DENİZCİLİK ALANINDA SİBER GÜVENLİK

Dr. Öğretim Üyesi Murat Selçuk Solmaz

Pîrî Reis Üniversitesi Öğretim Üyesi

SUNUM PLANI

- Siber güvenlik-Siber risk
- Siber saldırı-Tipleri-Safhaları
- Gemilerde siber saldırılara hassas sistemler
- Gemi seyir sistemlerine yapılabilecek siber saldırılar
  - GPS
  - AIS
  - ECDIS
  - ARPA-RADAR
- Siber güvenlik tedbirleri (Teknik-Yöntemsel)
- Siber risk yönetimi

SİBER GÜVENLİK

Küreselleşme

Dijital Dönüşüm (Digital Transformation)

Siber Riskler

Siber Güvenlik

DENİZCİLİK ALANINDA SİBER GÜVENLİK

Dijital Dönüşüm

Gemiler

Şirketler

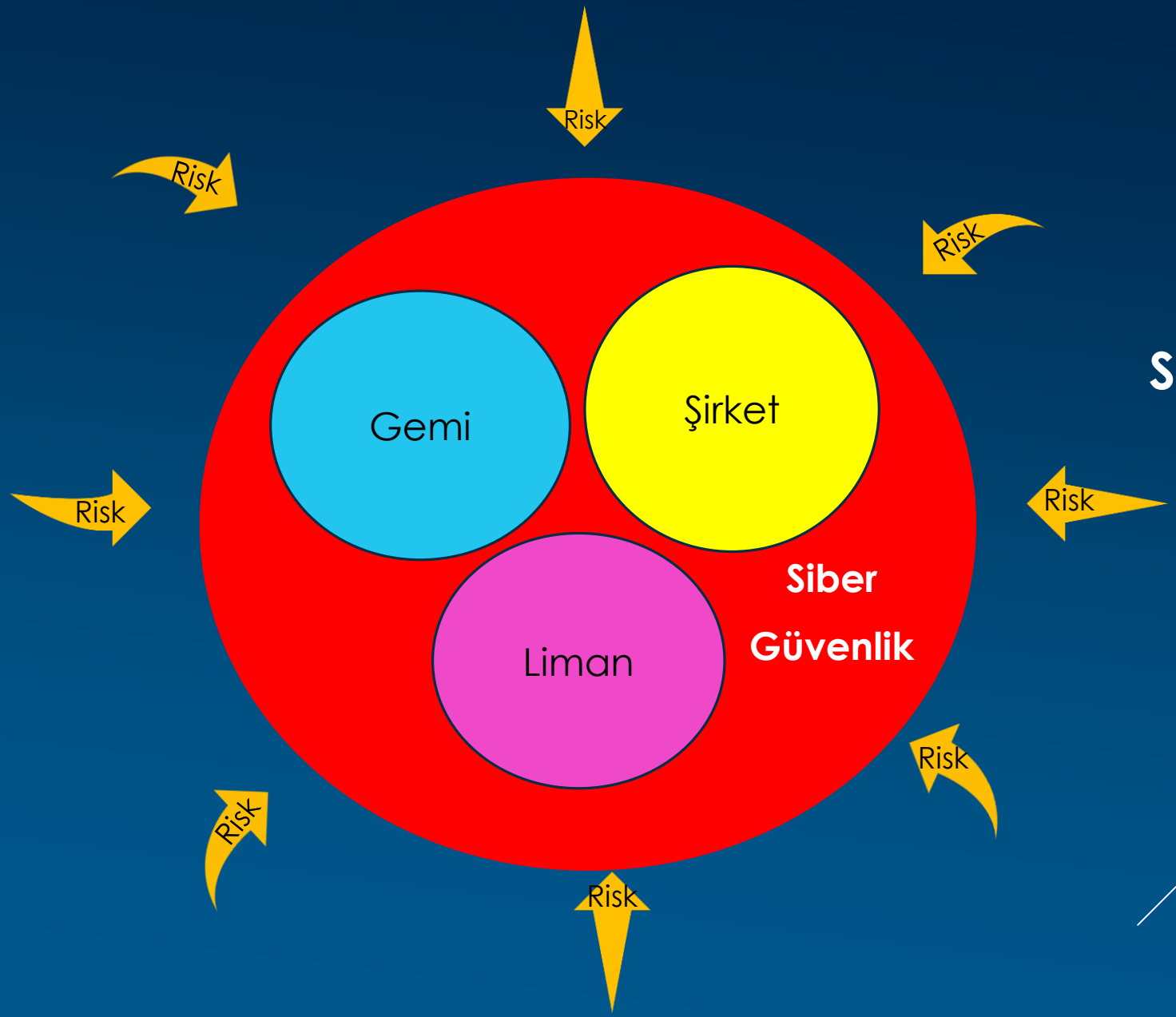
Limanlar

- IOT teknolojisi (Nesnelerin interneti-Internet of Things)
- Dijital ikiz teknolojisi (Digital Twin)
- Blokzinciri teknolojisi (Blockchain)

DİJİTAL DÖNÜŞÜM

- Otonom gemiler (Autonomous ships)
- Akıllı limanlar (Smart ports)

DENİZCİLİK ALANINDA SİBER GÜVENLİK



Siber Riskler

DENİZCİLİKTE SİBER RİSK

Bir teknoloji varlığının, bilgi veya sistemlerin bozulması veya kaybolması sonucunda gemicilikle ilgili operasyonel, emniyet veya güvenlik arızalarına neden olabilecek potansiyel bir durum veya olay tarafından ne ölçüde tehdit edilebileceğinin ölçüsü anlamına gelir.

DENİZCİLİKTE SİBER RİSK

Bozulma - Kaybolma

Kasıt yok

- Kullanıcı hatası
- Bilgisizlik
- Arıza

Emniyet tedbirleri

(SAFETY)

Kasıtlı

- Fiziksel saldırılar
- Siber saldırılar

Güvenlik tedbirleri

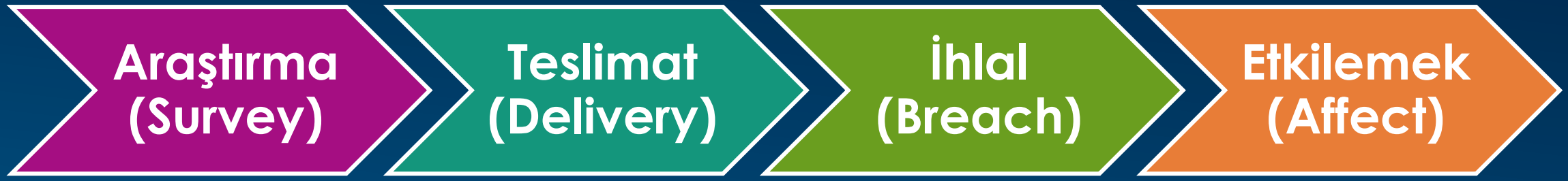
(SECURITY)

SİBER SALDIRI

Siber saldırı, bir teknoloji varlığını yok etme, ifşa etme, değiştirme, devre dışı bırakma, çalma veya bir varlığa yetkisiz erişim veya yetkisiz kullanım sağlama girişimi olarak tanımlanabilir.

SİBER SALDIRI TİPLERİ

- Malware
- MITM (Man in the Middle)
- Water Holing (Watering Hole)
- Denial of Service (DoS)
- Social Engineering
- Phishing
- Spear Phishing
- Brute Force Attack



SİBER SALDIRI SAFHALARI

GEMİLERDE SİBER SALDIRILARA HASSAS SİSTEMLER

- Köprüüstü sistemleri
  - Voyage Data Recorder (VDR)
  - ECDIS
  - GPS-GNSS (Global Navigation Satellite Systems)
  - AIS
  - Automatic Radar Plotting Aid (ARPA) / Radar
- Erişim kontrol sistemleri (CCTV, SSAS, BNWAS)
- Kargo elleçleme ve yönetim sistemleri
- Tahrik, makine yönetimi ve güç kontrol sistemleri
- Muhabere sistemleri
- Yolcu hizmet ve yönetim sistemleri
- Yolcular için internet ağı
- Personel internet ağı

GPS SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR

- **GPS Jamming (Karıştırma)**

GPS frekansında yayınlanan bir gürültü sinyali ile GPS'in kullanımı engellenir ve geminin emniyette seyir kabiliyeti devre dışı bırakılabilir. Bu durumda GPS arıza verir. Önlem için parazit önleyici cihazlar kullanılabilir.

- **GPS Spoofing (Aldatma)**

GPS'in yanlış GPS sinyali alarak yanlış konumu göstermesine neden olur Daha tehlikelidir. Çünkü GPS sahtekarlığı saldırısı durumunda bu saldırı tespit edilemeyebilir. Bu, geminin güvenli seyrini tehlikeye atar.

AIS SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR

- **Ship Spoofing (Gemi Aldatması)**

AIS üzerinde sahte bir gemi ekosu yaratır. Gemi, gerçek bir gemi gibi bayrak, hız, pozisyon, rota, varış yeri, kargo, gemi tipi, boyut, çağrı işareti ve MMSI bilgilerine sahip olabilir. Bu gemi çeşitli şekillerde kullanılarak kullanıcıların kafası karıştırılabilir.

- **Collision Spoofing (Çatışma Aldatması)**

AIS ekranında oluşturulan sahte bir eko ile çarpışma riski varmış gibi gösterilerek geminin ani olarak rotasının değiştirilmesi amaçlanır.

AIS SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR

- **AtoN (Aids-to-Navigation) Spoofing (Seyir yardımcısı Aldatması)**

AIS'in AtoN özelliği yardımıyla vardiya zabiti, alçak gelgitler, kayalık çıkıntılar ve sığlıklar gibi geminin çevresindeki tehlikeler konusunda uyarılır. Bu saldırıda vardiya zabitini geminin yönünü değiştirmeye zorlamak için sahte veriler oluşturulabilir.

- **Weather Forecasting Spoofing (Hava tahmini Aldatması)**

AIS, deniz akıntısı ve iklim durumu gibi çevresel faktörler hakkında bilgi sağlar. Yapılan saldırı ile yanlış hava durumu verileri gönderilir. Kaptan başka bir kaynaktan teyit etmediği taktirde geminin rotasını değiştirebilir.

AIS SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR

- **AIS Hijacking (AIS Kaçırılması)**

İki çeşidi vardır. Birincide saldırgan, gemiden yayınlanan AIS sinyallerini dinler ve değiştirir. Diğer versiyonda ise gerçek AIS sinyallerini bastırmak için daha güçlü sahte sinyaller iletilir. Her iki varyasyonda da alıcı istasyon, orijinal AIS mesajları yerine değiştirilmiş mesajları saldırgan tarafından alır.

- **Disruption Threats (Kesinti Tehditleri):**

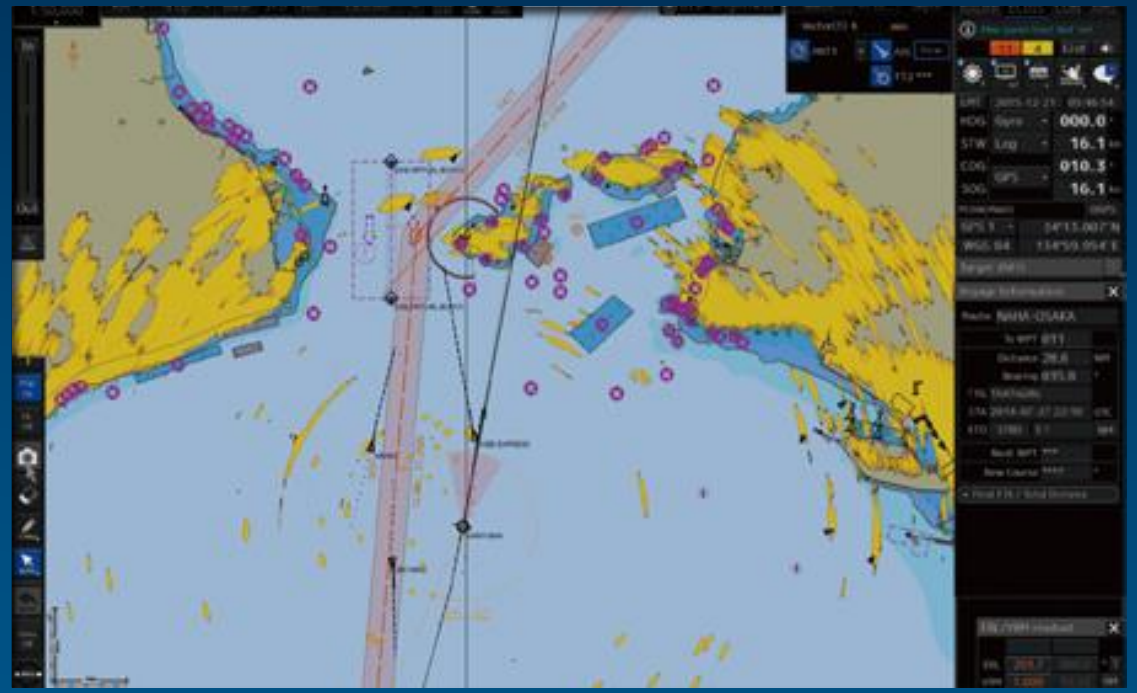
Üç çeşidi vardır (Slot Starvation, Frequency Hopping, Timing Attack). Saldırgan, denizcilik otoritesi gibi davranarak verdiği yanlış ynlendirmeler ile AIS sistemi kullanımını engeller.

AIS SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR

- **AIS-SART Spoofing (AIS-SART Aldatması)**

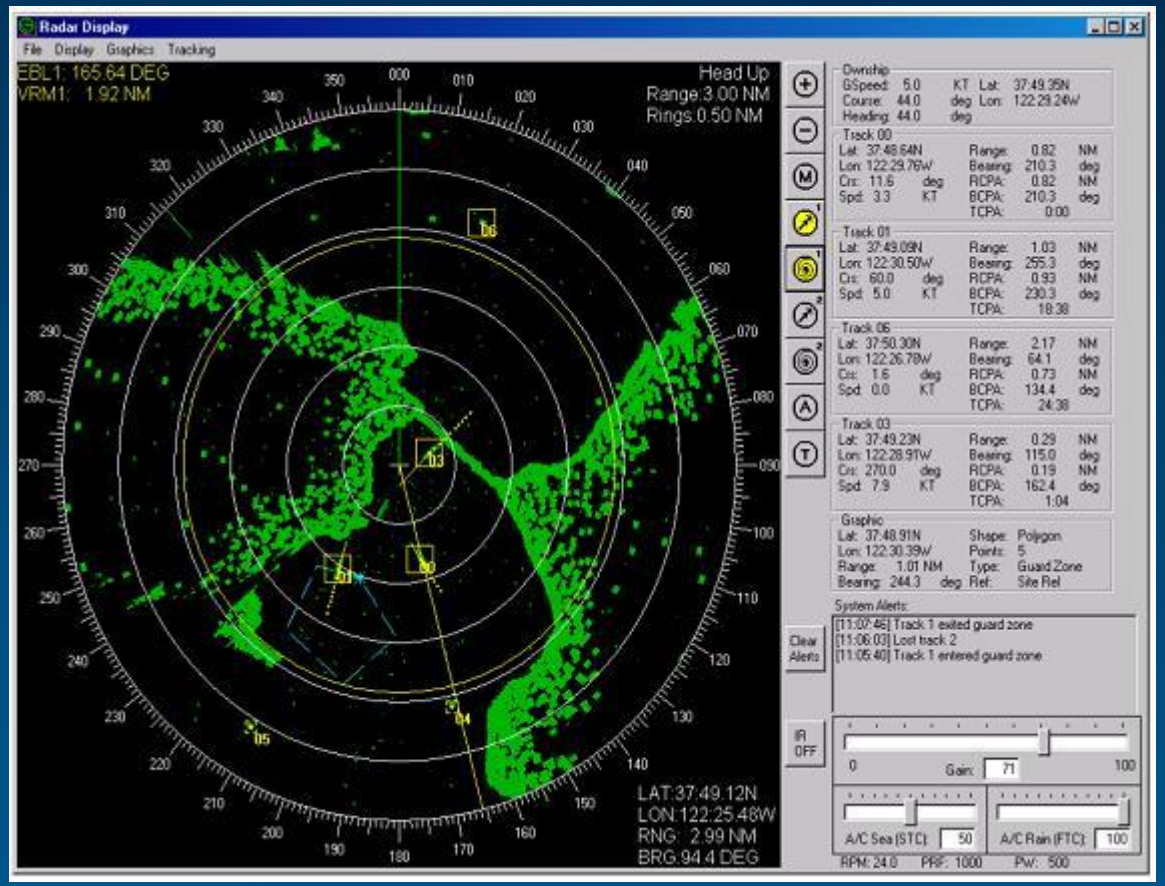
AIS, SAR (Arama ve Kurtarma) operasyonları için kullanılabilir. Gemilerde SART (Arama ve Kurtarma Transponderleri) adı verilen bir cihaz, geminin terk edilmesi durumunda kullanılır ve gemilerin ve uçakların yakınında kazazelerin diğer gemilerin radar ekranlarında görülebilmesini sağlar. AIS bu sinyali algılar ve uyarır. Bu saldırı nedeniyle, AIS SART alarmı vermeye zorlanır ve gemi mürettebatı olmayan kazazedelere yönelerek zaman kaybedebilir.

ECDIS SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR



- GPS koordinatlarının değiştirilmesi
- Sistemin komple çökertilmesi
- Elektronik haritaların değiştirilmesi

ARPA-RADAR SİSTEMİNE YAPILABİLECEK SİBER SALDIRILAR



- Sahte radar ekosu yaratma
- Ekoların silinmesi

SİBER GÜVENLİK TEDBİRLERİ

- Teknik tedbirler
- Yöntemsel Tedbirler

TEKNİK TEDBİRLERİ

- Anti-virüs yazılımları
- Sanal Özel Ağ (Virtual Private Network-VPN) kullanımı
- Şifreleme
- Yedekleme
- Güncel yazılım ve işletim sistemleri kullanılması
- Kablosuz ağların şifrelenmesi
- Uzaktan bağlantının güvenli hale getirilmesi
- USB, RJ-45 ve Kart Okuyucu gibi Koruma Arayüzleri
- Kısıtlı kullanıcı hesabı yaratma
- Sızma testleri
- Seyir sistemlerinin izole edilmesi
- ECDIS güncellemesi için özel USB
- ARPA Radar, AIS, ECDIS entegrasyonu
- Birleşik GPS ve GLONASS

YÖNTEMSEL TEDBİRLER

- Şirket politikasının oluşturulması-Plan geliştirilmesi
- Personel eğitimi-Farkındalık yaratılması
- Sorumlu personel atanması (Şirket-Gemi)
- Gemi bilgisayarındaki verilerin sınıflandırılması
- Bilgi sistem ekipmanların imhası
- Şifre kelimeleri ile çalışma
- Kritik Donanımın Fiziksel Güvenliği
- Değişim Yönetimi Prosedürü (Management of Change-MoC)

YÖNTEMSEL TEDBİRLER

- Uzaktan erişimin kısıtlanması
- Temel Performans Göstergesi (KPI) oluşturulması
- Risk Değerlendirmesi sistemi oluşturulması
- İnternet filtreleme sistemlerinin kullanılması
- Hassas sistemler envanter listesinin oluşturulması
- ECDIS'te elle de mevki atılması
- Uygun bir gözcülük yapılması

SİBER RİSK YÖNETİMİ

Bir siber riski belirleme, analiz etme, değerlendirme, iletme ve paydaşlar için alınan önlemlerin maliyet ve faydalarını dikkate alarak bu riski kabul etme, önleme, aktarma veya kabul edilebilir bir düzeye getirme süreci anlamına gelir.

AMAÇ

Siber risklere operasyonel olarak dirençli olan güvenli ve emniyetli deniz taşımacılığını desteklemektir.

SİBER RİSK YÖNETİMİ

ULUSLARARASI DENİZCİLİK ÖRGÜTÜ (IMO)

Emniyet Yönetim Sistemlerinde Denizcilik Siber Risk Yönetimi

(Maritime Cyber Risk Management in Safety Management Systems)

(Resolution MSC.428(98))

(16 Haziran 2017)

1 Ocak 2021'den sonra şirketin Uyumluluk Belgesi (Document of Compliance) ilk yıllık doğrulamasından geç olmamak üzere siber riskleri mevcut emniyetli yönetim sistemlerinde (ISM Kodunda tanımlandığı gibi) uygun şekilde ele alınmasını sağlamaya idareleri teşvik etmektedir.

ULUSLARARASI DENİZCİLİK ÖRGÜTÜ (IMO)

Denizcilik Siber Risk Yönetimine Ilişkin Kılavuzlar

(Guidelines on Maritime Cyber Risk Management)

(MSC-FAL.1/Circ.3)

(5 Temmuz 2017)

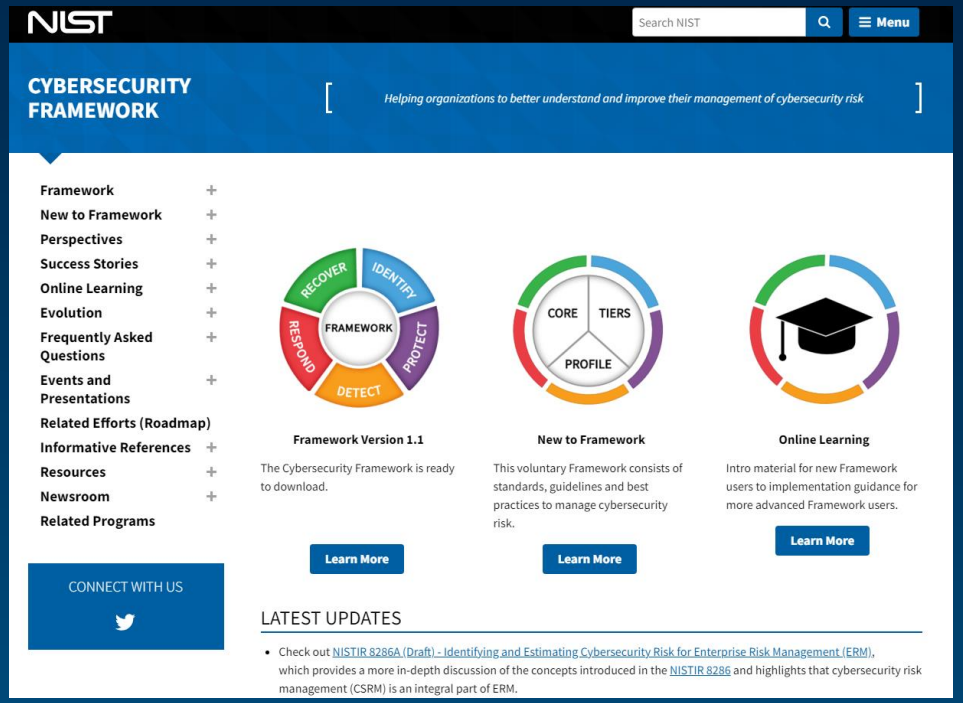
Deniz taşımacılığını siber tehditlerden ve güvenlik açıklarından korumak için denizcilik siber risk yönetimi konusunda öneriler sağlar ve etkili siber risk yönetimini destekleyen işlevsel unsurlar içerir.

https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf

International Organization for Standardization

https://www.iso.org/isoiec-27001-information-security.html

The National Institute of Standards and Technology (NIST)



https://www.nist.gov/cyberframework

FAYDALANILAN KAYNAKLAR

- Oruç A. (2020). Cybersecurity Risk Assessment For Tankers And Defence Methods. Yüksek Lisans tezi. Piri Reis Üniversitesi.
- https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
- https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.nist.gov/cyberframework

TEŞEKKÜRLER

Dr. Öğretim Üyesi Murat Selçuk Solmaz

Pîrî Reis Üniversitesi Öğretim Üyesi