*Güvenlik Bilimleri Dergisi / Journal of Security Sciences*

***Jandarma ve Sahil Güvenlik Akademisi***
***Güvenlik Bilimleri Enstitüsü***
***Güvenlik Bilimleri Dergisi, Mayıs 2025, Cilt:14, Sayı:1, 59-86***
***doi: 10.28956/gbd.1648674***

*Gendarmerie and Coast Guard Academy*
*Institute of Security Sciences*
*Journal of Security Sciences, May 2025, Volume:14, Issue:1, 59-86*
*doi: 10.28956/gbd.1648674*

**Makale Türü ve Başlığı / Article Type and Title**
Araştırma / Research Article
Denizcilik Sektöründe Siber Güvenlik, Kritik Altyapı ve Siber Dayanıklılık
Cyber Security, Critical Infrastructure and Cyber Resilience In The Maritime Industry

**Yazar(lar) / Writer(s)**
Gülsüm KORALTÜRK, Dr. Öğr. Üyesi, İstanbul Üniversitesi-Cerrahpaşa, Türkiye, gaydin@iuc.edu.tr, ORCID: 0000-0002-0092-4209

**Bilgilendirme / Acknowledgement:**
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.
Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 28.02.2025
Makale Kabul Tarihi / Accepted : 30.05.2025

**Atıf Bilgisi / Citation:**
Koraltürk G., (2025). Denizcilik Sektöründe Siber Güvenlik, Kritik Altyapı ve Siber Dayanıklılık, *Güvenlik Bilimleri Dergisi, 14(1), ss 59-86. doi: 10.28956/gbd.1648674*

# DENİZCİLİK SEKTÖRÜNDE SİBER GÜVENLİK, KRİTİK ALTYAPI VE SİBER DAYANIKLILIK


## Öz

*Günümüzde yaygın olarak kullanılan bilişim ve teknoloji ürünlerinin denizcilikte her alanda kullanıldığı bilinmektedir. Limanlar ve enerji tesisleri denizcilikte kritik altyapı tesisi olarak adlandırılmaktadır. Gemilere hizmet veren limanların ve enerji tesislerinin rolü tedarik zinciri içinde yük akışını kesintisiz olarak sağlamaktır. Bu noktada bilgi ve iletişim sistemlerinin süreçleri hızlandırılması açısından kullanımı vazgeçilmezdir. Denizcilikte meydana gelmiş siber saldırılar incelendiğinde dünyanın hemen hemen her bölgesinde siber saldırılara maruz kalındığını ve özellikle fidye yazılım saldırılarının gerçekleştiği görülmektedir. Devletler ve kuruluşlar denizcilik sektöründe olası siber saldırılara saldırılarda daha iyi koşullarda mücadele edilmesi için hazır bulunmak istemektedir. Yıllar içinde siber saldırıların çeşidi, türü ve sürekli olarak artması neticesinde tedarik zinciri liman ve enerji tesislerinin güvenliğini kritik olarak tanımlamıştır. Çalışmada denizcilikte siber saldırıların, liman, enerji tesislerinin ve bilgi teknolojilerinin önemi vurgulanarak denizcilik camiasının yeni düzenlemelerle beraber karşılaması gereken standartları açıklamıştır. Bu bağlamda, genel kavramlar sırasıyla Siber Güvenlik, Denizcilikte BT (Bilgi Teknoloji) ve OT (Operasyonel Teknoloji) kavramları, Tesis Altyapısının Önemi, Kritik Bilgi Altyapısı, IACS Standartları (Uluslararası Klas Kuruluş Standartları), ISO Bilgi Yönetim Standartları ile yürürlüğe giren Denizcilikte Siber Dayanıklılık Yasası açıklanmıştır. 2024 yılında yaşanan siber saldırılar incelendiğinde liman, enerji tesisleri ve denizcilik şirketlerinin siber saldırılara uğradığı tespit edilmiştir. Sonuç kısmında ise liman, gemi ve denizcilik tesislerin siber güvenliği ve siber güvenlik ilgili yapılan çalışmalarda gelinen en son noktalar ile alınan önlemler Türkçe olarak açıklanmıştır.*


***Anahtar Kelimeler:*** *Denizcilikte Siber Güvenlik, Kritik Altyapı, ISO Bilgi Standardı, Siber Dayanıklılık.*

# CYBER SECURITY, CRITICAL INFRASTRUCTURE AND CYBER RESILIENCE IN THE MARITIME INDUSTRY


## *Abstract*

*It is known that today's widely used information and technology products are used in every field of maritime. Ports and Energy facilities are called critical infrastructure facilities in maritime. The role of ports and energy facilities serving ships is to ensure uninterrupted cargo flow within the supply chain. At this point, the use of information and communication systems is indispensable in terms of accelerating processes. When cyber attacks that have occurred in maritime are examined, it is seen that cyber attacks are exposed in almost every region of the world and especially with ransomware attacks. States and organizations want to be ready in order to combat possible cyber attacks in the maritime sector in better conditions. As a result of the kind, type and continuous increase in cyber attacks over the years, the security of supply chain ports and energy facilities has been defined as critical. The study emphasizes the importance of cyber attacks, ports, energy facilities and information technologies in maritime and explains the standards that the maritime community must comply with new regulations. In this context, general concepts such as Cyber Security, Maritime IT (Information Technology) and OT (Operational Technology) concepts, Importance of Facility Infrastructure, Critical Information Infrastructure, IACS Standards (International Classification Society Standards), ISO Information Management Standards and the Maritime Cyber Resilience Law that is put in place were explained. When the cyber attacks experienced in 2024 were examined, it is determined that ports, energy facilities and maritime companies were cyber attacked. In the conclusion, the latest points reached in the studies conducted on cyber security and cyber security of ports, ships and maritime facilities and the measures taken were explained in Turkish.*


***Keywords:*** *Maritime Cyber Security, Critical Infrastructure, ISO Information Standard, Cyber Resilience.*

## GİRİŞ

Yükün ve yolcunun deniz yoluyla taşınması esnasında emniyetli ve güvenli bir şekilde sürecin gerçekleştirilmesi çok önemlidir. Gemi seyrinden, yükün yönetimine ve liman yönetimine kadar geçen iş akış süreçlerinde bilgi teknolojisinin kullanılmasıyla iş akışının çok hızlı bir şekilde yürütüldüğü görülmektedir. Nesnelerin interneti ile otonom limanların, otonom gemilerin ve otonom ekipmanların operasyon süreçlerini kolaylaştırdığı açıkça görülmektedir. Yapay zekâ ve mantık kapılarının kullanımıyla akıllı gemiler ile "Endüstriyel Nesnelerde İnterneti"nin kullanımı (Internet of Things-IoT) artmakta, siber saldırganların bilgiye erişebilirliği kolaylaştığı görülmektedir. Teknolojinin kullanılması artan siber güvenlik tehlikelerini beraberinde getirmektedir. Siber saldırganlar denizcilik ilgili alanlara yapılacak saldırılarda sistemleri kolay ele geçirebildiklerini fark etmişlerdir. Bu nedenle deniz ekosistemine yapılan siber tehditler gittikçe artmaktadır. Yaşanan saldırılar incelendiğinde limanların, gemilerin ve tesislerin siber güvenlik açıklıkları olduğu ortaya çıkmaktadır. Bu durum operasyonları tehlikeye atmakta, tedarik zincirlerini bozmakta, ekonomiyi ve uluslararası ticareti aksatmaktadır. Dolayısıyla yükün ve yolcunun fiziksel güvenliği ve bilgi sistemlerinin siber güvenliğini sağlamak için daha ciddi önlemlerin alınmasına ihtiyaç duyulmuştur. Siber saldırıların aşamaları sisteme sızarak bilgi toplama, sistem taraması ile parola ve kimlik bilgilerinin ele geçirme, sisteme erişim sağlama, erişilen sistemde kalmaya devam etme ve sistemden çıkarken de fark edilmemek için dolaşım izlerinin silinmesi olarak gerçekleşmektedir. Denizcilik sektörü üzerindeki siber saldırılar genellikle dört temel amaç etrafında şekillenmektedir: operasyon aşamalarında aksaklık yaratmak, mali dolandırıcılık yapmak, casusluk amacıyla bilgi çalmak, politik veya sosyal mesajlar vermektir. Siber saldırıları gerçekleştiren kuruluşlar; devletler, devlet destekli kuruluşlar, aktivistler, fırsatçılar, ticari casuslar, siber suçlular ve teröristler olarak sıralanabilir (BIMCO, 2019).

Denizcilik sektörü hizmet sağlayıcılarına bakıldığında yük ve yolcu taşımacılığı başta olmak üzere armatörler, broker kuruluşları, liman yönetimleri, tersane işletmeleri, gemi acente ve işletmeleri, forvarder işletmeleri, marina işletmeleri, klas kuruluşları, internet sağlayıcılar ve lojistik hizmet sağlayıcıları olarak sıralanabilmektedir. Özellikle liman tesisleri denizcilik sektörünü ekonomik açıdan destekleyen altyapı tesisleridir. Ulaştırma hizmetlerinde birçok stratejik iş birliğini içinde barındırmaktadır. Dahası tedarik zincirlerinin vazgeçilmez kritik noktalarıdır. En küçük bir siber saldırı esnasında limanlar ve tedarik zincir halkaları büyük zorluklarla karşı karşıya kalabilmektedir. Limana

yapılan siber saldırı sonucu sistemlere erişim sağlanamaması operasyonun liman içinde aksamasına neden olmaktadır. Barselona Kruvaziyer Limanı'na yapılan siber saldırı gibi birçok limana saldırılarda bulunulmaktadır. (The Norwegian Maritime Cyber Resilience Centre, 2024). Ayrıca tedarik zincirinin unsuru olan devlet kuruluşları, denizcilik şirketleri ve enerji tesislerine de yönelik siber saldırıların oldukça arttığı gözlenmektedir (Denizcilik Genel Müdürlüğü, 2024).

ABD'de 2001 yılında yaşanan 11 Eylül saldırıları sonrasında ABD siber güvenlik olaylarında oluşabilecek zafiyetleri önlemek için altyapı ve güvenlik konusunda önlemelerini sıkı bir şekilde denetlenir ve izlenebilir olmasını istemektedir. Yine Avrupa ülkeleri adına ENISA (Avrupa Birliği Siber Güvenlik Ajansı) çalışmalarını siber güvenlik üzerine yoğunlaştırmıştır.

Gittikçe artan saldırılar sonucunda uluslar, IMO, AB, Korean ve Turk Loydu gibi Klass Kuruluşları, BIMCO (The Baltic International Maritime Council), Intertanko, Intercargo, DSCA gibi denizcilik kuruluşları meslek grubu üyeleri ile çalışmalarda bulunmuş ve çeşitli kılavuzlar yayınlayarak yaşanan saldırıların nedenlerini incelemiştir. Bunları önlemek adına üyelerine rehber niteliğinde kılavuzlar ile bilgilendirmektedir. Bu çalışmada incelen 18 rehberde alınan önlemlere rağmen siber saldırılarının denizcilik sektörüne artarak devam ettiği gözlendiğidir. Yol gösterici kılavuz niteliğinde raporların denizcilik kuruluşlarına ve üyelerine dikkat edilmesi gereken hususları açıklamaktadır. Bununla birlikte Protect and Indemnity sigorta birliği gemi ve taşıma operasyonu esnasında taşıyanın ve taşıtanın yaşayacağı olası bir siber saldırıda siber dayanıklılık yasasına uyulmadığı takdirde sigorta teminat kapsamı dışında kalacağını duyurmuşlardır.

Günümüzde siber saldırıların yeni odak noktası denizcilik faaliyetleri olmaktadır. Yükün ve yolcunun fiziksel güvenliği, bilgi ve sistemleri siber güvenliği sağlamasında daha sıkı önlemlere ihtiyaç duyulduğudur. ENISA Denizcilikte, Siber Güvenlik ve Kritik Altyapı 2023 adlı raporu yayınlamıştır. Terminolojiye göre güvenlik, emniyet ve siber güvenlik kavramları, denizcilikte kritik altyapı (Critical Infrastructure-CI) olarak liman ve enerji tesislerini tanımlanmıştır. İkincil olarak da kritik bilginin altyapısının korunması (Critical Information Infrastructure-CII) belirtilmiştir. Denizcilikte Kritik Bilgi Altyapısı'nın güvenliğindeki emniyet ve siber güvenlik temel sorunlarının nedenlerinin tespit edilmesi istenmektedir. Böylelikle denizcilik sektöründeki karşı karşıya kalınan güvenlik sorunların azaltılması için taraflar için farkındalığın her kademede artırılması istenmektedir.

## ARAŞTIRMA YÖNTEMİ

Siber saldırıların çeşidi, türü ve sürekliliği artması nedeniyle tedarik zinciri liman ve enerji tesislerinin güvenliği kritik olarak tanımlamışlardır. Bu tanımlar sonucunda ülkeler, denizcilik örgütleri, bilgi teknolojileri ve sigorta kuruluşları dâhil olmak üzere siber saldırılarda sorumluluk kavramlarını yeniden tanımlamaktadır. Araştırmada denizcilikte siber güvenliğe ait gemi ve liman tesislerine yönelik ve kritik altyapıya ait mevcut araştırmalar incelenmiştir**.** Çalışmada aşağıdaki sorulara yanıt aranmıştır:

- Denizcilikte siber güvenlik için güncel yayınlanan raporlar nelerdir?
- Siber güvenlik için IMO, ABD, AB, Klas Kuruluşlarının getirdiği yeni yönergeler ve yasal düzenlemeler nelerdir?
- Denizcilikte BT, OT ve bina tesis yönetiminin önemi nedir?
- Denizcilikte siber saldırı çeşitleri nelerdir?
- 2024 yılı için gerçekleşen siber saldırılar nelerdir? En çok etkilenen taraflar kimlerdir?
- Siber Dayanıklılık Yasası, ISO Standartları, IACS Standartları kapsamları nelerdir?

Bu çalışma Denizcilikte Siber Saldırılar ile ilgili yayınlarda elde edilen bilgiler bir araya getirilerek hazırlanmıştır. Norveç Denizcilik Siber Saldırı Veri Bankası'ndan alınan 2024 yılına ait gerçekleşmiş siber saldırılar incelenmiştir. 2024 yılı için gerçekleşen siber saldırıların çeşitleri tespit edilmiştir. Denizcilikte siber saldırıların, tesislerinin önemi ve bilgi teknolojilerinin önemi vurgulanarak denizcilik camiasının yeni düzenlemelerle beraber karşılaması gereken standartlar açıklanmıştır. Bu bağlamda genel kavramlar sırasıyla Siber Güvenlik, Denizcilikte BT (Bilgi Teknoloji) ve OT (Operasyonel Teknoloji) kavramları, Tesis Altyapısının Önemi ve Kritik Bilginin Altyapısı, IACS standarları, ISO Bilgi Yönetim Standartları, yürürlüğe giren Denizcilikte Siber Dayanıklılık Yasası açıklanmıştır. Devletlerin, denizcilik örgütlerin ve klas kuruluşlarının raporlarında gelinen son noktalar tespit edilmiştir. Liman, Gemi ve Tesislerin Siber Güvenliği ve Siber güvenlik hakkında akademik çalışmalarda gelinen son noktalar açıklanmıştır. Çalışmanın hazırlanmasındaki bir önemli amaç da bu konuda az sayıda kaynak ve çalışmanın olmasıdır.

## LİTERATÜR TARAMASI

*ENISA CRIMSON III* raporunda ilk defa "Denizcilik Ekosistemi" kavramı (Maritime Environment-ME) limanlar, gemi, denizcilik şirketleri, gemi, tayfa ve yük, idari birimler, gümrük, diğer hizmet sağlayıcıları, kritik altyapı liman tesisleri ve internet sağlayıcılarını kapsadığı açıklanmıştır. Denizcilik ekosistem çevriminde sistemin akışı sürdürebilir olması önemli olduğu vurgulanmıştır. Teknoloji kullanılması artan siber güvenlik tehlikelerini beraberinde getirmektedir (Polemi N. ve Van Maale C., 2023). Özellikle deniz ekosisteminde itibar ve finansal kayıplara karşı karşıya kalınmaktadır. Bazı siber olaylar bu nedenle ortaya çıkarılmamakta hatta maruz kalan veri kayıpları da tam olarak bilinememektedir. Yaşanan finansal kayıplar ve zedelenen marka değeri uluslararası denizcilik kuruluşlarının bu konuda incelemeler yapılmasını ve gerekli yeni düzenlemeler getirilmesini doğurmuştur.

Sektöre yönelik güvenlik tehditleri üzerine yapılan ilk çalışmalar esas alındığında terörizm kavramı karşımıza çıkmaktadır (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006). ABD'de meydana gelen 11 Eylül saldırıları sonrasında ABD tesislerinin, liman ve enerji tesislerine yönelik "Denizcilik Sektöründe Siber Güvenlik Bakış Açısı" adlı raporu yayınladı (Servida, Erhardt, Savo, Kernkamp, & Polemi, 2011). Raporda, denizcilik sektöründe siber güvenlik anlayışının olmadığı vurgulanmıştır. 2015 yılında, "Denizcilik Sektöründeki Dijital Zafiyetler" adlı Norveç ülkesini ele alan rapor (Kristoffersen, Hartvigsen, Myrvang, & Torjusen, 2015) yayınlandı. Rapora göre sektördeki en büyük 10 zorluk belirlendi ve bu zorluklar nedeniyle saldırılara ve kazalara dair örneklere yer verildi. Aynı yıl, gemi iletişim ekipmanlarının saldırıya uğraması, taklit edilmesi ve hacklenmesinin en yüksek risk olarak kabul eden çalışma yayınlandı (Kretschmann, Rødseth, Tjora, Fuller, & Noble, 2015).

"Siber Güvenlik Farkındalığı" adlı 2016 yılında yayınlanan raporda denizcilikte siber güvenlik hakkında genel kavramlara yer verilmiştir (AMMITEC, 2016). Fransız Ulusal Güvenlik Ajansının yayınladığı "Gemilerde Siber Güvenlik için en iyi uygulamalar 2016" adlı rehberde, bilgi sistemleri ve bilgisayar ağlarının yavaş yavaş denizcilik dünyasını istila ettiğini ve gemilerin her yerinde mevcut sistemlerinin güvenliğinin artırılmasının gerekliliğini vurgulanmıştır (ANSSI, 2016).

İngiltere Deniz Sahil Güvenliği 2016 yılında "Limanlar ve Liman Sistemleri: Siber Güvenlik Uygulama Kodu" adlı raporunu 2020 yılında güncelleyerek ikinci versiyonunu yayınladı. Raporda limanlar ve liman sistemleri için siber güvenlik

uygulama kodunu içeriğini açıkladı. Limanlarda demirleyen gemilerin teknik sistemlerini korunmasıyla ilgili bilgilere yer verildi (UK Department for Transport and Maritime and Coastguard Agency, 2020).

The Oil Companies International Marine Forum (OCIMF) 2017 yılında "Tanker Yönetimi-Öz Değerlendirme" adlı kitabında operatörler ve gemi yönetim sistemlerinin sürekli iyileştirilmesini gerekliliğini vurguladı. Kitapta gemi yönetiminden balast yönetimine kadar 13 kriteri kapsayan performans değerlendirme programlarına değinildi. BIMCO Siber Güvenlik Maddesi 2019'a göre "Siber Güvenlik Olayı" tanımlandı. *DCSA "Gemilerde Siber Güvenlik Uygulama Kılavuzu 2020'de* Gemi sahipleri ve işletmecilerinin siber güvenliği anlamaları ve gemi personeli de dahil olmak üzere paydaşlarının bu konudaki farkındalığını artırmaları üzerine bilgilere değindi (DCSA, 2020). Uluslararası Limanlar Birliği (International Association of Port and Harbour-IAPH) yakın zamanda "Limanlar ve Liman Tesisleri için Siber Güvenlik Kılavuzu"nda liman otoritelerinin üst düzey yöneticileri tarafından siber güvenlik konusunun farkında olunmasını altını çizerek, siber tehditler ile başa çıkmak için öneriler sıraladı. Finlandiya Ulusal Acil Güvenlik Ajansı "Denizcilikte Siber Güvenlik-Gemiler için En İyi Uygulamalar" ve "Armatörler ve Gemi İşletmecileri için En İyi Uygulamalar" adlı raporları yayınladı. Bu raporlarda armatörler ve gemiler için siber güvenlik kurallarını açıkladı. (Finland National Emergency Supply Agency, 2021a) (Finland National Emergency Supply Agency, 2021b)(Finland National Emergency Supply Agency, 2021). Gemi yönetiminin üst yönetime katılması vurgulandı. BIMCO, "Dijital Ortam, bilişim teknoloji sistemleri, operasyonel teknoloji sistemleri, ağlar, internet tabanlı uygulamalar, cihazlar ve sistem verileri olduğunu açıkladı. Bu maddeler ile siber güvenlik farkındalığını artırmak istedi (BIMCO, 2019). BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF ve IUMI kuruluşları yayınladığı *"*Gemilerde Siber Güvenlik Hakkında Kılavuz v.5*"* yayınında siber risk yönetim yaklaşımının adım adım nasıl takip edilmesini açıkladı. Gerçekleşmiş saldırı örneklerini inceledi ve geliştirdiği çözüm senaryoları ile üyelerine kaynak olarak sundu (BIMCO, ve diğerleri, 2021).

ENISA 2019, "Liman Siber Güvenlik: Denizcilikte Siber Güvenlik için İyi Uygulamalar" adlı raporu AB raporunu yayınladı (ENISA , 2019). Bu raporda liman ekosisteminde yer alan kuruluşların, özellikle liman otoriteleri ve terminal operatörlerinin BT ve OT siber güvenlik stratejilerine değinildi. ENISA, "2020 Limanlar İçin Siber Risk Yönetimi" raporunda liman siber risk yönetiminin aşamalarını açıkladı (ENISA, 2020). ENISA "Tedarik Zinciri Siber Güvenliği

için İyi Uygulamalar" raporunda, Tedarik Zincirinde siber güvenlik uygulamalarında risk yönetimi süreçlerini belirleyerek siber dayanıklılık açısından izlenilmesi gereken adımları açıkladı.

İngiltere Ulaştırma Bakanlığı "Gemiler İçin Siber Güvenlik Uygulama Kodu 2023" adlı raporunda geminin siber güvenliği ve siber saldırı sonrasında hızlı bir şekilde sistemlerin nasıl eski hâline dönmesi üzerine bir inceleme yayınladı. ENISA "Deniz Kritik Altyapısında Siber Güvenlik: Afrika Limanlarına İlişkin Düşünceler 2023" adlı raporda ticari limanların bilgi sistemlerinin önemini vurgulayarak, günümüzde kritik altyapıların önemini ve bilgi sistemlerinin teknolojiye bağımlılığını açıklandı (ENISA, 2023). Bu nedenle, ENISA "Denizcilikte Siber Güvenlik ve Altyapı Raporu 2023"de Ağ ve bilgi sistemlerine ilişkin direktifleri kabul etti (ENISA, 2024). ENISA, "Tehditlere Bakış" adlı (ETL) raporda, düzenli olarak artan siber güvenlik tehditlerini yıllık bazda inceledi ve tehditleri azaltma önlemlerine değindi (ENISA, 2024a) (ENISA, 2024b).

KOREAN Klas kuruluşu raporunda, Gemi ve gemi üstü sistem ve ekipmanların Siber Dayanıklılığına ilişkin asgari gereksinimlerini açıkladı. Buna ilave olarak CIA (Confidentiality, Integrity, Availability) modeli olarak bilinen gizlilik, bütünlük ve kullanılabilirlik unsurlarını açıkladı (KOREAN Register, 2024) (ClassNK, 2024). Bu raporlara ilave olarak Turk Loydu "Gemiler ve Açık Deniz İçin Siber Güvenlik Kılavuzları" adlı raporunda Siber Dayanıklılığa ilişkin IACS UR (International Unified Requirements-UR) yeni düzenlemelerini vurguladı ve bilgisayar tabanlı sistemler için IACS UR E22'nin kapsamlı revizyonunu gidildi ve dikkat edilmesi gereken hususları açıkladı (Türk Loydu, 2023), (IACS-International Association of Classification Societies, 2025).

## 1. DENİZCİLİKTE SİBER GÜVENLİK YENİ DÜZENLEMELER VE STANDARTLAR

### 1.1. IMO Regülasyonu

Uluslararası Denizcilik Örgütü (IMO) yönergeleri, Uluslararası Gemi ve Liman Tesis Güvenliği (ISPS) Kodu ve Uluslararası Klas Kuruluşları Birliği (IACS) gereklilikleri gibi denizcilik endüstrisinde siber güvenlik için uluslararası ve ulusal düzenlemelere ve standartları yayınlanmıştır. Siber tehditleri yönetebilmek adına IMO'nun MSC-FAL.1/Circ.3 (IMO, 2022) yönergeleri ve MSC. 428(98) (IMO, 2017) yönergeleri getirilmiştir. Sektördeki tüm tarafların siber güvenlik konusunda kendi sistemlerini oluşturmasını ve bunu kurum kültürü olarak

benimsenmesi istemektedir. Uluslararası Gemi ve Liman Tesisi Güvenlik (ISPS) Kodu, gemilerin ve liman tesislerinin güvenliği için uluslararası bir standarttır. AB, sınır ötesi iş birliğini kolaylaştırmak için Temel Hizmet Sağlayıcılar ile Dijital Hizmet Sağlayıcılara düzenli raporlar sunacak olan Bilgisayar Güvenliği Olay Müdahale Ekipleri (Computer Incident Response Teams -CSIRT) olarak kurulmuştur (BIMCO, 2019 ve (ENISA, 2023).

### 1.2 AB Regülasyonu

Ağ ve Bilgi Sistemlerinin Güvenliği Direktifi (The Directive on Security of Network and Information Systems- NIS Directive), siber güvenlik konusunda AB çapındaki ilk kuralları temsil eder. NIS2 Direktifi, AB genelinde 18 kritik sektörde siber güvenliği destekler ve yasal çerçeve oluşturur. Ayrıca üye devletleri ulusal siber güvenlik stratejileri tanımlar. Yönerge, her üye devletin tedarik zinciri güvenliği, güvenlik açığı yönetimi ve siber güvenlik eğitimi ve farkındalığı için politikalar benimsemesini zorunlu kılmaktadır (EU , 2017).

Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunications Standards Institute- ETSI) üye devletlere "ETSI TR 103 456 V1.1.1 Siber" adlı Uluslararası Siber Güvenlik Standartlarını ait kuralları açıklayarak NIS COM (2017) 476 nihai teknik raporunda yayınladı (ETSI TR 103 456 V1.1.1 ). Raporda, Avrupa Birliği genelinde ağ ve bilgi sistemlerinin yüksek düzeyde ortak güvenliği için önlemleri belirleyen NIS Direktifinin uygulanmasına ilişkin tavsiyeler sundu.

**AB Siber Güvenlik Sertifikasyon Çerçevesi**; kişiye özel ve risk temelli AB sertifikasyon çizelgesi oluşturulmasına istemektedir. Buna uygun olarak sertifikalandırılmış BT ürünleri ve hizmetlerinin istenilen gerekliliklere uyduğunu doğrulayacaktır. Siber güvenlik yasasında yer alan bu kapsam 27 Şubat 2025 itibarıyla tedarikçiler için kullanılabilir olmaya başlayacaktır (EU, 2024).

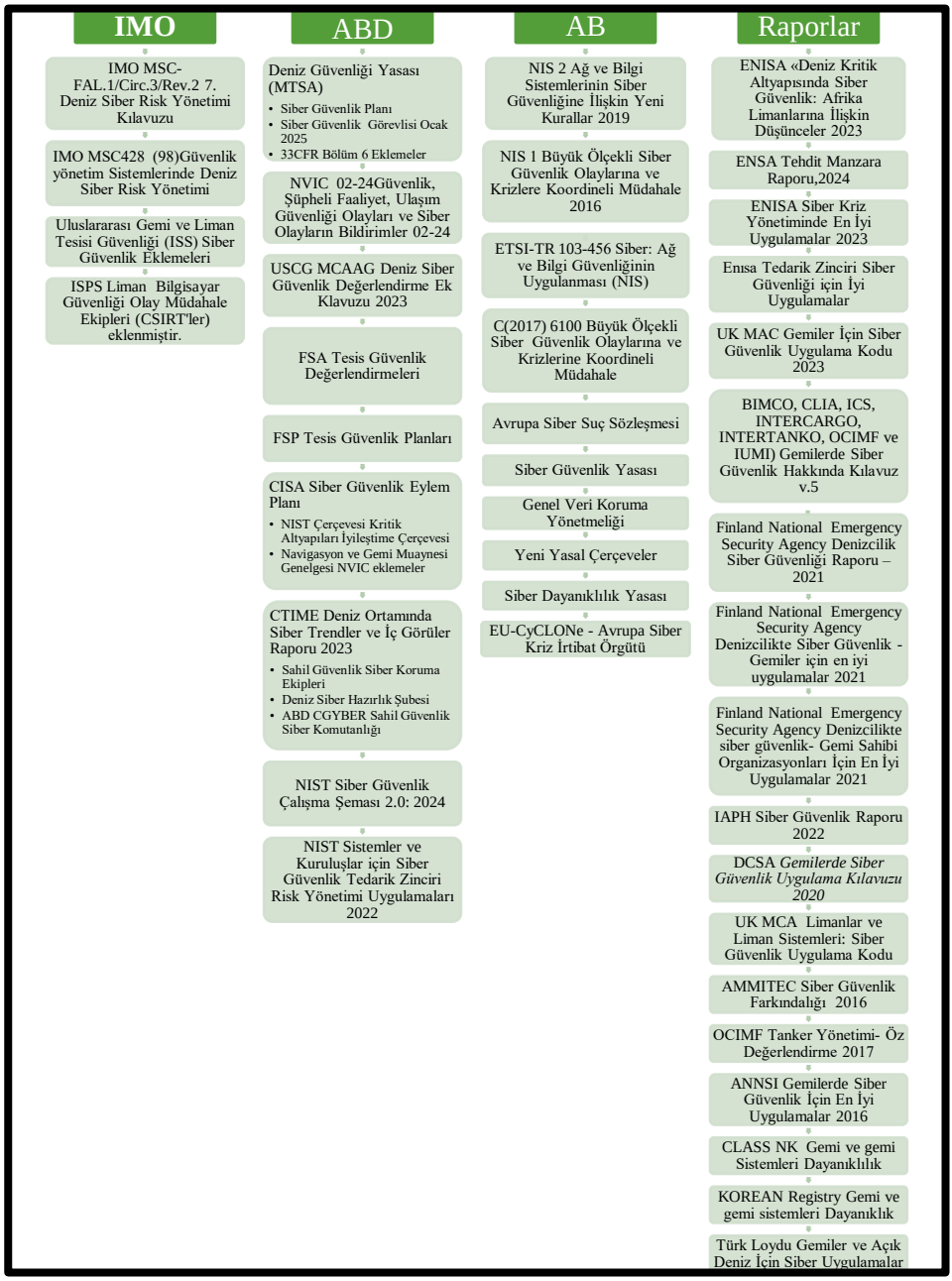
**Siber Dayanıklılık Yasası**, donanım ve yazılım dâhil olmak üzere dijital öğelere sahip ürünler ortak standartlar içerir. Daha güvenli bir dijital ortam sağlayarak tüketicileri ve işletmeleri siber tehditlerden korumayı hedeflemektedir (EU, 2022). Bu yasa 10 Aralık 2024'te yürürlüğe girmiştir. Yasada getirilen ana yükümlülükler 11 Aralık 2027 tarihinden itibaren denizcilik sektöründe geçerli olacağı açıklanmıştır. Kanun'un kapsamında nesnelerin interneti ("Internet of Things-IoT") gibi dijital bileşenlere sahip ürünlerin tüm tedarik zinciri ve yaşam döngüleri boyunca kullanım güvenliğini sağlayacak kuralları içermektedir (EU,

2022). Siber Dayanıklılık Yasası, somut ve somut olmayan dijital ürünlerin üreticileri ve satıcıları için ortak siber güvenlik kurallarını içerir. Dijital özelliklere sahip ürünlerin kullanımının güvenli olmasını, kullanıcılara güvenlik özellikleri hakkında yeterli bilgi verilmesini ve siber tehditlere karşı dayanıklı olmasını gerekliliğini vurgulamaktadır. Bundan sonra siber dayanıklılık yasası ile siber güvenlik sertifikasyonu olmayan sistemler kabul görmeyecek ve geçerli sayılmayacaktır.

### 1.3. ABD Regülasyonu

Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsünün Kritik Altyapı Siber Güvenliğini İyileştirme Çerçevesi (National Institute of Standards and Technology-NIST Çerçevesi) siber riskleri değerlendirmektedir (NIST, 2022). Amerika Birleşik Devletleri 2002 yılında yayınladığı Deniz Ulaşım Güvenliği Yasasına (Maritime Transportation Security Act- MTSA) yeni eklemeler getirmiştir (ABD, 2002). "Denizcilik Ulaşım Güvenliği Yasası" Burada 33 CFR (Federal Düzenlemeler Kanunu), Bölüm 6'nın geniş uygulanabilirliği ve bir siber olayın yeni tanımı yapılmıştır. Navigasyon ve Gemi Muaynane Sirkülesi (Navigation and Vessel Inspection Circulars) NVIC 02-24, 33 (USCG-United States Coast Guard, 2024) CFR Bölüm 101 ve 33 CFR Bölüm 6'da tanımlanan eklemeler yapılmıştır (ECFR.GOV, 2022). Bu yeni düzenleme ile Sahil Güvenlik, Federal Soruşturma Bürosu (FBI) ve Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cyber security and Infrastructure Security Agency-CISA) herhangi bir gemi, liman, liman veya sahil tesisini içeren veya tehlikeye atan gerçek veya tehdit altındaki bir siber olayın kanıtlarıyla birlikte bildirilmesini istemektedir (ECFR.GOV, 2025).

17 Ocak 2025'te ABD Sahil Güvenlik, deniz taşımacılığı sistemini (Maritime Transportation System-MTS) siber tehditlerden korumak için temel siber güvenlik gereksinimleri oluşturan yeni bir nihai kural yayınladı (USCG, 2025). Bu kural, bir siber güvenlik planı geliştirmek ve sürdürmek, bir siber güvenlik görevlisi (Cyber Security Officer- CySO) atanmasını ve MTS içinde siber güvenliği korumak için çeşitli önlemlere alınmasını değinmektedir.




**Şekil-1**: Denizcilikte Siber Güvenlik İçin Yapılan Çalışmaların ve Yönergeler

ABD Sahil Güvenlik Siber Komutanlığı (U.S. Coast Guard Cyber Command -CGCYBER) Deniz Ortamında Siber Trendler ve İçgörüler (Cyber Trends and Insights in the Marine Environment CTIME) raporunun yayınlandı. Sahil Güvenlik Siber Koruma Ekipleri (Cyber ProtectionTeam-CPT'ler) ve Deniz Siber Hazırlık Şubesi (Maritime Cyber Readiness Branch- MCRB) beraber hareket etmeleri ve teknik konularda bilgi alışverişinde bulunmalarını istedi (CGCYBER, 2025)

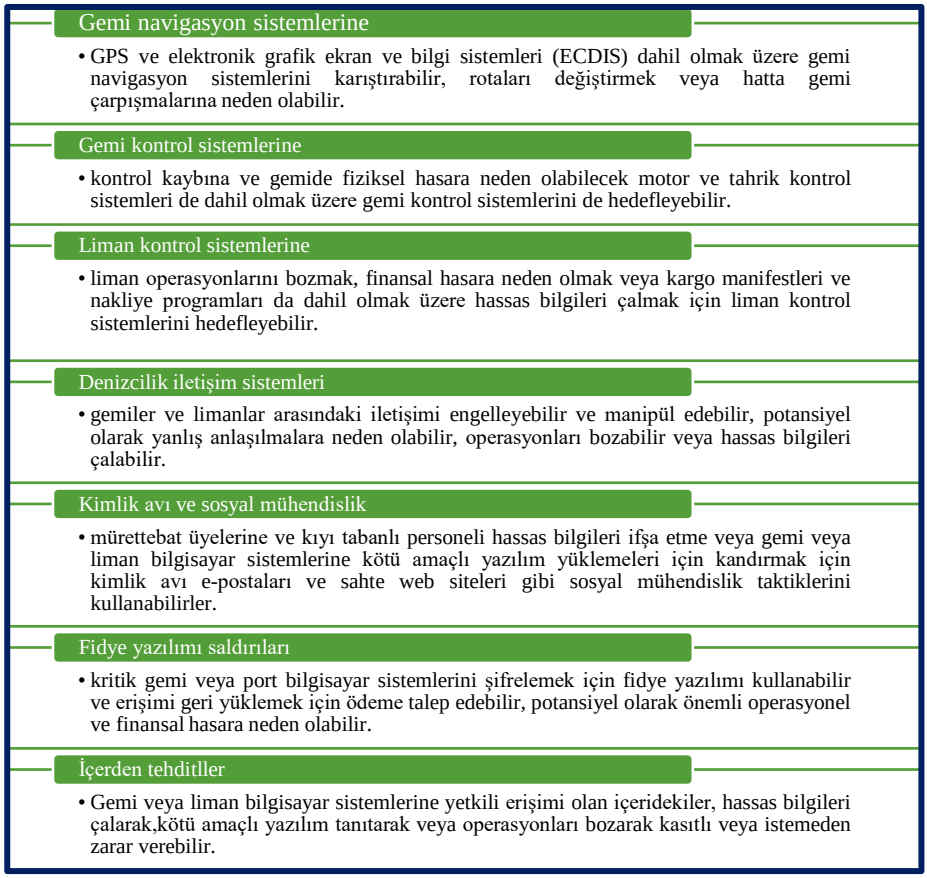
İnsan faktörü genellikle siber güvenlikteki zayıf halka olarak ifade edilmektedir. Özellikle gemi ve liman sistemlerine kimlik avı yöntemi ile müdahaleler gerçekleştiğinde büyük sonuçlar doğurabilmektedir. ISAC Bilgi Paylaşımı ve Analiz Merkezidir. NIS Yönergesi'ne göre, AB Üye Devletlerinin Bilgisayar Güvenlik Olayı Müdahale Ekipleri ('CSIRT'ler') veya Bilgisayar Acil Durum Müdahale Ekipleri (Computer Emergengy Respond Team -CERT) bulundurmaları gerekmektedir. Bu sayede olayların izlenmesi, olaylar hakkında erken uyarı, ikaz, olaylara müdahale ve durumsal farkındalık sağlanması hızlı bir şekilde gerçekleşebilecektir. Yukarıda bahsedilmiş olan Siber güvenlik konusunda yapılmış olan tüm yeni düzenlemelerin Şekil 1'de özet hâlinde gösterilmektedir.

AB ve ABD, liman ve enerji tesislerinin siber güvenliği, donanım ve yazılım ürünlerinin siber güvenliği, Ortak CyberSafe Ürünleri Eylem Planı ve yapay zekâ teknolojilerin siber güvenlik yönleri gibi alanlarda iş birliği diyaloglarını ilerletmiş ve aralarında siber diplomasi birimi oluşturmuşlardır (Eurpoean Union, 2025). AB ayrıca siber diyalogları Hindistan, Japonya, Kore Cumhuriyeti ve Brezilya gibi ülkeler ile de ilerletmektedir. Ülkeler iş birliklerini ikili Dijital Ortaklıklar, Dijital Diyaloglar ve Dijital İttifaklar adı altında kurdukları birliklerle beraber hareket etmek istemektedir (ÖKER, 2022).

## 2. DENİZCİLİKTE BİLİŞİM SİSTEMLERİNE YAPILAN SALDIRI ÇEŞİTLERİ

Denizcilikte Bilişim Sistemleri'ne yönelik düzenlenen saldırılar Şekil 2'de özetlenmiştir. Buna göre gemi navigasyon sistemlerine, gemi kontrol sistemlerine, liman kontrol sistemlerine ve denizcilik iletişim sistemlerine saldırılar gerçekleştiği görülmektedir. En çok saldırılarda hassas verilerin çalındığı bunun insan kaynaklı olduğu ve sisteme erişim sayesinde tesisin, limanın ve geminin komuta kontrolünün kaybedildiği ve sonuçlarında yükün, geminin, tesisin zarara uğradığı görülmektedir. Saldırılar sonucunda çevreye ve işletme itibarına verilen zarar, finansal kayıplar, operasyonun aksaması,

kaçırılma, aldatılma ve kandırılma gibi olayların yaşandığını dahası uluslararası casusluk ve terör faaliyetlerinde denizcilik kurumlarının ciddi zararlara uğradığı tespit edilmiştir (USCG, 2023).




**Şekil-2.** Denizcilikte Bilişim Sistemlerine Yapılan Saldırı Çeşitleri (USCG, 2023; BIMCO, ve diğerleri, 2021).

Siber saldırı düzenleyen ve adları bilinen belli başlı saldırgan gruplar tehdit unsuru oluşturmaktadır. Bu grupların bilinen bazıları Crop, 8base Alphy, LockBit 3.0, Play, Bianlian, Akira, Cactus olarak sıralanabilir (The Norwegian Maritime Cyber Resilience Centre, 2023, Akira, 2023, Lockbit, 2025). Bu grupların gerçekleştirdiği saldırılar incelendiğinde 2023 yılında Crop adlı grubu General Electric ve Rhenus Lojistik firmasına saldırılar gerçekleştirdi gözlenmektedir. ABD tarihinde bir enerji altyapısı hedefine yönelik en büyük siber saldırı olarak adlandırılan Lockbit 3. 0 adlı grubun Dp World ve Colonial Pipeline düzenlediği

**Liman Tesisi**

- NATO Lojistik Merkezine Trieste Limanına Yönelik DDoS Saldırıları, Ocak 2025
- Rijeka Limanına Yönelik 8Base fidye yazılım saldırısı ,Aralık 2024
- Brisbane Limanına DDoS Saldırısıyla Hacktivistlerin saldırısı Aralık 2024
- Seattle limanına Fidye Yazılımı saldırısı Ekim, 2024
- Bulgar Liman Altyapı Şirketine (BPIC) Siber Saldırı, Temmuz 2024
- Hint APT'ye ait kötü amaçlı Yazılım, Hint Okyanusu ve Akdeniz limanlarını yönelik hedef saldırılar, Temmuz 2024
- Lyon Terminaline 8Base fidye yazılımı grubu saldırısı
- İsrail Limanına Anonim Sudan tarafından düzenlenenDDoS saldırısı, Ocak 2024

**Enerji Tesisi**

- Vallianz Enerjiye Fidye Yazılımı saldırısı, Aralık 2024
- Halliburton Enerji şirketine fidye yazılımı saldırısı, Kasım 2024
- ABD sıvılaştırılmış doğal gaz (LNG) şirketi Tellurian'a RansomHub veri ihlali saldırısı Eylül, 2024
- Total Energies'e Karşı Hack Saldırısı, Temmuz 2024

**Devlet ve Devlet Kuruluşları**

- Filipinler Denizcilik Endüstrisi Otoritesi (MARINA) Hack Olayı, Haziran 2024
- Rus-Ukrayna gerginlikleriyle bağlantılı sahtekarlık olayı, Haziran 2024
- BAE Hükümeti'ne ait kara ve deniz taşımacılığı kurumuna ait hassas bilgilere güvenlik saldırısı, Haziran 2024
- Antlatic Balıkçılık Komisyonu'na (ASMFC) 8Base Rasnomware tarafından saldırı, Nisan 2024
- Filipin Sahil Güvenlik'in Facebook Sayfasının İkinci Kez Ele Geçirilmesi, Nisan 2024
- Italya'nın Kuzey Tiren otoritesine (ADSP Tirreno) Medusa Fidye Yazılımı Saldırısı, Mart, 2024
- İtalya Donanması "Marina Militare" Yönelik NoName057(16) grubu DDoS saldırısı, Şubat 2024
- "Filipin Sahil Güvenlik" Facebook Sayfasının Kaçırılması, Şubat 2024

**Denizcilik Şirketleri**

- Blackout Fidye Yazılımı Grubu Yunan Neda Denizcilik Şirketine saldırısı Kasım 2024
- Norwegian Gemi Hizmetlerine Akira fidye saldırısı, Kasım 2024
- ABD JAS nakliye ve lojistik sağlayıcısına Fidye yazılım saldırısı, Ağustos 2024
- Çinli Hacker Mustang Panda USB belleklerdeki kötü amaçlı yazılımla, Norveç, Yunanistan ve Hollanda'daki kargo şirketlerinin sistemlerini tehlikeye atılması, Temmuz 2024
- ElDorado Fidye Yazılımı Aracılığıyla Hırvat Tankerska Plovidbas (Nakliye Şirketi) Veri İhlali, Haziran 2024
- İtalyan nakliye ve lojistik şirketi Grendi Grubuna Yönelik Saldırı, Haziran 2024
- İsland Amerika Taşıma Şirketi'ne BinLian Fidye Yazılımı saldırısı, Haziran 2024
- Tekne perakendecisi olan MarineMax, Rhysida Ransomware Group Tarafından Hedef Alındı, Mart 2024
- Radiant Lojistik şirketinin sistemleri Hacklenmesi, Mart 2024
- Danimarka Nakliye web sitelerine yönelik NoName Fidye Yazılımı Saldırısı, Mart 2024
- Eastern Tersane Grubuna (Shipbuilding Group) LockBit fidye yazılımı saldırısı ve Siber Güvenlik İhlali, Şubat 2024
- TankerTrackers" çevrimiçi çökertmeye yönelik DDoS saldırısı, Ocak 2024

**AIS Sahteciliği**

- Çin AIS Sahteciliği aynı anda iki AIS transponder kullanılarak Tayvan'ın Kuzey Sahilinde Denizaltı Kablosuna Zarar Verilmesi,Ocak 2025
- Çin Filipinler'de AIS sahteciliği, Aralık 2024.
- LPG Taşıyıcıları Khor al Zubair limanından AIS Sahteciliği İran'dan yasa dışı gelen kargolar sanki Irak limanından yükleniyormuş gibi gözükmesi, Kasım 2024
- Tanker Atila konum gizlemesi- gemiden gemiye yasak petrol transferi- Karanlık Filo kavramı, Kasım 2024
- Rusya LNG Taşıyıcısı Pioneer Karanlıkta kaybolması Karanlık Filo, Ağustos 2024
- Kırım'da yaklaşık 50 geminin Simferol Havalimanında konumlandığı gösteren AIS sahtekarlığı olayı; Haziran 2024.

**Casusluk**

- Çin Denizlerindeki Şamandırlarlar ile Oşinografik Bilgi Toplaması, Ekim 2024.
- İran casus gemisi MV Behşad'ın bilgisayar sistemleri ABD siber saldırısıyla vurulması, Şubat 2024

**Sabotaj**

- Çin AIS Sahteciliği aynı anda iki AIS transponder kullanılarak Tayvan'ın Kuzey Sahilinde Denizaltı Kablosuna Zarar Verilmesi,Ocak 2025
- Çin Gemisi Baltık Denizi İnternet Kablo Sabotaj, Aralık 2024

**Şekil-3.** Denizcilikte Bilişim Sistemlerine Yapılan Siber Saldırı Örnekleri 2024

fidye yazılımı saldırısıdır. Saldırının sonucunda hattın sevkiyat operasyonlarını geçici olarak durdurulmuştur (MCAD Maritime Cyber Attack Database, 2025).

Şekil-3'te 2024 yılına ait gerçekleşen Siber Saldırı Vakaları görülmektedir. Saldıraya ait veriler Maritime Cyber Attack Veri Tabanından 2024 yılı seçilerek elde edilmiştir (MCAD Maritime Cyber Attack Database, 2025). 2024 yılı için 42 adet saldırı olduğu gözlenmiştir. Bu saldırılar incelendiğinde siber saldırılarının 8 tanesi Liman Tesislerine yönelik olduğu, 4 tanesinin Enerji Tesislerine yönelik olduğu, 8 tane saldırının devlet ve devlete ait kuruluşlara düzenlendiği, 12 tane saldırının denizcilik şirketlerine düzenlendiği, 6 tane siber saldırının AIS Sahteciliği üzerine gerçekleştirildiği, kablo ağlarına sabotaj üzerine 2 tane siber saldırı gerçekleştiği görülmektedir.

Ülkelerin saldırılardaki amacı sinyal bozma, konum aldatma, veri toplama gibi casusluk ve yasa dışı faaliyetler için kullandığı görülmektedir. Siber güvenlik zafiyetlerinin sonuçlarına bakıldığında sistemlerin saldırıya uğrayan kurumlarda ne kadar bir fiziki veri kaybı olduğu tam olarak bilinmemektedir. Dahası marka değerlerine korumak adına yaşadıkları itibar zedelenmesini ortaya çıkarmak istemedikleri anlaşılmaktadır. Liman tesislerine yönelik yapılan saldırıların fidye yazılım ve DDos saldırıları olduğu görülmektedir. Enerji tesislerine düzenlenen saldırıların fidye yazılım saldırıları ve veri ihlali saldırıları olduğu anlaşılmaktadır. Devlet kuruluşlarına yapılan saldırıları incelendiğinde kurumları ve ülke imajını zedelemek amacıyla fidye yazılım ve DDos saldırıları gerçekleştirildiği görülmektedir. Flipin Sahil Güvenliğin sosyal medya hesabına aynı yıl içinde ikinci kez ele geçirilmesi Devlet kuruluşuna itibar zedelenmesi yaşatmıştır.

Denizcilik şirketlerine yapılan siber saldırılar incelendiğinde 2024 yılı için yaygın olarak fidye yazılım saldırılarının gerçekleştirildiği görülmektedir. Blackout, Akira, BinLian, Lockbit, Rhysida Ransomware, NoName gibi siber saldırganların 2024 yılında saldırıda bulundukları görülmektedir (Akira, 2023) Rusya ve Çin AIS sahteciliğiyle konum gizlemesine başvurdukları gözlenmektedir. Karanlık Filo kavramı adı altında gemi konumlarının gizlenmesi, gemilerin AIS'de kaybolması ve gemiden gemiye yasak petrol transferi gibi olayların 2024 yılında yaşandığı görülmektedir.

## 3.DENİZCİLİK BİLGİ TEKNOLOJİLERİ VE YENİ DÜZENLEMELER

### 3.1. Denizcilikte BT, OT ve Kritik Altyapı Kavramları

ENISA 2019 raporuna göre limanların bugün karşı karşıya olduğu en önemli zorluk, etkili bilgi teknolojisi (BT) ve operasyonel teknoloji (OT) sistemlerinin kurulması için yapılmasını gereken düzenlemeler vurgulanmıştır. Bilgi teknoloji birimi ile operasyonel teknoloji biriminin işleyişe vakıf olamadıkları tespit edilmiştir. Yeni program satın alınması ve güncellenmesi esnasında bu iki birimin özellikle beraber iş birliği içinde çalışması gerektiği ve mümkünse işe alımlarda OT bilen BT'lerin tercih edilmesi istenmektedir (BIMCO, ve diğerleri, 2021). ABD Maritime Cybersecurity Assessment and Annex Guide (MCAAG) adlı raporunda BT sistemlerine siber ataklar, OT sistemine siber ataklar, bina kontrol sistemlerine gerçekleştirilen saldırılar olarak üç grupta toplamıştır. MCAAG'de ek olarak ABD bina kontrol sistemlerini tanımlayarak BT ve OT sistemlerinde ayrı olmasını ifade eder. Bunu da bir konteyner terminalindeki birbirine bağlı sistemlere örnek ile açıklayarak bina kontrol sistemlerinin ayrı bir güvenlik kontrol duvarı olması gerektiğini vurgular. BT, OT ve BCS'nin ayrılmasını istemektedir. Bina kontrol sistemlerinde; bilgisayar ağı, donanım, fiziksel ve kablosuz bağlantılar, iletişim protokolleri ve yazılım içermektedir örneğin ulaştırma çalışanları kimlik bilgileri okuyucuları ve yangın alarm sistemlerini içeren bina kontrol sistemlerinin ağ mimarisi düzenlenirken personelin güvenliği ve emniyetinin de doğrudan sorumlu tutulmasını istemektedir (USCG, 2023).

AB ve BIMCO raporunda belirtilen bir diğer husus da OT ve BT dışında sorumluk ve görev dağılımına değinilmiştir. Buna göre şirket kademesinin en alt biriminden en üst tepe yönetime kadar siber güvenlik için sorumluluk paylaşımı açıkça belirtilmiş ve sürekli olarak kayıtlar altına alınması istenmiştir. Örneğin genel müdür, siber güvenlik politikası oluşturulmasında ve bunun takip edilmesinde birincil sorumlu olarak belirtmiştir. Daha alt kademe olan insan kaynaklarının sorumluluğu ise siber güvenlik risk eğitimlerini gemi personeline düzenli olarak verilmesi olarak ifade edilmiştir. Bir tesiste hangi sistemlerin bulunduğunu, her sistem için ilişkili güvenlik açıklarını ve arızaların sonuçlarını anlamak, Tesis Güvenlik Ofisi (Facility Safety Officer-FSO) ve Siber Güvenlik Ofisinin (Cybersecurity Officer-CySO) siber saldırılara karşı planlama ve koruma birimlerinin oluşturulmasını istemektedir (BIMCO, ve diğerleri, 2021; ENISA, 2023) (ENISA, 2023a). Bilgi teknolojileri, Operasyonel Teknoloji ve Bina Kontrol Sistemlerinin genel kapsamına Şekil-4' te değinilmiştir. Bu

kapsamda OT sistemlerinin yanı sıra bina kontrol sistemlerinin içeriklerinin önemli olduğuna, bu alanların da izlenebilir olması gerektiğine değinilmiştir.

| Bilgi Teknolojisi Sistemleri | OT şunları içerir | Bina Kontrol Sistemleri |
|---|---|---|
| • Terminal İşletim Sistemi<br>• E-posta Sunucuları<br>• Kurumsal Kaynak Planlama<br>• Satış<br>• Envanter Kontrol<br>• Muhasebe<br>• Web Sunucuları<br>• İnsan Kaynakları<br>• Telekomünikasyon | • Taşıma ve transfer sistemleri gibi denetleyici kontrol ve veri toplama (SCADA) sistemleri<br>• Otomatik veya yarı otomatik<br>• konteyner elleçleme sistemleri:<br>• istifleme vinçleri,<br>• gemi-kara vinçleri,<br>• raylı gantry'ler,<br>• otomatik kılavuzlu araçlar<br>• Otomatik konteyner izleme sistemleri<br>• Konum, izleme ve navigasyon için gemi iletişim arayüzü (AIS) | • fiziksel güvenlik erişim kontrol mekanizmaları<br>• Ulaştırma Çalışanları Kimlik Bilgileri (TWIC) okuyucuları)<br>• yangın alarm sistemlerini içeren tesisteki personelin güvenliğinden ve emniyeti<br>• İç Aydınlatma Sistemleri<br>• Asansörler ve Yürüyen Merdivenler Erişim Kontrolü<br>• Hava Kalitesi Isıtma Soğutma (HVAC) Sistemleri<br>• Yangın Alarmı/Sprinkler Sistemleri<br>• Gözetim Sistemleri/İzinsiz Giriş Algılama |

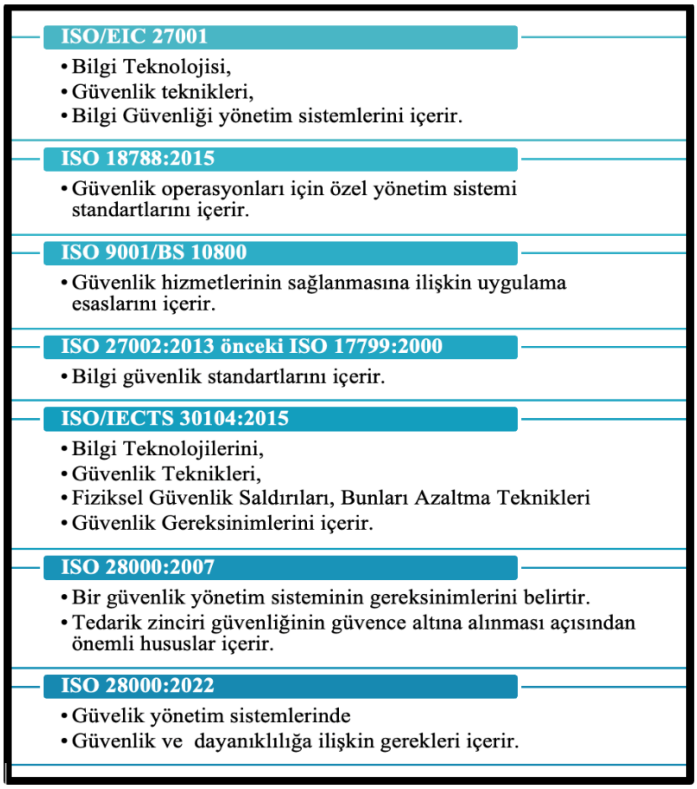
**Şekil-4**: Bilgi Teknolojileri, Operasyonel Teknoloji ve Bina Kontrol Sistem İçerikleri

Bunlara ilave olarak yeterli eğitim imkânının olamamasıdır. Gemide ve limanda çalışan personelin çoğu, siber güvenlik konusunda sınırlı bilgiye sahip olduğu için potansiyel riskleri öngörüp önlem almakta yetersiz kalabilmektedir. Dahası günümüzde otonom gemiler gibi karmaşık sistemlerin denizcilik sektöründe kullanılıyor olması siber güvenlik önlemlerini sistemlere uyarlamanın zor olduğunu göstermektedir (BIMCO, ve diğerleri, 2021, ENISA, 2023).

Diğer bir önemli zorluk ise gemilerde internet erişiminin sınırlı olmasıdır. Denizcilik sektöründe internet bağlantısının hızı ve sürekliliği; çoğunlukla düşük düzeyde kalmakta, bu da çevrim içi eğitimlerin uygulanmasını zorlaştırmakta ve siber güvenlik farkındalığının tam olarak anlaşılamamasına neden olmaktadır. Son yıllarda bazı denizcilik şirketleri, yüksek hızlı uydu internet bağlantılarına yatırım yaparak bu sorunu çözmeye çalışmaktadır ancak bu çözüm henüz sektör genelinde yaygınlaşmamıştır (BIMCO, ve diğerleri, 2021).

### 3.2. Denizcilikte Bilgi Güvenliği Yönetimi, Siber Bilgi Güvenlik Standartları ve Yeni Yönergeler

**ISO27000**, güvenlik kavramını tanımlar. ISO 27001 bilgi güvenliği yönetimleri standart sistemi olarak bilinmektedir. Kurumların bilgi güvenliğinin sağlanmasında insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Bilgi varlıklarını korumayı ve ilgili taraflara güvenli kontrolleri sağlar. ISO/IEC 27001 iki kategoriye ayrılır. Buna göre limanın CII'si olan bir kuruluş Bilgi Güvenliği Yönetim Sistemi (Information Security Management System-ISM) ile ilgilenir. ISO 27001'e göre limanın, güvenlik alanındaki standartlarını en iyi şekilde karşılanması istenmektedir. Ayrıca ISO 27001 fiziksel güvenlik çevresi, fiziksel giriş kontrolleri ve tesislerin fiziksel güvenliği gibi terimleri açıklar (ISO-ISO/EIC27001, 2022).




**Şekil- 5.** Denizcilikte Bilgi Güvenliği Yönetiminde Kullanılan ISO

**ISO2800x** ise standart bir ISO olarak tedarik zinciri güvenliği ve özellikle deniz taşımacılığında tedarik zincirleri için yönergeleri içerir (ISO 28000:2022, 2022).

Özellikle nesnelerin internetinde kullanılan otomasyon sistemleri, ağ iletişimleri ve güvenlik kontrolleri endüstriyel otomasyon ve kontrol sistemleri için güvenlik, IACS ortamında kullanılan uygulamalara yama yönetimi (güncelleme), güvenlik sağlayıcıları için program gereksinimleri ve risk değerlendirilmelerini yapar ve süreci geliştirmek için standartlarını açıklar (ISO-ISO/IEC TS 30104:2015, 2022). Yukarıda bahsedilen ISO standartları Şekil- 5'te özet olarak gösterilmektedir:

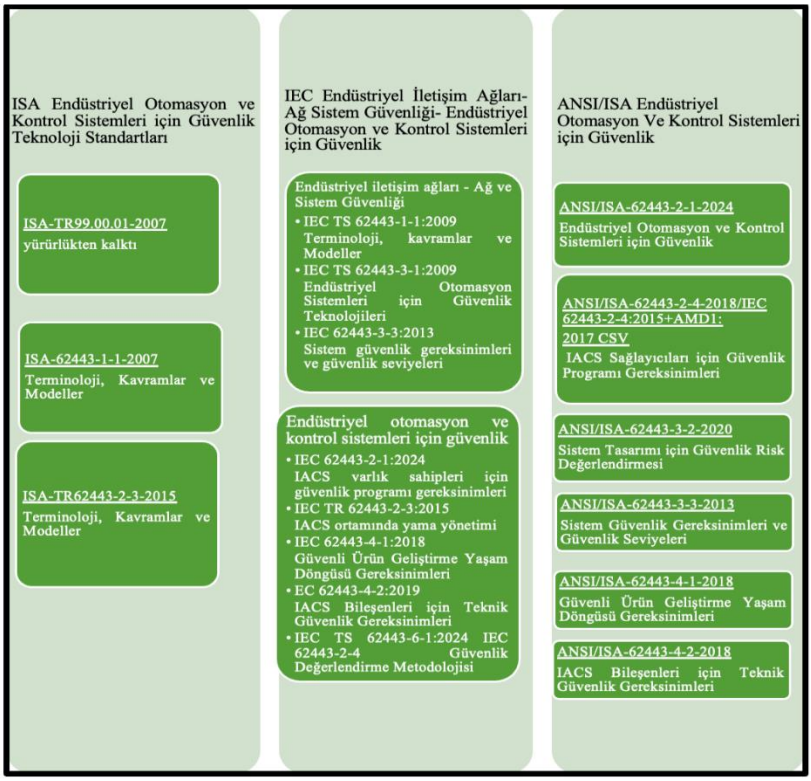
Benzer şekilde Terminal İşletim Sistemlerine (Terminal Operation System-TOS), Liman Topluluk Sistemlerine (Port Comunity System-PCS) gemilerin navigasyon sistemlerine yapılan saldırılar, kritik mekanik cihazlarda ise arızaya veya hasara neden olabilir (örneğin, konteyner vinçleri, kilitleri emniyet ve mekanik sistemler) kesintiye ve daha kötüsü, can kaybına, kargonun çalınmasına veya bir geminin imha edilmesine neden olabilir. PCS Port Comunity System güvenliği, dahili işleyişlerin gizlendiği ve yalnızca girdilerin ve çıktıların bilindiği kriptografik bir "kara kutu" olarak ele alınır (ENISA, 2023).

### 3.3 Nesnelerin İnterneti, IACS Uygulamaları ve Siber Dayanıklılık Yasası

Uluslararası Klas Kuruluşları Dernekleri Birliği (International Association of Class Societies-IACS), IACS Tavsiye 166 yayınladı (IACS-International Association of Classification Societies, 2025). Bu tavsiyede; Gemilerin siber güvenliğini sağlamak ve siber olayların oluşumunu azaltma ve etkilerini hafifletmek için asgari siber dayanıklılık gereklilikleri belirlenmiştir. IACS'nin Birleşik Gereksinimleri (Unified Requirements- UR) **"UR E26"**; Gemilerin siber dayanıklılığı geminin tasarımı, inşası, devreye alınmasını ve operasyonel ömrü boyunca hem OT hem de BT ekipmanlarının geminin ağına güvenli bir şekilde entegre edilmesini sağlamayı amaçlamaktadır. Bu UR, Tanımlama, Koruma, Algılama, Yanıtlama ve Kurtarma olarak 5 temel işlevi kapsamaktadır. **"UR E27";** Gemideki Sistem ve Ekipmanların Siber Dayanıklılığına ilgili standartları içermektedir. Denizcilikte Endüstriyel Otomasyon Sistemleri için Kullanılan Yeni Standartlar ve İçerikleri aşağıdaki şekilde özetlenmiştir (IACS-International Association of Classification Societies, 2025). Klas kuruluşları bu standartların yerine getirilmesini istemektedir.

Gemideki sistemlerin ve ekipmanların siber dayanıklılığı için gereklilikleri sağlar ve kullanıcılar ile gemideki bilgisayar tabanlı sistemler arasındaki ara yüz ile ilgili ek gereklilikleri sağlar (ClassNK, 2024). UR'ler, 1 Temmuz 2024'ten itibaren inşa sözleşmesi yapılan yeni gemilere uygulanacak olup gemilerde uygulama kapsamını, onay sürecini, izlenilmesi gereken adımları ve gemi ve gemi üstü sistem ve ekipmanların Siber Dayanıklılığına ilişkili CIA modelini unsurlarını açıklanmıştır (KOREAN Register, 2024).

Ne yazık ki denizcilik paydaşlarının çoğu, fiziksel tehditlere ve zayıflıklara odaklanan ve siber tehditleri görmezden gelen standartlaştırılmamış, uyumlaştırılmamış güvenlik yönetimi uygulamaları kullanmaktadır. Hem fiziksel hem de siber güvenlik olayları, limanların, gemilerin ve tüm tedarik zincirinin işleyişini tehlikeye atarak ekonomik kesintilere, enerji tesislerine ve kaynaklarına erişimi engelleyerek uluslararası ticareti aksatmaya sebep olmaktadır.




**Şekil-6.** Denizcilikte Endüstriyel Otomasyon Sistemleri için Kullanılan Yeni Standartlar ve İçerikleri

Dahası tedarik zincirlerinin kesintiye uğraması, limanlar ve zincir içindeki tüm birimlerin uygun güvenlik protokollerine sahip değillerse uluslararası teröristlerin hedefi hâline gelebilmektedir.

Böylelikle siber tehditlerin belirlenmesi, korunma, algılama, yanıt ve toparlanma aşamalarını içeren bir siber güvenlik yönetim çerçevesi daha kolay anlaşılacaktır. Bu sayede sektörde limanlardan tedarik sürecinin en alt noktasına kadar siber saldırılara maruz kalabilecek şirketlerin saldırılarından en az zarar ile tehlikelerin önlenmesi hedeflenmektedir. Devletlerin casusluk olayları incelendiğinde teknoloji geliştirme ve önemli ulusal altyapı projelerinde kuruluşlara yapılan siber casusluk operasyonları dikkat çekmektedir. Çin ve Rusya kurumlara karşı en fazla casusluk yapan ülkeler arasında yer almaktadır. (T.C. Ulaştırma Altyapı Bakanlığı, 2023). Enerji tesislerinin güvenliği yüklerin taşınması esnasında sinyal bozma, AIS'e müdahale ederek karanlık filo ve çevresi sarıldığı hissi yaratma gibi örnek olaylar gerçekleşmiştir.

BIMCO, çeşitli denizcilik dernekleri, nakliye şirketleri ve siber güvenlik danışmanlık şirketleriyle iş birliği yaparak Gemilerde Siber Güvenlik Kılavuzu'nun güncellenmiş 5. sürümünü yayınladı. Bu revizyon, siber tehdit operatörleri ve stratejileri hakkında yeni bakış açıları içerdi. Ayrıca ağlar, sistemler, bağlantılar, donanımlar, süreçler gibi değişikliklere yanıt olarak siber güvenlik risk değerlendirmesinin düzenli olarak güncellenmesinin gerekliliğini ifade etti.

## 4. SONUÇ

"Denizcilikte Kritik Altyapı" kavramı giderek artan bir ekonomik öneme sahiptir. Bilgisayar korsanları limanların, gemilerin uydu sistemlerin ve kargo yönetim sistemlerine fiziksel ve siber saldırılar karşı kimi zaman savunmasız kalabilmektedir. Bu tür saldırılar bir gemiyi devre dışı bırakabilir, yükü ele geçirebilir, başka yöne yönlendirebilir veya çalabilir ve aynı zamanda hassas verileri tehlikeye atabilir.

Denizcilik endüstrisinde teknolojinin kullanımı arttıkça Kritik Altyapı ve Kritik Bilgi Altyapısı kavramları daha önemli hâle gelmektedir. Son yıllarda bilgisayar korsanlığı, veri ihlali ve fidye yazılımı saldırılarında artış olduğu buna bağlı olarak komuta kontrollerinde kayıpların yaşandığı gözlenmektedir. Saldırganlar, hedeflerine ulaşmak için herhangi bir insan ve teknoloji kombinasyonunu kullanarak gemi liman ve tesislere hedef almaktadır. Bu nedenle, denizcilik otoriteleri, liman gemiler ve denizcilik endüstrisinde yaşanan

siber saldırıların engellenmesini istemektedir. Denizcilik sektörü aksaması duraksaması kapanması söz konusu olduğunda ciddi kayıplara neden olduğu aşikârdır. Yayınlanan tüm kılavuzlarda denizciliğin, çevrenin, yükün ve gemilerin emniyetini ve güvenliğini iyileştirmeyi esas alındığı anlaşılmaktadır.

Siber Dayanıklılık Yasası ile denizcilik sektörüne getirilen yeni düzenlemeler denizcilikte tüm paydaşlarının belirtilen hususlara uymasını istemektedir. Deniz Sigorta Şirketleri de yeni gemi inşa, yükleme ve kiralama kontrat sözleşmeleri için poliçe teminatı kapsamına "Siber Dayanıklılık Yasası ve Siber sertifikasyon çerçevesinin gereklerinin yerine getirilmesi" ibaresini eklemiştir. Gerekli tedbirlerin alınmaması söz konusu olduğunda oluşacak mağduriyetlerin teminat kapsamı dışında bırakılacağı, maddi hasarın tazmin edilmeyeceği duyurulmuş, bun durum sözleşmelere yeni ek maddeler ile belirtilmiştir.

Denizcilikte Siber Dayanıklılık Yasası sayesinde tüm deniz ekosisteminde BT, OT ve Bina Kontrol sistemlerinin daha da güçlü ve takip edilebilir bir şekilde izlenecektir. Güvenlik Sertifikasyonuna sahip olmayan kuruluşların ve ürünlerin sistem içinde dolaşımına ve erişimine izin verilmeyecektir.

Siber Denetleme Birimler kurulması ile sistem ve süreçler daha kolay izlenecektir. İş süreçleri, ekipman, eğitim, olaylara önceden hazırlıklı olma, olay müdahalesi ve kurtarma yönetiminin daha hızlı gerçekleşmesi beklenmektedir. Ayrıca yeni denizcilik sektörüne uyumlanmış olan gemilerin siber güvenliğini sağlamak için siber olayları azaltmak ve bu olayların etkilerini hafifletmek için getirilen ISO ve IACS standartları süreçlerin daha iyi kontrol edilmesine imkân sağlayacaktır.

Dahası AB ve ABD diğer ülkeler arasında siber diplomasi süreçleri ile bilgi paylaşımı yapılmasında mutabakata varılmıştır. Böylelikle hedefli saldırıları önlemede hızlı harekete geçmesini, ülkelerin ve sistemlerin ortak ittifakla daha az zarar görmesini belki de hiç zarar görmemesini sağlayacaktır. Dahası siber saldırganların yüklü miktarda fidye taleplerinin engellenmesine, kuruluşların marka değerini ve itibarının korumaya devam etmesine, genellikle insan kaynaklı olan veri ihlali ile sistem kayıpları ve hassas bilgi ele geçirilmesinin önlenmesine ve enerji ve liman tesislerinde kritik bilginin ve kritik altyapının sürekli olarak korunmasına imkân verecektir.

**KAYNAKÇA**

AMMITEC. (2016). *Cyber Security Awareness.*

DCSA. (2020). *DCSA Implementation Guide for Cyber Security on Vessels v1.0.* Digital Container Shipping Association.

The Oil Companies International Marine Forum (OCIMF). (2017). *Tanker Management and Self Assessment 3 - A Best Practice Guide.*

ANSSI. (2016). *Best Practices for cybersecurity on-board ships.* Agence nationale de la sécurité des systèmes d'information.

ClassNK. (2024). *ClassNK releases Guidelines for Cyber resilience of ships.*

KOREAN Register. (2024). *Cyber Resilience Approval/Survey Guide for Ship Automation Systems.*

T.C. Ulaştırma Altyapı Bakanlığı. (2023). *Ulusal Siber Güvenlik Stratejisi 2020-2023.* T.C. Ulaştırma Alt yapı Bakanlığı: https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf adresinden alındı

Polemi N. ve Van Maale C., 2. R. (2023). *Cybersecurity in Maritime Critical Infraastructure Reflection of American Ports.* The European Union through the Critical Maritime Routes Monitoring, Support and Evaluation Mechanism (CRIMSON III),.

BIMCO, Chamber of Shipping America, Digital Containership Association, INTERCARGO, InterManager, INTERTANKO, . . . WSC. (2021). *THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS.* BIMCO: https://www.bimco.org/products/publications/titles/the-guidelines-on-cyber-security-onboard-ships/ adresinden alındı

Finland National Emergency Supply Agency. (2021b). *Maritime Cybersecurity-Best Practices for Vessels.* https://www.huoltovarmuuskeskus.fi/en: https://www.huoltovarmuuskeskus.fi/en/a/new-maritime-cyber-security-guidelines-for-shipping-companies-and-ships adresinden alındı

Finland National Emergency Supply Agency. (2021a). *Maritime Cybersecurity Report- Finnish Maritime Cybersecurity Maturity Current state report and best practices for the Finnish Maritime sector.* https://www.huoltovarmuuskeskus.fi/en:

https://www.huoltovarmuuskeskus.fi/files/87d5a22180c40cedd9cf89d2a2e2f026a18e31c8/maritime-cybersecurity-report.pdf adresinden alındı

Finland National Emergency Supply Agency. (2021). *Maritime Cybersecurity-Best Practices for Shipowner Organisation.* https://www.huoltovarmuuskeskus.fi: https://www.huoltovarmuuskeskus.fi/files/6236df888931eb8ad0bbc3ea23f3d2a04d5cbd56/cybersecurity-best-practices-for-shipowner-organisations.pdf adresinden alındı

IAPH. (2021). *IAPH Cybersecurity Guidelines for Ports and Port Facilities.* https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf adresinden alındı

ISO-ISO/EIC27001. (2022). *nformation security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO: https://www.iso.org/standard/27001 adresinden alındı

IMO. (2022). *Guidelines on Maritime Cyber Risk Management.*

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., & Ortiz, D. S. (2006). *Maritime Terrorism Risk and Liability.* RAND Corporation.

Servida, A., Erhardt, J.-B., Savo, J., Kernkamp, A., & Polemi, N. (2011). *Analysis of Cyber Security Aspects in the Maritime Sector.* ENISA.

Kristoffersen, P. B., Hartvigsen, T., Myrvang, P., & Torjusen, A. (2015). *Digitale Sårbarheter Maritim Sektor.* Lysneutvalget.

Kretschmann, L., Rødseth, Ø., Tjora, Å., Fuller, B., & Noble, H. (2015). *D9.2: Qualitative assessment.* Kretschmann, L., Rødseth, Ø., Tjora, Å., Fuller, B.S., Noble, H., Horahan, J.: (2015).

IMO. (2022). MSC-FAL.1/Circ.3/Rev.2. Guidelines on Maritime Cyber Risk Management.

IMO. (2017). MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems. .

NIST. (2022, Temmuz 10). NIST Risk Management Framework CSRC.

EU. (2022, Eylül 15). Cyber Resilience Act.

EU. (2024). The EU Cybersecurity Certification Framework.

ABD. (2002). Maritime Transportation Security (MTSA).

ECFR.GOV. (2025, Şubat 02). 33 Cfr part 6 Protection and Security of Vessels, Harbors and Waterfront Facilities.

USCG-United States Coast Guard. (2024, Şubat). Navigation and Vessel Inspection Circular No. 02-04.

USCG. (2025, Ocak 17). Final Rule: Cybersecurity in the Marine Transportation System.

USCG. (2025). https://www.dco.uscg.mil/Our-Organization/CGCYBER/. adresinden alındı

*CGCYBER*. (2025, Şubat). United States Coast Guard: https://www.dco.uscg.mil/Our-Organization/CGCYBER/ adresinden alındı

Eurpoean Union. (2025, Şubat). *Cyber-Diplomacy*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies adresinden alındı

ÖKER, U. (2022). *Türkiye'de Kritik Altyapı ve Siber Güvenlik.* Konrad-Adenauer-Stiftung Türkiye. Türkiye'de Kritik Altyapı ve Siber Güvenlik adresinden alındı

The Norwegian Maritime Cyber Resilience Centre. (2024). *Cyber Annual Threatment Assessment.*

The Norwegian Maritime Cyber Resilience Centre. (2023). *Cyber Annual Threatment Assessment.*

Türk Loydu. (2023). *Guidelines on Cyber Security for Ships and Offshore Units January 2023* .

IACS-International Association of Classification Societies. (2025). *IACS UR E26 and E27 Press Release*. https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release adresinden alındı

USCG. (2023). *Maritime Cybersecurity Assessment and Annex Guide (MCAAG).* https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment%20%20Annex%20Guide%20(MCAAG)_released%2023JAN2023.pdf?ver=NE11YUspj_kNa3xRoMd0TQ%3D%3D adresinden alındı

ISO-ISO/IEC TS 30104:2015. (2022). *ISO/IEC TS 30104:2015*. https://www.iso.org/standard/56890.html adresinden alındı

ISO 28000:2022. (2022). *ISO 28000:2022*. https://www.iso.org/standard/79612.html adresinden alındı

ClassNK. (2024). *ClassNK releases Guidelines for Cyber resilience of ships.*

UK Department for Transport and Maritime and Coastguard Agency. . (2016). *Guidance Ports and port systems: cyber security code of practice.*

UK Department for Transport and Maritime and Coastguard Agency. (2020). *Guidance Ports and port systems: cyber security code of practice.*

BIMCO. (2019). *BIMCO Cyber Security Clause.* https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019 adresinden alındı

EU . (2017, Eylül 13). *Commision Recommendation EU 2017/1584.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017H1584 adresinden alındı

*ETSI TR 103 456 V1.1.1* . (tarih yok). https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf adresinden alındı

NIST. (2022). *Special Publication 800 NIST SP 800-161r1-upd1Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf adresinden alındı

ECFR.GOV. (2022, Temmuz). *33 CFR Part 105 -- Maritime Security: Facilities.* https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-105 adresinden alındı

ENISA. (2020). *Cyber risk Management for Ports Guidelines for cybersecurity in the maritime sector*. ENISA (2020) Cyber risk Management for Ports Guidelines for cybersecurity in the maritime sector. adresinden alındı

ENISA . (2019). *Port Cybersecurity - Good practices for cybersecurity in the maritime sector* .

ENISA. (2024). *REPORT ON THE STATE OF CYBERSECURITY IN THE UNION.*

ENISA. (2024a). *Threat Landscape 2024.*

ENISA. (2024b). *Best Practices for Cyber Crisis Management.*

Denizcilik Genel Müdürlüğü. (2024.). *Dünya Denizciliğindeki Son Gelişmeler,*. https://denizcilik.uab.gov.tr/uploads/pages/aylik-yayinlar/du-nya-denizcilig-indeki-son-gelis-meler-bu-lteni-2024-12.pdf adresinden alındı

International Standard Organisation: ISO/IEC 27001. (2022). *ISO/IEC27001*. (ISO, Editör, & ISO/IEC27001, Prodüktör) ISO/IEC27001: https://www.iso.org/standard/27001 adresinden alındı

*LockBit 3.0 Ransomware Attack on BR Logistics USA*. (2024). https://maritimecybersecurity.nl/incident/N0r68486b3 adresinden alındı

*Ransomware attack by Akira*. (2023). https://maritimecybersecurity.nl/incident/Qbq6kRboY1 adresinden alındı

*MCAD Maritime Cyber Attack Database Map List view Info Report Monti Ransomware Attack on Magsaysay Maritime Corporation and Magsaysay Global Services, Inc.* (2024xk). h https:/maritimecybersecurity.nl/listview?page=3 alındı

*MCAD Maritime Cyber Attack Database Map List view Info Report* . (2024-2025). https://maritimecybersecurity.nl/incident/

ENISA. (2023). *The European Union through the Critical Maritime Routes Monitoring, Support and Evaluation Mechanism (CRIMSON III)*. ENISA.

ENISA. (2023a). *Good Practices for Supply Chain Cybersecurity,*. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity adresinden alındı

Csrc.nist.gov. 2022. NIST Risk Management Framework | CSRC. [online] Available at: <https://csrc.nist.gov/projects/risk-management/about-rmf> [Accessed 10 July 2022]. .