydalanım amaçlarındaki çeşitlilik, bu alanların hukuki rejiminin tespit edilmesi ve bu alanlardaki faaliyetleri düzenleyen kuralların gerekliliğini ortaya çıkarmıştır.

İnsanlığın gelişim sürecinin karalar üzerinde tamamlanmasının ardından denizleri fethetme arzusu sonucu denizleri keşfetme ve denizlerden faydalanma arzusunu ortaya çıkarmıştır. Bunun sonucunda denizel alanlarda ortaya çıkan ihtilafların çözümü için belirli düzenlemelerin yapılması zarureti doğmuştur. Uluslararası deniz hukuku bu ihtiyaçlar doğrultusunda şekillenmeye başlamıştır. Deniz hukuku genel anlamıyla deniz alanlarının hukuki rejimini, gemilerin seyrüseferini ve denizlerin çeşitli kullanımlarını düzenleyen kuralları kapsamaktadır.

Uluslararası deniz hukukunun kurucusu Hugo Grotius günümüz uluslararası hukukun kurucuları arasında sayılan 1609 yılında yayınlanan “Mare Liberum” adlı eserinde ortaya koyduğu denizlerin serbestliği fikri uluslararası deniz hukukunun temel ilkelerinden birisi olarak kabul edilmektedir[64].

Uluslararası deniz hukuku, devletlerarası deniz alanlarına ilişkin egemenlik uyuşmazlıkları ile ilgili deniz hukuku dalıdır. Devletlerin egemenlik hakları doğrultusunda, denizdeki ulaşım ticari olsun ya da olmasın bu alanlardan geçişlerinin ve hukuki rejimlerinin tespit edilmesi gerekmektedir.

Denizciliğin niteliği ve tarihsel gelişimi gereği deniz hukuku da örf ve adet hukuku kaynaklı gelişmiştir. Ancak İkinci Dünya Savaşı’ndan sonra denizel alanların artan siyasi önemi ve Sanayi Devrimi ile gerçekleşen dönüşümün deniz taşımacılığına yansması sonucu ekonomik öneminin artmasına paralel olarak Birleşmiş Milletler öncülüğünde deniz hukukunu standardize etme çalışmaları başlamıştır. Bu sürecin sonunda 29 Nisan 1958 tarihli Cenevre Sözleşmeleri ve 10 Aralık 1982 tarihli Birleşmiş Milletler Deniz Hukuku Sözleşmesi ortaya çıkmıştır.

1982 tarihli Birleşmiş Milletler Deniz Hukuku Sözleşmesi ise deniz hukukuna ilişkin hususları en ayrıntılı şekilde düzenleyen sözleşmedir. Bu sözleşmeye Avrupa Birliği ve 167 devlet taraftır[65].

Deniz ticareti kurallarının kanun hükmüne dönüştüğü önemli bir tarihi belge yalnızca avarya hükümlerinin yer aldığı ve tam metin olarak günümüzde bulunmayan Lex Rhodia/ Rodos Kanunu'dur[66]. Rodoslu denizcilerin deniz ticaretine ilişkin geleneksel uygulamalarından oluşan kanun, milattan önce ikinci ve üçüncü yüzyıllar arasında hukuki bir düzenlemeye dönüştürülmüştür[67].

Deniz ticaret hukukuna ilişkin yapılan bir diğer kanun ise Consolate Del Mare'dır. Roma kanunları ile temellendirilen Consolate Del Mare deniz ticaret hukukuna ilişkiyapılan önemli bir kanundur. Bu kanun, Avrupa'da yürürlüğe giren ilk modern deniz ticaret kanunu olarak kabul edilmektedir[68]. Kanun, İspanya, Fransa, İtalya ve İngiltere'nin deniz ticaret kanunlarına kaynaklık etmiştir.

Deniz ticaretinin yaygınlaşmasıyla deniz ticaretinin koşullarını, rizikolarını ve uyuşmazlık çözüm yollarını açıklayan düzenlemelere ihtiyaç duyulmaya başlanmıştır. Türk hukukunda deniz ticareti ile ilgili düzenlemeler Türk Ticaret Kanunu 5. Kitabı ile yapılmıştır.

Uluslararası deniz ticareti konusunda düzenlemeler ise çeşitli sözleşmelerle yapılmıştır. Bu sözleşmeler sırasıyla;

1924 Brüksel Sözleşmesi, 1968 Visby Protokolü, 1978 Hamburg Sözleşmesi, 2009 Rotterdam Antlaşması'dır.

1924 yılında Brüksel'de imzalanan "Lahey (Hague) Kuralları" olarak bilinen "Konişmentoya Müteallik Bazı Kaidelerin Tevhidi Hakkındaki Milletlerarası Sözleşme" ilk çok taraflı uluslararası sözleşme olarak bilinmektedir.

Brüksel Kuralları, 1968 yılında bir protokol ile revize edilmiş ve "Hague-Visby Rules" olarak anılmaya başlanmıştır.

Birleşmiş Milletler Ticaret ve Kalkınma Konferansı'nın önerisi ile oluşturulan "Hamburg Kuralları" 1978 yılında imzalanan ancak 1 Kasım 1992'de yürürlüğe giren kurallar Türkiye tarafından henüz onaylanmamıştır.

2009 Rotterdam Antlaşması “Tamamen veya Kısmen Deniz Yoluyla Uluslararası Eşya Taşıma Sözleşmelerine İlişkin Birleşmiş Milletler Andlaşması” başlığı ile anılmaktadır. Türkiye tarafından onaylanmayan bir diğer antlaşmadır.

Uluslararası deniz ticaretinin sağlıklı şekilde yürütülmesinde en önemli olan kurum ise Uluslararası Denizcilik Örgütü (International Maritime Organization - IMO)’dür. Sorumluluk alanı uluslararası denizyolu taşımacılığında emniyet ve güvenliği sağlayıcı ve bunları geliştirici önlemler almak olan; ayrıca, çevre kirliliğini önlemek, uluslararası gemi trafiğini rahatlatacak mevzuat düzenlemeleri gerçekleştiren IMO, en önemli aktörlerdendir. Merkezi Londra’da bulunan IMO’nun 175 üye devleti ve üç ortak üyesi bulunmaktadır.

Deniz güvenliği, çevresel kaygılar, yasal konular, teknik işbirliği, deniz güvenliği ve deniz taşımacılığının verimliliği IMO’nun temel gündemleridir. IMO’nun çalışmaları beş komite aracılığıyla yürütülür ve bunlar teknik alt komiteler tarafından desteklenir. IMO sözleşmeleri, temel IMO sözleşmeleri, deniz güvenliği ve emniyeti ile gemi/liman etkileşimi ile ilgili sözleşmeler, deniz kirliliğinin önlenmesine ilişkin sözleşmeler, sorumluluk ve tazminatı kapsayan sözleşmeler, gemilerin tonaj ölçümü ve kurtarmaya ilişkin sözleşmeler olarak gruplandırılmıştır.

Artan denizcilik siber güvenlik tehditleri, çözümlenmesi zor hukuki sorunlar yaratmaya başlamıştır. Bunlardan bazıları; yargı yetkisi, meşru müdafaa, güç kullanımı, zarar vermeme, devlet sorumluluğu, durum tespiti, icra ve iade ve/veya suçluların kovuşturulması gibi sorunlardır. Bu yasal sorunlardan bazıları, denizcilik siber güvenliği için genel olarak siber güvenlikten daha karmaşık yapıda sorunlar ortaya çıkarabilmektedir. Bunun nedeni, denizcilik endüstrisinin benzersiz doğası ve bayrak, liman, kıyı ve diğer devletlerin yetki alanları arasındaki karmaşık etkileşim, rekabet ve ulusal yetki alanı dışındaki alanlar da dahil olmak üzere değişen egemenlik haklarına ve yargı yetkilerine sahip deniz bölgelerinin varlığıdır. Denizcilik siber suçları için uluslararası bir düzenlemenin olmaması, tek bir siber vakada birden fazla ülkenin yargı yetkisinin söz konusu olabilmesi sebebiyle bu alanı içinden çıkılmaz hukuki karmaşalara sürüklemektedir. Sonuç olarak artan denizcilik siber güvenlik riskleri, önleme, yargı yetkisi ve sorumluluk ile ilgili yasal zorluklara sebep olmaktadır.

IMO yasal araçlarının yanı sıra, siber uzay, devlet sorumluluğu, terörizm, silahlı çatışma, deniz savaşı ve güç kullanımını düzenleyen uluslararası hukuk da deniz siber güvenliği ile ilgili olacaktır. Spesifik konulardaki anlaşmazlıklara rağmen, Devletler siber uzayda uluslararası düzenlemelere duyulan ihtiyaç konusunda fikir birliğine sahiptir[69].

IMO, öncelikle deniz taşımacılığının güvenliği ve deniz kirliliğinin önlenmesi ile ilgilenir. Ancak Örgüt gemilerin neden olduğu kirlilik gibi hasarların sorumluluğunu ve tazminini kapsayan düzenlemeler de getirmiştir.

IMO'nun kirliliği önleme konusundaki teknik çalışmalarının yoğunlaşmasına yol açan 1967'deki Torrey Kanyonu felaketi, sorumluluk ve tazminat konusundaki çalışmaların da katalizörü olmuştur. Dünyanın ilk büyük tanker felaketinin ortaya çıkardığı yasal sorunlarla ilgilenmek için ad hoc bir Hukuk Komitesi kurulmuş ve Komite kısa süre sonra IMO Konseyi'nin daimi bir yan organı haline gelmiştir. Hukuk komitesi IMO'da ortaya çıkan herhangi bir yasal sorunu ele almak için yılda iki kez toplanmaktadır.

Deniz Emniyeti Komitesi (MSC), hem yolcu gemilerini hem de her türlü yük gemisini kapsayan, IMO'nun kapsamına giren deniz emniyeti ve deniz güvenliği ile ilgili tüm konularla ilgilenmektedir. Bu, SOLAS Sözleşmesinin ve tehlikeli mallar, can kurtarma cihazları ve yangın güvenlik sistemlerini kapsayan ilgili kodların güncellenmesini de içermektedir. MSC ayrıca, denizcilerin eğitimi ve sertifikasyonuna ilişkin STCW Sözleşmesi'nde yapılan değişiklikler de dahil olmak üzere insan unsuru konularını da ele almaktadır. MSC'nin güncel gündeminde, hedefe dayalı standartlar, otonom gemiler, korsanlık ve gemilere karşı silahlı soygun, siber güvenlik, e-seyrüsefer ve Küresel Deniz Tehlike ve Güvenlik Sisteminin (GMDSS) modernizasyonu dahil olmak üzere çok çeşitli konular bulunmaktadır. Örgüt ayrıca, gemilerin neden olduğu kirlilik gibi hasarların sorumluluğunu ve tazminini kapsayan düzenlemeler de getirmiştir.

Torrey Kanyonu tarafından gündeme getirilen ana konular petrol kirliliğinin neden olduğu zarardan kimin sorumlu tutulacağı, sorumluluk belirleme temeli ve zararın tazmin düzeyi olmuştur. Örneğin, iki gemi arasındaki bir çarpışmadan kaynaklanan hak taleplerinin çözüme kavuşturulması için hâlihazırda yerleşik prosedürler mevcuttur. Ancak Torrey Kanyonu gibi büyük bir kirlilik felaketi üçüncü tarafları içermekte ve neden olunan hasar çok büyük boyutlara ulaşabilmektedir. Sorumluluğun

belirlenmesini sağlayan ve ödenmesi gereken tazminatın ödenmesini sağlayan bir sistemin kurulması tüm bu açılardan önemli olarak değerlendirilmiştir.

Siber saldırılar hakkında ise IMO 2017 yılında bağlayıcı olmayan bir siber kılavuz ve ISM Kodunun uygulanmasına ilişkin bir kararı kabul etmiştir. Ancak hala denizcilik siber güvenliğine ilişkin potansiyel riskler düzenleyici kurumlardan yeterli ilgiyi görmemiştir.

Çizelge 3.1: IMO düzenlemeleri [70].

Düzenlenen Alan	Hukuki Araç
Deniz Emniyeti ve Güvenliği	SOLAS Konvansiyonu ISM Kodu ISPS Kodu Siber Risk Kılavuzu MSC. 428(98) Siber Risk Kararları
Deniz Trafiğinin Düzenlenmesi	FAL Konvansiyonu
Denizlerde Terörizm	SUA Konvansiyonu SUA Sabit Platform Protokolü

Deniz siber risk yönetimine ilişkin yönergelerin (MSC-FAL.1/Circ.3) amacı tehditler ve güvenlik açıklarından korunmak için deniz siber risk yönetimi konusunda tavsiyeler vermektir. Yönergeler denizcilik endüstrisindeki tüm kuruluşlara yönelik siber emniyet ve güvenlik yönetimi uygulamalarını teşvik etmek için düzenlenmiştir. Yönergelerde, risk yönetimi süreçlerinin geliştirilmesi ve uygulanmasına ilişkin ayrıntılar ve rehberlik için üye devletlerin ve ilgili bayrak devletlerinin gereksinimlerinin yanı sıra ilgili uluslararası düzenlemelere ve ilgili denizcilik endüstri standartlarına uyulması tavsiye edilmektedir.

Yönergelerde bu kılavuz ilkelerin, IMO tarafından oluşturulan emniyet ve güvenlik yönetimi uygulamalarını tamamlayıcı nitelikte olduğu söylenmektedir.

IMO'nun yayınladığı siber güvenlik düzenlemesi uyarınca[71];

Siber teknolojiler, denizciliğin emniyeti ve güvenliği ve deniz çevresinin korunması için kritik olan çok sayıda sistemin işletilmesi ve yönetimi için gerekli hale gelmiştir. Bazı durumlarda, bu sistemler uluslararası standartlara ve Bayrak İdaresi gerekliliklerine uygun olacaktır. Ancak bu sistemlere erişim, birbirine bağlanma veya ağ oluşturma yoluyla oluşturulan güvenlik açıkları, ele alınması gereken siber risklere yol açabilir. Savunmasız sistemler aşağıdakileri içerebilir;

- Köprüüstü sistemleri,
- Kargo elleçleme ve gemi yönetim sistemleri,
- Sevk ve makine yönetimi ile güç kontrol sistemleri,
- Erişim kontrol sistemleri,
- Yolcu servis ve yolcuyönetim sistemleri,
- Yolculara açık ağlar,
- İdari ve mürettebat refah sistemleri ve
- İletişim sistemleri. Ancak savunmasız sistemler sayılanlar ile de sınırlı değildir.

Uygulamada, "siber" terimi çeşitli bağlamlarda kullanılmaktadır ve terimin tek tip bir tanımı yoktur. Oxford İngilizce Sözlüğü siberi "bilgisayar, bilgi teknolojisi ve sanal gerçeklik kültürüyle ilgili veya bu kültürün özelliği" olarak tanımlarken, Cambridge İngilizce sözlüğü "bilgisayarları, özellikle interneti içeren, kullanan veya bunlarla ilgili" olarak tanımlar. Her ikisi de kapsamlı tanımlardır, ancak terimin iyi bir tanımını sağlayıp sağlamadığı şüphelidir.

IMO, Emniyet Yönetim Sistemlerinde deniz siber risk yönetimi (çözünürlük MSC.428(98)), operasyonel olarak siber risklere karşı güvenli ve emniyetli deniz taşımacılığını desteklemek için siber risk tehditlerini belirlemeye ve güvenlik açıkları hakkında farkındalığı artırmaya yönelik acil ihtiyaç varlığından yola çıkarak oluşturulmuştur.

MSC. 428(98) uyarınca idarelerin, klas kuruluşlarının, armatörlerin ve gemi operatörlerinin, gemi acentelerinin, ekipman imalatçıların, hizmet sağlayıcıların, limanların ve liman tesislerinin ve diğer tüm denizcilik endüstrisi paydaşlarının, gemiciliği mevcut ve ortaya çıkan siber tehditler ve güvenlik açıklarından korumaya yönelik çalışmaları hızlandırmaları gerektiği kabul edilerek "Onaylanmış bir emniyet yönetim sisteminin, ISM Kodunun MSC 428(98) işlevsel gereksinimlerine ve amaçlarına uygun olarak siber risk yönetimini dikkate alması gerektiğine karar vermiştir." Şirketler, en geç 1 Ocak 2021'den sonraki ilk yıllık doğrulamasından önce Uyumluluk Belgelerinin (DOC), siber güvenliğin güvenlik yönetim sistemlerinin ayrılmaz bir parçası olduğunu göstermelidir.

3.2 Taşıyanın Sorumluluğu Değerlendirmesi

3.2.1 Taşıyan kavramı

Konumuz kapsamında taşıyanın tanımını yapmak, sorumluluğun değerlendirilmesi bahsi için oldukça önemlidir. Uluslararası düzenlemeler ve iç hukukumuzda; taşıyan, fiili taşıyan, akdi taşıyan, donatan ve charterer gibi pek çok farklı kavram mevcuttur. Ancak en basit şekliyle taşıyan, navlun sözleşmesi karşılığında deniz yoluyla eşya taşımayı üstlenen kişidir[72]. Bu tanımdan anlaşıldığı üzere “taşıyan” kavramı bakımından belirleyici olan taşıma işleminin icra edilmesinden ziyade taşımanın yapılmasının vaad edilmesidir. Taşıyan, üstlendiği taşımayı bizzat yerine getirebileceği gibi, gemi işleten biri ile akdedeceği sözleşme aracılığı ile de ifa edebilir[73]. Gemi işleten ile akdedilen sözleşme TTK çerçevesinde şu şekilde düzenlenmiştir;

- Donatan ve gemi işletme müteahhidi ile akdedilen navlun sözleşmesine asıl navlun sözleşmesi
- Asıl navlun sözleşmesi aracılığıyla yapılacak olan diğer navlun sözleşmesine ise alt navlun sözleşmesi denmektedir.

Fiili taşıyan kavramı ilk kez 1929 tarihli Uluslararası Hava Taşımalarına İlişkin Bazı Kuralların Birleştirilmesi Hakkında Varşova Sözleşmesi’ni değiştiren 1961 tarihli “Akid Taşıyıcı Dışında Bir Kimse Tarafından Gerçekleştirilen Taşımalara Dair Ek Sözleşme”de(Guadajara Protokolü) yer almıştır[74]. Protokole göre fiili taşıyıcı, akdi taşımayı kısmen veya tamamen gerçekleştiren ve kısmen gerçekleştirdiği taşıma bakımından Varşova Konvansiyonu uyarınca ardışık taşıyıcı olmayan akdi taşıyıcıdan başka bir şahsı ifade eder.

Ardından fiili taşıyan kavramı 1974 tarihli “Yolcuların ve Bagajların Denizyolu Taşınmasına Dair Atina Sözleşmesi” ile deniz yolu ile yapılan taşımalar bakımından hükme bağlanmıştır[75]. Sözleşmenin 1(b) maddesi uyarınca fiili taşıyan, taşıyandan farklı bir kişi olup, bir geminin maliki, chartereri veya işleteni olarak, taşımanın tamamını veya bir kısmını fiilen gerçekleştiren kişidir.

Denizde eşya taşımaya ilişkin Lahey ve Lahey/Visby Kuralları’nda fiili taşıyana ilişkin özel bir düzenleme mevcut değildir.

Hamburg Kuralları'nda ise, hem fiili taşıyanın yükle ilgiliye karşı sorumluluğu, hem akdi taşıyanın fiili taşıyan ve onun adamlarının eylemlerinden sorumluluğu hakkında düzenlemeler mevcuttur (HK M. 10, 11)[76]. Hamburg Kuralları madde I(II) uyarınca, taşımanın gerçekleştirilmesi taşıyan tarafından kısmen veya tamamen kendisine bırakılan her şahıs ile böyle bir ifa kendisinden beklenen diğer bütün şahısları ifade eder[77].

Rotterdam Kuralları ise, Atina Sözleşmesi'nde fiili taşıyan kavramı 1/6a maddesinde 'ifa eden taraf' (performing party) ve 1/7 maddesinde ise 'limanda faaliyet gösteren kuruluşlar' (maritime performing party) şeklinde tanımlanmıştır[78].

Türk Ticaret Kanunu Madde 1191'de ise fiili taşıyan, taşımanın gerçekleştirilmesi kısmen veya tamamen kendisine bırakılan kişi olarak tanımlanmıştır.

3.2.2 Taşıyanın sorumluluğunun uluslararası konvansiyonlar ve Türk hukuku kapsamında değerlendirilmesi

Denizcilik sektöründe gerçekleşen siber saldırılardan taşıyanın sorumluluğu, kanaatimce geminin denize elverişliliği bahsi altında irdelenmelidir. Keza geminin siber güvenlik tedbirlerini almadan yola çıkması halinde maruz kalacağı GPS yanıltması yahut ECDIS saldırısı gibi saldırılar sonucu yükün varma limanına geç teslimi; siber saldırılar sonucu gemideki yükün hasara ve ziyaa uğraması da geminin elverişsizliğinin ortaya çıkardığı sonuçlar olarak değerlendirilebilecektir. Bu anlamda Türk Hukuku ve uluslararası sözleşmelerde pek çok düzenleme mevcuttur.

Türk Ticaret Kanunu'nda donatanın, kaptanın, taşıyanın ve fiili taşıyanın sorumlulukları ayrı ayrı düzenlenmiştir.

Türk Ticaret Kanunu'nda taşıyanın gemiyi başlangıçta denize, yola, yüke elverişli halde bulundurmama, eşyayı izinsiz başka gemiye yükleme ve aktarma, izinsiz güvertede taşıma ve haklı bir sebep olmaksızın rotadan ayrılma gibi bazı sebepleri ile eşyanın zıya veya hasara uğraması ya da geç tesliminden doğan zararlardan sorumluluk hakkında düzenlemeler getirilmiştir. TTK Madde 1141 uyarınca, taşıyan her türlü navlun sözleşmesinden kaynaklanan taşıma fiilini gerçekleştirirken geminin denize, yola ve yüke elverişli halde bulundurulmasını sağlamakla yükümlüdür. Bu maddenin devamında taşıyana dikkat ve özen gösterme yükümlülüğü de yüklenmiştir. Ancak kanundan dikkat ve özen gösterme yükümlülüğünün kapsamı yeterince anlaşılmamaktadır.

Taşıyanın sorumluluğu başlıklı Madde 1178'de ise taşıyanın sözleşmesel yükümlülüğü kapsamında yükle ilgili yükleme, istif, elden geçirme, taşınma ve gözetimi ve benzeri gibi konularda tedbirli taşıyandan beklenen dikkat ve özeni göstermesi yükümlülüğü getirilmiştir. Maddenin devamında geç teslim, hasar ve zıyaaya ilişkin sorumluluk, eşyanın/yükün taşıyanın himayesinde olduğu sırada ortaya çıkması halinde düzenlenmiştir.

Bu düzenlemeler çoğunlukla uluslararası konvansiyonlardan iç hukukumuzaya uyarlanan düzenlemeler niteliği taşımakta ve konvansiyonlarda sınırı çizilen taşıyanın sorumluluğu bahsi de çoğunlukla bu ana başlıklara odaklanmaktadır.

Tüm konvansiyonlarda ortak olarak düzenlenen yükün zıya veya hasara uğraması ya da geç tesliminden doğan zarardan sorumluluk dikkat çekilmesi gereken düzenlemelerden biridir. Zıya, sebebi ne olursa olsun, taşıyanın teslim aldığı yükü, geminin varma limanına ulaşmasından sonra, teslim etmesi gereken süre içinde, teslim almaya yetkili olan şahsa teslim etme yeteneğinden tamamen veya kısmen yoksun olmasıdır [79]. Yükün zıya olması ise yükün tamamen yok olmasından ya da değerini tümüyle yitirmesinden; fiziki olarak asli niteliğini kaybetmesine yol açacak şekilde değişime uğramasından veya daimi olarak yahut belirsiz bir süre için taşıyanın elinden çıkmış bulunmasından kaynaklanabilir [80]. Çalınma; müsadere edilme; haczedilme; batma; teslim almaya yetkili olmayan bir kişiye teslim edilmiş olma; yanlışlıkla ara limanda boşaltılma; taşıyan yahut kaptan tarafından satılmış olma; başka bir konişmento üzerinden yüklendiği için diğer bir yükle karışmış ya da sebebi açıklanamayan şekilde kaybolmuş olması halinde ise yükün taşıyanın elinden çıkması söz konusudur[81].

Taşıyanın geçici bir süre için yükü teslim etmek iktidarından yoksun olması halinde ise zıya durumu söz konusu olmayacaktır. Bu geçici sürenin sınırı TTK m. 1178/f. 5 uyarınca altmış gün olarak belirlenmiştir. Söz konusu hükme göre, TTK m. 1178/f. 4 uyarınca teslim süresinin dolmasından itibaren, aralıksız altmış gün içinde teslim edilmeyen eşya zayi olmuş kabul edilebilecektir.

Hasar, sebebi ne olursa olsun yükün maddi varlığının bozulması veya kötüleşmesi ve bu yüzden değerinin düşmesidir[82]. Yükün geç teslim edilmesi sonucunda maddi varlığı herhangi bir zarara uğramayan ancak piyasa değeri düşen bir yükün hasara

uğradığından söz edilemez[83]. Bu halde gecikme zararı üzerinden bir değerlendirme yapılmalıdır.

Hasar, eşyanın/yükün tamamında meydana gelebileceği gibi eşyanın/yükün bir kısmında da meydana gelmiş olabilir. Bir yük partisinin bir kısmında meydana gelen hasar, hasar görmemiş kısmın değerinde de azalmaya yol açıyorsa yükün tamamının hasara uğradığının kabulü gerekir[84].

Yükün hasara uğraması sonucu iktisadi değeri de tamamen ortadan kalktıysa yahut asli niteliğini tamamen yitirdiyse de yükün zıyaa uğradığı kabul edilir.

Tüm konvansiyonlarda düzenlenen bir diğer sorumluluk hali ise taşıyanın gemiyi denize, yola ve yüke elverişli halde bulundurma yükümlülüğüdür. Denize elverişlilik, geminin fiziki varlığının, somut yükle birlikte gerçekleştirilecek belirli yolculukta, tamamıyla olağanüstü olanlar dışındaki deniz tehlikelerine karşı koymaya elverişli olmasını ifade etmektedir[85]. Kanaatimizce denize elverişlilik bahsi altında değerlendirilmesi gereken denizlerde gerçekleşen siber saldırılardan taşıyanın sorumluluğunun anlaşılabilmesi için konunun açıkça irdelenmesine ihtiyaç vardır.

Özellikle geminin denize ve yola elverişliliğinin sağlamasına yönelik önlemler TTK Madde. 932'ye göre geminin teknik yönetimi kapsamında değerlendirilir. Dolayısıyla başlangıçta geminin denize elverişsizliğe neden olan bir kusurun teknik kusur teşkil etmesi yüksek ihtimaldir. Taşıyanın geminin başlangıçtaki elverişsizliğinden kaynaklanan zararlardan sorumluluğu ise TTK m. 1141 hükmüne tâbidir. Taşıyan, başlangıçtaki elverişsizlik söz konusu olduğunda teknik kusura dayanarak sorumluluktan kurtulma imkanı bulamayacaktır[86]. Dolayısıyla TTK m. 1141'de aranan koşullar gerçekleştiğinde taşıyan elverişsizliğin neden olduğu zararlardan sorumludur.

Geminin yolculuk sırasında elverişsiz hâle gelmesi TTK m. 1179 hükmünün kapsamına girdiğinden, taşıyanın bu çerçevede teknik kusurdan sorumsuzluğa dayanması mümkündür[87]. Ancak bu durumda geminin yolculuk sırasında gerçekleşen bir siber saldırı halinde elverişsiz hale gelmesi ayrıca değerlendirilmelidir. Taşıyanın siber güvenlik ile ilgili alması gereken önlemleri almaması yahut geminin IMO tarafından zorunlu tutulmuş siber güvenlik yönetim sistemine sahip olmaması halinde taşıyanın, yerine getirmesi gereken yükümlülüklerini yerine getirmediğini söylemek yerinde olacaktır.

Uluslararası sözleşmelerde de taşıyanın gemiyi denize elverişli halde bulundurma yükümlülüğü düzenlenmiştir.

Lahey, Lahey/Visby Kuralları'nın 3. maddesinin 1. fıkrasına göre taşıyan yolculuğun başlangıcında gemiyi yolculuğa elverişli hale getirmek, tüm gerekli teçhizatla donatmak, gerekli tedarikleri sağlamak, geminin ambarlarının ve soğuk hava depolarının ve yüklerin tesellüm, nakil ve muhafaza edilmek üzere yerleştirilmiş olduğu bütün diğer kısımlarını elverişli ve yüke uygun vaziyete getirmek için makul bir gayret göstermesi zorunlu tutulmuştur[88]. Makul gayretin tanımı ise konvansiyon kapsamında yapılmamıştır.

Lahey, Lahey/Visby Kuralları'na göre taşıyanın yolculuğun başlangıcında gemiyi denize, yola ve yüke elverişli hale getirmemesinden kaynaklanan sorumluluğu, yüklemenin başladığı an ile yolculuğun başladığı an arasında kalan zaman dilimindedir[89].

Lahey, Lahey/Visby Kuralları'na göre taşıyanın yüke özen gösterme sorumluluğu ise kusur sorumluluğu olarak tanımlanmıştır[90]. Lahey, Lahey/Visby Kuralları'nda taşıyanın yüke özen gösterme sorumluluğuna yer verilmiş ancak taşıyanı bu sorumluluktan muaf tutan detaylı bir liste de kurallara eklenmiştir. Bu listedeki en önemli kurallar ise, ortaya çıkan zayi olma ve hasar durumunun; taşıyanın hata ve ihmalden olmaksızın gerçekleşen bir yangından kaynaklanması ve geminin yönetiminden yahut navigasyon hatasından kaynaklanması durumunda taşıyanın sorumluluğuna gidilememesidir [91]. Siber saldırı sonucu gerçekleşecek bir navigasyon yanıltması ise geminin siber tehditlere karşı korunması için gerekli teçhizatla donatma kapsamında değerlendirilecek; taşıyanın, gemiyi denize elverişlili ve yüke uygun vaziyette bulundurması yükümlülüğü kapsamında olduğu için sorumluluktan muaf tutulamayacaktır.

Lahey, Lahey/Visby Kuralları'nda yer alan genel sorumsuzluk kaydına göre ise, taşıyanın ve adamlarının sorumluluklarının kanıtlanamaması durumunda, taşıyan sorumlu olmayacaktır.

Lahey, Lahey/Visby Kuralları'na göre taşıyanın ihmali, hatası veya konvansiyonda bahsedilen yükümlülüklerini yerine getirmemiş olması ya da eksik yerine getirmiş olmasından kaynaklanan yükte meydana gelen zayi olma veya hasara uğrama gibi durumlardan kaynaklanan sorumluluktan istisna tutan veya taşıyanın bu

sorumluluklarını azaltan herhangi bir sözleşme hükmü veya anlaşma hükümsüz olur[92].

Hamburg Kuralları'nda ise yükün zayi olması, hasara uğraması veya geç teslim edilmesi hallerinde oluşacak zararlardan doğan sorumluluk düzenlenmiştir[93].

Hamburg Kuralları'nın 4. maddesi uyarınca yükün taşınmak üzere teslim alındığı an ile varma limanında teslim edildiği an arasındaki sürede meydana gelen yükün zayi olması, hasara uğraması veya geç teslim edilmesi durumunda taşıyanın bu yüzden ortaya çıkan zarardan ve gecikmeden sorumlu olduğu yönünde karine doğmaktadır. Bu karinenin çürütülebilmesi için taşıyan, adamları veya görevlileri doğan zararı önlemek için alınması makul ölçüde beklenebilecek bütün tedbirlerin alındığını kanıtlamakla yükümlüdür. Taşıyan, adamları veya görevlileri sadece kusurlu bulundukları hallerden sorumludur. Kusursuzluklarını ispatlamaları halinde ise yükün zayi olması, hasara uğraması veya geç teslim edilmesiyle oluşan zarardan sorumlu olmaktadır[94]. Tüm bunlara gereksinim olmasının sebebi ise kusur karinesine dayanan sorumluluğun, taşıyanın aleyhine kabul edilen karineyi çürütmemesi halinde taşıyanın kusurlu sayılmasını ve kusurlu sayıldığı için de sorumlu tutulmasını gerektirmesidir[95].

Hamburg Kuralları'nın 5. maddesinin 7. Fıkrasında taşıyan ve adamlarının kusurları oranında yükün zayi olması, hasara uğraması veya geç teslim edilmesinden sorumlu oldukları düzenlenmiştir[96]. Bu düzenleme ile amaçlanan, başka bir sebep ile taşıyan ve adamlarının kusurunun hasar ve zararın meydana gelmesinde etkili olması halinde, taşıyanın kendi kusurundan ortaya çıkan kısmını ispatlamasıdır[97].

Hamburg Kuralları'na göre, taşıyan veya adamları meydana gelen olay ve bundan doğan zararı önleyebilmek için makul surette istenebilecek olan bütün tedbirleri almış olduklarını ispat ederek sorumluluktan kurtulabilir.

Hamburg Kuralları'na göre taşıyanın yalnızca geçici bir süre için yükü teslim etme yeteneğinden yoksun olduğu hallerde, yükün zayi olması söz konusu olmayacaktır. Hamburg Kuralları'nın 5. maddesinin 3. Fıkrasına göre yükün zayi olmuş olarak değerlendirilebilmesi için, 60 gün içerisinde teslim edilmemesinin söz konusu olması gerektiği belirtilmiştir.

Hamburg Kuralları'nın 5. maddesinin 2. fıkrasında ise geç teslimin tanımı ise navlun sözleşmesinde öngörülen süre zarfında yahut taraflar arasında herhangi bir sözleşme

yok ise olayın özelliklerine göre, tedbirli taşıyanın uyması makul surette beklenebilecek olan süre içinde teslim edilmemesi olarak yapılmıştır.

Rotterdam Kuralları yürürlükte değildir. Ancak taşıyana yüklenen sorumluluğa ilişkin değerlendirmesi sebebiyle ele alınacaktır. Rotterdam Kuralları'nda taşıyan yüke zilyet olduğu müddetçe sorumlu tutulmaktadır. Rotterdam Kuralları'nda yükümlülükler yük yalnızca denizde taşınırken değil, taşıyanın sorumluluğundaki tüm taşıma sürecine uygulanmaktadır[98].

Rotterdam Kuralları'nın 13. maddesinde; Taşıyana 12. Madde hükümlerince tanımlanan sorumluluk süresi ve madde 26 uyarınca taşıyanın özen yükümlülüğü kapsamında teslim alma, yükleme, elden geçirme, istifleme, taşıma, muhafaza etme boşaltma ve teslim etme faaliyetleri düzenlenerek, taşımanın diğer safhaları da sözleşmesel sorumluluğa dahil edilmiştir. Bu yönüyle Rotterdam Kuralları, Lahey, Lahey/Visby Kuralları'ndan ayrılmaktadır.

Rotterdam Kuralları'nda taşıyanın gemiyi denize, yola ve yüke elverişli bir halde bulundurma yükümlülüğü yolculuk sonuna kadar genişletilmiştir[99]. Düzenleme uyarınca taşıyan, gemiyi yolculuğa elverişli hale getirmek ve yolculuğa elverişli halde tutmakla, gemiyi gerekli tüm mürettebat, ekipman ve erzakla donatıp yolculuk sonuna kadar bu halde tutmakla, yükün taşınacağı kısımların ve geminin diğer kısımları ile yükün üstünde veya içinde taşınacağı konteynerlerinde yüke uygun ve güvenli olmasını sağlamakla yükümlü tutulmuştur.

Marina Insurance Act 1906 madde 39/4 uyarınca geminin elverişliliği sigorta koruması sağlanmış seferdeki geminin denizdeki olağan tehlikelere karşı koyacak makul uygunlukta olması halinde denize elverişli olarak kabul edileceği belirtilmiştir[100].

Uluslararası Güvenlik Yönetim Kodu(ISM Code) da geminin başlangıçtaki elverişliliğine ilişkin esaslar getirmiştir. UGYK ile belirlenen esasların yerine getirilmesi halinde gemiyi işleten için düzenlenen “Uygunluk Belgesi” ve gemi için düzenlenen “Güvenlik Yönetimi Sertifikası”, geminin denize, yola ve yüke elverişliliğine etkili olan konularda gereken özenin gösterilip gösterilmediğine karine teşkil edecektir [101]. Bu belgelere sahip olmayan ya da bu belgelerin tespit ettiği olgularının aksinin ispatlanması halinde taşıyanın şahsi kusurundan ve sorumluluğundan bahsedilebilecektir.

Olası bir siber saldırı ile geminin navigasyon sistemine müdahale edilerek rotasından saptırılması sonucu, yükün geç teslimi gündeme gelecektir. Bu durumda taşıyanın, siber güvenlik ile ilgili yükümlülüklerini yerine getirirken kendisinden beklenen dikkat ve özeni gösterip göstermediği değerlendirmesi yapılması gerekecektir. Yine taşıyanın, gemiyi denize elverişli halde bulundurma yükümlülüğü kapsamında değerlendirilmesi gereken geminin siber risklere karşı donanımının sağlanması da değerlendirilmesi gereken hususlardandır. Hangi durumlarda siber saldırıların teknik kusur olarak kabul edileceği henüz tanımlanmamıştır. Keza denize elverişlilik bahsi altında tartışılması gereken mutlak sorumsuzluk sebepleri içinde sayılan teknik kusur ve ticari kusur ayrımı da taşıyanın sorumluluğunun belirlenmesi öneme haizdir.

Bunun yanı sıra denizel alanda gerçekleşen siber saldırılar hem emniyet hem güvenlik sorunu olmaları sebebiyle yalnızca hukuki değil cezai sorumluluğa da yol açabilecektir. Günümüzde bu alanın tam olarak düzenlenmemiş olması siber saldırılar sonucu hayatını kaybeden gemi insanları ya da siber saldırı sonucu gemilerin kusurlu çatmaya karışması gibi açılardan da değerlendirilmelidir.

3.2.3 Mutlak sorumsuzluk sebepleri

Kanaatimizce gemiyi denize elverişli halde bulundurma yükümlülüğü kapsamında değerlendirilmesi gereken siber risklere karşı donanımın sağlanması, mutlak sorumsuzluk sebepleri başlığı altında da değerlendirilmelidir. Türk Ticaret Kanunu'ndaki mutlak sorumsuzluk sebepleri geminin sevki ve başkaca teknik yönetimindeki kusur, yangın, denizde kurtarma, eşyanın cins ve değerinin kasten yanlış bildirilmesi olarak 4 başlık altında düzenlenmiştir.

Siber risklere karşı donanımın sağlanması geminin sevki ve başkaca teknik yönetimindeki kusur olarak değerlendirildiğinde mutlak sorumluluk sebebi sayılabilecektir. Ancak kanaatimizde başlangıçtaki elverişsizlik olarak değerlendirilmelidir. Geminin başkaca teknik yönetimi doktrinde açıkça tanımlanmamış ve sınırları çizilmemiş bir kavramdır. Başkaca teknik yönetim kusuru, geminin sevki dışındaki yönetimine ilişkin olan ve başlangıçtaki elverişsizlik yahut yüke özen borcunun ihlali kapsamında değerlendirilemeyecek kusur olarak tanımlanabilir[102]. Özellikle gemi makinelerinin ve teçhizatının kullanımında ortaya çıkan geminin başkaca teknik yönetimine ilişkin kusur; gemi henüz hareket halinde değilken veya limanda bekleme halindeyken dahi söz konusu olabilmektedir. Geminin

elverişsizliğine sebep olan ve geminin yolculuğa başlamasından önceki süreçte meydana gelen bir teknik kusur söz konusuysa taşıyan buna dayanarak sorumluluktan kurtulma imkanı bulamayacaktır[103].

Geminin sevki veya teknik idaresi tanımı ile geminin devamlı hareketinin sağlanması ifade edilmekte; hatalı rota tayini sonucu karaya oturma gibi haller geminin teknik sevk ve idaresine ait bir kusur olarak kabul edilmektedir.

Seyir kusuru, geminin denizde hareketi ile ilgili yapılması gerekenler ve alınması gereken tedbirler ile ilgili kusurlu halleri tanımlarken; bütün manevra hareketleri, dümen ve makine kumandaları, mevki tayini, radar, ışıklandırma, işaret verme, deniz trafik kurallarına uyma ve benzeri durumlar da bu kapsamda değerlendirilmekte; teknik sevk ve idare kusuru(fault in navigation) olarak kabul edilmektedir. Bu durumda geminin siber donanımının seyir sırasında bozulması ya da

TTK Madde 1180 uyarınca daha çok yükün menfaati amacıyla alınan önlemler, geminin teknik yönetimine dahil sayılmayacaktır[104]. Yükün menfaati amacıyla alınan önlemler; yükün yüklenmesi, istifi, elden geçirilmesi, taşınması ve boşaltılmasına ilişkin tüm hazırlık ve icra faaliyetleri ile yolculuk sırasında yükün korunması ve gözetimine yönelik önlemlerdir[105].

Burada yapılması gereken en önemli ayrım “teknik kusur” ve “ticari kusur” ayrımıdır. Teknik kusur, geminin korunması ve emniyetine ilişkin cihaz ve parçaların kötü ve yanlış kullanılmasındaki kusur iken, yükün korunması iyi halde muhafaza edilmesine ilişkin cihazların gereği gibi kullanılamaması ticari kusurdur.

Yük ile ilgili yapılan işlemler, geminin stabilitesini temin etmek amacıyla yükün istiflenmesi örneğinde olduğu gibi geminin menfaati için de yapılabilir. Ancak, yalnızca yüke hizmet eden bir aracın/tesisatın kullanılmasındaki hata ticari kusur olacaktır. Gemide yükle ilgili vinçlerin kullanımındaki veya ambarları soğutma, havalandırmadaki teçhizatların hatalı veya ihmalen yanlış kullanımı, yüke ilişkin bir kusur olarak değerlendirilmeli ve ticari kusur olarak ele alınmalıdır[106]. Gemilerde kullanılan teknolojik sistemler ise hem geminin korunması ve emniyetine ilişkin cihaz ve parçalar ile ilintiliyken hem de yükün korunması ve iyi halde muhafaza edilmesine ilişkin cihazları da içermektedir.

Yükün hasar ve kaybına ilişkin açılan davalarda, taşıyanın kusurunun ispatı kural olarak davacıya düşmektedir. Taşıyan olayda kendisine yüklenecek bir kusur

olmadığını, ya da kusurun gemi adamlarının “sevk ve diğer teknik idare” kapsamında olduğunu ileri sürerek bu konudaki sorumluluktan kurtuluş beyinnelerine dayanmaması durumunda ise ispat yükü taşıyana düşmektedir.

Taşıyan olayda, yükteki zararın adamlarının geminin sevkine veya başkaca teknik idaresine ait bir fiili veya yangın neticesi meydana geldiğini ve kendisinin bir kusuru bulunmadığını ispat etmekle yükümlüdür.

Taşıyanın yalnızca şahsi kusurundan kaynaklana yangın sonucu meydana gelen zararlardan sorumlu olduğu taşıyanın şahsi kusurundan kaynaklanmayan bu kapsamda adamlarının TTK Madde 1179/2 kusuruyla sebebiyet verdikleri yangından ileri gelen zararlardan ise sorumsuz olduğu TTK Madde 1180/1’de düzenlenmiştir. Ancak geminin yolculuğun başlangıcındaki elverişsizliğinden kaynaklanan yangın, mutlak sorumsuzluk sebebi kapsamında değildir. Ancak yangın ile sefere elverişsizlik arasında herhangi bir illiyet bağı kurulamadığı takdirde, taşıyan yangından ileri gelen zararlardan sorumlu tutulamayacaktır.

Türk Ticaret Kanunu’nda düzenlenen diğer mutlak sorumsuzluk halleri siber saldırılardan doğabilecek taşıyanın sorumluluğunun kapsamından uzak olduğu için değerlendirilmemiştir.

4. METODOLOJİ

4.1 AHP Metodu

Karar verme yöntemleri iki farklı gruba ayrılır: sezgisel yöntemler ve analitik yöntemler[107]. Büyük miktarda bilgi topladığımız karar verme, “günümüzde bir matematik bilimi haline gelmiştir” [108].

Analitik Hiyerarşi Prosesi, ilk olarak 1968 yılında Myers ve Alpert tarafından ortaya çıkarılmış ve 1977’de ise Profesör Thomas Lorie Saaty tarafından bir model olarak geliştirilerek karar verme problemlerinin çözümünde kullanılabilmesinin yolu açılmıştır[109]. Karar vermede matematiksel yöntemler hızlı, doğru ve güvenli çözümler sağlamaktadır. Bir kararın kalitesi, matematiksel yöntemlerin kullanılmasıyla da belirlenir. Bu nedenle, bazı akademisyenler optimum karar vermenin “matematiksel optimizasyon problemi”ne eşit olduğunu savunmaktadır[110].

AHP güçlü bir matematiksel temele sahiptir ve alternatiflerin değerlendirilmesi ve seçilmesi sürecinde kullanılmaktadır[111]. AHP'ye göre karar verme geniş ve karmaşık bir süreçtir çünkü AHP hem fiziksel hem de sosyal alanlarda karar vermek için kullanılabilmektedir[112].

AHP, kişilerin kendi karar verme mekanizmalarını tanıması için yönlendirme yaparak daha iyi kararlar alınmasını sağlayan bir yöntemdir[113]. Tanımlanmış bir karşılaştırma skalası kullanılarak ikili karşılaştırmalarla hiyerarşideki karar noktalarına ilişkin önem farklılıklarının yüzde dağılımları tespit edilmektedir. Yüzde dağılımları tespit edilerek sistematik bir yaklaşımla sayısal performans ölçümleri, subjektif değerlendirmeler ile birleştirilmekte ve ardından sonuçlaştırılmaktadır [114]. Sonuç olarak AHP kriter önceliklerinin belirlenmesini ve belirlenen bu kriter önceliklerinden yola çıkarak alternatiflerin değerlendirilmesini, söz konusu belirlenen amaç ya da amaçları gerçekleştirecek verimli ve doğru kararların alınmasını sağlar.

Bunu yaparken de karar vericilerin/uzmanların bilgi ve deneyimlerinden etkin olarak yararlanılır.

Analitik Hiyerarşi Yöntemi, her seviyede birbirinden bağımsız olan faktörlerin sıralandıkları hiyerarşik yapıda değerlendirilmesinde kullanılır[115].

Analitik Hiyerarşi Yönteminde kararı alan ve çoğunlukla kararın uygulayıcısı olan kişiler karar sürecinde yer aldığı ve kendi öznel değerlendirmelerini de modele yansıtılabildikleri için sonuçları anlama, yorumlama ve benimseme konusunda daha başarılıdır. Bu durum da sonuçların uygulanma olasılığını diğer modellere göre arttırır.

4.2 AHP Yapısının Oluşturulması

AHP'nin ana aşamaları[116]:

- Problemin tanımı ve hiyerarşik bir yapının oluşturulması,
- Kriterlerin ikili karşılaştırmaları,
- Karşılaştırma matrisinin normalleştirilmesi ve tutarlılığın ölçülmesi şeklindedir.

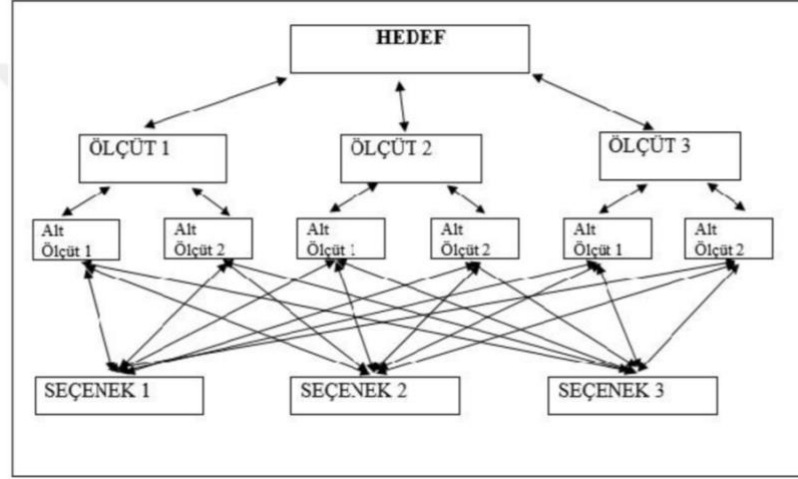
Bireyler veya örgütler ihtiyaçlarını saptamak ve bu ihtiyaçlarına çözüm bulma adına yapmayı düşündükleri eylemlerin planlanması, problem tanımlama olarak ifade edilebilir. İlgili problem tanımlandıktan sonra AHP yönteminin uygulama aşamalarına geçilir (Ishizaka ve Labib, 2011).

Hiyerarşik yapının oluşmasında etkili olan ve önemli noktalar aşağıdaki gibidir (Saaty, 1990):

1. Hiyerarşik yapı, problemi mümkün olan en gerçek şekilde temsil etmelidir.
2. Soruna etki eden tüm alt etmenler hesaba katılmalıdır.
3. Çözümde etkisi olabilecek tüm yayın ve dökümanlar dikkate alınmalıdır.
4. Sorun bağlamında etkili olacak katılımcılar için bir karar verilmelidir.

Hiyerarşinin en tepesinde ana amaç vardır. Sırasıyla altında, karar üzerinde etkiye sahip olan ana ölçütler onunda altında ise bu ana ölçütlere bağlantılı olan alt ölçütler bulunmaktadır. En aşağıda ise kararlara alterantif olabilecek seçenekler vardır (Kocakaya, 2019).

Şekil 2.'de AHP karar verme süreci gösterilmektedir.



Şekil 4.1: AHP karar verme süreci.

4.3 AHP Değerlendirme Formu ve Datalar

Uygulama olarak: AHP ile Denizcilik Sektöründeki Siber Gelişmelerin Deniz Ticaretine Etkileri çalışması yapılmıştır. AHP anketi ile daha önce belirlenen ana başlıklar olan; teknolojik gelişmeler, siber saldırı, siber saldırı sonuçları, siber saldırılardan taşıyanın ticari sorumluluğu, siber saldırılardan taşıyanın cezai sorumluluğu, IMO düzenlemeleri ikili karşılaştırmaları deniz güvenliği ve denizcilik uzmanları tarafından yapılan seçimler neticesinde sonuçlandırılmıştır.

Teknolojik Gelişmeler

Çizelge 4.1: AHP alt ve ana boyutlar.

A	Teknolojik Gelişmeler
A1	Deniz ticareti ile ilgili evrakların(konışmento ve benzeri) interaktif ortama taşınması
A2	Gemilerin daha hızlı çalışması ve makineleşmesi sonucu sürekli ve hızlı veri akışı
A3	Veri depolama ve donanımda gerçekleşen bulut devriminin sağladığı güçlü veri çözümleri
A4	Gemi ile kıyı bağlantısının iyileştirilmesi sayesinde, kıyıda yüzlerce mil uzaktaki geminin performansı hakkında edinilen gerçek bilgi
A5	Gaz emisyonları, kargo sıcaklığı ve benzeri gibi gemilerdeki bileşenlerle ilgili gerçek zamanlı verilerin toplanmasındaki bakım ve güvenlik verimliliği
A6	Gaz emisyonları, kargo sıcaklığı ve benzeri gibi gemilerdeki bileşenlerle ilgili gerçek zamanlı verilerin toplanmasıyla azalan işletme maliyeti ve ihmalden kaynaklanan arıza riski
A7	Denizcilik altyapılarının IP tabanlı sistemler aracılığıyla birbirine bağlanarak ortak bir operasyon resmi sunması
A8	Otonom gemilerde insan gücüne duyulan bağımlılığın azalması
A9	Otonom gemilerin yaygınlaşmasıyla gemi kazalarında azalan insan faktörü ve insan hatasını
A10	Otonom gemilerin yaygınlaşması

Çizelge 4.1 (devam): AHP alt ve ana boyutlar.

B	Siber Saldırıları
B1	Sinyal bozma saldırıları
B2	Sahtecilik saldırıları
B3	Zayıf şifre politikası
B4	Radar saldırıları
B5	Fidye yazılımı saldırıları
C	Siber Saldırı Sonuçları
C1	Geminin kaçırılması
C2	Ağ sistemleri ile haberleşme kaybı
C3	Değerli verilerin çalınması
C4	Gemi operasyonlarının kesintiye uğraması
C5	Can ve mal kaybı
C6	Ekipmanların zarara uğraması
C7	İletişim sistemi ve bilgisayar sisteminin bozulması
C8	Kargo ve operasyon yönetiminde gecikmeler
C9	Haksız maddi kayıplar
C10	Tesislere fiziki zarar
D	Siber Saldırılarından Taşıyanın Ticari Sorumluluğu
D1	Geminin yola elverişli olmaması
D2	Geminin yüke elverişli olmaması
D3	Geminin sefere elverişli olmaması
D4	Eşyanın zıya veya hasara uğraması
D5	Yükün geç teslimi
D6	Ticari kusur
D7	Geminin sevki ve başkaca teknik yönetimindeki kusur
D8	Yüke hizmet eden bir tesisatın kullanılmasındaki hata
D9	Dümen ve makine kumandaları, mevki tayini, radar ve işaret verme gibi kusurlar
E	Siber Saldırılarından Taşıyanın Cezai Sorumluluğu
E1	Çatma
E2	Yükün zıya veya hasara uğraması
E3	Deniz kirliliği
E4	Denizdeki suçlara karşı koruma
E5	Petrol tankerlerine saldırı
E6	Nükleer gemilere saldırı
E7	Tehlikeli madde taşıyan gemilere saldırı
E8	Deniz emniyetinin tehlikeye girmesi
E9	Kıyı emniyetinin tehlikeye girmesi
F	IMO Sözleşmeleri
F1	Denizde Can Emniyeti Uluslararası Sözleşmesi(SOLAS)
F2	Gemilerden Kaynaklanan Kirliliğin Önlenmesine İlişkin Uluslararası Sözleşme(MARPOL)
F3	Petrol Kirliliğinden Doğan Zararın Hukuki Sorumluluğu ile İlgili Uluslararası Sözleşme(CLC)
F4	Petrol Kirliliği Zararlarının Tazmini İçin Uluslararası Bir Fonun Kurulmasına İlişkin Uluslararası Sözleşme(FUND 1992)
F5	Nükleer Maddelerin Denizden Taşınmasında Hukuki Sorumlulukla İlgili Sözleşme(NUCLEAR), 1971
F6	Deniz Alacaklarına Karşı Mesuliyetin Sınırlandırılması Hakkında 1976 Tarihli Uluslararası Sözleşme(LLMC)
F7	Tehlikeli ve Zararlı Maddelerin Deniz Yoluyla Taşınmasından Doğan Kirlilik Zararlarının Tazmini ve Sorumluluğa İlişkin Uluslararası Sözleşme(HNS), 1996(ve 2010 Protokolü)
F8	Gemi Yakıtlarından Kaynaklanan Petrol Kirliliği Zararın Hukuki Sorumluluğu Hakkına Uluslararası Sözleşme, 2001
F9	Enkaz Kaldırmaya İlişkin Nairobi Sözleşmesi, 2007

4.4 Bulgular

4.4.1 A faktörü için AHP analizi

Çizelge 4.2: Faktörü için AHP analizi (1).

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	4.67	4.83	2.86	3.14	3.26	3.68	5.83	2.86	1.76
A2	0.21	1.00	4.80	2.95	4.24	3.05	5.80	4.09	4.02	2.73
A3	0.21	0.21	1.00	1.57	1.11	2.32	4.09	3.86	1.60	3.09
A4	0.35	0.34	0.64	1.00	2.27	2.23	1.77	3.92	3.26	1.88
A5	0.32	0.24	0.90	0.44	1.00	1.19	4.90	2.50	1.89	3.26
A6	0.31	0.33	0.43	0.45	0.84	1.00	7.20	3.49	1.72	4.22
A7	0.27	0.17	0.24	0.56	0.20	0.14	1.00	0.80	1.53	1.53
A8	0.17	0.24	0.26	0.25	0.40	0.29	1.26	1.00	0.13	0.13
A9	0.35	0.25	0.63	0.31	0.53	0.58	0.65	7.46	1.00	3.04
A10	0.57	0.37	0.32	0.53	0.31	0.24	0.65	7.58	0.33	1.00
SUM	3.76	7.81	14.05	10.92	14.04	14.29	31.00	40.52	18.34	22.65
Criteria Weights	0.24	0.19	0.10	0.10	0.08	0.09	0.04	0.02	0.07	0.06

Çizelge 4.3: A faktörü için AHP analizi (2).

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	Criteria Weights
A1	0.27	0.60	0.34	0.26	0.22	0.23	0.12	0.14	0.16	0.08	0.24
A2	0.06	0.13	0.34	0.27	0.30	0.21	0.19	0.10	0.22	0.12	0.19
A3	0.06	0.03	0.07	0.14	0.08	0.16	0.13	0.10	0.09	0.14	0.10
A4	0.09	0.04	0.05	0.09	0.16	0.16	0.06	0.10	0.18	0.08	0.10
A5	0.08	0.03	0.06	0.04	0.07	0.08	0.16	0.06	0.10	0.14	0.08
A6	0.08	0.04	0.03	0.04	0.06	0.07	0.23	0.09	0.09	0.19	0.09
A7	0.07	0.02	0.02	0.05	0.01	0.01	0.03	0.02	0.08	0.07	0.04
A8	0.05	0.03	0.02	0.02	0.03	0.02	0.04	0.02	0.01	0.01	0.02
A9	0.09	0.03	0.04	0.03	0.04	0.04	0.02	0.18	0.05	0.13	0.07
A10	0.15	0.05	0.02	0.05	0.02	0.02	0.02	0.19	0.02	0.04	0.06
SUM	1	1	1	1	1	1	1	1	1	1	

Çizelge 4.4: A faktörü için AHP analizi (3).

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	Weighted Sum Values	Criteria Weights
A1	0.24	0.91	0.48	0.29	0.26	0.30	0.14	0.14	0.19	0.10	3.06	0.24
A2	0.05	0.19	0.47	0.30	0.36	0.28	0.23	0.10	0.27	0.16	2.41	0.19
A3	0.05	0.04	0.10	0.16	0.09	0.21	0.16	0.09	0.11	0.18	1.19	0.10
A4	0.08	0.07	0.06	0.10	0.19	0.21	0.07	0.10	0.22	0.11	1.20	0.10
A5	0.08	0.05	0.09	0.04	0.08	0.11	0.19	0.06	0.13	0.19	1.02	0.08
A6	0.07	0.06	0.04	0.05	0.07	0.09	0.28	0.09	0.11	0.24	1.11	0.09
A7	0.07	0.03	0.02	0.06	0.02	0.01	0.04	0.02	0.10	0.09	0.46	0.04
A8	0.04	0.05	0.03	0.03	0.03	0.03	0.05	0.02	0.01	0.01	0.29	0.02
A9	0.08	0.05	0.06	0.03	0.04	0.05	0.03	0.18	0.07	0.18	0.78	0.07
A10	0.14	0.07	0.03	0.05	0.03	0.02	0.03	0.19	0.02	0.06	0.63	0.06
Analiz Geçerliliği için $CR_D < 0,10$ olmalı												Lamdama x
												CI_D
												0.22
												CR_D
												0.14

4.4.2 B faktörü için AHP analizi

Çizelge 4.5: B faktörü için AHP analizi (1).

	B1	B2	B3	B4	B5
B1	1.00	3.71	4.45	3.03	2.03
B2	0.27	1.00	2.49	3.63	1.91
B3	0.22	0.40	1.00	1.60	0.76
B4	0.33	0.28	0.63	1.00	0.16
B5	0.49	0.52	1.32	6.41	1.00
SUM	2.32	5.91	9.89	15.66	5.85
Criteria Weights	0.41	0.22	0.10	0.07	0.20

Çizelge 4.6: B faktörü için AHP analizi (2).

	B1	B2	B3	B4	B5	Criteria Weights
B1	0.43	0.63	0.45	0.19	0.35	0.41
B2	0.12	0.17	0.25	0.23	0.33	0.22
B3	0.10	0.07	0.10	0.10	0.13	0.10
B4	0.14	0.05	0.06	0.06	0.03	0.07
B5	0.21	0.09	0.13	0.41	0.17	0.20
SUM	1	1	1	1	1	

Çizelge 4.7: B faktörü için AHP analizi (3).

	B1	B2	B3	B4	B5	Weighted Sum Values	Criteria Weights
B1	0.41	0.81	0.44	0.21	0.41	2.28	0.41
B2	0.11	0.22	0.25	0.25	0.39	1.21	0.22
B3	0.09	0.09	0.10	0.11	0.15	0.54	0.10
B4	0.14	0.06	0.06	0.07	0.03	0.36	0.07
B5	0.20	0.11	0.13	0.44	0.20	1.09	0.20
							Lamdamax
							CI_D
							CR_D
			Analiz Geçerliliği için	CR_D<0,10 olmalı			

4.4.3 C faktörü için AHP analizi

Çizelge 4.8: C faktörü için AHP analizi (1).

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
C1	1.00	7.20	3.66	3.87	3.67	3.68	3.06	2.75	3.26	4.62
C2	0.14	1.00	1.92	3.71	3.86	3.26	2.66	2.95	3.07	3.11
C3	0.27	0.52	1.00	1.12	2.09	1.90	1.26	3.04	0.89	2.02
C4	0.26	0.27	0.89	1.00	5.05	3.85	2.24	4.23	2.87	3.27
C5	0.27	0.26	0.48	0.20	1.00	1.75	1.10	2.90	1.69	0.85
C6	0.27	0.31	0.53	0.26	0.57	1.00	0.23	1.25	0.36	1.33
C7	0.33	0.38	0.79	0.45	0.91	4.27	1.00	7.20	4.60	5.80
C8	0.36	0.34	0.33	0.24	0.34	0.80	0.14	1.00	0.49	0.55
C9	0.31	0.33	1.12	0.35	0.59	2.78	0.22	2.05	1.00	1.48
C10	0.22	0.32	0.49	0.31	1.18	0.75	0.17	1.82	0.68	1.00
SUM	3.43	10.92	11.21	11.49	19.27	24.05	12.09	29.19	18.90	24.03
Criteria Weights	0.27	0.16	0.08	0.13	0.06	0.04	0.13	0.03	0.06	0.04

Çizelge 4.9: C faktörü için AHP analizi (2).

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	Criteria Weights
C1	0.29	0.66	0.33	0.34	0.19	0.15	0.25	0.09	0.17	0.19	0.27
C2	0.04	0.09	0.17	0.32	0.20	0.14	0.22	0.10	0.16	0.13	0.16
C3	0.08	0.05	0.09	0.10	0.11	0.08	0.10	0.10	0.05	0.08	0.08
C4	0.08	0.02	0.08	0.09	0.26	0.16	0.19	0.14	0.15	0.14	0.13
C5	0.08	0.02	0.04	0.02	0.05	0.07	0.09	0.10	0.09	0.04	0.06
C6	0.08	0.03	0.05	0.02	0.03	0.04	0.02	0.04	0.02	0.06	0.04
C7	0.10	0.03	0.07	0.04	0.05	0.18	0.08	0.25	0.24	0.24	0.13
C8	0.11	0.03	0.03	0.02	0.02	0.03	0.01	0.03	0.03	0.02	0.03
C9	0.09	0.03	0.10	0.03	0.03	0.12	0.02	0.07	0.05	0.06	0.06
C10	0.06	0.03	0.04	0.03	0.06	0.03	0.01	0.06	0.04	0.04	0.04
SUM	1	1	1	1	1	1	1	1	1	1	

Çizelge 4.10: D faktörü için AHP analizi (2).

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	Weighted Sum Values	Criteria Weights
C1	0.27	1.13	0.31	0.51	0.22	0.14	0.39	0.09	0.19	0.19	3.44	0.27
C2	0.04	0.16	0.16	0.48	0.23	0.13	0.34	0.10	0.18	0.13	1.95	0.16
C3	0.07	0.08	0.08	0.15	0.13	0.07	0.16	0.10	0.05	0.08	0.98	0.08
C4	0.07	0.04	0.08	0.13	0.30	0.15	0.29	0.14	0.17	0.13	1.50	0.13
C5	0.07	0.04	0.04	0.03	0.06	0.07	0.14	0.10	0.10	0.03	0.68	0.06
C6	0.07	0.05	0.04	0.03	0.03	0.04	0.03	0.04	0.02	0.05	0.42	0.04
C7	0.09	0.06	0.07	0.06	0.05	0.16	0.13	0.24	0.28	0.24	1.37	0.13
C8	0.10	0.05	0.03	0.03	0.02	0.03	0.02	0.03	0.03	0.02	0.36	0.03
C9	0.08	0.05	0.09	0.05	0.04	0.11	0.03	0.07	0.06	0.06	0.63	0.06
C10	0.06	0.05	0.04	0.04	0.07	0.03	0.02	0.06	0.04	0.04	0.45	0.04
Analiz Geçerliliği için CR_D<0,10 olmalı												Lamdama x
												CI_D
												0.15
												CR_D
												0.10

Çizelge 4.11: D faktörü için AHP analizi (3).

	D1	D2	D3	D4	D5	D6	D7	D8	D9	Weighted Sum Values	Criteria Weights		
D1	0.21	0.73	0.44	0.20	0.18	0.24	0.08	0.15	0.14	2.37	0.21	11.07	
D2	0.04	0.14	0.14	0.50	0.29	0.12	0.14	0.17	0.13	1.67	0.14	11.93	
D3	0.06	0.12	0.12	0.60	0.20	0.03	0.13	0.15	0.08	1.50	0.12	12.21	
D4	0.20	0.05	0.04	0.19	0.78	0.17	0.30	0.19	0.24	2.15	0.19	11.47	
D5	0.17	0.07	0.09	0.03	0.14	0.31	0.25	0.14	0.22	1.41	0.14	10.16	
D6	0.06	0.08	0.24	0.03	0.03	0.07	0.07	0.08	0.03	10.72	0.07	10.74	
D7	0.13	0.05	0.04	0.04	0.03	0.04	0.05	0.06	0.05	0.49	0.05	10.08	
D8	0.05	0.03	0.03	0.04	0.04	0.03	0.03	0.04	0.09	0.38	0.04	10.35	
D9	0.07	0.05	0.07	0.04	0.03	0.11	0.05	0.02	0.05	0.48	0.05	10.53	
Analiz Geçerliliği için CR_D<0,10 olmalı												Lamdama x	10.95
												CI_D	0.11
												CR_D	0.07

4.4.4 E faktörü için AHP analizi

Çizelge 4.12: E faktörü için AHP analizi (1).

	E1	E2	E3	E4	E5	E6	E7	E8	E9
E1	1.00	4.80	3.20	1.95	1.85	0.80	1.66	3.62	1.26
E2	0.21	1.00	3.80	2.08	2.82	1.09	0.88	1.09	1.09
E3	0.31	0.26	1.00	1.09	1.09	1.09	1.09	1.09	1.09
E4	0.51	0.48	0.92	1.00	1.09	1.09	1.09	1.09	1.09
E5	0.54	0.35	0.92	0.92	1.00	1.00	1.09	1.09	1.09
E6	1.25	0.76	0.92	0.92	0.92	0.92	1.09	1.09	1.09
E7	0.60	1.13	0.92	0.92	0.92	0.92	1.00	1.09	1.09
E8	0.28	0.92	0.92	0.92	0.92	0.92	0.92	1.00	1.09
E9	0.80	0.92	0.92	0.92	0.92	0.92	0.92	0.92	1.00
SUM	5.50	10.63	13.51	10.71	11.52	9.14	9.73	12.07	9.87
Criteria Weights	0.21	0.14	0.09	0.09	0.09	0.11	0.09	0.08	0.09

Çizelge 4.13: E faktörü için AHP analizi (2).

	E1	E2	E3	E4	E5	E6	E7	E8	E9	Criteria Weights
E1	0.18	0.45	0.24	0.18	0.16	0.09	0.17	0.30	0.13	0.21
E2	0.04	0.09	0.28	0.19	0.24	0.14	0.09	0.09	0.11	0.14
E3	0.06	0.02	0.07	0.10	0.09	0.12	0.11	0.09	0.11	0.09
E4	0.09	0.05	0.07	0.09	0.09	0.12	0.11	0.09	0.11	0.09
E5	0.10	0.03	0.07	0.09	0.09	0.12	0.11	0.09	0.11	0.09
E6	0.23	0.07	0.07	0.09	0.08	0.11	0.11	0.09	0.11	0.11
E7	0.11	0.11	0.07	0.09	0.08	0.10	0.10	0.09	0.11	0.09
E8	0.05	0.09	0.07	0.09	0.08	0.10	0.09	0.08	0.11	0.08
E9	0.14	0.09	0.07	0.09	0.08	0.10	0.09	0.08	0.10	0.09
SUM	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	

Çizelge 4.14: E faktörü için AHP analizi (3).

	E1	E2	E3	E4	E5	E6	E7	E8	E9	Weighted Sum Values	Criteria Weights
E1	0.21	0.69	0.28	0.18	0.17	0.08	0.16	0.31	0.12	2.18	0.21
E2	0.04	0.14	0.33	0.19	0.25	0.14	0.08	0.09	0.10	1.38	0.14
E3	0.07	0.04	0.09	0.10	0.10	0.12	0.10	0.09	0.10	0.80	0.09
E4	0.11	0.07	0.08	0.09	0.10	0.12	0.10	0.09	0.10	0.86	0.09
E5	0.11	0.05	0.08	0.08	0.09	0.12	0.10	0.09	0.10	0.83	0.09
E6	0.26	0.11	0.08	0.08	0.08	0.11	0.10	0.09	0.10	1.02	0.11
E7	0.13	0.16	0.08	0.08	0.08	0.10	0.09	0.09	0.10	0.92	0.09
E8	0.06	0.13	0.08	0.08	0.08	0.10	0.09	0.08	0.10	0.81	0.08
E9	0.17	0.13	0.08	0.08	0.08	0.10	0.09	0.08	0.09	0.90	0.09
Analiz Geçerliliği için											
CR_D olmalı											
CR_D <0,10											
Lamdamax 9.60											
CI_D -0.04											
CR_D -0.03											

4.4.5 F faktörü için AHP analizi

Çizelge 4.15: F faktörü için AHP analizi (1).

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	1.00	5.60	3.40	4.20	2.40	2.20	3.60	1.60	4.60
F2	0.18	1.00	1.80	2.80	3.40	2.80	2.00	2.60	4.40
F3	0.29	0.56	1.00	3.20	3.00	2.20	2.40	1.09	1.09
F4	0.24	0.36	0.31	1.00	1.09	1.09	1.09	1.09	1.09
F5	0.42	0.29	0.33	0.92	1.00	1.09	1.09	1.09	1.09
F6	0.45	0.36	0.45	0.92	0.92	1.00	1.09	1.09	1.09
F7	0.28	0.50	0.42	0.92	0.92	0.92	1.00	1.09	1.09
F8	0.63	0.38	0.92	0.92	0.92	0.92	0.92	1.00	1.09
F9	0.22	0.23	0.92	0.92	0.92	0.92	0.92	0.92	1.00
SUM	3.70	9.28	9.56	15.80	14.56	13.13	14.10	11.56	16.53
Criteria Weights	0.28	0.18	0.13	0.07	0.07	0.07	0.07	0.08	0.06

Çizelge 4.16: F faktörü için AHP analizi (2).

	F1	F2	F3	F4	F5	F6	F7	F8	F9	Criteria Weights
F1	0.27	0.60	0.36	0.27	0.16	0.17	0.26	0.14	0.28	0.28
F2	0.05	0.11	0.19	0.18	0.23	0.21	0.14	0.22	0.27	0.18
F3	0.08	0.06	0.10	0.20	0.21	0.17	0.17	0.09	0.07	0.13
F4	0.06	0.04	0.03	0.06	0.07	0.08	0.08	0.09	0.07	0.07
F5	0.11	0.03	0.03	0.06	0.07	0.08	0.08	0.09	0.07	0.07
F6	0.12	0.04	0.05	0.06	0.06	0.08	0.08	0.09	0.07	0.07
F7	0.08	0.05	0.04	0.06	0.06	0.07	0.07	0.09	0.07	0.07
F8	0.17	0.04	0.10	0.06	0.06	0.07	0.07	0.09	0.07	0.08
F9	0.08	0.02	0.10	0.06	0.06	0.07	0.07	0.08	0.06	0.06
SUM	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	

Çizelge 4.17: F faktörü için AHP analizi (3).

	F1	F2	F3	F4	F5	F6	F7	F8	F9	Weighted Sum Values	Criteria Weights	
F1	0.28	1.00	0.43	0.28	0.17	0.16	0.24	0.13	0.29	2.97	0.28	10.69
F2	0.05	0.18	0.23	0.18	0.24	0.20	0.13	0.21	0.28	1.70	0.18	9.55
F3	0.08	0.10	0.13	0.21	0.21	0.16	0.16	0.09	0.07	1.20	0.13	9.39
F4	0.07	0.06	0.04	0.07	0.08	0.08	0.07	0.09	0.07	0.62	0.07	9.36
F5	0.12	0.05	0.04	0.06	0.07	0.08	0.07	0.09	0.07	0.65	0.07	9.30
F6	0.13	0.06	0.06	0.06	0.06	0.07	0.07	0.09	0.07	0.67	0.07	9.40
F7	0.08	0.09	0.05	0.06	0.06	0.07	0.07	0.09	0.07	0.63	0.07	9.56
F8	0.17	0.07	0.12	0.06	0.06	0.07	0.06	0.08	0.07	0.76	0.09	9.56
F9	0.06	0.04	0.12	0.06	0.06	0.07	0.06	0.07	0.06	0.61	0.06	9.48
Analiz CR_D<0,1 olmalı												
Geçerliliği 0 için												
											Lamdamax	9.59
											CI_D	-0.05
											CR_D	-0.03

4.4.6 Main factors

Çizelge 4.18: Main factors (1).

	A	B	C	D	E	F
A	1.00	0.17	0.17	9.00	0.50	2.00
B	6.00	1.00	0.13	0.14	0.25	7.00
C	6.00	0.14	1.00	0.11	5.00	2.00
D	3.00	0.17	0.17	1.00	0.50	2.00
E	2.00	0.20	0.20	2.00	1.00	3.00
F	0.50	0.14	8.00	0.50	0.33	1.00
SUM	18.50	1.82	9.66	12.75	7.58	17.00
Criteria Weights	0.18	0.22	0.22	0.09	0.12	0.18

Çizelge 4.19: Main factors (2).

	A	B	C	D	E	F	Criteria Weights
A	0.05	0.09	0.02	0.71	0.07	0.12	0.18
B	0.32	0.55	0.01	0.01	0.03	0.41	0.22
C	0.32	0.08	0.10	0.01	0.66	0.12	0.22
D	0.16	0.09	0.02	0.08	0.07	0.12	0.09
E	0.11	0.11	0.02	0.16	0.13	0.18	0.12
F	0.03	0.08	0.83	0.04	0.04	0.06	0.18
SUM	1.00	1.00	1.00	1.00	1.00	1.00	

Çizelge 4.20: Main factors (3).

	A	B	C	D	E	F	Weighted Sum Values	Criteria Weights
A	0.18	0.04	0.04	0.80	0.06	0.36	1.47	0.18
B	1.05	0.22	0.03	0.01	0.03	1.25	2.60	0.22
C	1.05	0.03	0.22	0.01	0.59	0.36	2.25	0.22
D	0.53	0.04	0.04	0.09	0.06	0.36	1.11	0.09
E	0.35	0.04	0.04	0.18	0.12	0.54	1.27	0.12
F	0.09	0.03	1.72	0.04	0.04	0.18	2.10	0.18
								Lamdamax 10.91
								CI_D 0.10
								CR_D 0.07
								Geçerli
								Analiz CR_D<0,10 olmalı
								Geçerliliği için

Bu çalışmada AHP tekniği kullanılarak teknolojik gelişmelerin deniz ticareti ve taşıyanın sorumluluğu için önemli olan ana ve alt boyutları belirlenmiştir. Ana boyutlar karşılaştırıldığında;

Siber Saldırı ve Siber Saldırı Sonuçları 0.22 oranla en önemli faktör olarak belirlenirken, Teknolojik Gelişmeler ve IMO Sözleşmeler 0,18 oranla ikinci önemli faktör olmuş, Siber Saldırılarından Taşıyanın Cezai Sorumluluğu ise 0,12 oranla üçüncü sırada yer almıştır.

Yukarıda görüldüğü gibi teknolojik gelişmelerin en önemli ana boyutu “Siber Saldırıları” ve “Siber Saldırı Sonuçları” olarak belirlenmiştir.

Teknolojik Gelişmeler ana boyutunun alt boyutlarının öncelik sıralaması şu şekilde olmuştur;

1. Deniz ticareti ile ilgili evrakların interaktif ortama taşınması (0,24),
2. Gemilerin daha hızlı çalışması ve makineleşmesi sonucu sürekli ve hızlı veri akışı (0,19),
3. Veri depolama ve donanımda gerçekleşen bulut devriminin sağladığı güçlü veri çözümleri (0,10)
4. Gemi ile kıyı bağlantısının iyileştirilmesi sayesinde, kıyıdan yüzlerce mil uzaktaki geminin performansı hakkında edinilen gerçek bilgi (0,10)

Siber Saldırıları ana boyutunun alt boyutlarının öncelik sıralaması şu şekilde olmuştur;

1. Sinyal Bozma (0,41),
2. Sahtecilik (0,22),
3. Fidyeye Yazılım Saldırıları (0,20)

Siber Saldırı Sonuçları ana boyutunun öncelik sıralaması şu şekilde olmuştur;

1. Geminin Kaçırılması (0,27),
2. Ağ Sistemleri ile Haberleşme Kaybı (0,16)
3. Gemi Operasyonlarının Kesintiye Uğraması (0,13)
4. İletişim Sistemi ve Bilgisayar Sisteminin Bozulması (0,13)

Siber Saldırılarından Taşıyanın Ticari Sorumluluğu ana boyutunun alt boyutlarının önem sıralaması şu şekilde olmuştur;

1. Geminin Yola Elverişli Olmaması (0,21)
2. Eşyanın Zıya veya Hasara Uğraması (0,19)
3. Geminin Yüke Elverişli olmaması (0,14)
4. Yükün Geç Teslimi (0,14)

Siber Saldırılarından Taşıyanın Cezai Sorumluluğunun ana boyutunun alt boyutlarının önem sıralaması şu şekilde olmuştur;

1. Çatma (0,21)
2. Yükün Zıya veya Hasara Uğraması (0,14)
3. Nükleer Geminin Saldırı (0,11)

IMO Sözleşmeleri ana boyutunun alt boyutlarının önem sıralaması şu şekilde olmuştur;

1. Denizde Can Emniyeti Uluslararası Sözleşmesi(SOLAS) (0,28)
2. Gemilerden Kaynaklanan Kirliliğin Önlenmesine İlişkin Uluslararası Sözleşme(MARPOL) (0,18)
3. Petrol Kirliliğinden Doğan Zararın Hukuki Sorumluluğu ile İlgili Uluslararası Sözleşme(CLC) (0,13)

Tüm bu sonuçlar birlikte değerlendirildiğinde, teknolojik gelişmeler sektör için önemli bulunurken; deniz güvenliğine ilişkin siber önlemler öncelikli değerlendirilmiştir. IMO sözleşmeleri için önem sırasında dikkat çeken husus denizde can emniyetinden sonra kirlilik ile ilgili sözleşmelerin denizcilik uzmanları tarafından çok önemli olarak değerlendirilmesidir.

4.7 Benzer Vakalar

Bir gemiye siber saldırı yapmak için gereken teknoloji gittikçe yaygınlaşırken bu bilgilere erişim de gittikçe kolaylaşmaktadır. Deniz taşımacılığının maruz kaldığı siber saldırıların pek çok örneği vardır. Maruz kalınabilecek saldırılara örnek vermek gerekirse hackerlerin kimyasal yük taşıyan bir geminin navigasyon sistemine veya GPS sistemine müdahale ederek çatmaya sebep olması ve bunun sonucu gerçekleşen pek çok emniyet ve güvenlik sonuçlarıdır. Bu çatma sonucu ortaya çıkabilecek tehlikeler çevre kirliliği, faaliyetlerin kesilmesi nedeni ile kazanç kaybı, liman faaliyetlerinin durması, geminin tam zıyaı veya hasara uğraması, gemi adamlarının veya yolcuların bedeni zarara uğraması veya ölmesi, yükün zıyaı veya hasara uğraması olarak ortaya çıkabilecektir.

Mayıs 2017'de, bir ABD Donanması gemisi ile bir Güney Kore balıkçı teknesi arasında siber saldırı sebebiyle çatma gerçekleşmiştir. Şubat 2017'de, Kıbrıs'tan Cibuti'ye giden 8250 Twenty-Foot Equivalent Unit (TEU) gemisi tamamen hacklenmiştir[117]. Saldırı sırasında yaklaşık 10 saat boyunca saldırganlar, geminin navigasyon sistemini ele geçirmiş ve kaptanın gemiyi tekrar faaliyete geçirmek için herhangi bir işlem yapmasını engellemiştir. Bir diğer GPS karıştırma saldırısında, Güney Kore tarafından 280'den fazla geminin seyir sistemi sorunları yaşadığı bildirilmiştir; GPS sinyali

bilgisayar korsanları tarafından engellenmiş ve bazı GPS sinyallerinin ölmesine ve diğerlerinin yanlış veri almasına neden olmuştur[118].

Başka bir olayda bir ABD gemisinin gemideki kontrol sistemi ağına kötü amaçlı yazılım bulaşmıştır[119]. Gemideki kontrol sistemi ağı genellikle elektronik çizelgeleri güncellemek, kargo verilerini yönetmek ve kıyı tarafındaki tesislerle iletişim kurmak için kullanılmaktadır. FBI, söz konusu saldırıda gemideki güvenlik stratejilerinin eksikliğinin geminin kontrol sistemlerinde kritik kimlik bilgisi madenciliği ve GDPR ihlaline neden olan böyle bir saldırının ana nedeni olarak bildirmiştir. Benzer başka bir saldırıda, bilgisayar korsanları bir ABD Donanması yüklenicisinin yerleşik bilgisayarlarını uzaktan ele geçirerek çok büyük miktarda yüksek hassasiyetli veri (614 GB) çalmıştır[120]. 2020 yılında iki gemiye AZORult truva atı aracılığıyla Hermes 2.1 fidye yazılımı bulaştırılmış; yazılım, bir e-postaya eklenmiş makro etkin bir Word belgesi olarak gelmiş ve yönetim ağlarındaki birden çok iş istasyonu etkilenmiştir.

2021'de, birden fazla Yunan nakliye şirketi, bir BT danışmanlık firmasının sistemleri aracılığıyla yayılan bir fidye yazılımı saldırısına uğramıştır[121]. Bu olay, gemi sahipleri, gemi yöneticileri ve denizcilik endüstrisi için BT tedarik zinciri riskinin gerçekliğini göstermiştir. Bu saldırı dolayısıyla pek çok kişi de zarara uğramıştır.

Başka bir siber olayda yeni inşa edilmiş bir kuru yük gemisi, ECDIS'ine bilinmeyen bir virüs bulaştığı için birkaç gün boyunca sefer yapamaz duruma gelmiştir. Bu durumda saldırının sebep olduğu enfeksiyonun kaynağı ve araçları tespit edilemediği için sefere çıkmada yaşanan gecikme ve onarım masrafları yüz binlerce doları bulmuştur[122].

Limanların bilişim teknolojileri sistemlerinde ki denizel altyapıyı etkileyen bir dizi ilişkili siber saldırı/olay yaşanmaktadır. En sık görülen saldırı türleri kimlik avı, kötü amaçlı yazılım, sosyal mühendislik, kaba kuvvet ve hizmet reddidir. Gemilerin yanı sıra limanlar da kötü amaçlı siber yazılımlardan etkilenmektedir. Mart 2020'de Marsilya limanı “Mespinoza/Pysa” fidye yazılımıyla saldırıya uğramıştır. Bu olayda, denizel altyapılar, saldırının ana hedefi olan Aix-Marseille-Provence'daki bilgi sistemleriyle olan bağlantılarından dolayı saldırıdan etkilenmiştir[123]. Maersk liman sistemi etkileyen diğer bir olayda, dünya çapında birçok nakliye şirketini de etkileyen “NotPetya” kötü amaçlı yazılımının neden olduğu büyük bir siber saldırı olmuştur.

Maersk'in gemileri ile denizde ve karadaki 76 liman terminali çalışamaz hale gelmiştir[124]. Bu olayı 2020'de nakliye şirketi CMA CGM SA'ya yönelik, ağındaki bazı sunucuları etkileyen ve müşterilerin şirketin bilgi teknolojileri uygulamalarına ve rezervasyon sistemlerine dışarıdan erişimini engelleyen ciddi bir fidye yazılımı saldırısı izlemiştir[125]. 2022 yılında Houston Limanı, önceden bilinmeyen bir güvenlik açığını içeren bir parola yönetim programını içeren bir saldırının hedefi olmuştur. Bilgisayar korsanları, ağ erişimini kontrol etmek için gereken oturum açma kimlik bilgilerini sızdırmak için kullandıkları ağlara erişim sağlayan kötü amaçlı yazılımı yüklemek için bu saldırıyı kullanmışlardır[126]. Saldırı girişimi başarıyla engellenmiş ve hiçbir sistemin etkilenmemesi sağlanmıştır.

AHP tekniği kullanılarak yapılan öncelik sıralamasında ortaya çıkan sonuçlar ve gerçekleşen vakalar arasında ki paralellik durumun ciddiyetini ortaya çıkarmıştır. Siber saldırı sonuçları arasında Geminin Kaçırılması, Ağ Sistemleri ile Haberleşme Kaybı, Gemi Operasyonlarının Kesintiye Uğraması, İletişim Sistemi ve Bilgisayar Sisteminin Bozulması sıklıkla görülen siber saldırılar olarak tespit edilmiş ve erişilen benzer vakalar bulunan sonuçlarla uyumlu görülmüştür. Yine önceliklendirilen siber saldırılar Sinyal Bozma, Sahtecilik ve Fidye Yazılımı Saldırıları olarak belirlenmiş ve yine erişilen vakalarda gerçekleşen siber saldırı biçimleri bulunan sonuçlarla uyumlu görülmüştür.

Tüm bu olaylar göstermektedir ki modern siber saldırılar navigasyonu manipüle etmek veya kargoyu kurcalamanın çok ötesine geçmiştir. Önlem alınmadığı halde yerel ve küresel tedarik zincirlerini bozulması ve hatta gemideki mürettebatın veya yolcuların hayatlarını riske girmesi söz konusu olabilecektir. Gerçekleşen sonuçlardan kimin sorumlu olduğu meselesi ise tazminatlar ve ceza sorumluluğu için oldukça önemli olmaktadır.

5. SONUÇ VE DEĞERLENDİRMELER

Bu çalışmada taşıyanın, denizlerde gerçekleşen siber saldırılardan sorumluluğuna ilişkin öne çıkan farklı boyutların ve risklerin belirlenmesi ve bunlara yönelik yeni çözümler sunulması amaçlanmıştır. Halihazırda ulusal ve uluslararası alanda yapılan siber güvenlik düzenlemeleri denizcilik sektörüne yönelik çözümler üretmekten oldukça uzaktır. Siber suçların yapısı gereği sınır tanımaz oluşu ve basit bir araçla dahi gerçekleştirilebilmeleri tehditin boyutunu ve etkilerini büyütmektedir.

Denizcilik sektörünün teknolojik sistemlere bağımlılığının her geçen gün artması ile sektörünün teknolojik sistemlere bağımlı hale gelmesi, siber saldırı risklerinin de büyümesine sebep olmaktadır. Denizcilik sektörünün çoğunlukla büyük denizcilik firmalarının elinde şekillendiği göz önünde bulunduğunda, gerçekleşen olası saldırı ve olası zararlardan sorumluluğun çerçevesinin çizilmesi gerekliliği de ortadadır.

Kanaatimce, siber saldırılar sonucu uğranan zararlardan taşıyan iki yönden sorumlu olmaktadır. Birincisi taşıyanın sözleşmeden doğan ticari sorumluluğu diğeri ise taşıyanın üçüncü kişilere karşı cezai sorumluluğu. Taşıyanın, yük sahibine karşı aralarında yapılmış bulunan navlun sözleşmesi kapsamında sorumluluğu pek çok uluslararası konvansiyon ve iç hukukumuzda düzenlenmiş; hangi hallerde sorumluluğu doğacağı hangi hallerde mutlak sorumsuzluk hali mevcut olduğunun sınırları çizilmiştir.

Türk Ticaret Kanunu'nda taşıyanın gemiyi başlangıçta denize, yola ve yüke elverişli halde bulundurmama, eşyayı izinsiz başka gemiye yükleme ve aktarma, izinsiz güvertede eşya taşıma ve haklı bir sebep olmaksızın rotadan ayrılma gibi bazı sebepler ile eşyanın ziya veya hasara uğraması ya da geç tesliminden doğan zararlardan sorumluluk hakkında düzenlemeler mevcuttur. Geminin siber güvenlik açıklarıyla sefere çıkması kanaatimce taşıyanın gemiyi başlangıçta denize elverişli halde bulundurma sorumluluğu kapsamında değerlendirilmelidir.

Uluslararası konvansiyonlarda da geminin güvenliğinin sağlanması, geminin denize elverişli olması kapsamında değerlendirilmektedir. İlerleyen dönemlerde gemilere

gerçekleştirilecek siber saldırılar sonucu yüke zarar gelmesi, yükün zıya olması yahut geç teslim edilmesi halinde, taşıyanın siber güvenlik önlemleri ile ilgili almış olduğu tedbirlerden sorumluluğu bahsini ortaya çıkaracaktır. Keza taşıyanın sorumluluğu yalnızca taşıdığı yükle sınırlı değerlendirilmeyecek, deniz atmosferini etkileyen pek çok olası durum zincirleme sonuçlar doğuracaktır.

Günümüzde taşıyanın üçüncü kişilere verdiği zararlar P&I sigortaları kapsamında değerlendirilmektedir. Üçüncü kişiye verilen zararlara örnek vermek gerekirse; şamandıraya, usturmaçaya zarar verilmesi, denizin kirletilmesi, personelin kaza geçirmesi gibi durumları sigorta kapsamı için örnek gösterebiliriz. Ancak çoğunlukla bu sigortalarda siber saldırılar Enstitü Siber Saldırısı Hariç Tutma Klozu (10.11.2003 CL.380) ile sigorta kapsamı dışında bırakılmaktadır.

Siber saldırılarla ilişkili hukuki sorumluluk, sözleşmeden doğan sorumluluğu, üçüncü kişilere verilen zarar sorumluluğunu ve diğer potansiyel ihlalleri içermektedir. Bu nedenle, öncelikle saldırıya uğrayan tarafın sorumlu olup olmadığının ve hangi koşullar altında sorumlu tutulacağının değerlendirilmesi gerekmektedir.

Örneğin, kullanıma sunulan bir yazılım güncellemesini uygulamayan bir nakliye şirketinin öngörülemezlik iddiasında bulunması veya bir mücbir sebep hükmüne başvurusu(mevcut olması durumunda) bu alanda regülasyon eksikliğinden destek bularak mümkün olmamalıdır. Taşıyan, siber saldırı yoluyla güvenlik açığından yararlanılmasına neden olmuş veya uygun güvenlik standartlarını uygulayamamışsa üçüncü kişiye verilen zarardan sorumluluk açısından çatmaya sebep olan siber saldırı vasıtasıyla kaçırma durumunda, geminin başlangıçta 'denize uygun' olmadığını kabul etmek gerekmektedir. Keza siber saldırı sonucu mal ve/veya can kaybı olması durumunda taşıyanın sorumluluğu istisna olmaksızın kabul edilmelidir.

Değerlendirilmesi gereken en önemli soru ise, sigorta şirketlerinin siber bağlantılı gerçekleşen saldırı/olay yahut başkaca zararlardan sorumluluğu karşılayıp karşılamadığıdır. Yapılan araştırmalara göre herhangi bir siber saldırıdan kaynaklanabilecek maliyetlerin %92'sinin sigortasız olduğu tahmin edilmekte ve mevcut teminatların hem sınırlı hem de kısıtlı olduğu düşünülmektedir.

Tüm bu hususlar göz önünde bulundurulduğunda denizcilik sektörüne ilişkin temel gündemi deniz güvenliği, çevresel kaygılar, yasal konular, teknik işbirliği, deniz

taşımacılığının verimliliği olan IMO'nun siber güvenlik ile ilgili kararları ve düzenlemeleri de yetersiz kalmaktadır.

Büyük denizcilik şirketleri, olası riskler yerine günlük ticaretin içinde karşılaşılan risklere odaklanmayı şirket karlılığı adına daha verimli olarak değerlendirmektedir. Bunun sonucu olarak kolektif bir düzenleme hareketi istenilen boyutlarda gerçekleşmemiştir.

Deniz alanlarının uluslararası niteliği ve sınıraşan suçlardan olan siber saldırı suçlarının niteliği gereğince, uluslararası alanda bir hukuki düzenlemenin yapılması gerekliliği ortadadır. Küreselleşmenin artan etkisi 90'lı yıllarda, sınıraşan suçların ilerleyen yıllarda daha uluslararası bir karakter kazanmasının temellerini atmıştır. Bu açıdan değerlendirildiğinde denizel alanda gerçekleşen siber saldırılardan kimin ne şekilde cezalandırılacağı yahut taraflar arasındaki sözleşmelerde kusurlu ifa halinde nasıl bir sorumluluk doğacağının uluslararası bir regülasyonla düzenlenmesi şarttır. Aksi halde taşıyanın başına gelen bir siber saldırının aktörü çok büyük rakip firmalar olabilecek ancak siber saldırıların niteliği gereği gerçekleştirildikleri kaynağın belirlenmesinin zorluğu sebebiyle, fiili gerçekleştirenler tespit edilemezken taşıyan hem cezai hem ticari pek çok sorunla başbaşa kalacaktır. Yine büyük taşımacılık şirketlerin navlun sözleşmesi gereği yüklerini taşıdığı taşıtan şirketlerin gizli verileri, siber saldırılar kapsamında veri ihlalleriyle ele geçirilebilecek; bunun sonucu olarak hem taşıyan hem taşıtan büyük zararlara uğrayıp; sosyal mühendislik, fidye yazılımı ve benzeri araçlarla daha da büyük zararlara uğratılabilecektir.



KAYNAKLAR

- [1] **Review of Maritime Transport** (2020). *United Nations Conference on Trade and Development, United Nations 2021*. 30 Ağustos 2021 tarihinde https://unctad.org/system/files/officialdocument/rmt2020_en.pdf adresinden edinilmiştir.
- [2] **Review of Maritime Transport** (2020). *United Nations Conference on Trade and Development, United Nations 2021*. 30 Ağustos 2021 tarihinde https://unctad.org/system/files/officialdocument/rmt2020_en.pdf adresinden edinilmiştir.
- [3] Denizcilik Ekonomisi s. 48
- [4] **Cengiz, H.** (t.y.). Küresel Deniz Ticareti ve Deniz Taşımacılığı.
- [5] **Kraska, J. ve Pedrozo, R.** (2013). *International maritime security law*. Leiden-Boston: Martinus Nijhoff Publishers.
- [6] **Klein, N.** (2011). *Maritime security and the law of the sea*. New York: Oxford University Press.
- [7] **Klein, N.** (2011). *Maritime security and the law of the sea*. New York: Oxford University Press
- [8] **Del Pozo, F., vd.** (2010). *Maritime Surveillance in Support of CSDP*. The Wise Pen Team Final Report to EDA Steering Board.
- [9] **Url-1** <<http://www.earsiv.etu.edu.tr/bitstream/handle/20.500.11851/3549/607881%20%281%29.pdf?sequence=1&isAllowed=y>>, erişim tarihi 10.01.2022.
- [10] **Germond, B.** (2015). The geopolitical dimension of maritime security. *Marine Policy*, 54, 137-142.
- [11] **Simon, B.** (2017). Cyber Security. 18–22.
- [12] **Bolat, P. ve Kayisoğlu, G.** (2019). Antecedents and consequences of cybersecurity awareness: A case study for Turkish maritime sector. *Journal of ETA Maritime Science*, 7(4), 344-360.
- [13] **Güneşoğlu, B., Kayışoğlu, G. ve Bolat, P.** (2021). Cyber security risk assesment for seaports: A case study of a container port. *Computers and Security*, 103, 1-22.
- [14] Standardization Sector and O F Itu. ITU-T. 1205, 2008.
- [15] **Çiftçi**, Her Yönüyle Siber Savaş, sf. 6.
- [16] **Canlı**, Siber Güvenlik, sf. 8
- [17] Singer/Friedman, Siber Güvenlik ve Siber Savaş, s. 101.

- [18] **Kuhn, K., Bicakci, S. ve Shaikh, S. A.** (2021). Covid-19 digitalization in maritime: Understanding cyber risks. *WMU J. Marit. Aff.*, 193-214.
- [19] **Daffron, J., Ruffle, S., Coburn, A., Copic, J., Quantrill, K., Strong, K. ve Leverett, E.** (2019). *Shen attack: Cyber risk in asia pacific ports, centre for risk studies*. Cambridge.
- [20] **Androjna, A., Brcko, T., Pavic, I. ve Greidanus, H.** (2020). Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.*, 8(10), 776.
- [21] Oceans and the Law of the Sea Report of the Secretary General Assembly Resolution (2022). 74/247,
- [22] **Measures Toward Enhancing Maritime Cyber Security** (2014). Submitted By Canada and the United States. IMO Doc. MSC 94/4/1.
- [23] **Measures Toward Enhancing Maritime Cyber Security** (2014). Submitted By Canada and the United States. IMO Doc. MSC 94/4/1.
- [24] **Zarzuelo, I. L. P.** (2021). Cybersecurity in ports and maritime industry: reasons for raising awareness on this issue. *Transp. Policy*, 100, 1-4.
- [25] **Greenberg, A.** (2018). *The untold story of NotPetya, the most devastating cyberattack in history*. Wired.
- [26] **Yazıcıoğlu, Y.** (1997). *Bilgisayar suçları*. İstanbul: Alfa Yayınları.
- [27] **Dülger, M.** (2020). *Bilişim suçları ve internet iletişim hukuku*. İstanbul: Seçkin Yayınevi.
- [28] **Dülger, M.** (2020). *Bilişim suçları ve internet iletişim hukuku*. İstanbul: Seçkin Yayınevi.
- [29] **Boğaç, E. ve Songür, M.** (1999). *Açıklamalı bilgisayar ve internet terimleri sözlüğü*. Ankara: Hacettepe-Taş Yayınevi.
- [30] **Dülger, M. V.** (2016). *Bilişim suçları*.
- [31] Sieber, s. 20.
- [32] **Penros, R.** (2000). **Bilgisayar ve zeka: Kralın yeni usu I** (10. Baskı). (T. Dereli, Çev.). Ankara: Tübitak Popüler Bilim Kitapları.
- [33] **Akgül, M.** (2004). *Bilgi toplumu nedir? Ne değildir?*. *Güncel Hukuk*, 6, 15-17.
- [34] **İmre, N.** (2020). Turizm sektöründe sosyal medya kullanımı üzerine bir değerlendirme. *Türk Turizm Araştırmaları Dergisi*, 4(2), 1655-1670.
- [35] **Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. ve Bellekens, X.** (2022). Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13, 22.
- [36] **Url-2** <https://www.marinetraffic.com/en/ais/home/centerx:12.0/centery:25.0/zoom:4>, erişim tarihi 14.01.2022.
- [37] **Svilicic, B., Kamahara, J., Celic, J. ve Bolmsten, J.** (2019). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMUJ. Marit. Aff.*, 18, 509–520.

- [38] **Kavallieratos, G., Diamantopoulou, V. ve Katsikas, S. K.** (2020). Shipping 4.0: Security requirements for the cyber-enabled ship. *IEEE Trans. Ind. Inform.*, 16, 6617-6625.
- [39] **Androjna, A., Brcko, T., Pavic, I. ve Greidanus, H.** (2020). Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.*, 8, 776.
- [40] **Lisa, V.** (2013). *\$80 Million Yacht Hijacked by Students Spoofing GPS Signals*. 31 July. 12 Aralık 2022 tarihinde <https://nakedsecurity.sophos.com/2013/07/31/80-million-yachthijacked-by-students-spoofi> adresinden edinilmiştir.
- [41] **Url-3** <https://nakedsecurity.sophos.com/2013/07/31/80-million-yachthijacked-by-students-spoofing-gps-signals> (accessed on 31 January 2022).ng-gps-signals, erişim tarihi 31.01.2022.
- [42] **Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø. ve Nesheim, D.** (2021). A retrospective analysis of maritime cybersecurity incidents. *Int. J. Mar. Navig. Saf. Sea Transp.*, 15, 4.
- [43] **Analytica, O.** (2019). Global maritime security risks rise with GNSS use. *Emerald Expert Briefings*, Oxford, UK: Oxford Analytica.
- [44] **Tam, K. ve Jones, K.** (2018). Cyber-risk assessment for autonomous ships. *Proceedings of the 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity)*, Scotland, UK, (s. 1–8).
- [45] **Tam, K. ve Jones, K.** (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Marit. Aff.*, 18, 129-163.
- [46] **Wu, Z., Pan, Q., Yue, M. ve Ma, S.** (2018). An approach of security protection for VSAT network. *Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, (s. 1511-1516). New York, NY, USA.
- [47] **Santamarta, R.** (2015). Maritime security: Hacking into a Voyage Data Recorder (VDR). 10 Ocak 2022 tarihinde <https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/> adresinden edinilmiştir.
- [48] **Alcaide, J. I. ve Llave, R. G.** (2020). Critical infrastructures cybersecurity and the maritime sector. *Transp. Res. Procedia*, 45, 547–554.
- [49] **Wu, Z., Pan, Q., Yue, M. ve Ma, S.** (2018). An approach of security protection for VSAT network. *Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, (s. 1511-1516). New York, NY, USA.
- [50] **Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. ve Bellekens, X.** (2022). Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13, 22.

- [51] **Heffner, C.** (2021). *Exploiting Surveillance Cameras Like a Hollywood Hacker*. 10 Ocak 2021 tarihinde <https://privacy-pc.com/articles/exploiting-network-surveillance-cameras-like-a-hollywood-hacker.html>, adresinden edinilmiştir.
- [52] **Bugeja, J., Jonsson, D. ve Jacobsson, A.** (2018). An investigation of vulnerabilities in smart connected cameras. *Proceeding of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Athens, Greece, (s. 537–542).
- [53] **Bugeja, J., Jonsson, D. ve Jacobsson, A.** (2018). An investigation of vulnerabilities in smart connected cameras. *Proceeding of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Athens, Greece, (s. 537–542).
- [54] **Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. ve Bellekens, X.** (2022). Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13, 22.
- [55] **Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S. ve Tedeschi, P.** (2020). Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Commun. Mag.*, 58, 90–96.
- [56] **DNV-GL** (2016). *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*. DNV-GL Corporate Report DNVGL-RP-0, 2016.
- [57] **Çiftçi, H.** (2013). *Her yönüyle siber savaş*. TÜBİTAK Yayınları.
- [58] **Canlı, S.** Siber Güvenlik, s. 8
- [59] **Singer/Friedman, S.** Siber Güvenlik ve Siber Savaş, s. 101.
- [60] **Rid, T. ve Mcburney, P.** (2013). Cyber-Weapons. *Rusi Journal*, February, Marc 2012 (Ş. Çelik, Çev.). Stuxnet saldırısı ve ABD'nin siber savaş stratejisi: Uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi çerçevesinde bir değerlendirme, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), 142.
- [61] **Tezcan, D., Erdem, M. R. ve Önok, M.** (2017). *Uluslararası ceza hukuku*. Ankara: Seçkin.
- [62] **Erdem, A.** (t.y.). Uluslararası deniz hukukuna hakim olan ilkeler kapsamında kitle imha silahlarının yayılmasını engellemeye yönelik tedbirlerin değerlendirilmesi. *Adalet Dergisi*, (67), 445-490.
- [63] **Tutak, E.** (2022). Uluslararası deniz hukukunda deniz uyuşmazlıklarının çözümüne ilişkin en etkin başvuru yolunun bulanık AHP yaklaşımıyla belirlenmesi. *İktisadi ve İdari Araştırmalar Dergisi (Journal of Economics and Management Research)*, 1(1), 1.
- [64] **Ertekin, E.** (2011). Akdeniz dünyasının bilinen ilk denizcilik kanunu: Rodos avarya kanunu. *Antik Çağda Doğu Akdeniz'de Deniz Ticareti ve Uluburun Gemisi*, III. Türk Deniz Ticareti Sempozyumu,

<http://tdtts.deu.edu.tr/akdeniz-dunyasinin-bilinen-ilk-denizcilik-kanunu-rodos-avarya-kanini/> adresinden edinilmiştir.

- [65] **Nobel, D. R.** (1988): *The principles of islamic* (Yayımlanmamış doktora tezi). The Faculty of Laws in Candidacy for the Degree of Doctor of Philosophy, London.
- [66] **Reddie, J.** (1841). *An historical view of the law of maritime commerce*. Edinburg: William Blackwood and Sons.
- [67] **Urrutia, B.** (2006). The EU regulatory action in the shipping sector: A historical perspective. *Maritime Economics & Logistics*, 8, 202-221.
- [68] **Karahan, C. B.** (2011). *Avrupa Birliği denizcilik politikaları ve tarihsel olarak denizcilik ile ilgili geliştirilmiş olan hukuksal mevzuat* (Doktora tezi).
- [69] **Resolution MSC** (2017). 428(98) *Maritime Cyber Risk Management in Safety Management Systems IMO Doc.* (MSC 98/23/ Add. 1), Annex.
- [70] **Karim, M. S.** (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?. *Marine Policy*, 143, 105138.
- [71] **Resolution MSC** (2017). 428(98) *Maritime Cyber Risk Management in Safety Management Systems IMO Doc.* (MSC 98/23/ Add. 1), Annex.
- [72] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. İstanbul.
- [73] Madde Metni: Actual carrier means any person to whom the performance of the carriage of the goods, or of part of the carriage has been entrusted by the carrier, and includes any other person to whom such performance has been entrusted.
- [74] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. s.41 vd. , İstanbul.
- [75] **Atamer, K.** (2002). Atina Sözleşmesinde ve Türk Ticaret Kanunu tasarısında deniz yolu ile yolcu taşıma sözleşmesi. *BATİDER*, 24(3),103-213., s. 115.
- [76] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. s.42 vd. , İstanbul.
- [77] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. s.45,İstanbul.
- [78] **Değirmenci, N. K.** (t.y.). Taşıyanın “fiili taşıyanın hata ve ihmallerinden” doğan sorumluluğu ile yararlanabileceği sorumsuzluk şartı. *Journal of Istanbul University Law Faculty*, 73(1), 389-419.
- [79] **Ülgener**, Taşıyanın Sorumsuzluk Halleri.
- [80] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. İstanbul.
- [81] **Kender, Ç.** Navlun Sözleşmesi, s. 141.
- [82] **Şamlı, K. Y. ve Yazıcıoğlu, D. E.** (t.y.). Yeni Türk Ticaret Kanunu’na göre taşıyanın ziya, hasar ve geç teslimden sorumluluğu.
- [83] **Schaps, Abraham**, Das Seerecht, Ss 606/12 s. 630.

- [84] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. İstanbul.
- [85] **Carver, T. G., Treitel, S. G. ve Reynolds, F. M. B.** (2005). *Carver on bills of lading*. London: Sweet & Maxwell.
- [86] **Kender, Ç.** Deniz Ticaret Hukuku, s. 149.
- [87] **Kender, Ç.** Denizde Mal Taşıyanın Sorumluluğu, s. 80.
- [88] **Ping-Fat, S.** (2002). Carrier's liability under the Hague, Hague-visby and Hamburg rules. The Hague.
- [89] **Ping-Fat, S.** (2002). Carrier's liability under the Hague, Hague-visby and Hamburg rules. The Hague.
- [90] **Karan;** The Carrier's Liability Under International Maritime Conventions The Hague, Hague Visby, and Hamburg Rules, p. 83.
- [91] **Reynolds and Tsimplis;** Shipowners' Limitation of Liability, p. 254
- [92] Lahey, Lahey/Visby Kuralları Madde 3 Fıkra 8.
- [93] **Wilson;** Carriage of Goods by Sea, s.216
- [94] **Yetiş Şamlı;** 6102 Sayılı Türk Ticaret Kanunu'na Göre Taşıyanın Zıya, Hasar ve Geç Teslimden Sorumluluğu, s. 58.
- [95] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. İstanbul.
- [96] **Yazıcıoğlu, E.** (2000). *Hamburg kurallarına göre taşıyanın sorumluluğu Lahey/Visby kuralları ile karşılaştırmalı olarak*. İstanbul.
- [97] **Yetiş Şamlı;** 6102 Sayılı Türk Ticaret Kanunu'na Göre Taşıyanın Zıya, Hasar ve Geç Teslimden Sorumluluğu, s. 68.
- [98] **Günay,** Hazırlık Çalışmalarının Işığında Lahey/Visby Kuralları (Rotterdam Kuralları ile Karşılaştırmalı Olarak), s. 94
- [99] **Ülgener,** *Obligations and liabilities of the carrier*. (M. D. Güner Özbek, Der.). The United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea.
- [100] Marine Insurance Act, m.39/4
- [101] **Yazıcıoğlu,** Deniz Ticaret Hukuku, s. 390
- [102] **Çağa,** Kender, Navlun Sözleşmesi, s. 158
- [103] **Url-4** <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6102.pdf>, erişim tarihi 10.10.2022.
- [105] **Karan,** The Carrier's Liability, s. 291.
- [106] **Yarahoğlu, K.** (2001). Performans değerlendirmede analitik hiyerarşi prosesi. *Dokuz Eylül Üniversitesi İ.İ.B.F. Dergisi*, 16(1), 129-142.
- [107] **Anderson, B. F.** (2002). *The three secrets of wise decision making*. Portland, OR, USA: Single Reef Press.
- [108] **Figuena, J., Greco, S. ve Ehrgott, M.** (Ed.). (2005). *Multiple criteria decision analysis, state of the art surveys*. Berlin, Germany: Springer.

- [109] **Yaralıoğlu, K.** (2001). Performans değerlendirmede analitik hiyerarşi prosesi. *Dokuz Eylül Üniversitesi İ.İ.B.F. Dergisi*, 16(1), 129-142.
- [110] **Michalski, D. J., Bearman, C.** (2014). Factors affecting of decision making of pilots who fly in Outback Australia. *Saf. Sci.*, 68, 288–293.
- [111] **Singh, B.** (2016). Analytical hierarchical process (ahp) and fuzzy ahp applications-a review paper. *Int. J. Pharm. Technol.*, 8, 4925–4946
- [112] **Saaty, R. W.** (1987). The AHP—what it is and how it is used. *Math. Model*, 9, 161–176.
- [113] **Saaty, T. L. ve Vargas, L.G.** (1987). Uncertainty and rank order in the analytic hierarchy process. *European Journal of Operational Research*, 32(1), 107-117.
- [114] **Tektaş, A. ve Hortaçsu, A.** (2003). Karar vermede etkinliği artıran yöntem: Analitik hiyerarşi süreci ve mağaza seçimine uygulanması. *İktisat İşletme ve Finans Dergisi*, (18), 52-61.
- [115] **Min, H.** (1994). Location analysis of international consolidation terminal using the AHP. *Journal of Business Logistics*, 15(2), 25-44.
- [116] **Podvezko, V.** (2009). Application of AHP technique. *Journal of Business Economics and Management*, (2), 181-189.
- [117] **Roberts, F. S., Egan, D., Nelson, C. ve Whytlaw, R.** (2019). Combined cyber and physical attacks on the maritime transportation system. *NMIOTC Marit. Interdiction Oper. J.*, 2019, 18, 22.
- [118] **Oruc, A. ve Mimarest, M. S. M.** (2020). Claims of state-sponsored cyberattack in the maritime industry. *Proceedings of the 15th International Naval Engineering Conference & Exhibition*, Delft, The Netherlands.
- [119] **Winder, D.** (2019). *U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit By Cyberattack*. 31 Ocak 2022 tarihinde <https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=61b920e741aa>, adresinden edinilmiştir.
- [120] **Cooper, H.** (2018). *Chinese Hackers Steal Unclassified Data from Navy Contractor*. 2018. 31 Ocak 2022 tarihinde <https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html>, adresinden edinilmiştir.
- [121] **Roberts, F. S., Egan, D., Nelson, C. ve Whytlaw, R.** (2019). Combined cyber and physical attacks on the maritime transportation system. *NMIOTC Marit. Interdiction Oper. J.*, 2019, 18, 22.
- [122] **The Guidelines on Cybersecurity Onboard Ships** (2018). 3 Şubat 2022 tarihinde https://safety4sea.com/wp-content/uploads/2018/12/BIMCO-Guidelines-on-cyber-security-onboard-ships-2018_12.pdf, adresinden edinilmiştir.
- [123] **Seo, S. H., Lee, B. H., Im, S. H., Jee, G. I. ve Kim, K. S.** (2018). Efficient spoofing identification using baseline vector information of multiple receivers. *GPS Solut.*, 22, 1–14.

- [124] **Team, E.** (t.y.). *Maersk Line: Surviving from a Cyber Attack*. 3 Şubat 2022 tarihinde <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyberattack/>, adresinden edinilmiştir.
- [125] **Rosehana Amin, R. D. ve Jones, D.** (2021). *Part 1: A Very Modern Form of Piracy: Cybercrime against the Shipping Industry—Rapidly Developing Risks*. 3 Şubat 2022 tarihinde <https://www.clydeco.com/en/insights/2021/03/a-very-modern-form-of-piracy-cybercrime-against-th> adresinden edinilmiştir.
- [126] **Elliott, L.** (t.y.). *Port of Houston Target of Suspected Nation-State Hack*. 3 Şubat 2022 tarihinde <https://www.nbcnews.com/tech/security/port-houston-target-suspected-nation-state-hackrcna2249> adresinden edinilmiştir.

ÖZGEÇMİŞ

Ad-Soyad : Melis GEDİKOĞLU

ÖĞRENİM DURUMU:

- Lisans** : 2019, İstanbul Üniversitesi, Hukuk Fakültesi, Hukuk

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2020 yılında PanDog markasını kurdu.
- Şubat 2021’de Gedikoğlu Hukuk Bürosu’nu kurarak serbest avukatlığa başladı.