KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DENİZ ULAŞTIRMA İŞLETME MÜHENDİSLİĞİ ANABİLİM DALI

GEMİ ELEKTRONİK SEYİR YARDIMCI SİSTEMLERİNE YÖNELİK SİBER SALDIRI RİSKİNİN BAYES AĞI METODU İLE DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Barış AYDIN

MART 2021
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DENİZ ULAŞTIRMA İŞLETME MÜHENDİSLİĞİ ANABİLİM DALI

GEMİ ELEKTRONİK SEYİR YARDIMCI SİSTEMLERİNE YÖNELİK SİBER SALDIRI RİSKİNİN BAYES AĞI METODU İLE DEĞERLENDİRİLMESİ

Barış AYDIN

ORCID : - - -

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce

"DENİZ ULAŞTIRMA İŞLETME YÜKSEK MÜHENDİSİ"

Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 22 / 02 /2021

Tezin Savunma Tarihi : 31 / 03 /2021

Tez Danışmanı : Doç. Dr. Özkan UĞURLU

ORCID : - - -

Trabzon 2021

ÖNSÖZ

Endüstrinin en önemli kollarından biri olan ve dünya genelinde ticari malların %90'ına yakınının taşındığı denizcilik sektörü, teknolojik gelişmelerin takibinde ve onlara adaptasyonda en tembel sektör olarak tarif edilmektedir. Otomobil endüstrisinde onlarca yıl önce hayata geçirilmeye başlanan siber güvenlik uygulamaları denizcilik endüstrisinin en önemli parçası olan gemilerde kısıtlı olarak 1 Ocak 2021'den itibaren Uluslararası Denizcilik Örgütü (IMO) talimatıyla uygulanmaya başlanmıştır. Günümüzde boyu 400 metreyi, su çekimi 25 metreyi aşan gemiler 300.000 ton akaryakıt, 24.000 TEU konteyner veya 400.000 ton kuru yük taşıyabilecek kapasitededir. Yakın gelecekte insansız, otonom ticari gemiler de dünya denizlerindeki yerini alacaktır. Gemilerde kazaları, can kaybını, maddi zararları, doğanın kirlenmesini önlemek, sürdürülebilir bir çevre, insan sağlığı ve ticaret için gerekli önlemler uluslararası kurallar çerçevesinde alınmaktadır. Siber güvenlik, belirtilen tüm bu etmenleri doğrudan etkileme potansiyeli taşımakta olduğundan gemi gibi uydu ve telsiz bağlantısının, bilgisayar ve otomasyon alt yapısının kritik sistemlerde kullanıldığı bir ortamın siber güvenli olması önem arz etmektedir. Denizcilik sektörünün siber güvenlik konusunda kısa zamanda halletmesi gereken birçok önemli detay bulunmaktadır. Bu çalışmanın amacı teknolojik anlamda siber güvenli gemi seyir yardımcı sistemleri altyapısının nasıl oluşturulabileceği anlamında eksiklikleri gidermeye yardımcı olmak ve tavsiyede bulunmaktır.

Tez çalışmam boyunca desteğini esirgemeyen Sayın Doç. Dr. Özkan UĞURLU'ya teşekkür ve saygılarımı sunarım. Ayrıca, yardım ve desteklerinden dolayı Sayın İshak ALTINPINAR ve Sayın Serdar YILDIZ'a teşekkürü bir borç bilirim.

Bu tez çalışmasını, her zaman yanımda olan, maddi ve manevi desteğini hiçbir zaman esirgemeyen eşim Seda GAYRETLİ AYDIN, kızım Melisa ve oğlum Mustafa Kemal'e ithaf ediyorum.

Barış AYDIN
Trabzon 2021

TEZ ETİK BEYANNAMESİ

Yüksek Lisans Tezi olarak sunduğum “Gemi Elektronik Seyir Yardımcı Sistemlerine Yönelik Siber Saldırı Riskinin Bayes Ağı Metodu ile Değerlendirilmesi” başlıklı bu çalışmayı baştan sona kadar danışmanım Doç. Dr. Özkan UĞURLU’nun sorumluluğunda tamamladığımı, verileri kendim topladığımı, analizleri kendim yaptığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim. 31/03/2021

Barış AYDIN

İÇİNDEKİLER

Sayfa No

Yüksek Lisans Tezi

ÖZET

Gemi Elektronik Seyir Yardımcı Sistemlerine Yönelik Siber Saldırı Riskinin Bayes Ağı Metodu ile Değerlendirilmesi

Barış AYDIN

Karadeniz Teknik Üniversitesi
Fen Bilimleri Enstitüsü
Deniz Ulaştırma İşletme Mühendisliği Anabilim Dalı
Danışman: Doç. Dr. Özkan UĞURLU
2021, 121 Sayfa, 8 Sayfa Ek

Siber (bilişim) suçları dünya genelinde en hızlı yaygınlaşan suç şekli olarak değerlendirilmektedir. Maddi ve manevi zararları azımsanmayacak miktarlara ulaşabilecek siber tehditlere karşı endüstrinin her dalında personelin eğitilmesi, risk değerlendirme prosedürlerinin geliştirilmesi, teknolojik yatırımlar gibi önlemler alınmaktadır. Bu çalışma, konunun teknolojik yönüyle analizine dayandırılmış ve gemide kullanılmakta olan elektronik seyir yardımcı sistemlerden Konum Belirleme Sistemi, Otomatik Tanımlama Sistemi (AIS), Elektronik Harita Gösterimi ve Bilgi Sistemi (ECDIS) ile Otomasyon, Haberleşme, Bilgisayar Sistemi'nin siber saldırıya uğrama olasılıkları incelenmiştir. Bu 4 sistem temel alınarak akademik yayınlara, deneysel çalışmalara, gerçekleşmiş siber olaylara, ilgili kurum ve kuruluşların önerilerine istinaden hazırlanan düğümler ile bir Bayes Ağı oluşturulmuştur. Son yarım yüzyılda kaza analizi de olmak üzere birçok alanda kullanılan Bayes Ağı, olayı (kazayı) meydana getiren faktörler arası ilişkiyi koşullu olasılık yaklaşımı kullanılarak gerçeğe en yakın şekilde ortaya koymaya imkan sağlamaktadır. Koşullu olasılık değerleri 8 tane uzmanın görüşlerine dayandırılmıştır. Yapılan analiz ile en riskli unsurun ECDIS ve Otomasyon, Haberleşme, Bilgisayar Sistemi olduğu anlaşılmıştır. Ekipman ve oluşturulacak sistem altyapısı içeriği konularında gemilerin siber güvenlik durumlarını arttıracak tavsiyelerde bulunulmuştur.

Anahtar Kelimeler: Siber güvenlik, Siber saldırı, Seyir, Bayes Ağı.

Master Thesis

SUMMARY

Analysing Risk of Cyber Threat to Ship Electronic Navigation Auxilary Systems with Bayesian Network Method

Barış AYDIN

Karadeniz Technical University
The Graduate School of Natural and Applied Sciences
Department of Maritime Transportation and Management Engineering
Supervisor: Assoc. Prof. Dr. Özkan UĞURLU
2021, 121 Pages, 8 Pages Appendix

Cybercrime is considered to be the fastest spreading type of crime worldwide. In every branch of the industry measures such as training of personnel, developing risk assessment procedures and technological investments are taken against cyber threats, material and moral damages of which can reach substantial amounts. This study is based on analysing of subject in technology aspect and examination of cyber vulnerability probability of Positing System, AIS, ECDIS and Automation, Communication, Computer Systems which are parts of ship navigation auxiliary systems. Literature review, experimental works, cyber incidents occurred in maritime sector, recommendations of institutions and organizations are taken into account to form nodes of a Bayesian Network that includes above said systems. The Bayesian Network, which has been used in many fields, including accident analysis, in the last half century, enables to reveal the relationship between factors that cause the event (accident) in the most realistic way by using the conditional probability approach. Conditional probability values of the Bayesian Network has been determined by 8 different experts. As a result, it is identified that ECDIS and Automation, Communication, Computer Systems are most cyber vulnerable parts of the ship. Recommendations regarding to equipments and content of system infrastructure are expressed to increase cyber security degree of ships.

Key Words: Cyber security, Cyber attack, Navigation, Bayesian Network.

ŞEKİLLER DİZİNİ

Sayfa No

TABLOLAR DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

AA : Ortalama Anlaşma (Average Agreement)
AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ABS : Amerikan Denizcilik Bürosu (American Bureau of Shipping)
AIS : Otomatik Tanımlama Sistemi (Automatic Identification System
APT : Gelişmiş Sürekli Tehdit (Advanced Persistent Threat)
ARPA : Otomatik Radar Plotlama Desteği (Automatic Radar Plotting Aid)
ASC : Otonom Gemi Deneteleyicisi (Autonomous Ship Controller)
AtoN : Seyir Yardımcısı (Aids to Navigation)
BE : Temel Olay (Basic Event)
BGAN : Geniş Bant Küresel Alan Ağı (Broadband Global Area Network)
BIMCO : Baltık ve Uluslararası Denizcilik Konseyi (Baltic and International Maritime Council)
BİT : Bilgi ve İletişim Teknolojileri
BN : Bayes Ağı (Bayesian Network)
BNWAS : Köprüstü Seyir Takip ve Alarm Sistemi (Bridge Navigation Watch Alarm System)
BTK : Bilgi Teknolojileri ve İletişim Kurumu
CBS : Cross Border Security
CC : Konsesus Katsayısı (Consensus Coefficient)
CD : Yoğun Disk (Compact Disk)
CDI : Kimyasal Madde Dağıtım Enstitüsü (Chemical Distribution Institute)
CDMA : Kod Bölmeli Çoklu Erişim (Code Division Multiple Access)
CIO : Bilişim Kurulu Başkanlarının (Chief Information Officer)
CISO : Baş Bilgi Güvenliği Yöneticisi (Chief Information Security Officer)
CFCS : Danimarka Savunma İstihbarat Servisi Siber Güvenlik Merkezi (Danish Defence Intelligence Service Centre for Cyber Security)
CMS : İçerik Yönetim Sistemi (Content Management System)
COSCO : China Ocean Shipping (Group) Company
CPU : Merkezi İşlem Birimi (Central Process Unit)

CSO : Şirket Güvenlik Zabitlerinin (Company Security Officer)
db : Desibel
DDoS : Dağınık Hizmet Dışı Bırakma (Distributed Denial of Service)
DHS : ABD İç Güvenlik Bakanlığı (US Department of Homeland Security)
DNV-GL : Det Norske Veritas–Germanischer Lloyd
DMZ : Çevre Ağı veya Sivil Bölge (Demilitarized Zone)
DP : Dinamik Konumlandırma (Dynamic Positining)
DR : Parakete Mevkii (Dead Reckoning)
DoC : Şirket Uygunluk Belgesi (Document of Compliance)
DoS : Hizmet Dışı Bırakma (Denial of Service)
ECDIS : Elektronik Harita Gösterimi ve Bilgi Sistemi (Electronic Chart Display and Information System)
EDR : Yönetilen Uç Nokta Atak tespiti ve Yanıtlama (Managed Endpoint Detection And Response)
EGM : Emniyet Genel Müdürlüğü
eLORAN : Genişletilmiş Uzun Mesafeli Seyir (Enhanced Long Range Navigation)
EMSA : Avrupa Deniz Emniyet (European Maritime Safety Agency)
ENC : Elektronik Seyir Haritaları (Electronic Navigation Chart)
EP : Tahmini Mevki (Estimated Position)
EUROSTAT : Avrupa İstatistik Ofisi (Statistical Office of the European Communities)
ETA : Tahmini Varış Zamanı (Estimated Time of Arrival)
FBI : Federal Soruşturma Bürosu (Federal Bureau of Investigation)
FDMA : Frekans Bölmeli Çoklu Erişim (Frequency Division Multiple Access)
FEMA : Federal Acil Durum Yönetim Kurumu (Federal Management)
FPS : Bulanık Olasılık Puanı (Fuzzy Possibility Score)
FPT : Dosya Transfer Protokolü (File Transfer Protocol)
FPVA : İlk İlke Güvenlik Açığı Değerlendirmesi (First Principle Vulnerability Assesment)
GCHQ : Birleşik Krallık Hükümeti İletişim Genel Merkezi (Government Communications Headquarters)
GB : Gigabayt
GLONASS : Globalyana Navigatsionnaya Sputnikovaya Sistemaa
GMDSS : Küresel Denizcilik Tehlike ve Güvenlik Sistemi (Global Maritime Distress

Safety System)

GNSS : Küresel Uydu Seyir Sistemi (Global Navigation Satellite Systems)

GPS : Küresel Konum Belirleme Sistemi (Global Positioning System)

HP : Hewlett-Packard

IBS : Entegre Köprüüstü Sistemleri (Integrated Bridge Systems)

ICS : Endüstriyel Kontrol Sistemleri (Industrial Control Systems)

ICT : Bilgi ve İletişim Teknolojileri (Information and Communication Technologies)

IHO : Uluslarası Hidrografi Dairesi'nin (International Hydrography Office)

IHS : Information Handling Services

ILA : Uluslararası Loran Kurumu (International Loran Association)

IMO : Uluslararası Denizcilik Örgütü (International Maritime Organization)

INS : Entegre Seyir Sistemi (Integrated Navigation System)

IRISL : İran Devlet Denizcilik Şirketi (Islamic Republic of Iran Shipping Lines)

IoT : Nesnelerin İnterneti (Internet of Things)

IP : İnternet Protokol Adresi (Internet Protocol Address)

ISM : Uluslararası Emniyetli Yönetim (International Safety Management)

IT : Bilgi Teknolojileri (Information Technologies)

JWC : Jordan Wylie Consultant International

LAN : Yerel Ağ Bağlantısı (Local Area Network)

LEO : Alçak Dünya Yörünge (Low Earth Orbit)

Mbps : Bir saniyedeki megabit cinsinden veri hızı (Megabit per second)

MCA : İngiltere Denizcilik ve Sahil Güvenlik Ajansı (Britain Maritime and Coastguard Agency)

MI5 : İngiliz İç istihbarat Teşkilatı (Military Intelligence Section 5)

MDR : Mishcon de Reya Group

MEO : Orta Dünya Yörüngesi (Medium Earth Orbit)

MMSI : Denizcilik Seyyar Hizmet Kimlik Numarası (Maritime Mobile Service Identity)

MSC : Deniz Emniyeti Komitesi (Maritime Safety Committee)

NITC : İran Ulusal Tanker Şirketi (National Iranian Tanker Company)

NK : Class Nippon Kaiji Kyokai

OCIMF : Petrol Şirketleri Uluslararası Denizcilik Forumu (Oil Companies

	International Marine Forum)
OT	: Operasyonel Teknoloji (Operational Technology)
PDF	: Taşınabilir Belge Biçimi (Portable Document Format)
PKI	: Açık Anahtar Altyapısı (Public Key Infrastructure)
PLC	: Programlanabilir Mantıksal Denetleyici (Programmable Logic Controller)
PSGP	: Liman Güvenlik Hibe Programı (Port Security Grant Program)
Res.	: Önerge, Karar (Resolution)
RA	: Değişken Anlaşma (Relative Agreement)
RCU	: Buluşma Kontrol Ünitesi (Rendezvous Control Unit)
RoRo	: Ro-Ro Gemisi (Roll-on Roll-off)
SAR	: Arama Kurtarma (Search and Rescue)
SCADA	: Denetleme Kontrol ve Veri Toplama Sistemleri (Supervisory Control and Data Acquisition)
SDN	: Yazılım Tabanlı Ağlar (Software Defined Networks)
SMB	: Sunucu İleti Bloğu (Server Message Block)
SMI	: Ship Management International
SOLAS	: Denizde Can Güvenliği Uluslararası Sözleşmesi (International Convention for Safety of Life at Sea)
SPAWAR	: Donanması Uzay ve Deniz Savaşları Sistem Komutanlığı (US Navy Naval Information Warfare Information Systems Command)
SSAS	: Gemi Güvenlik Uyarı Sistemi (Ship security Alert System)
SSO	: Gemi Güvenlik Zabitlerinin (Ship Security Officer)
STCW	: Gemiadamlarının Eğitimi, Vardiya Tutma ve Sertifikalandırılması Hakkında Uluslararası Sözleşme (The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers)
SQL	: Yapılandırılmış Sorgu Dili (Structured Query Language)
TCP/IP	: Gönderi Kontrol Protokolü / İnternet Protokolü (Transmission Control Protocol/Internet Protocol)
TDMA	: Zaman Bölmeli Çoklu Erişim (Time Division Multiple Access)
TEU	: Yirmi Ayak Eşdeğer Birimi (Twenty-foot Equivalent Unit)
TFN	: Üçgen Bulanık Sayı (Triangular Fuzzy Number)
UAB	: Ulaştırma ve Altyapı Bakanlığı
UDP	: Kullanıcı Veribloğu İletişim Kuralları (User Datagram Protocol)

UNCTAD : Birleşmiş Milletler Ticaret ve Kalkınma Konferansı'nın (United Nations Conference on Trade and Development)

URL : Standart Kaynak Bulucu (Uniform Resource Locator)

USB : Evrensel Seri Veriyolu (Universal Serial Bus)

USCG : Birleşik Devletler Sahil Güvenliği (United States Coast Guard)

UTC : Eşgüdümlü Evrensel Zaman (Coordinated Universal Time)

VHF : Çok Yüksek Frekkans (Very High Frequency)

VDR : Sefer Veri Kaydedicisi (Voyage Data Recorder)

VPN : Sanal Özel Ağ (Virtual Private Network)

VSAT : Çok Küçük Açıklıklı Terminal (Very Small Aperture Terminal)

VTS : Gemi Trafik Hizmetleri (Vessel Traffic Services)

Ya. : Yarımada

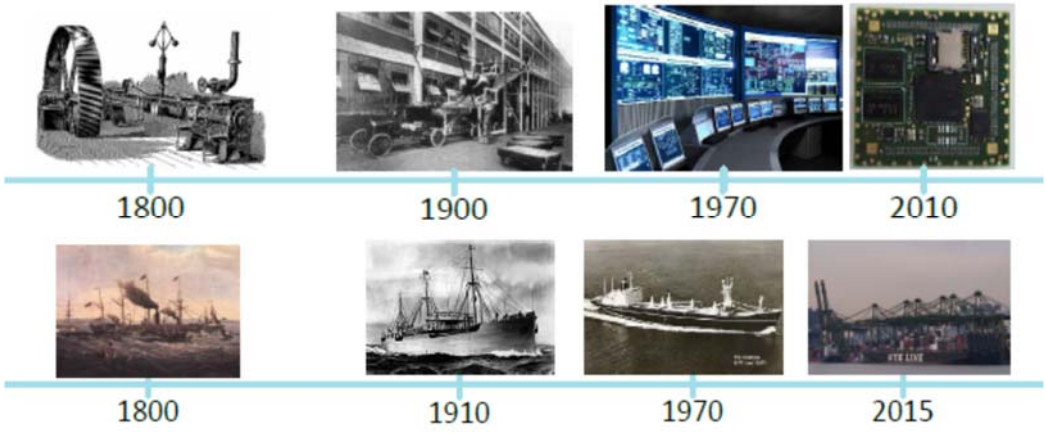
1. GENEL BİLGİLER

1.1. Giriş

Dünya genelinde taşımacılık yüzde 80 ile 90 arasında değişen oranda deniz yolu ile yapılmaktadır (UNCTAD, 2018). Deniz ticareti hacmi 2017 yılında %4,1 ile önceki 5 yılın en yüksek seviyesinde, 2018 yılında ise %2,7 artış göstermiştir (UNCTAD, 2019). Avrupa Birliği'nde (AB) 2002 ile 2019 yılları arasında deniz yolu taşımacılığının ithalattaki payı %40'dan %55'e, ihracattaki payı ise %38'den %45'e çıkmıştır (EUROSTAT, 2020). Rakamlardaki artış miktarı gelişmiş ekonomiler için deniz taşımacılığının önemini göstermektedir.

Gıda ürünlerinden elektronik aletlere, akaryakıttan yeraltı madenlerine kadar birçok nihai ürünün ve ham maddenin bir noktadan başka bir noktaya aktarıldığı deniz yolu taşımacılığının en önemli unsurlardan biri gemidir. Endüstrinin ihtiyaçlarına cevap verebilmek için zaman içerisinde gemiler Şekil 1'de gösterildiği üzere teknolojiye ayak uydurarak değişik tiplerde, sürekli büyüyen ebatlarda ve farklı amaçlarda kullanılabilecek şekilde inşa edilmektedir (Rødseth, 2016). 1712 yılında Thomas Newcomen'in imal ettiği buhar makinesinin 1781 tarihinde James Watt tarafından geliştirilmesi ile 1. Sanayi devriminin en önemli aktörü buhar makinesi sanayide uygulanabilir hale gelmiştir. Böylelikle dokuma tezgahlarından trenlere kadar birçok alanda buhar makinesi kullanılmaya başlanmıştır (Eğilmez, 2018). Birinci sanayi devrimi ile yelkenle ve kürekle çalışmakta olan gemilerde buhar gücü de kullanılmaya başlanmıştır, sonrasında sadece buhar gücüyle hareket eden daha büyük gemiler inşa edilmiştir. 20. Yüzyılın başlarında 2. Sanayi Devrimi büyük fabrikaların bant sistemlerinde seri üretimin başladığı, elektriğin ve içten yanmalı motorların yaygın ve etkin olarak kullanıldığı dönemdir (Kobylinski, 2016). Bu süreçte gemilerde de artık dizel makineler kullanılmaya başlanmıştır böylelikle gemilerin ebatları ve seyir hızları daha da artmıştır. 20. yüzyılın ortaları ise elektronik ve bilgisayar teknolojilerinin endüstrinin her aşamasında kullanılmaya başlandığı 3. Sanayi Devrimi dönemidir (Soylu, 2018). Kısmen halen içerisinde olduğumuz bu süreçte, gemilerin hem köprüüstü sistemleri hem de makine dairesi sistemleri olabildiğine elektronikleşmiş ve bilgisayarlaşmıştır. Dijital cihazların birbirlerini kontrol ettiği otomasyon sistemlere sahip

gemiler emniyet, çevresel faktörler ve ekonomik öncelikler açısından artık büyük bir öneme sahiptir.



1. Yelkenden buhara: İnşaa edilen ilk buharlı transatlantik SS Great Wester, 1838 yılındaki ilk seferinde.
2. Dizel makine: 1911 yılında B&W Copenhagen tarafından inşaa edilen uzakyol sefer yapabilen makineli ilk gemilerden Selinda.
3. 1969 yılında Kongsberg tarafından yapılan ilk tam dijital makine kontrol sistemli gemi olan M/S Taimyr.
4. Siber-fiziksel sistemler: İleri otomasyon sistemlerine sahip NYK Adonis gemisi Singapur Limanı'nda

Şekil 1. Endüstri devrimleri ile gemilerin gelişimi (Rødseth, 2016).

4. Sanayi Devrimi, 2011 yılında Almanya'da yapılan Hannover Fuarında ilk defa sözü edilerek hayatımıza girmiştir. 4. Sanayi Devrimi kavramının temeli; endüstriyel üretim sürecinde yer alan tüm birimlerin birbiriyle iletişimine, bütün ilgili verilere gerçek zamanlı olarak ulaşılabilmesine dayanmaktadır. Bu veriler sayesinde mümkün olan en fazla katma değerin sağlanması amaçlanmaktadır (Brettel vd., 2014). Bu yenilik, şirketlerin; rekabet şartlarına ayak uydurabilmeleri ve daha kaliteli ürün üretebilmeleri için kullanılan bir sisteme, makineye ya da elektronik cihaza internet üzerinden erişim sağlayabilmesi anlamındadır.

3. Sanayi Devrimiyle elektronikleşmeye başlayan gemiler, uydular sayesinde konumlarını en doğru şekilde tespit edebilmekte, her türlü haberleşme sistemi ve değişik amaçlar için karmaşık bilgisayar sistemleri ile donatılmaktadırlar. Günümüzde ise 4. Sanayi Devrimi ve onun öncüsü internet sayesinde okyanusun ortasında seyir yapmakta olan bir gemi içerisindeki karmaşık bilgisayar sistemleri dünyanın diğer ucundaki gemi

işletmecisinin ofisinden saniyelerle ölçülebilecek bir gecikmeyle görsel veya sayısal olarak takip edilebilmektedir. 4. Sanayi Devriminin gemiler için bir sonraki adımı ise halen üzerinde çalışılmakta olan insansız gemi projeleridir. Üzerinde hiçbir canlı kullanıcı bulunmayan, süper hızlı sensörler, işlemciler ve bilgisayarlarla donatılmış sistemlere sahip akıllı gemiler yakın gelecekte denizlerde dolaşmaya başlayacaktır (Hogg ve Ghosh, 2016; Rolls-Royce Plc, 2016).

Sürekli gelişmekte olan bu teknolojik süreç birtakım sorunları da beraberinde getirecektir. Bunlardan bir tanesi de elektronik ve uydu bağlantılı bir sistemin maruz kalabileceği siber (bilişim) saldırı tehdididir (Mileski vd., 2018). Siber güvenlik tehdidi düşünülmeden hayata geçirilecek herhangi bir sistemin dışarıdan erişilebilir veya kontrol edilebilir hale gelmesi büyük riskler meydana getirmektedir. Bu konu, günde oluşturacağı 60 GB bilgiyi karadaki ilgili istasyona uydu bağlantısı ile göndermesi gereken insansız gemi için de günümüzde kullanılan gemilerin geleneksel operasyon sistemlerine gelişmiş Bilgi ve İletişim Teknolojileri (ICT) eklenmiş bir gemi için de aynı derecede önemlidir (Kobylinski, 2016; Katsikas, 2017).

Siber tehdit gemiler için bir güvenlik sorunu olarak değerlendirildiğinde iki konuya çözüm getirilmelidir. Birinci konu, geminin her zaman için "denize elverişli" (sea worthy) olması gerektiği gibi günümüzde artık "elektronik elverişli" (e-worthy) olması da gerektiğidir. Buna bağlı olarak, gemilerin elektronik elverişli olmasını sağlayacak teknik altyapı ve kurallar hayata geçirilmelidir (Tucci, 2017). İkinci konu olarak da gemiadamlarının siber tehdit, siber güvenlik ve siber emniyet konularındaki farkındalıklarını arttıracak eğitimlerin, prosedürlerin ve uygulamaların geliştirilmesi gerekliliğidir (Lee vd., 2017).

Mileski vd. (2018), denizcilik endüstrisinin siber güvenlik konusunda diğer endüstri dallarına göre 10 ile 20 yıl arasında geride olduğunu savunmaktadır. 2008 yılında sadece 600 adet gemide sürekli uydu interneti erişimi bulunmaktayken 2017 yılında yaklaşık 30.000 adet gemide sürekli uydu interneti erişimi bulunmaktadır. Bu nedenle gemiler siber anlamda eski dönemlere göre daha riskli durumdadır (CFCS, 2017). IHS Markit ile Baltık ve Uluslararası Denizcilik Konseyi'nin (BIMCO) 22 Temmuz 2016'da yaptıkları siber güvenlik anketine göre, denizcilik sektöründeki siber saldırıların %21'i ticari kayba sebebiyet vermektedir, gerçekleşmiş siber saldırıların %4'ü gemilerdeki sistemleri etkilemeye yöneliktir (IHS Markit, 2016). Haziran 2017'de AP Moller Maersk'in uğradığı NotPetya virüsü saldırısının şirkete maliyetinin en iyi ihtimalle 300 milyon dolar olduğu

belirtilmektedir (Daum, 2019). Sektörün sorunlara bakış açısındaki tembelliği, gelişen teknolojilerin kullanımındaki kısa zaman içinde artış, bunun yanında siber korsanların ve saldırıların her geçen gün sayısının ve şirketlere maliyetlerinin artması yukarıda bahsedilen temel iki soruna en kısa zamanda çözüm getirilmesini gerektirmektedir.

Literatürde gemilere yönelik siber güvenlik tehdidi konusunun teknolojik yönüne ilişkin çok sayıda çalışma bulunmamaktadır. Çalışmanın amacı, teknolojik anlamda siber güvenli gemilerin nasıl oluşturulacağı konusundaki eksiklikleri gidermek ve konu ile ilgili literatüre katkıda bulunmaktır. Tez çalışması, gemilerde kullanılmakta olan 4 seyir yardımcı sistem olan Konum Belirleme Sistemi, Otomatik Tanımlama Sistemi (AIS), Elektronik Harita Gösterimi ve Bilgi Sistemi (ECDIS) ile Bilgisayar, Haberleşme, Otomasyon Sistemi'nin siber güvenlik değerlendirmesine dayandırılmıştır. Değerlendirme için, akademik, deneysel ve teknik çalışmalardaki tespitler ve önerilerden, gerçekleşmiş olayların analizinden elde edilen bilgilerden, ilgili kurum ve kuruluşların önerilerinden yararlanılmıştır. Bunlar ışığında, belirtilen 4 sistem ile gemilerdeki siber saldırı olaylarının modellemesi yapılmıştır. Uzman değerlendirmeleri kullanılarak gemilerin karşılaşabileceği siber güvenlik tehdidinin oluşma olasılığı hesaplanmıştır. Gemilerde kullanılabilecek yüksek siber güvenliğe sahip sistemler hakkında tavsiyelerde bulunulmuştur.

1.2. Siber Güvenlik

Siber (cyber) sözcüğü sibernetik (Cybernetics) kelimesinin ön ekidir ve bu kelimenin kısaltması olarak kullanılmaktadır (Ning vd., 2018). Siber kelimesinin Türkçe karşılığı bilişimdir. Bilişimin tanımı; insanların teknik, ekonomik ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilim dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimidir (Altunok ve Çakmak, 2009). Wiener ise sibernetiği, hayvanda ve makinede kontrol ve iletişim bilimi olarak tanımlamaktadır (Ashby, 1957).

Siber güvenlik; bilgisayar programlarını, internete bağlı elektronik sistemleri ve ağ yapılanmalarını siber saldırılardan korumak amacıyla geliştirilen politikalardır (Betz ve Stevens, 2011). Bu politikaların temel amacı yetkisiz kişilerin kritik bilgilere ulaşmasını engellemek, mevcut sistemleri kendi çıkarları doğrultusunda manipüle etmelerinin önüne geçmektir, mevcut sistemler üzerinde yapılan tüm bilgi alma, değişiklik yapma ve yönetim süreçlerinin yetkili mercilerin denetimi altında gerçekleştiğine emin olmaktır (Limba vd.,

2017). Daha geniş anlamda siber güvenlik; siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak maksadıyla kullanılan araç, politika, güvenlik kavramları, risk yönetim yaklaşımları, güvenlik teminatları, faaliyetler, eğitimler, uygulamalar ve teknolojiler bütünüdür. Bu tanım, kurum ve kuruluşlara ait bilgi işlem donanımlarını, personeli, altyapıyı, uygulamaları, hizmetleri, elektronik haberleşme sistemlerini ve siber ortamda iletilen, saklanan tüm bilgileri kapsamaktadır (BTK, 2020).

Siber güvenliğinin 4 temel bileşeni bulunmaktadır, Watkins ve Wallace' e (2008) göre bunlara son 2 bileşeni de eklemek mümkündür.

- Gizlilik (Confidentially): Bilginin üçüncü şahıslar tarafından ele geçirilmesinin engellenmesi için yapılması gereken uygulamalardır.
- Bütünlük (Integrity): Bilginin aktarımı sırasında herhangi bir değişikliğe uğramasının engellenmesidir.
- Erişilebilirlik (Availability): Sistemin hizmet verememe veya kullanılamama gibi nedenlerle maddi veya manevi kayıplara neden olmayacak şekilde işletilebilmesidir.
- Doğrulama (Authentication): Kullanıcının kim olduğunun sorgulandığı, şifre ve kullanıcı ismi tanımlanması gerektiren süreçtir.
- Yetkilendirme (Authorization): Kullanıcılara, yetkilerin atanması ve hangi kullanıcının ne kadar yetkili olduğunun belirlenmesi işlemidir.
- Hesap (Account): Hangi kullanıcının ne işlem yaptığının kontrol edilebildiği unsurdur.

1.3. Siber Suç ve Siber Casusluk

Siber suç, bilişim sistemine izinsiz ve hukuka aykırı bir şekilde girilmesi ve sonrasında yapılan zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemlerdir (EGM, 2020; Wall, 2007). Siber casusluk; internet, iletişim ağları, yazılım ve/veya bilgisayarlar kullanılarak kişilerden, rakiplerden, gruplardan, hükümetlerden veya düşmanlardan hassas, gizli bilgiler gibi sırların askeri, siyasi, ekonomik avantaj sağlamak için yasa dışı yöntemler kullanılarak elde edilmesidir (Nickolov, 2020).

1.4. Siber Tehdit

Siber tehdit, siber ortamda bulunan verinin gizliliği, bütünlüğü ve erişilebilirliğine yönelik istenmeyen durumlara yol açabilme yeteneği veya siber ortamdaki güvenlik açığını kullanma potansiyeline sahip olabilmektir. Charney (2009), siber tehditlerin değerlendirilmesi ve zararlarının azaltılmasının zor bir iş olduğunu belirtmiştir ve bu durumu 6 madde ile özetlemiştir. Bunlar,

- Kötü niyetli aktörlerin çeşitliliği
- Aktörlerin amaç çeşitliliği
- Saldırı çeşitliliği sağlayan teknik imkânların fazlalığı
- Tehdidin gerçekliğinin fark edilmesinin uzun sürmesi
- Tehdidin sonuçlarının öngörülememesi
- Siber alandaki aktivitenin taşıdığı yıkıcı potansiyelin korkutucu ve iç karartıcı yapısıdır.

Yaşar ve Çakır (2015), siber güvenliğe yönelik tehditleri insan kaynaklı ve doğa kaynaklı olarak ikiye ayırmaktadır.

1. İnsan Kaynaklı Tehditler: İnsanların doğrudan veya dolaylı olarak katılımının olduğu tehditlerdir. Bilinçli tehdit oluşturacak eylemler; zararlı kod, virüs ile casusluk gibi faaliyetleri kapsamaktadır. Bilinçsiz tehdit oluşturacak eylemler ise hatalı sistem yapılandırmaları, dikkatsizlik, yazılım hataları olarak ifade edilebilir.
    - İç Tehdit: Eğitimsiz, bilinçsiz kullanıcıların farkında olmadan bir parçası oldukları tehdit türüdür. Bu tehdit türünde kullanıcı davranışları, Bilgi ve İletişim Teknolojileri (BİT) sistemlerinin normal fonksiyonlarında aksamalar veya açıklıklar oluşmasına, hatta kötü niyetlilerin bu açıklıkları kullanarak sisteme dışarıdan sızmasına neden olmaktadır.
    - Dış Tehdit: BİT sistemleri veya bu sistemler üzerinde barınan siber varlıklara karşı genellikle internet üzerinden, yetkisiz, izinsiz ve kötü niyetliler tarafından gerçekleştirilen art niyetli eylemler bütünüdür.
2. Doğa kaynaklı tehditler: Doğal afet; insan ile ilgili bir sebebe dayanmayan, doğal etkilerden kaynaklanan tehditlerdir. Örneğin elektrik kesintileri veya iklimlendirmeden kaynaklanan sistem aksaklıkları bu tür tehditlerdir.

Uluslararası Denizcilik Örgütü'ne (IMO) göre denizde siber risk; bilgi veya sistemlerin bozulması, kaybolması, tehlikeye girmesi sonucunda denizcilikle ilgili

operasyon, emniyet, güvenlik hatalarına neden olabilecek bir durum tarafından teknolojik varlığın ne ölçüde tehdit edildiği anlamındadır (IMO, 2016).

1.5. Siber Saldırı

Siber saldırı, ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemlerdir (UAB, 2016). Siber saldırılar temel olarak 4 değişik şekilde gerçekleşmektedir. Bunlar, engelleme (Interruption), dinleme (Intercept), değiştirme (Modification) ve uydurmadır (Fabrication). Allen (2001), bu aşamaları aşağıdaki gibi özetlemektedir;

- Kaynak ve hedef sistemler arasındaki bilgi akışı ve erişimin engellenmesi
- Kaynak hedef ve sistemler arasındaki iletişimin yetkisiz olarak dinlenip veri elde edilmesi
- Kaynak bilgisayardan elde edilen verinin değiştirilip yine aynı yerden geliyormuş izlenimi ile hedef sisteme yönlendirilmesi
- Sahte ve uydurma veri üretip hedef sistemlere gönderilmesi.

Siber saldırının aşamaları için kullanılan "Siber Saldırının Yaşam Döngüsü" (Cyber Kill Chain); hedefin belirlenmesi ve bilgi toplama, keşif, zafiyet taraması, açıkların istismar edilmesi, sistemin ele geçirilmesi ve kazanç, izlerin temizlenmesi aşamalarından oluşmaktadır. Bu aşamalar aşağıda belirtilen şekilde açıklanmaktadır (Garba, 2019; Haraide vd., 2018; Yiğit ve Akyıldız, 2014).

- Bilgisayar korsanının hedef hakkında açık kaynaklardan bilgi edinmeye çalışması,
- Saldırganın, kurban ve hedefin nasıl çalıştığı hakkında yeterli bilgiyi elde etmesi, elindeki bilgi ile kurbanın kullandığı internet bağlantılı cihazlarındaki açıklara erişmesi,
- Saldırganın, hedefin bilgi teknolojileri sistemlerinden doğrudan fayda sağlamayı amaçlaması veya kurbanın bilgi teknolojileri sistemlerini kaynak olarak kullanıp başka bir hedefe saldırı gerçekleştirmesi,
- Saldırganın erişim sağladığı bilgi teknolojileri sistemlerinde, erişimi kalıcı veya en uzun süreli bir şekilde devam ettirmesi,

- Siber korsanların, kurbanın bilgi teknolojileri sistemlerini ele geçirip amaçlarına yani planladıkları bilgiye veya kazanca ulaşmasında sonra sisteme erişmek için izledikleri yolu gizlemek ve bunun hedef sistemin yöneticileri tarafından tespitini imkânsız hale getirmek için izleri saklama yöntemleri kullanması.

1975'den itibaren birkaç virüs ve solucan gibi zararlı yazılım geliştirilmiştir. 1982 yılında 15 yaşındaki Rich Skrenta'nın Appel II işletim sistemi için yazdığı Elk Cloner isimli virüs ilk siber saldırı aracı olarak günümüze kadar hazırlanmış sayısı belirsiz zararlı yazılımın öncüsü kabul edilmektedir. Elk Cloner, yüklü olduğu disketin sokulduğu her bilgisayara bulaşmaktaydı. Virüs bulaşmış bilgisayara sokulan her diskete de virüs geçmekteydi. Virüs bulaşmış bilgisayar kapatılıp yeniden başlatıldığı her 50. defada bilgisayar ekranına bir şiir gelmekteydi (Sophos, 2013).

En etkili ve en bilinen siber saldırıların başında ise Stuxnet adı verilen saldırı gelmektedir. Stuxnet, Haziran 2010'da fark edilen ve İran'ın uranyum zenginleştirmek için kullandığı en önemli nükleer tesis olan Natanz'a saldırmak için geliştirilmiş olan bir siber silahtır. Natanz'daki nükleer tesiste kullanılan Denetleme Kontrol ve Veri Toplama Sistemleri (SCADA) kullanıldığı diğer tüm tesisler gibi internet ağından güvenlik gerekçeleriyle koparılmış olarak işletilmekteydi. Yani bu sisteme internet üzerinden virüs bulaştırmak mümkün değildir. Virüs bulaştırma işleminin, evrensel seri veriyolu (USB) gibi harici bir ekipmanın sisteme dahil edilerek üçüncü şahıslar tarafından gerçekleştirildiği düşünülmektedir (Langher, 2011; Lindsay, 2013).

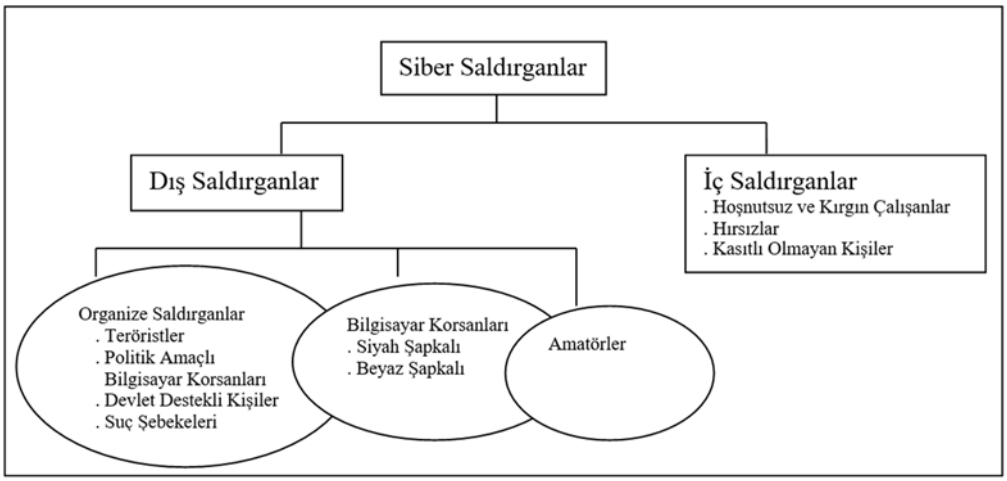
Nükleer santralde Siemens marka kontrol sistemleri kullanılmaktaydı. Stuxnet, Siemens yazılımını geçerek santrifüjlerin dönüş hızlarının belirlenmesinde kullanılan Programlanabilir Mantıksal Denetleyici (PLC) ünitelerinin yönetimini ele geçirmiştir (Lagouvardou, 2018). Görevini yapmaya başlamadan önce, SCADA ekranlarından almış olduğu 21 saniyelik santrifüjlerin normal çalışma durumuna ait ekran görüntüsünü görevini yaptığı sürece defalarca göstererek kontrol mühendislerini yanıltmayı başarmıştır. Arka planda, santrifüjlerin dönüşünü 100 milisaniye gibi olağanüstü bir zaman aralığında hızlandırıp yavaşlatarak ömürlerini azaltmıştır. Kırılan veya parçalanan santrifüjlerin yerine yenilerinin takılması gerekmiştir. 1000'e yakın santrifüjü hasara uğratmıştır ve bunlardan 600 tanesi değiştirilmiştir (Çelik, 2013). Stuxnet, bir anda tüm sistemi parçalamak, tüm santrifüjleri kırmak için değil de uzun vadede gizlice bu parçaların kullanım ömürlerini azaltmak için dizayn edilmiştir. Bu şekilde, nükleer zenginleştirme süreci tamamen sekteye

uğramasa da İran'ın uranyum zenginleştirme planlarında en azından 2 yıllık bir üretim aksaması yaşadığı düşünülmektedir (Buchan, 2012).

Mayıs 2010'da Ukrayna bilişim şirketi Virusblokada'nın Microssoft Windows işletim sistemlerinde zararlı etki gösterme olasılığı bulunan bir virüs tespit etmesi üzerine İsrail anti virüs programı yazılım şirketi Kaspersky, Amerikan yazılım şirketi Microsoft ve Amerikan bilişim güvenlik şirketi Symantec'in de dahil olduğu bir araştırma başlatılmıştır. Natanz'daki nükleer santrale yönelik ilk saldırının 22 Haziran 2009'de, ikincisinin ise 7 Temmuz 2009'da gerçekleştirildiği belirlenmiştir. Yani, saldırıların gerçekleştirilmesi ile tespit edilmesi arasında yaklaşık bir yıl zaman farkı vardır (Çelik, 2013). Ayrıca Stuxnet bulaşmış bir sistemde kullanılan her USB bellek daha sonra hangi bilgisayarda kullanılırsa Stuxnet o bilgisayara da bulaşmaktadır (Lagouvardou, 2018). Symantec'in yapmış olduğu araştırmada 155'in üzerinde ülkede 40.000'e yakın internet protokol adresinde (IP) Stuxnet virüsüne rastlanmış olup bunların %60'ı İran'da bulunmaktadır (Symantec, 2011). Önde gelen denizcilik ve petrol şirketlerinden Chevron'un da bilişim sistemlerinin Stuxnet virüsünden etkilendiği rapor edilmiştir (Kessler, 2019).

1.6. Siber Saldırganlar ve Amaçları

Han ve Dongre'a (2014) göre siber saldırıyı yapanlar, iç saldırganlar ve dış saldırganlar olarak iki gruba ayrılmaktadır. Şekil 2'de bu grupların detayları belirtilmiştir.



Şekil 2. Siber saldırgan sınıflandırması (Han ve Dongre, 2014).

Her grup, saldırganın amaçlarına göre kendi içinde aşağıda açıklandığı gibi sınıflara ayrılmaktadır (Han ve Dongre, 2014; Silgado, 2018; MDR, 2019).

1. Dış Saldırganlar

- Organize Saldırganlar: Amaçlarına göre 4 sınıfa ayrılmaktadırlar.
  - Teröristler: Siyasi bildiri yapma peşinde olan, karşıtlarında veya toplumdan korku yaymaya veya kendi politik kazançlarına göre hedeflerine psikolojik ve fiziksel zarar vermeye çalışan kişilerdir. Ekonominin veya ulusal kuruluş ve kritik yapıların bozulmasını amaçlamaktadırlar.
  - Politik Amaçlı Bilgisayar Korsanları: Temel amaçları farkındalık yaratmaktır. Korku yayarak değişim yapma peşinde olmayan, sisteme zarar vermiş olsalar da sadece siyasi bildiri amaçlı eylem yapan kimselerdir. Hassas bilgileri ifşa etmeyi ve medyanın dikkatini çekmeyi amaçlarlar. Temel ilgi alanları petrol ve gaz endüstrisi başta olmak üzere endüstrinin yarattığı çevre kirliliği ayrıca balina avcılığı gibi hassas konulardır.
  - Devlet Destekli Kişiler: Hükümetler adına bilgi toplayan veya sabotaj yapan iyi eğitimli, iyi finanse edilen, sıkı organize olmuş, azımsanmayacak derecede bilimsel destek alan kişilerdir. Bilgiyi zarar uğratmayı, ticari bilgiler dahil hassas bilgileri, savunma planlarını, kişisel verileri, fikri hakları çalmayı ve kendi çıkarları veya hükümetler için kullanmayı amaçlamaktadırlar.
  - Suç Şebekeleri: Genelde kontrol, güç veya para peşinde olan profesyonel organize suç gruplarıdır. Bilgi avantajı sağlamayı, kaçakçılık yapmayı buna bağlı olarak konteyner bilgilerine ulaşmayı, yük işletim sistemi bilgelerine ulaşmayı, Küresel Konum Belirleme Sistemi'nden (GPS) hedefleri için bilgiye ulaşmayı, bilgi ve ağı zayıflatmayı, sahte yük transferi yapmayı ve fidye almayı amaçlarlar.
- Bilgisayar Korsanları: Amaçlarına göre 2 sınıfa ayrılmaktadırlar.
  - Beyaz Şapkalı Bilgisayar Korsanları (White Hat Hacker): Bilgisayar sahibinin onayı ve bilgisi dahilinde bilgisayar sistemindeki zayıflıkları tespit etmek veya sistemi geliştirmek için bilgisayara giren kişidir.
  - Siyah Şapkalı Bilgisayar Korsanları (Black Hat Hacker): Meydan okuma veya kendi camialarında nam salmak amacıyla yasa dışı şekilde ve hedef sisteme zarar vermek için bilgisayara giren kişidir. Bilgi çalmayı, çaldıkları bilgiyi satmayı, çaldıkları bilgi için fidye istemeyi, zarar verdikleri sistemi

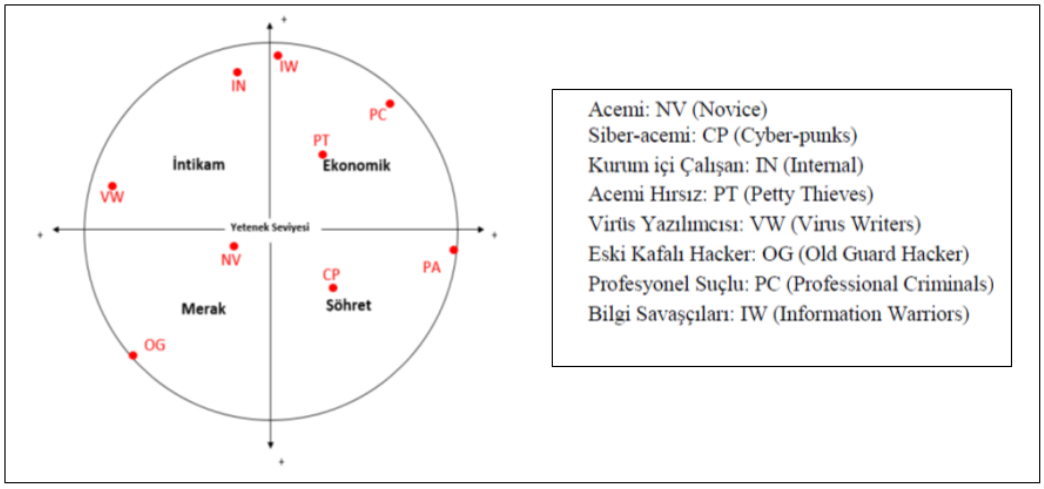
tekrar çalışır duruma getirmek için fidye istemeyi, bilgi avantajı sağlamayı amaçlamaktadırlar.

- Amatörler: Az yetenekli kişilerdir. Bunlar genelde bilgisayar korsanı olmayıp internette tehlikeli işler yapan anlamında "script kiddies" veya çaylak olarak adlandırılır. Bazıları eğlence için bazıları ise bir bilgisayar korsanı grubuna girebilmek adına yeteneklerini sergilemek için bu faaliyetleri yapmaktadırlar.

2. İç Saldırganlar

- Hoşnutsuz ve Kırgın Çalışanlar: Kurum içinde çalışıyor olan veya kısa zaman içinde işine son verilmiş çalışanlar misilleme saldırıları düzenleyebilmekte veya dahili sistemlerin emniyetini tehdit edebilmektedir.
- Hırsızlar: Finansal olarak desteklenen kişilerdir. Kişisel kazançları için sistemleri kendi çıkarlarına kullanıp şirket varlıklarını istismar edebilmektedirler.
- Kasıtlı Olmayan Kişiler: İstemeden dış saldırılara olanak tanıyan fakat doğrudan saldırı yapmayan kişilerdir.

Şekil 3'de siber saldırgan profilinin 2 boyutlu çember modeli verilmiştir. Bu modele göre, merkezden uzağa gidildikçe saldırganın, ilgili çeyrek dairede belirtilen amacına dair kabiliyeti artmaktadır (Irmak ve Erkek, 2016).



Şekil 3. Siber saldırgan profilinin 2 boyutlu çember modeli (Irmak ve Erkek, 2016).

Amaçları bilinen bazı siber saldırıların sonuçları aşağıda belirtilmiştir,

- 2011 yılında Birleşik Krallık'ta fikri mülkiyet hırsızlığı 9,2 milyar pound ile en pahalı siber suç olmuştur. Aynı yıl Birleşik Krallık'ta sanayi casusluğundan kaynaklı zarar 7,6 milyar pounddur. 2012 yılında İngiliz İç İstihbarat Teşkilatı (MI5) başkanının, önde gelen petrol şirketi yöneticilerine vermiş olduğu bilgide, heklenme sonucu petrol sahaları ve keşif bilgilerinin çalınması nedeni ile her yıl milyarlarca dolar kayba uğranmaktadır (Becrypt, 2020).
- 2014 yılında yapılan Information Security Breaches araştırmasında Birleşik Krallık'taki büyük şirketlerin %81'i maliyeti 600.000 ile 1,5 milyon pound arasında değişen siber saldırılara uğradığı belirtilmektedir (GCHQ, 2015).
- Juniper tarafından 2015 yılında yapılan bir araştırmada 2019 yılı itibariyle siber saldırıların dünya genelindeki maliyetinin 2015 yılındaki maliyetin 4 katına çıkarak 2,1 trilyon dolara ulaşacağı belirtilmektedir (Silgado, 2018).
- 2015 yılında, ABD Personel Yönetim Ofisi'nden 21 milyon kayıt, Athem şirketinden 70 milyon sağlık bilgisi kaydı, Ashley Madison şirketinden kişilerin eşlerini aldattıklarına dair 37 milyon kayıt dahil yaklaşık 150 milyon kayıt çalınmıştır (Global Security, 2015).
- 2016 yılında Hindistan Donanması için denizaltı inşa etmekte olan Fransız DCNS firması siber saldırıya uğramıştır ve denizaltı savaş sistemleri evraklarını da içeren 22.000 evrak çalınmıştır (Broadhurst, 2017).
- 2016 yılında ABD Donanması sistemleri heklenmiş ve 134.000 donanma personelinin kişisel bilgileri ifşa edilmiştir (Broadhurst, 2017).
- 2016 yılında Avrupa'nın en büyük elektrik kablosu üreticisi olan Leoni AG'nin muhasebe sorumlusu siber saldırganlar tarafından kandırılmış ve şirket 34 milyon pound kayba uğramıştır (Rider, 2018).
- 2015 yılında İzlandalı bir balıkçılık şirketinin web sitesine, şirketin balina avcılığı yapıyor olması nedeniyle siber saldırı yapılmıştır. Yine 2015 yılında bir İtalyan şirkete, ahlak dışı hükümet yönetimlerini destekliyor olma iddiası ile protesto amaçlı siber saldırı yapılmıştır. Şirketin birçok hassas bilgisi ifşa edilmiş ve şirket önemli derecede itibar kaybına uğramıştır. 2016 yılında Nissan, bir Japon şirketi olması ve Japonların Antartika'da balina avcılığı yapıyor olması sebebiyle siber saldırıya uğramıştır. 2018 yılında bazı İtalyan kuruluşlar çevre kirliliğine ve

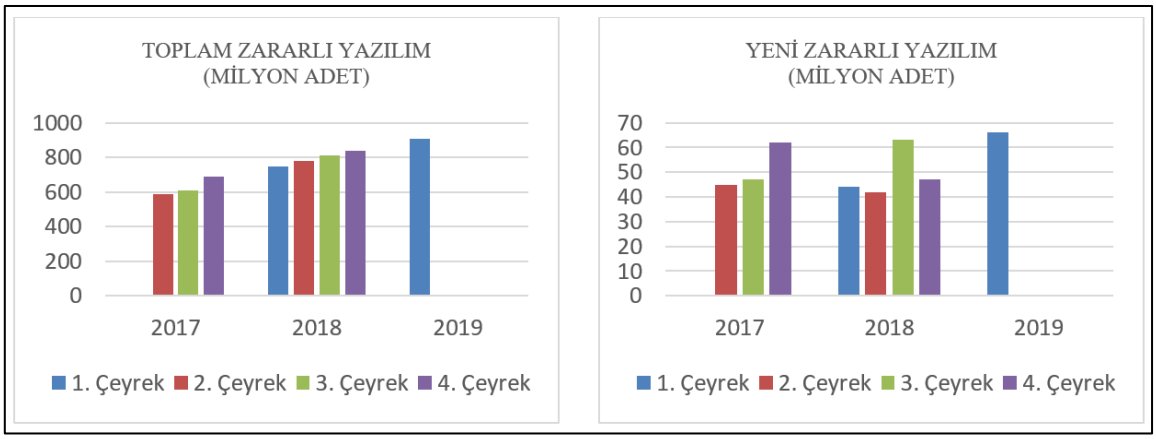
küresel ısınmaya sebep oldukları gerekçesiyle siber saldırıya uğramıştır (MDR, 2019).

Siber saldırganların faaliyetlerinin saldırıya uğrayan kurban üzerindeki sonuçları da önemli bir konudur. Siber saldırıya uğradıktan sonra dışarıdan araştırma ve inceleme için teknik yardım alınması gerektiği durumda güvenlik danışmanları ile saldırılan sistemlerin ve verilerin tamir edilmesi, yenilenmesi için ücret ödenmesi gerekmektedir. Saldırı süresince ticari ve operasyonel faaliyetlerin yavaşlaması veya askıya alınması nedeniyle gelirlerde azalma veya tamamen durma yaşanmaktadır. Saldırının çalışanlar üzerinde etkileri dikkat dağılması şeklinde görülebilmektedir, bu da faaliyetlerde yavaşlama ve yine gelirlerde azalma anlamına gelmektedir. Hukuki konular ve gerekiyorsa tazminat ödeme işlemleri zaman kaybı yaratacaktır ve ilave maliyet getirecektir. Şirketler açısından en önemli sonuç ise itibarlarının zarar gördüğü, kötü yönde reklamlarının yapıldığı, şirkete karşı güven kaybı yaşanacağı ve siber saldırıya bağlı olarak gelecekteki karın ve olanakların azalacağı düşüncesidir (Brasington ve Park, 2016; Justers, 2020).

Denizcilik sektörü ve gemi özelinde yukarıda belirtilen ekonomik sonuçların yanında daha geniş anlamda sorunlar da söz konusudur. GPS, ECDIS, AIS gibi gemi sitemlerine yönelik sinyal karıştırma veya yanıltma yöntemleri ile siber saldırılar gerçekleştirilebilir. Ayrıca bilgisayar tabanlı gemi sitemlerini doğrudan kontrol altına alabilmek için internet üzerinden veya harici bellek ile zararlı yazılımlar kullanma yöntemi ile de siber saldırılar yapılabilir. Gemilere yönelik tüm bu siber saldırılar, çatışma veya yangın gibi emniyet riskleri oluşturabileceği gibi çevre kirliliği gibi daha üst seviye sorunlara da yol açabilir (Silgado, 2018).

1.7. Siber Saldırı Yöntemleri

Canbek (2005), kötü niyetli olarak nitelendirilen siber korsanların; var olan bilgi ve bilgisayar güvenliği sistemini aşmak, zafiyete uğratmak, kişileri zarara uğratmak, sistemlerin işleyişini aksattırmak, durdurmak gibi kötü amaçlarla siber saldırılar yaptıklarını belirtmiştir. McAfee Labs Tehdit Raporu Ağustos 2019'a göre zararlı yazılım sayılarına ait grafikler Şekil 4'de verilmiştir (McAfee, 2019).



Şekil 4. Zararlı yazılım sayıları (McAfee, 2019).

Saldırganlar amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi bilgi güvenliği için büyük bir önem arz etmektedir (Canbek ve Sağıroğlu, 2007). Saldırı yöntemlerinden en bilinenleri ve en tehlikeli olanları aşağıda detaylı açıklanmış, diğer yöntemler ise sadece listelenerek belirtilmiştir.

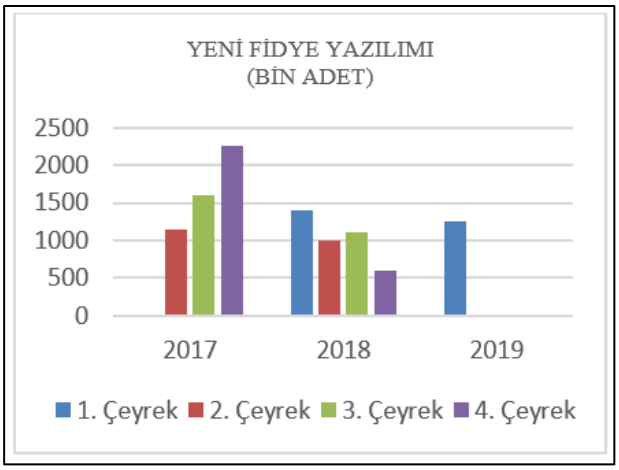
1) Virüs: Bilgisayar yazılım dilleri kullanılarak hazırlanan virüsler aslında birer bilgisayar uygulaması veya programıdır. Virüsler, bilgisayarda yüklü bulunan programlara yerleşirler, bilinen faydalı programların aksine amaçları bulaştıkları bilgisayarın çalışmasını olumsuz yönde etkilemektir. Bilgisayar virüsleri kendilerini gizlemeyi ve daha fazla kaynağa yerleşmeyi amaç edinmişlerdir (Krutz ve Vines, 2007). Virüsler, saldırı amacıyla kullanılmaya başladıkları 1980'li yıllardan itibaren hızlı bir gelişim göstermiştir. Her geçen gün virüsler bulaştıkları programlarda kendilerini daha iyi gizleyebilmekte ve daha da zararlı olabilmektedir. Buna karşılık kullanıcılar sistemlerindeki virüs tehdidini tespit amaçlı anti virüs programları kullanmaktadırlar (Sağıroğlu vd., 2018; Nachenberg, 1997). Federal Soruşturma Bürosu (FBI) verilerine göre 2003 yılında Amerika Birleşik Devletleri'ndeki (ABD) işletmelerin %82'si virüs saldırısına uğramıştır ve bu eylemler 200 milyar dolarlık bir kayba neden olmuştur (Shah, 2004).

2) Solucan (Worm): Bilişim sistemi ağları arasında bağımsız olarak dolaşan, kendi kendini kopyalayabilen ve kendini aktif hale getirebilen, herhangi bir donanım ve yazılıma zarar verme zorunluluğu olmayan yazılımlardır. Solucanlar, güvenlik açığını buldukları herhangi bir bilgisayara yerleşir ve daha sonra kendini defalarca kopyalayarak aynı ağa tanımlı tüm bilgisayarlara yayılır (Guinchard, 2011). Virüslerin aksine çoğalmaları için

başka programlara ihtiyaç duymazlar. Solucanlar genelde sistemlerde arka kapı açarak bu sistemleri başka saldırılarda kullanırlar. Son dönemlerde virüs-solucan karışımı programlar da görülmeye başlanmıştır (Sağıroğlu vd., 2018).

3) Truva Atı (Trojen Horse): Truva atı, yararlı gibi görünen fakat bulundurduğu gizli kod nedeniyle bilişim sistemine zarar veren bir yazılımdır. Truva atları bilgisayarı arkadan yönetmek için arka kapı açan yazılımlar olup kendi başlarına herhangi bir işlem yapamazlar ve bilgisayar sahibi tarafından çalıştırılmaları gerekmektedir (Turhan, 2010). Truva atları yararlı bir programla sisteme girer, bunun en yaygın şekli e posta ve onun ekleri ile bulaşmasıdır (Dashora, 2011).

4) Fidye Yazılım (Ransomware): Fidye yazılımları ile bilginin erişilebilirliğini engellenip, bilgi sahibinin bu erişimi tekrar sağlayabilmesi karşılığı ödeme talebinde bulunulmaktadır. Zararlı yazılım içeren internet sitelerine girilmesi veya e posta eklerinden bulaşabilmektedir. Fidye yazılımları; bilgi iletişim teknolojisi kullanıcısının cihaz veya bilgisayarındaki bilgileri şifreleyerek kullanılamaz hale getirirler. Şifrelenmiş bilginin geri dönüşü, uygun parolanın girilmesi gibi deşifre ile mümkün olduğundan, bu şifre saldırganlar tarafından yüksek paralar karşılığında kurbana iletilmektedir. Fakat fidyenin ödenmesi sistem verilerine yeniden erişimi de garanti etmemektedir. Ödemeler genelde Bitcoin cinsinden yapılmaktadır, bu da saldırganların kimliğinin ve yerinin tespitini zorlaştırmaktadır (Sağıroğlu vd., 2018). Birleşmiş Milletler Uyuşturucu ve Suç Ofisi, Dünya Bankası ve Interpol'ün yayımladığı bir raporda, 2005 ile 2012 yılları arasında Somali açıklarında yapılan korsanlık faaliyetleri sonucu korsanların 300 ile 400 milyon dolar arası fidye elde ettiği belirtilmektedir. Kaçırılan 179 gemiden 152 tanesi fidye ödemiştir. %85'lik bu oranın korsanlar adına gayet başarılı olduğu belirtilmiştir. Bu yüzdenin yüksek olması suç unsurlarının karına olacak şekilde fidye ödemesi konusunda mağdurların ne derece istekli ve seçeneksiz olduklarının bir göstergesidir. Bu verilere bağlı olarak, siber güvenlik konusunda fidye yazılımlara dikkat edilmesi gerektiği vurgulanmıştır (CyberKeel, 2014). McAfee Labs Tehdit Raporu Ağustos 2019'a göre yeni fidye yazılımı sayılarına ait grafikler Şekil 5'de verilmiştir (McAfee, 2019).



Şekil 5. Yeni fidye yazılımı sayıları (McAfee, 2019).

5) Oltalama (Phishing): Bilişim sistemleri kullanıcılarının, kandırılmaları veya ikna edilmeleri neticesinde kişisel bilgilerinin alınması ve kişilerin bilgisayar sitemlerine gönderilen virüsler aracılığıyla sistemin ele geçirilmesi girişimidir. Bu durumda elde edilen bilgiler dolandırıcılık faaliyetlerinde kullanılabileceği gibi sisteme zarar vermek maksadıyla da kullanılmaktadır (Patel and Zaveri 2010). Oltalama saldırılarında genelde kurbana sahte bağlantı (link) içeren elektronik posta gönderme yöntemi kullanılır. Gelen bu e posta banka, resmi kurum ve benzeri yerlerden gelmiş gibi gözükmektedir. Linke tıklanması durumunda tüm kişisel ve diğer önemli bilgiler saldırgan tarafından ele geçirilmektedir (Pajunen, 2017).

Gartner Group'un 2004 yılında yaptığı bir çalışmada, sadece ABD'de oltalama e posta saldırılarının her yıl 2,4 milyar dolar zarara yol açtığı ve yetişkin internet kullanıcılarının yaklaşık %5'inin başarılı bir oltalama saldırısına maruz kaldığı belirtilmiştir (Jakobsson ve Ratkiewicz, 2006). Dünya genelinde 7 gün 24 saat, basit yazılımlar tarafından rastgele oluşturulan 156 milyondan fazla oltalama e postası gönderilmektedir. Bu e postalardan 16 milyon tanesi şirketlerin güvenlik sistemlerinden geçmekte, 8 milyon tanesi ise açılıp okunmaktadır (Belmont ve Caponi, 2014). Mailfronter'ın Mart 2005'de yaptığı bir çalışmaya göre, insanların kendilerine gelen e postanın oltalama e posta olduğunun farkına varma oranı %83 iken, normal bir e posta olduğunun farkına varma oranı ise %52'dir (Jakobsson ve Ratkiewicz, 2006).

6) Hizmet Dışı Bırakma (DoS), Dağınık Hizmet Dışı Bırakma (DDoS): Hizmet aksattırma saldırıları, yetkisiz erişim veya sistem kontrolünü ele geçirmeye yarayan saldırılardan farklı bir amaç için gerçekleştirilen saldırılardır. Bu saldırının amacı;

bilgisayarı, sunucuyu veya ağı kaldırabileceğinden daha fazla yüke maruz bırakarak sistemi kullanılmaz hale getirmektir. Bu tip saldırılar genelde bant genişliği, boş disk alanı veya Merkezi İşlem Birimi (CPU) zamanı gibi bilgi işlem kaynaklarının tüketilmesi; yönlendirme (routing) bilgileri gibi yapılandırma bilgilerinin bozulması ve fiziksel ağ bileşenlerinin bozulması şeklinde yapılmaktadır. Ağ üzerinde kilit önem taşıyan bir sunucuya yapılan bu tip bir saldırı, tüm ağın işlemez hale gelmesine yol açabilmektedir. Bu saldırıları önlemek için tüm ağın analizi gerektiğinden, saldırıların önüne geçilmesi çok zordur. DDoS saldırıları, tek bir kaynaktan değil de birden fazla ele geçirilmiş konak bilgisayardan, tek bir hedefe doğru yapılan hizmet aksattırma saldırısıdır (Canbek ve Sağıroğlu, 2007).

7) Gelişmiş Sürekli Tehdit (APT): İleri düzey, özel ve kapsamlı saldırıları içerisinde barındıran bir saldırıya verilen isimdir. Geliştirilmeleri, bulaştırılması ve operasyonel olarak kullanımı, çok amaçlı kullanım için değil belirli bir hedefe yöneliktir. Bu saldırı türü; içerisinde sıfır gün saldırıları bulunan, işletim sistemi ve mimarilerinin zafiyetlerini kullanan, sinsice saklanan ve geleneksel metotlar ile bulunamayan, içerisinde casus yazılımlar olabilen, anti viral yazılımların tespit etmesinin mümkün olmadığı, ileri düzey teknik ve teknolojileri kapsayan, ileri düzey uzman olmayan kişilerin fark etmesinin mümkün olmadığı, son dönemde yapay zeka yaklaşımlarını da içinde barındıran kapsamlı saldırılardır. Saldırganların bir ağa sızıp, bu ağ üzerinde fark edilmeden uzun süre boyunca kritik verileri ele geçirmesi olarak tanımlanır. Ağa doğrudan zarar vermek yerine ağdaki güvenlik, üretim ve finansal bilgilerini ele geçiren saldırganlar, elde ettikleri verileri daha büyük terörizm amaçları için kullanılabilir (Sağıroğlu vd., 2018; Chen vd., 2018).

8) Arka Kapılar (BackDoor): Bilgisayar üzerinde sıradan incelemeler ile bulunamayacak bir metottur. Normal kimlik kanıtlama süreçlerini atlatıp ve saldırganın konu bilgisayara uzaktan erişimini sağlayan yöntemler arka kapı olarak adlandırılmaktadır. Arka kapı, kurulu bir program şeklinde olabileceği gibi var olan meşru bir programın içinde, o programı yazan kişi tarafından belgelendirilmemiş bir biçimde kasten bırakılmış da olabilir. Bu tür saldırılarda özellikle Truva atı programları yoğun bir şekilde kullanılmaktadır (Canbek ve Sağıroğlu, 2007).

9) Kök Kullanıcı Takımı (Rootkit): En tehlikeli grup olarak nitelendirilen kök kullanıcı takımları bulundukları sistemde kendilerini çok iyi gizleyen programlardır. Kök kullanıcı takımları kendilerini işletim sisteminin derinliklerine saklarlar ve tespit edilebilmeleri güçtür. Bu saldırıda, sistem dosyalarının değiştirilmesi amaçlanmaktadır. Kök kullanıcı takımları, genellikle sistemde bulunan çekirdek (kernel) açıkları kullanılarak, kök yetkisinin

kazanılması sonucu bulaşmaktadırlar. Anti-virüs yazılımları kök kullanıcı takımlarını tespit etmekte zorlanmaktadır. Tespit edilse dahi sistemden temizlemek güç olduğundan anti-virüs yazılımlarına ek olarak bir takım güvenlik yazılımları kullanılmalıdır. Bu doğrultuda, sadece kök kullanıcı takımlara yönelik geliştirmiş bazı anti-virüs programları mevcuttur (Can ve Akbaş, 2014).

10) Haberleşme Bandının Karıştırılması (Jamming): Kablosuz ağ ile haberleşen tüm sistemler için en tehlikeli saldırı türüdür. Yeteri kadar güce sahip bir karıştırıcı ile haberleşme bandı bastırılmaya, dolayısıyla cihazlar arasındaki haberleşme engellenmeye çalışılmaktadır. Karıştırıcının gücüne bağlı olarak ağın bir kısmı hedef alınabileceği gibi tüm ağ da hedef olarak seçilebilir. Karıştırma işlemi kesintisiz olarak yapılabileceği gibi ara ara karıştırma işlemini durdurarak da gerçekleştirilebilir (Özçelik, 2017).

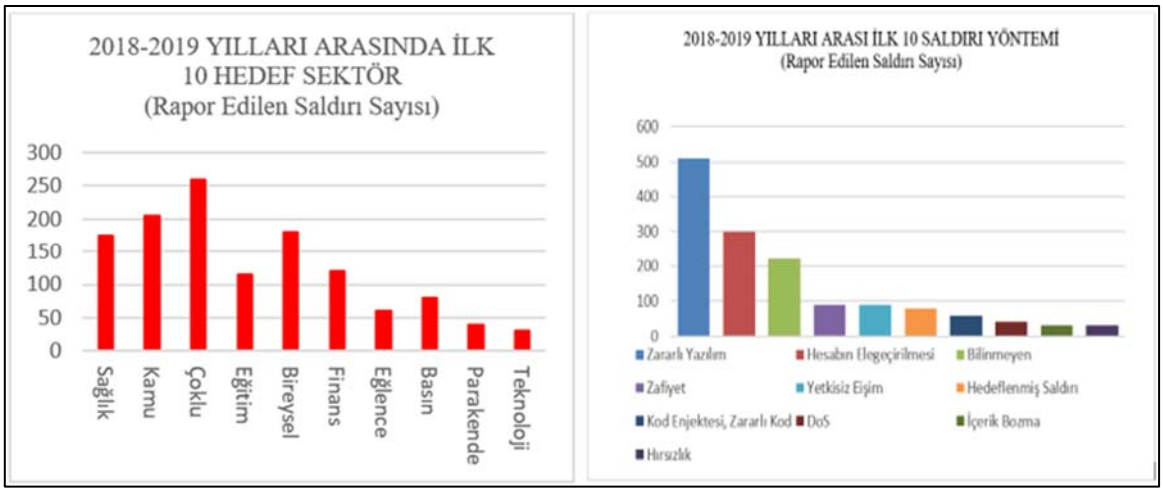
11) Sinyal Aldatma (Spoofing): Sinyal aldatma saldırısının amacı alıcı istasyona yanlış sinyal göndermek ve alıcının yanlış sinyal ile mevki veya zaman hesaplaması yapması için aldatılmasıdır. GPS P kodlu sinyaller üst düzeyde şifrelendiği için aldatma sinyallerinden etkilenmeleri çok zordur. Fakat sivil kullanıma açık olan C/A kodlu sinyaller; sinyal yapıları, yayılım spektrum kodları ve modülasyon metotlarının halka açık olması itibariyle aldatma saldırılarına karşı daha zayıftır. Alıcı istasyona gelen sinyallerin kesildiği engelleme veya karıştırma saldırılarının aksine gizlice yapılan aldatma saldırısı GPS cihazı tarafından doğrudan ayırt edilemez. Bu nedenle alıcıya yerleştirilecek sinyal aldatma tanımlayıcı gibi bir ekipmanla bu tür saldırılar tespit edilebilir (Wen vd., 2005; Shin vd., 2010).

12) Diğer Saldırı Yöntemleri (Aslay, 2017; Sağıroğlu vd., 2018; Saeed vd., 2013; Uma ve Padmavathi, 2013).

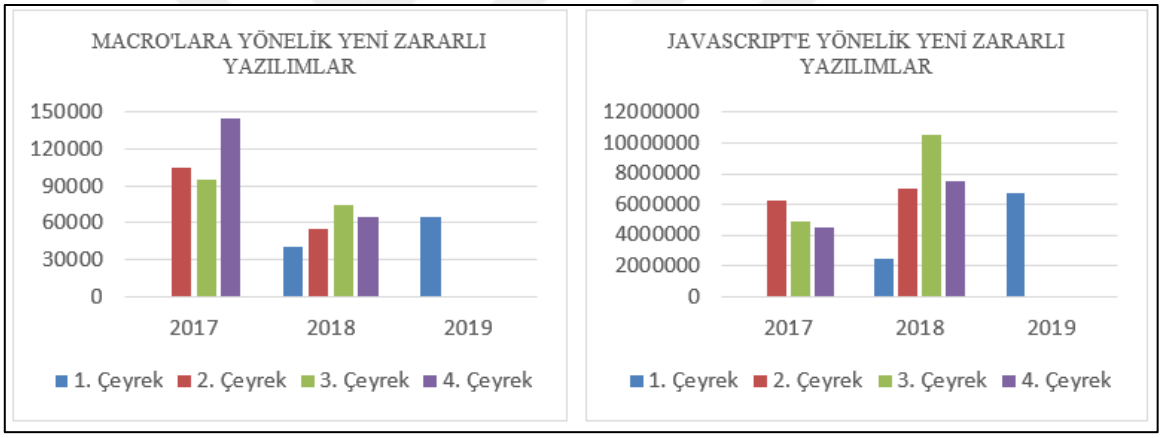
- Casus Yazılım (Spyware)
- Sosyal Mühendislik (Social Engineering)
- Su Kaynağı Saldırısı (Water Holing)
- Port Taraması (Port Scanning)
- Kaba Kuvvet Saldırısı (Brute Force)
- Hedef Odaklı Kimlik Avı (Spear-Phishing)
- Tedarik Zinciri Saldırısı (Supply Chain Attack)
- Ortadaki Adam Saldırısı (Man in the Middle Attack)
- IP Aldatması (IP Spoofing)
- ARP Zehirlenmesi (ARP Poisoning)
- Ağ Dinleme (Network Sniffing)

- İstenmeyen e-posta (Spam e-mail)
- Botnet / Zombi Bilgisayar
- İstem Dışı Ticari Reklam ve Tanıtım Yazılımları (Adware)
- Klavye İzleme Yazılımları (Key Logger)
- Yerine Geçme (Masquerading)
- Mantık Bombası (Logic Bomb)
- Bizans Saldırıları (Byzantine Attacks)
- Bilgi ve Veri Aldatmacası (Data Diddling)
- Salam Tekniği (Salami Techniques)
- Süper Darbe (Super Zapping)

McAfee Labs Tehdit Raporu Ağustos 2019'a göre siber saldırılara hedef olan ilk 10 sektör ve tercih edilen ilk 10 saldırı yöntemi grafikleri Şekil 6'da verilmiştir (McAfee, 2019). Bu saldırı yöntemleri dışında makrolar ve JavaScript konuları da önem arz etmektedir. 1990'ların sonunda Microsoft Office programı içerisine makrolar eklenmiştir ve 1999'da Melissa solucanı ile makrolar en büyük siber zafiyet haline gelmiştir. Virüslü makro kodu içeren Dridex trojeni Microsoft Word dokümanlarını etkilemekte ve sonrasında sisteme zararlı yazılım indirmektedir. Web içeriklerinde çoklukla kullanılmakta olan JavaScript; kullanıcıların internet tarayıcısını zararlı bir web sitesine yönlendirmekte, böylelikle sisteme virüs bulaştırmak için araç olarak kullanılmaktadır. Yaygın olarak kullanılan bu özellikler siber güvenlik konusunun sadece IT departmanını ilgilendiren bir konu olmadığını, her bilgisayar kullanıcısının bu konuya hassasiyet göstermesi gerektiğini açıklamaktadır (GCHQ, 2015). McAfee Labs Tehdit Raporu Ağustos 2019'a göre Macro'lara ve JavaScript'e yönelik yeni zararlı yazılım sayıları grafikleri Şekil 7'de verilmiştir (McAfee, 2019).



Şekil 6. İlk 10 hedef sektör ve ilk 10 saldırı yöntemi (McAfee, 2019).



Şekil 7. Macro ve JavaScript'e yönelik yeni zararlı yazılım sayıları (McAfee, 2019).

2013 yılında yayınlanan Mandiant raporuna göre, siber saldırganlar tespit edildikleri andan ortalama 243 gün önce sisteme girmiş bulunmaktadır. Saldırıların %63'ü üçüncü kişiler tarafından rapor edilmiştir ve saldırıların hepsi kişilere ait herhangi bir bilginin çalınması ile sonuçlanmıştır. 2013 Verizon Veri İhlal Araştırmaları Raporu'na (DBIR) göre ise, meydana gelen 47.000 saldırıdan %69'u üçüncü kişiler tarafından rapor edilmiştir. Saldırıların %29'unda sosyal mühendislik kullanılmıştır, %76'sında kimlik bilgileri çalınmıştır, %70'den fazlası son 30 gün içerisinde işten çıkarılmış olan eski çalışanların IP hırsızlığı sonucu meydana gelmiştir (Skrlec vd., 2014). Temmuz 2016'da IHS Markit ve BIMCO tarafından 300 şirketin katılımıyla yapılan anketin sonuçlarına göre, katılımcıların

%25'inin kimlik bilgileri çalınmış, %77'si virüs, %57'si oltalama, %23'ü hedef odaklı kimlik avı, %18'i ise DoS saldırısına maruz kalmıştır (Lee vd., 2017). Allianz tarafından her yıl yapılan ve sekizincisi 2019 yılında denizciliği de içeren 22 sektörü kapsayan 86 ülkeden 2.400 risk yöneticisi uzman ile Risk Barometer Raporu hazırlanmıştır. Rapora göre, %37 ile listenin birinci sırasında yer alan siber saldırılar ilk defa dünya genelindeki tüm şirketler için birinci risk unsuru olarak değerlendirilmiştir. 2018 yılında hazırlanan raporda ise siber saldırılar ilk beş tehdit arasında bulunmaktadır (Allianz, 2019).

1.8. Denizcilik Sektöründe Siber Güvenlik Farkındalığı

Mileski vd. (2018), denizcilik endüstrisinde kullanılan demirden yapılmış mekanik ekipmanların karşılaşabileceği en önemli tehlike paslanmaymış gibi görünse de denizciliğin, dijital ve internet teknolojilerinden kaynaklı tehlikelerden de uzak olmadığını belirtmiştir. Araştırmalar, denizciliğin geleneksel olarak değişikliklere en yavaş uyum sağlayan endüstri kolu olduğunu, denizcilik sektöründeki siber güvenlik farkındalığının diğer taşımacılık sektörlerine göre daha az olduğunu ortaya koymaktadır. Ayrıca, gemilerdeki ve liman kritik altyapılarındaki haberleşme, seyir ve operasyonel bileşenlerin iyileştirme konusunun diğer endüstri kollarına göre çok yavaş ilerlediği belirtilmektedir (Shaw ve Ayerst, 2017).

Thompson'a (2019) göre; konvansiyonel insanlı gemiler, çalışan insan sayısı azaltılmış teknolojik gemiler ve insansız otonom gemiler kısa zaman içerisinde aynı sularda bulunacaktır. Bu teknolojik çeşitlilik ile büyük veri (big data), yeni sensörler ve bilgi analitiğinin emniyetli seyir koşullarını ne ölçüde destekleyeceği önümüzdeki yirmi veya otuz yılın anahtar konusu olacaktır. Bununla ilişkili olarak çözüm bulunması ve yeni kuralların ortaya konulması gereken konulardan biri de siber güvenliktir.

Gemilere yönelik siber tehditler matematiksel olarak kağıt üzerinde, deneysel olarak veya laboratuvar ortamında ispatlanmıştır. Yaşanan birçok rapor edilmiş siber olay veya resmi olarak rapor edilmemiş siber olaylardan çıkarılan dersler sonucunda siber güvenlik konusunda teknik çözümler geliştirilmektedir. Otonom gemiler, gemiadamı yani insan faktörünü denklemden çıkararak teoride denizciliği siber güvenlik de dahil daha güvenli hale getirme düşüncesine dayanmaktadır. Teknik çözümler ve otonom gemiler ile siber güvenlik ve siber emniyet kalitesi arttırılarak siber güvenlik konusundaki ihtiyaçlar gelecek için karşılanabilecektir (Muccin, 2016). Fakat günümüzde insan faktörünün halen gemi denklemi içinde yer alıyor olduğu bir gerçektir. Gemilerde meydana gelen kazaların %80'e yakınının

insan hatasından kaynaklandığı bilinmektedir. Siber saldırıların %99'u bilinmekte olan zafiyetlerden kaynaklanmaktadır ve bunlarında yaklaşık %90'ı için hazırda yazılım güncellemeleri mevcuttur (Global Security, 2015).

Plymouth Üniversitesi'nde denizcilik sektöründeki siber güvenlik gereksinimlerine çözüm sunmak için kurulan Cyber-MAR ve Cyber-SHIP Lab'da etkin görevlerde bulunan Kevin Jones, denizcilik sektörünün gün geçtikçe daha da dijitalleşmesine rağmen siber tehditlere karşı hiç de korunaklı durumda olmadığını belirtmiştir. Gemi tipi, büyüklüğü ve yaşı çeşitliliğinin yanında kullanılmakta olan ekipman çeşitliliğinin de gemiden gemiye değişiklik gösteriyor olmasının siber güvenlik gereksinimlerinin anlaşılmasını zorlaştırdığını savunmaktadır (Tam vd., 2019).

Hayes'e (2016) göre, teknoloji denizcinin en iyi arkadaşı fakat en kötü düşmanıdır. Denizcilik endüstrisinin siber güvenlik konusunda başarılı olabilmesi için endüstrinin ileri düşünceli davranıp standartlaşmış plan ve prosedürler geliştirmesi, aksaklıklara dayanıklı hale gelmesi gerekmektedir. Günümüzde denizcilik sektörünün siber güvenlik konusunda korunmasız olmasının başlıca sebebi siber güvenlik gibi bir tehlikenin görmezden geliniyor olmasıdır. Önde gelen denizcilik şirketlerinden Stena AB'de Baş Bilgi Güvenliği Yöneticisi (CISO) olarak görev yapan Magnus Carling'e göre, Titanik gemisinin kaptanının buzdağının yaklaşıyor olduğuna dair çevredeki gemilerden gelen bilgileri göz ardı ettiği gibi bazı sistem yöneticileri, şirketlerinin siber saldırıya uğrayabileceğini bazen görmezden gelmekte bazen de buna dair belirtileri yanlış değerlendirmektedir. Birçok insan siber güvenliğin IT departmanının sorumluluğunda olduğunu ve bunun dışında kendilerinin konu hakkında yapabilecekleri bir şeyleri olmadığı sonucuna varmaktadır. Bu düşünce tarzının siber güvenlik konusunda doğrudan fakat negatif yönlü bir etkisi bulunmaktadır (CyberKeel, 2014).

Cyberkeel, 2014 yılında küresel konteyner gemisi filosunun %94'ünü elinde bulunduran en büyük 50 konteyner gemisi şirketi arasında siber zafiyet araştırması yapmıştır. Çalışmada, SHODAN testi kullanılarak sistemlerin Yapılandırılmış Sorgu Dili (SQL) saldırılarına karşı zafiyeti ve bilgisayarlarda kullanılan sistemlerin versiyonlarının bilinen zafiyetler içerip içermediği araştırılmıştır. Sonuçta, şirketlerin %37'sinin sistemlerinde zafiyet tespit edilmiştir. 6 tanesinin sistemlerindeki kullanıcı isimlerinin rahatlıkla elde edilebilir durumda olduğu anlaşılmıştır. Dünya genelinde konteyner taşımacılığının %38'ini kontrol eden 8 taşıyıcı firmada kullanılan e ticaret uygulamaları için parola olarak "password" kelimesi kullanılmakta olduğu, 2 firmada parola olarak "X" harfi

kullanılmakta olduğu, en üst 20 taşıyıcı firmanın sistemlerinde alan adı dolandırıcılığı mevcut olduğu tespit edilmiştir (Jensen, 2015; Jensen 2015b).

JWC'nin CSO Alliance ve Conventry Üniversitesi ile yaptığı, 12 ay süren "Cyber Security, The Unknown Threat At Sea" isimli çalışmada, katılımcıların %50'sinden fazlası siber güvenlik ya da siber emniyet konusuna inanmamaktadır ve bunun IT departmanı ile ilgili olduğunu düşünmektedir (Wylie, 2017). Aynı çalışmada, şirket güvenlik zabitlerinin (CSO) %67'sinin siber tehditlerin ciddi bir sorun olmadığını düşündüğü, bilişim kurulu başkanlarının (CIO) %100'ünün gemiadamları için herhangi siber güvenlik eğitimi düzenlememekte olduğu, gemi güvenlik zabitlerinin (SSO) %91'inin verdikleri eğitimlerde siber güvenlik konusuna değinmiyor olduğu, denizcilik sektöründeki siber olayların %80 oranında insan hatası kaynaklı olduğu sonuçları çıkmıştır. Siber tehditlerle mücadele için bilgi ve yeterliliğin gerektiği vurgulanmıştır (SMI, 2017).

Güncellenmemiş veya güncellemesi artık yayınlanmıyor olan eski yazılım veya sistemlerin kullanılması çok büyük siber güvenlik zafiyetleri yaratmaktadır. Amerikan Donanması Uzay ve Deniz Savaşları Sistem Komutanlığı'nda (SPAWAR) bile 100.000'in üzerinde bilgisayarda güncellenmeyen bir versiyon olan Windows XP işletim sistemi kullanılmaktadır. ABD donanması bu eski programları değiştirmek yerine her yıl 9 milyon dolarlık kaynak harcayarak bu işletim sistemi programları için destek almaktadır. Denizcilik sektöründe faaliyet göstermekte olan bir siber güvenlik şirketinin yapmış olduğu çalışmada, şirketlerin %37'sinin kullandığı Microsoft yazılımlarını güncellemek için doğru dosyaları indirmedikleri ve sistemlerinin siber saldırılara açık halde olduğu belirtilmektedir (Jones vd., 2016).

ABD'de Federal Acil Durum Yönetim Kurumu (FEMA) ülke genelindeki limanları taşıdıkları güvenlik risklerine göre değerlendirip güvenlik amacıyla kullanmaları için Liman Güvenlik Hibe Programı (PSGP) adı altında yardım yapmaktadır. 2002 – 2012 yılları arasında Amerikan limanlarına 2,6 milyar dolar PSGP ödemesi yapılmış olup bunun sadece 6 milyon dolarının siber güvenlik için harcandığı tespit edilmiştir. 2012 yılında toplamda 97.500.000 dolar PSGP ödenmiştir, aynı yıl için Baltimore, Houston, Los Angles, Long Beach, Vicksburg ve Beaumont limanlarının PSGP'den aldıkları ödemeleri ne amaçla harcadıkları araştırılmıştır. En riskli liman kategorisinde bulunan Los Angles limanının siber güvenlik konusunda 1.650.000 dolar harcama yapan tek liman olduğu tespit edilmiştir (Kramek, 2013).

24 Ekim 2018'de Jones Walker LLP tarafından ABD'de bulunan küçük, orta ve büyük ölçekli 126 denizcilik şirketinin üst düzey yöneticileri ve teknik çalışanlarıyla Denizcilik Siber Güvenlik Sörveyi yapılmıştır. Bazı önemli sonuçlar aşağıdaki gibidir;

- Katılanların %69'u denizcilik sektörünün bütün olarak siber tehlikelere hazır olduğunu,
- Katılanların %36'sı çalışmakta olduğu şirketin siber tehditlere karşı hazır olduğunu,
- Gemi sahiplerinin %31'i şirketlerinin siber saldırılara karşı hazır olduğunu belirtmiştir.

Diğer sonuçlar Tablo 1'de verilmiştir. Cevaplardaki oranların zıtlığı bu şirketlerin gerçek bir siber saldırıya maruz kalıp kalmadıklarının farkındalar mı sorusunu akla getirmektedir (Jones Walker LLP, 2018).

Tablo 1. Anket sonuçları

	Küçük Ölçekli İşletme	Orta Ölçekli İşletme	Büyük Ölçekli İşletme
Potansiyel bir siber tehlikeye karşı hazırlıklı olma durumu	%6	%19	%100
Son bir sene içerisinde başarılı ile sonuçlanmış veya tespit edilip etkisiz hale getirilmiş bir siber saldırı ile karşılaşma durumu	%7	%40	%78

Pang tarafından 2008 yılında siber güvenlik konusundaki farkındalığın ölçülmesi amacıyla denizcilik alanında faaliyet gösteren 7 kuruluşun katıldığı bir çalışma yapılmıştır. Katılımcılar, denizcilik sektöründeki finans değerinin ve işlemlerin büyüklüğünün siber korsanları saldırı düzenlemek için çok cezbetmeyeceğini düşünmektedir. Katılımcıların 3 tanesi, virüs saldırısına uğradıklarını fakat önemli bilgi veya para kaybı yaşamadıklarını, siber güvenlik konusunda almış oldukları önlemleri yeterli gördüklerini belirtmiştir. Siber güvenlik yatırımlarına dair,

- 3 katılımcı, yeni güvenlik teknolojileri ve sistemlerine yatırım yapmak amaçlı mevcut siber güvenlik protokollerini ve eğitim kurslarını değerlendirdiklerini belirtmiştir.

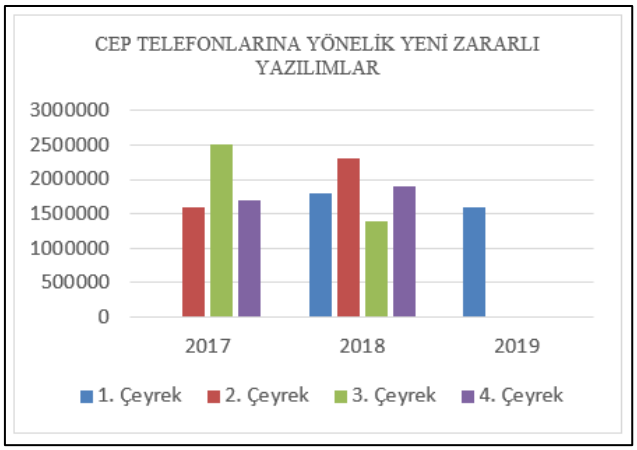
- 3 katılımcı, piyasada mevcut anti virüs yazılımlarının virüs, solucan, kötü amaçlı e posta tespiti için yeterli olduğunu düşünmekte ve yeni yatırım yapmamayı planlamaktadır.
- 1 katılımcı ise başarı ile sonuçlanacak bir siber saldırı yaşamadıkları sürece konu hakkında ilave harcama yapmayacaklarını belirtmiştir.

Siber güvenlik eğitimleri konusunda,

- 3 katılımcı siber güvenlik konusunda çalışanlarına eğitim verilmekte olduğunu belirtmiştir.
- 1 katılımcı ise personele verilen eğitim ve talimatların uygulanıp uygulanmadığının takip edilemiyor olması nedeniyle konu hakkında bir verim alınamayacağını düşünmektedir.

Sonuç olarak, sektördeki siber güvenlik farkındalığının düşük olduğu, denizcilik sektöründeki finans akışının büyüklüğü itibariyle siber saldırganları cezbetmeyeceği düşüncesinin geçerli olamayacağı belirtilmiştir. Ayrıca, insan faktörünün konu hakkında en önemli unsur olduğu, gerekli eğitim ve politikalar ile konu hakkında önlemler alınması gerektiği vurgulanmıştır (Pang, 2018).

Futurenautics tarafından 2012 yılından itibaren her yıl 3.000 gemiadamının katılımıyla yapılmakta olan Crew Connectivity Survey'de ilk defa 2015 yılında akıllı telefon dizüstü bilgisayar, harici bellek gibi elektronik ekipmanları geçerek gemiadamlarının gemide yanlarında bulundurdukları birinci sıradaki elektronik cihaz konumuna gelmiştir. Android işletim sistemi ile çalışan akıllı telefonların içerisinde virüs veya zararlı yazılım bulunma ihtimali %90'ken IOS işletim sistemiyle çalışan bir akıllı telefonda zararlı yazılım bulunma ihtimali %80'dir. Yapılan çalışmada gemiadamlarının %43'ü şimdiye kadar çalışmış oldukları gemilerin bilgisayarlarında virüs veya zararlı yazılım bulunduğunu bildiklerini, %88'i siber güvenlik veya siber hijyen konularında şimdiye kadar hiç eğitim veya tavsiye almadıklarını belirtmiştir (Adamson, 2016). Şekil 8'de cep telefonlarına yönelik yeni zararlı yazılımların yıllara göre dağılımı verilmiştir (MacAfee, 2019).

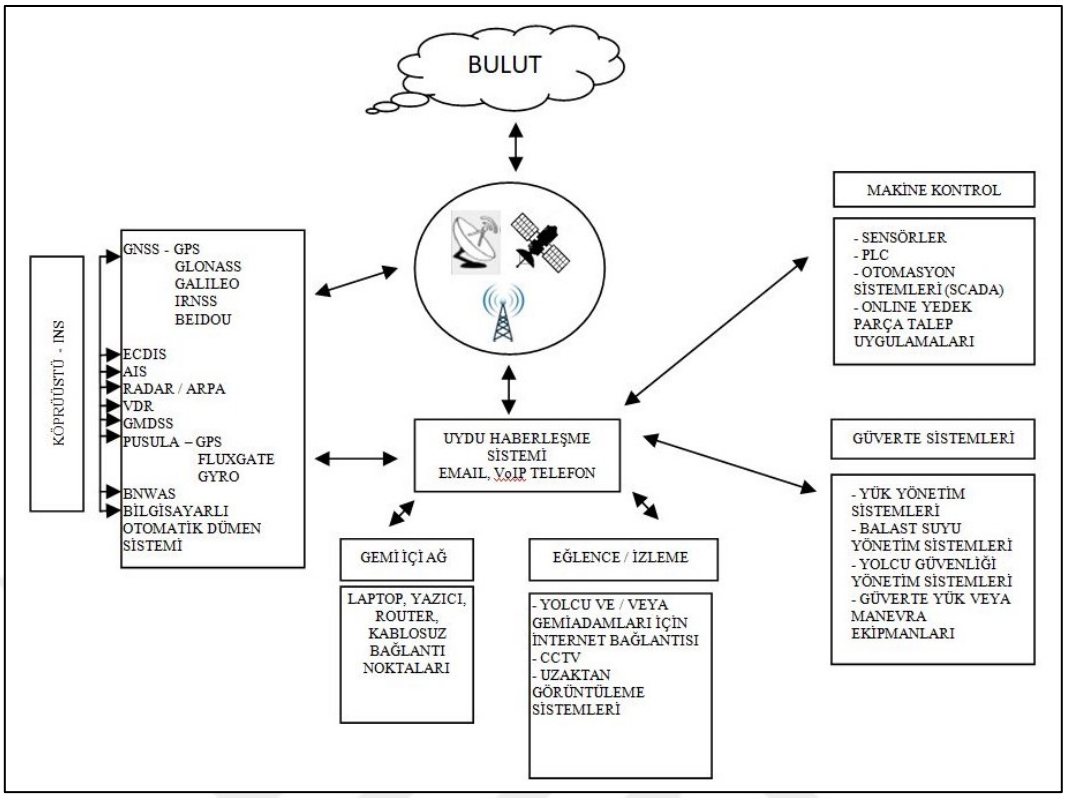


Şekil 8. Cep telefonlarına yönelik yeni zararlı yazılım dağılımı (McAfee, 2019).

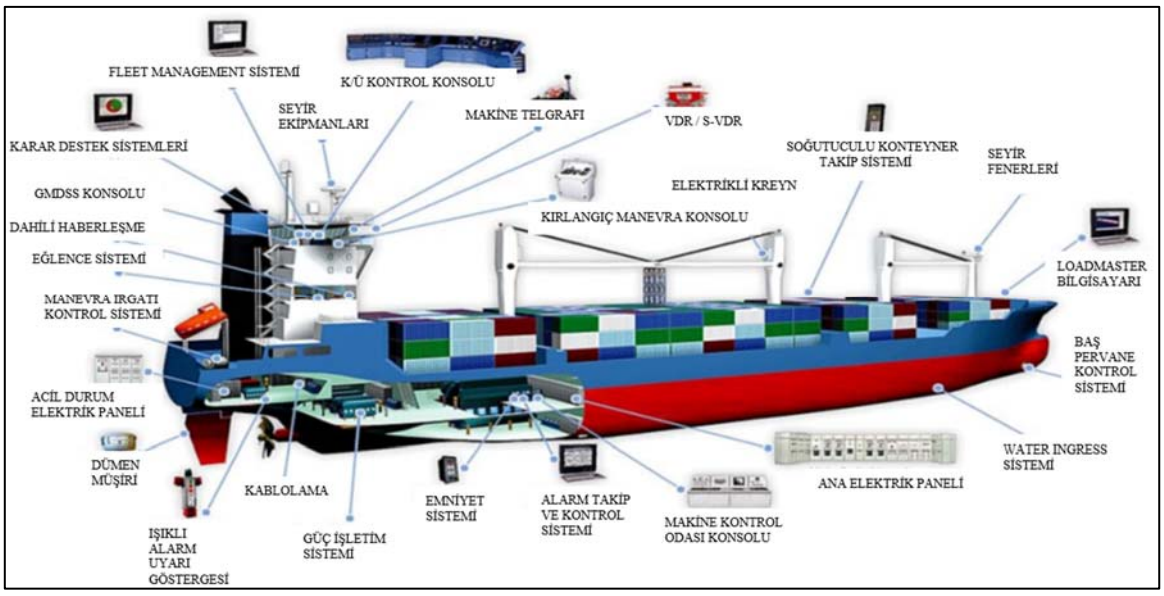
2018 yılında Inmarsat Araştırma Programı, Nesnelerin İnterneti (IoT) tabanlı çözümlere hazır olunup olunmadığını ve buna dair algıyı ölçmek için değişik sektörlerden 750 katılımcıyla "The Industrial IoT on Land at Sea" isimli bir çalışma yapmıştır. Denizcilik sektöründen çalışmaya katılanların %55'i verileri saklama yöntemlerinin, %50'si zayıf ağ güvenliğinin, %44'ü verinin yanlış kullanılmasının veya işlenmesinin kendileri için siber saldırı nedeni olabileceğini belirtmiştir. Denizcilik firmalarının sadece %25'i IoT tabanlı güvenlik çözümleri üzerine çalışmakta olduklarını açıklamıştır (Broadhurst, 2019).

1.9. Siber Saldırı Riski Taşıyan Gemi Sistemleri

Gemilerde kullanılmakta olan ve siber saldırıya maruz kalabilecek sistemlerin genel bir şeması Şekil 9'da verilmiştir. Şekil 10'da ise gemide kullanılmakta olan Endüstriyel Kontrol Sistemleri (ICS) bir gemi modeli üzerinde belirtilmiştir (DHS, 2016).

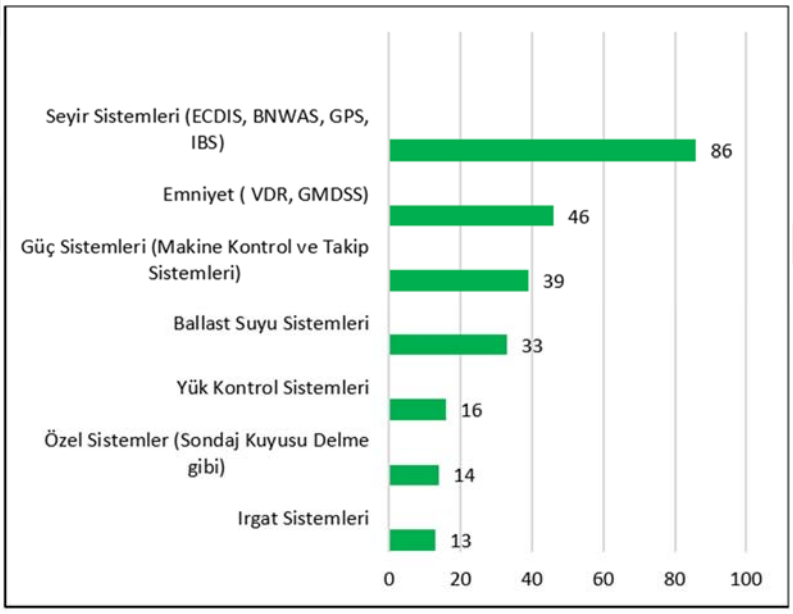


Şekil 9. Siber saldırıya maruz kalabilecek gemi sistemleri



Şekil 10. Gemi kullanılan Endüstriyel Kontrol Sistemleri (DHS, 2016).

IHS Markit tarafından 2018 yılında denizcilik sektöründen 350 katılımcı ile yapılan ankete göre, gemilerde kullanılmakta olan ve siber güvenlik tehdidi içeren sistemlere dair grafik Şekil 11' de verilmiştir (IHS Markit, 2018). ECDIS, GPS ve diğer ekipmanları içeren seyir sistemleri %86 ile siber saldırılara karşı en riskli unsur olarak belirlenmiştir. North of England P&I Kulübüne göre, siber ihlallerin %67'si bilgi teknolojileri (IT) sistemlerinin işlevselliği nedenlidir. Gemiler için siber saldırıya hedef olabilecek en zayıf sistem ECDIS'dir, ayrıca denizcilik sektöründeki siber saldırı kurbanlarının %48'inin sisteminde bilgi çalınmış, %21'i ise ticari kayba uğramıştır (SMI, 2017). Tez çalışmasının amacına yönelik gemide kullanılmakta olan ve siber saldırı riski yüksek olan 4 sistem incelenmiştir. Bunlar; Konum Belirleme Sistemleri, ECDIS, AIS ve Otomasyon, Haberleşme, Bilgisayar Sistemi'dir.



Şekil 11. Gemide kullanılan sistemlerin siber saldırıya uğrama olasılığı (IHS Markit, 2018).

1.9.1. Konum Belirleme Sistemleri

1) Küresel Konumlandırma Sistemi (Global Positioning System - GPS): ABD tarafından 1960'lı yıllarda uydu tabanlı konum belirleme sistemi çalışmaları başlatılmıştır. 1970'li yıllarda uzay bölümünün ilk uydularının göreve başlamasıyla sistem askeri amaçlı kullanılma açılmıştır. 1994 yılında, yeni uydular uzaya yerleştirilmiştir ve sistem 24 uydu

ile tam kapasite sivil kullanıcıların da hizmetine sunulmuştur (Cojocaru, 2009; Gürses, 2013). Son yıllarda etkin hizmet için sistem genelde 31 uydu ile çalıştırılmakta olup, Kasım 2020 itibariyle sistemde 31 operasyonel uydu mevcuttur.

Uydular eşit aralıklı 6 dairesel yörüngede konumludur. Orta Dünya Yörüngesinde (MEO), 55 derece kuzey ve güney enlemlerinin izdüşümlerini arasında 20.200 km yörüngesel yükseklikte konumlu uydular yaklaşık 26.600 km yörüngesel çapta dünya etrafındaki bir tam dönüşlerini 11 saat 58 dakikada tamamlamaktadır (İçen, 2018).

Sistemin çalışma prensibi, izleme istasyonları vasıtasıyla her bir uydudan alınan bilgilerin, uydu yörüngelerinin çok hassas hesaplandığı ana kontrol istasyonuna gönderilmesidir. Ana kontrol istasyonu tarafından güncellenen seyir bilgilerinin yer antenleri vasıtasıyla uydulara gönderilmesi ile uyduların mesafeleri hesaplanmaktadır. Kullanıcılar yerdeki konumlarını uzaydaki uydulardan olan mesafelerini ölçerek belirlemektedir, uydular hassas referans noktası gibi kullanılmaktadır. Her bir GPS uydusu hassas konum ve zaman sinyali göndermekte, kullanıcı alıcısı da kendisine ulaşan sinyalin zaman gecikmesini ölçerek, görünen uydunun mesafesini hesaplamaktadır (Gürses,2013). Diferansiyel GPS (DGPS) sisteminde uydudan tespit edilen kullanıcı konumunun, dünya üzerinde konumu belli olan bir istasyonla sağlamasının yapılması, istasyonun uydudan aldığı konumdaki hata miktarının uzun dalga radyo frekansı ile kullanıcıya iletilmesi ve aynı düzeltmenin kullanıcı için de yapılması prensibi ile çalışmaktadır (Özen, 2014).

GPS uyduları, aynı frekansı kullanarak farklı kodlar göndermektedir. Kodlama için Kod Bölmeli Çoklu Erişim (CDMA) yöntemi kullanılarak L1 ve L2 bantlarından yayın yapılmaktadır. C/A kodlu L1 sinyallerini sivil kullanıcılar, P kodlu L1 ve L2 sinyallerini ise askeri ve diğer yetkili kullanıcılar kullanabilmektedir. Gelecekte L1C, L2C, L5 bantlarında sivil kullanım için L1M, L2M bantlarında da askeri kullanım için yayın yapılıp sinyal kalitesi sinyal karıştırmaya (jamming) ve sinyal aldatmaya (deception) karşın daha güçlü duruma getirilmesi planlanmaktadır. GPS sistemi 0,8 metre hata payı ile hizmet vermektedir, yeni eklenecek uydular ile bu hata payının gelecekte 0,4 metreye düşürülmesi planlanmaktadır (Dawoud, 2012; İçen, 2018).

2) GLONASS (Globalyana Navigatsionnaya Sputnikovaya Sistemaa): 1970'li yıllarda Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) tarafından başlatılan uydu tabanlı konum belirleme sistemi çalışmaları sonucu ilk uydu 1982 yılında uzaya gönderilmiştir. 1993 yılında 12 uydu ile sistem askeri kullanıma açılmıştır. 1995 yılında sistem 24 uydu ile çalışmaya başlamıştır. 2000'li yıllarda uyduların yenilenme çalışmaları hızlandırılmış, 2011

yılında modernleştirilmiş sistem hizmete girmiş ve sivil kullanıcıların kullanımına açılmıştır (Cojocaru, 2009; İçen, 2018).

24 operasyonel ve 2 yedek toplam 26 adet uydu eşit aralıktaki 3 dairesel yörüngede konumludur. Uydular; 64,8 derece kuzey ve güney enlemlerinin izdüşümü arasında 19.100 km yükseklikte, yaklaşık 25.500 km yörüngesel çapta, dünya etrafındaki tam dönüşlerini 11 saat 15 dakika 44 saniyede tamamlamaktadır (İçen, 2018).

GLONASS yer istasyonları vasıtasıyla GLONASS uyduları izlenmektedir. Uydu sinyallerinden mesafe bilgileri toplanmaktadır. Uydu zamanı, uydu durumu ve her bir uydunun seyir mesajı değerleri işleme tabi tutulup mesafe bilgisi güncellenmekte ve güncellenmiş bilgiler uydulara gönderilmektedir. Konum verileri Quantum Optik İzleme İstasyonlarındaki lazer ölçüm cihazları kullanılarak periyodik olarak kalibre edilmektedir. Bu nedenle her bir GLONASS uydusu özel olarak bu maksatla lazer yansıtıcıları taşımaktadırlar. Sistem zamanlaması yüksek hassasiyetli hidrojen atom saati ile sağlanmaktadır (Gürses, 2013).

GLONASS sisteminde her uydu aynı koda sahip olup kendine ait bir frekansta yayın yapmaktadır. 1.598,0625 – 1.609,37 Mhz aralığında L1 sinyali, 1.242,9345 – 1.251,625 Mhz aralığında L2 sinyali gönderilmektedir. Kodlama yöntemi olarak Frekans Bölmeli Çoklu Erişim (FDMA) kullanılmaktadır. C/A ve P kodlu sinyaller her bir bantta 14 taşıyıcı frekanstan yayınlanarak sistem sivil ve askeri amaçlı hizmet vermektedir. Hizmete alınacak yeni modern uydular ile FDMA yanında CDMA ile de kodlama yapabilecek, sitemin diğer uydu konumlandırma sistemleri ile uyumlu çalışması sağlanacaktır. Böylelikle L3, L3OC gibi farklı bantlarda da sinyal gönderilebilecektir. Diğer sistemlere nazaran GLONASS'ın yüksek enlemlerdeki kullanılabilirliği daha fazladır. Sivil kullanım için yayınlanan sinyallerde hata oranı 1,2 metre kadardır. Bölgesel ve yerel destek sistemleri diferansiyel düzeltmeleri ile hata miktarı 1 metreye kadar inmektedir. Askeri kullanım için hata miktarı 0,1 metre ile 0,03 metre arasında değişmektedir (Dawoud, 2012; İçen, 2018).

3) GALILEO: Avrupa Birliği ve Avrupa Uzay Ajansı, Mart 2002'de ABD kontrolündeki GPS'e alternatif olarak Galileo olarak isimlendirilen yeni bir uydu konumlandırma sistemini geliştirmeyi kararlaştırmıştır. Bu uydu sistemi, 2014 yılında 24 uyduyla hizmete başlamıştır, 2020 yılı sonuna kadar tam işlevsel olarak çalışması beklenmektedir. 3 farklı yörüngesel düzlemde yerden 23.222 km yükseklikte, 56 derece kuzey ve güney enlemleri izdüşümleri arasında konumlanmış, her bir yörüngede 8 operasyonel 2 yedek toplam 30 bulunmaktadır. Uydular yaklaşık 29.600 km yörüngesel

çapta dünya etrafındaki bir tam dönüşünü 14 saat 4 dakika 42 saniye tamamlamaktadır. Kodlama tekniği olarak CDMA kullanılmaktadır. L1, E1, E5, E6 bantlarında arama kurtarma ve sivil kullanım gibi amaçlar için hizmet vermesi planlanmaktadır. Şu anki hata miktarı 10 km olup kısa zamanda 5 km olacak şekilde iyileştirilmeler yapılmaktadır (İçen, 2018).

4) BEIDOU: Beidou, Çin devleti tarafından geliştirilen uydu tabanlı konum belirleme sistemidir, COMPASS adı ile de bilinmektedir. BeiDou Seyir Uydu Sistemi, üç aşamalı olarak geliştirilmektedir. Küresel kapsamaya sahip olması planlanan BeiDou Faz 3' ün kurulumu devam etmektedir ve 2020 yılı sonunda bitirilmesi planlamaktadır. Küresel kapsama sahip olacak BeiDou Faz 3 tamamlandığında; orta yörüngede 27, eğik yer eş-zamanlı yörüngede 3 ve yer-sabit yörüngede 5 tane olmak üzere toplam 35 uydudan oluşacaktır. BeiDou Faz 3 uydu takımında, yer-sabit yörüngeli uydular 58,75 derece doğu, 80 derece doğu, 110,5 derece doğu, 140 derece doğu ve 160 derece doğu boylamlarında yer almaktadır. Eğik yer eş-zamanlı 3 yörünge düzlemi, yükselme düğüm açıları arasında 120 derece açı bulunacak biçimde düzenlenmiştir, yer izleri ekvatoru 118 derece doğu boylamında kesmekte ve aynı boylamı merkez alarak "8" şekli çizmektedir. Her 8 saatte bir uydulardan biri ekvatordan geçmektedir. BeiDou Faz 3'te 3 adet orta yörünge düzlemi bulunmaktadır. Her yörünge düzleminin yükselme düğüm açıları arasında 120 derece eş aralıklar bulunmaktadır. Yerden yükseklikleri yaklaşık 21.525 km olan orta yörüngelerin yörünge yarıçapları 27.900 km'dir. Orta yörüngeli bir uydu, yörüngedeki bir turunu yaklaşık olarak 12 saat 52 dakikada tamamlamaktadır. CDMA kodlama yöntemi kullanan uydular aynı frekans üzerinden B1, B2, B3 ve S sinyalleri göndermektedir. Sistemin hata mesafesi yaklaşık 10 metredir (İçen, 2018).

5) Genişletilmiş LORAN (eLORAN): Yeryüzünde kurulu LORAN (Long Range Navigation – Uzun Mesafeli Seyir) sistemi, hiperbolik radyo sinyallerinin kullanıldığı bir konum belirleme sistemidir. Gönderilen 2 hiperbolik radyo sinyalinin gecikme zamanları arasındaki farktan enlem ve boylam elde edilmektedir. 1930'lu yılların sonunda üzerinde çalışılmaya başlanmıştır. Sistemin 1980'li yıllarda geliştirilen versiyonu LORAN C 1990'lı yıllarda uydu tabanlı konum belirleme sistemlerinin yaygınlaşmaya başlamasıyla tercih edilmemeye başlanmıştır. Yakın geçmişte, uydu tabanlı konum belirleme sistemlerinin maruz kalabileceği siber tehditlere istinaden kullanıcılara daha güvenli bir sistem arayışına girilmiş ve ABD'nin 2008 yılında GPS'in yedeği olarak duyurduğu eLORAN sisteminin geliştirilmesine başlanmıştır (Lo vd., 2009; Son vd., 2019).

ELORAN sisteminde kullanılan yüksek güçteki göndericilerden yayınlanan düşük frekanstaki sinyallerin LORAN-C sinyallerinden tek farkı ilave edilen data bandıdır. Bu özellik ile düzeltme, uyarı ve sinyal bütünlük bilgileri kullanıcılara iletilebilmektedir. Sinyaller karada bulunan, yükseklikleri 200 metreye ulaşan antenlerden yayınlanmaktadır. Sistemin genel kontrol ve gözetiminin yapıldığı Kontrol İstasyonları, sinyal erimi içerisinde bulunan ve sinyal kalitesini Kontrol İstasyonuna bildiren Referans İstasyonları sistemin diğer parçalarıdır (ILA, 2007).

Şu an için hata mesafesi IMO kriteri olan maksimum 10 metrenin üzerindedir (Safar vd., 2010). Sistemin menzili 500 – 1200 deniz mili arasındadır ve sadece alt yapının mevcut olduğu bölgelerde kullanılabilmektedir. Çin, İngiltere başta olmak üzere Kıta Avrupası, Baltık ülkeleri, ABD, Rusya, Güney Kore, Hindistan var olan LORAN-C alt yapılarını geliştirip eLORAN'a uyumlu hale getirmek çabasındadır.

1.9.2. ECDIS

Elektronik Harita Gösterimi ve Bilgi Sistemi, kâğıt harita yerine oluşturulan bilgisayar tabanlı seyir bilgi sistemidir. Elektronik Seyir Haritaları (ENC) kapsam, yapı ve format olarak standartlaştırılmıştır. ENC, seyir bilgi sistemlerinde kullanılmak üzere sadece ülkelerin deniz haritalarını üretmekle yükümlü Hidrografi Daireleri tarafından, Uluslararası Hidrografi Dairesi'nin (IHO) belirlemiş olduğu S-57 / S-100 Standardına göre hazırlanmış vektör haritalardır. ENC bir veri tabanıdır ve harita bilgileri bu veri tabanı içinde nitelikleri tanımlanmış nokta, çizgi ve alanlar şeklinde depolanmaktadır. ENC, içerisindeki veri sorgulanmaya açık olduğu için akıllı haritadır. Ayrıca, kullanıcının ihtiyaçlarına cevap verecek şekilde haritanın ekran üzerinde gösterimine imkân tanıdığı için ENC esnek haritadır. Harita üzerinde yer alan ve kullanıcı açısından büyük öneme sahip bilgiler; harita ölçeği, haritanın yapımı hakkında açıklayıcı notlar, uyarıcı notlar, harita numarası, yayın tarihi ve şekli, üretici basım notu, küçük düzeltmeler notu, köşe koordinatları kâğıt haritadaki bulunduğu gibi göze tanıdık yerlerinde bulunmasalar da ENC'nin sorgulamaya açık bölümlerinde yer almaktadır. ENC'lerin hukuka aykırı çoğaltılmasını engellemek üzere Ekim 2003'te IHO S-63 Veri Koruma Standardı kabul edilmiş, ENC ve ECDIS üreticileri ile ürün kullanıcılarını içine alan bir şifreleme sistemi kurulmuştur. Bu sistemin temelinde ENC'lerin kendisine tanımlı donanım haricinde çalışmasını engellemek yatmaktadır.

ENC'ler şifrelendikten sonra son kullanıcıya sunulmak üzere IHO tarafından da tavsiye edildiği şekilde Bölgesel Dağıtım Merkezleri tarafından dağıtılmaktadır (Gürses, 2013).

ECDIS, sisteme bağlanan elektronik seyir yardımcılarından elde ettiği verileri ekran üzerinde görüntüleyebilme kabiliyetine de sahiptir. Gemi üzerinde bulunan cihazın IMO tarafından belirlenen ECDIS performans standartları ile uyumlu olması gerekmektedir. ECDIS cihazı performans standartları gereği, AIS cihazından civardaki gemilerin tanıtıcı bilgilerini, GNSS cihazından geminin konumu ve yere göre hızını, radar cihazından ekran görüntüsünü, gyro pusuladan pruva değerini, geminin emniyet ve diğer faktörlerine bağlı olarak başka sensörlerden ilgili değerleri almaktadır (IMO, 2017; IHO, 2019; Svilicic vd., 2020). Vardiya zabitinin ECDIS kullanma yeterliliğine sahip olabilmesi için IMO model kurs 1.27 eğitimi almış ve başarıyla tamamlamış olması gerekmektedir (IMO, 2006). ECDIS'in arızalanması durumunda geminin emniyetli seyrine devam edebilmesi adına yedek ECDIS sisteminin standartları hakkında IMO bazı kurallar belirlemiştir (IMO, 2017). Bu standartların uygulanması ile yedek sistem devreye alındığında seyrin devamının emniyeti sağlanmış olacaktır (Svilicic vd., 2020). Ana ECDIS arızasında kağıt haritasız seyre devam edebilmek için, yedek ECDIS sisteminin 2 ayrı ECDIS istasyonundan oluşması, ikisinin ayrı güç kaynaklarının ve ayrı konum sensörlerinin olması gerekmektedir (Brčić ve Žuškin 2018; Weintrit 2018; Svilicic vd., 2020).

1.9.3. AIS

Otomatik Tanımlama Sistemi (AIS), deniz emniyeti/güvenliği ile ilgili bilgilerin gemiler ve sahil istasyonları arasında iletişimi sağlayan otomatik ve devamlı bir yayın sistemidir. AIS, Zaman Bölmeli Çoklu Erişim (TDMA) teknolojisini kullanan seyyar çok yüksek frekans (VHF) deniz bandında çalışmaktadır. Denizde Can Güvenliği Uluslararası Sözleşmesi (SOLAS) Bölüm V gereği AIS cihazı 31 Aralık 2004 tarihinden itibaren SOLAS'a tabi bütün gemilerde IMO Kararı MSC.99(73), 2000 gereği bulunmak zorundadır. IMO kararı MSC.74(69), EK-3, 1998' de AIS için tanımlanan performans standartlarına göre AIS, gemilerin birbirlerini ve seyir emniyeti ile ilgili makamlar tarafından etkili bir şekilde izlenmesine olanak sağlamıştır. Halihazırda iki tip ip AIS mevcuttur. A ve B Sınıf olarak adlandırılan AIS'ler sınıflarına göre gönderdikleri bilgiler değişse de genel olarak; Seyir Durumu, Dinamik Bilgiler ve Statik Bilgilerin yayınını yapmaktadırlar. Seyir durumu ile ilgili bilgiler; geminin demirde, makine gücüyle hareket halinde, kumanda altında değil

veya manevra gücü kısıtlı gibi bilgilerini kapsamaktadır. Dinamik Bilgiler; gyro pusuladan gelen pruva değeri, GPS'ten gelen konum, yere göre sürat ve yere göre rota bilgileri ve dönüş oranı göstergesinden gelen dönüş oranı gibi değişken bilgileri kapsamaktadır. Statik Bilgiler ise; AIS ilk kurulurken girilen, Denizcilik Seyyar Hizmet Kimlik Numarası (MMSI), IMO gemi numarası, telsiz çağrı adı, gemi adı, gemi tipi ve ebatları gibi değişmeyen bilgileri kapsamaktadır (Gürses, 2013).

AIS cihazı bu bilgilerden oluşturduğu dijital mesajı VHF radyo dalgaları ile çevredeki gemi, arama kurtarma (SAR) uçağı, seyir yardımcısı (AIS AtoN), AIS SART, gemi trafik hizmetleri (VTS), sahil istasyonu gibi diğer AIS istasyonlarına iletir. Yersel (terrestial) yani sadece VHF anteni kullanılan sistemlerde VHF anteninden gönderilen sinyalin erimi anten yüksekliğine, antenin yerleştirildiği yerdeki baca, direk gibi engellere (kör noktalara), antenin sinyal çıkış gücüne, antenin etrafındaki dağ, koy gibi coğrafi engellere ve atmosferik koşullara bağlı olarak 20 milden 200 mile kadar değişkenlik gösterebilir. Uydu (satellite) AIS ise yersel AIS VHF anteninden çıkan sinyalin alçak dünya yörünge (LEO) uyduları tarafından alınması ve uyduların bu sinyali diğer istasyonlara yayması prensibi ile çalışmaktadır. Böylelikle uydu AIS sinyal erimi VHF AIS'den daha geniş bir kapsama yayılmaktadır (Turgut, 2019).

Uydu AIS sisteminin kapsam alanı avantajına karşın, alçak dünya yörünge uydu sayısının şu an için az olması sebebiyle mevcut uyduların yayınlanan tüm AIS mesajlarını kaldıramayacak olması, AIS istasyonlarının sinyal çıkış kuvvetinin düşük olmasına istinaden gönderilen sinyalin her koşulda uyduya ulaşamaması, belli koşullar sağlandığında aynı slottan birden fazla istasyonun mesaj gönderebileceğine istinaden gemi trafiğinin yoğun olduğu bölgelerde uyduya aynı slot üzerinden gelen data paketlerinin çakışması sonucu veri eksilmesi oluşması gibi sorunlar mevcuttur. Tüm bunlar AIS mesajlarının yayınladığı mevcut iki frekansa ilave olarak uydu sistemi için üçüncü frekansın oluşturulması ve teknik iyileştirmeler ile giderilip sistem daha güvenli çalışır hale getirilecektir (Jackson, 2012; Challamel vd., 2012; Chen, 2014; Ho vd., 2018).

1.9.4. Otomasyon, Haberleşme, Bilgisayar Sistemi

Modern gemilere entegre edilmiş bilgisayar sistemleri, özel donanım ve yazılım çözümleri ile seyir, tahrik veya yakıt sistemi gibi belirli ihtiyaçların otomasyonunu

sağlamaktadır. Bunlar; gemi personelinin, geminin durumuna dair bilgileri gerçek zamanlı ve güvenilir şekilde temin edebileceği, zaman ve maliyet tasarrufu sağlayan donanımlardır. Köprüüstü seyir sistemleri, haberleşme sistemleri, yük işletim sistemleri, makine ve teçhizat işletim sistemleri, personel eğlence sistemleri, yolcu hizmetleri işletim sistemleri gemide kullanılmakta olan bilgisayar sistemlerine dayalı otomasyon altyapılarından bazılarıdır. Belirtilen bu sistemler birbirleriyle ilişkili olup, en basit olan sisteme dahi yönelik siber saldırının en önemli sistemlerden biri olan köprüüstü seyir sistemlerini etkileme potansiyeli mevcuttur (Caprolu vd., 2020). Günümüzde teknolojik gelişmelere paralel olarak her türlü bilgisayar sistemleri ürünü gemilerde yer bulmaktadır. Carnival Cruise Line'a ait OASIS sınıfı 360 metre uzunluğundaki yolcu gemilerinde 900 adedin üzerinde kablosuz erişim noktası (Wireless Access Point), 30.000 adedin üzerinde IP portu, 1.200 adet kablosuz telefon, 600.000 metre fiber kablo ile bağlantılı 44 adet ağ anahtarı istasyonu (Network Switching Location) bulunmaktadır (Boyes, 2013). Yapılan bir araştırmaya göre sıradan bir gemide bulunan PLC sayısı 36 adede kadar ulaşabilmektedir (Muccin, 2016).

1.10. Siber Saldırı Olayları

Gemilere yönelik siber saldırılar GPS, AIS, ECDIS ve bilgisayar sistemlerini hedef alan planlı veya istemsiz olarak çeşitli yöntemlerle gerçekleştirilmiş olaylardır. Kurumlara yönelik saldırılar ise genelde bilgisayar sistemlerini hedef alan planlı, belirli bir amaç için yapılmış saldırılardır. Denizcilik sektöründe gemi ve kurumlara yönelik siber saldırılara ilişkin siber saldırı olayları aşağıda açıklanmıştır.

1) Karadeniz'de GPS Sinyal Karıştırma Olayı: Karadeniz'de 44 derece 15,7 dakika kuzey enlemi ve 037 derece 32,9 dakika doğu boylamı mevkiinde 22 Haziran 2017 tarihinde 07:10 UTC'de seyir yapmakta olan geminin GPS sinyallerine müdahale edilmiştir. Gemi kaptanından alınan bilgiye göre olay cihazın teknik arızası nedenli değildir, olay anında çevrede bulanan diğer 20 gemi de GPS sinyali müdahalesinden etkilenmiştir. Gemi, GPS cihazı üzerinde görülen mevkiinin gerçekte 17 deniz mili güney doğusunda bulunmaktadır (Daum, 2019). Bazı kaynaklara göre gemiler karadan 32 km içeride, Sochi havalimanında bulunmaktadır (MDR, 2019).

2) Güney Kore'de GPS Sinyal Karıştırması Olayı: Nisan 2015'de 1.000'e yakın hava aracı ve 250'den fazla deniz aracı Kuzey Kore devletinin desteklediği öne sürülen kişiler tarafından gerçekleştirilen GPS sinyali karıştırma olayından etkilenmiştir. Doğru mevkiini

belirleme zorluğu çeken birçok gemi limana geri dönmek zorunda kalmıştır, birçok gemi de aynı sorundan dolayı diğer gemiler için tehlike oluşturabilecek duruma düşmüştür (Lagouvardou, 2018). 2016 yılında yine Kuzey Kore devletinin sorumlu görüldüğü ve 6 gün süren GPS sinyalleri karıştırma olaylarından 1.007 uçak ve 715 gemi etkilenmiştir (Son vd., 2019).

Texas Üniversitesinden T. Humphreys, RNT (Reseilient Navigation and Timing Foundation) ve teknoloji şirketi Palantir tarafından desteklenen C4ADS kurumunun yapmış olduğu çalışmaya göre, Rusya devleti 2016 yılından itibaren, GPS sinyallerini etkilemek suretiyle başta Karadeniz kıyısındaki Kırım bölgesi olmak üzere 10 farklı bölgede 1.311 sivil gemiyi etkileyen 9.883 siber olaydan sorumlu tutulmaktadır. Aynı araştırmada, Rusya'nın üst düzey yetkililerinin halka açık yerlerde yaptıkları faaliyetler sırasında, stratejik yapıların ve tesislerin korunması amaçlı, Suriye gibi savaş alanlarında avantaj sağlamak amaçlı hava trafiğini de olumsuz etkileyecek şekilde GPS sinyali etkileme faaliyetlerinin sıklıkla yapıldığı vurgulanmış ve bu faaliyetler verilerle ispatlanmaya çalışılmıştır (C4ADS, 2019). Bu olaylar Kessler (2019) tarafından da teyit edilmektedir.

3) Gemi Personeli: Zabit kendi cep telefonunu şarj etmek amacıyla USB bağlantısı ile ECDIS cihazına bağlamıştır. Cep telefonu içerisindeki varlığından haberdar olunmayan virüs ECDIS yazılımını etkilemiştir ve ECDIS içerisindeki haritaların bazılarının silinmesine, bazılarının ise bozulmasına sebep olmuştur. Durumun teknisyen çağırılarak düzeltilmesi 2 gün sürmüştür ve gemi sefer programını ertelemek zorunda kalmıştır (Tucci, 2017).

4) Tanker: Asya'da bir limana gelmiş olan 80.000 tonluk tankerdeki bir zabit çıktı alınması gerekli bazı evrakları içeren USB belleği gemi bilgisayarında kullanmış ve gemi bilgisayar sistemlerine virüs girmesine sebep olmuştur. Başka bir zabit virüslü gemi bilgisayar sistemine indirdiği ECDIS güncellemelerini yine USB belleğe yüklemiş, belleği ECDIS cihazına sokmuş ve ECDIS yazılımı da virüsten etkilenmiştir. Olay, ECDIS'in bozulmasına, kullanılması gereken haritaların silinmesine neden olmuştur ve geminin seyre çıkamamasına sebep olmuştur (URL-1).

5) İngiltere Denizcilik ve Sahil Güvenlik Ajansı (MCA) Sasser Virüsü: 2004 yılında e posta yoluyla birçok sektörü etkileyen Netsky B. virüsünden sonra aynı yılın Nisan ayında başlayıp değişik versiyonlarıyla Mayıs ayında devam eden Sasser virüsü aralarında MCA'nın da olduğu kuruluşları etkilemiştir. Kurumun e posta sistemi ve ECDIS'i virüsten etkilenmiş ve kullanım dışı kalmıştır. Kurumun IT personeli sistemi düzeltmek için çalışma

yaparken kurum bir tehlike durumu mesajı alındığında kurtarma yardım operasyonu için kağıt haritalar üzerinde mevki koyup çalışacak şekilde önlem almıştır (Shah, 2004).

6) ECDIS'deki Virüs Nedeniyle Geminin Seyrinin Gecikmesi: Kağıt harita kullanmayan, ECDIS ile seyir yapacak şekilde donatılmış yeni inşa bir geminin ECDIS sistemine bulaşmış virüs tespit edildiği için geminin seyre çıkmasında gecikme yaşanmıştır. Gemi personeli tarafından sorun teknik bir arıza olarak algılanmıştır, siber bir konu olabileceği düşünülmemiştir. Gemiye çağrılan teknisyen her iki ECDIS sisteminde de virüs tespit etmiştir. Virüs karantinaya alınıp sistem çalışır hale getirilmiştir. Virüsün kaynağı bilinmiyor olmakla beraber süreç gemi için yüz binlerce dolar mali kayba neden olmuştur (BIMCO, 2020).

7) Entegre Seyir Sistemi'nin (INS) Seyir Sırasında Bozulması: Trafiğin yoğun ve görüşün kısıtlı olduğu bir durumda, INS ile donatılmış bir gemide seyir sırasında tüm seyir sistemleri arıza vermiştir. Gemi limana varıncaya kadar iki gün boyunca bir radar ve yedek kağıt haritaları ile seyir yapmıştır. Varış limanında yapılan incelemede, bir önceki limanda gemiye gelmiş olan ECDIS teknisyeninin sisteme yüklediği yazılım güncellemesinin, eski versiyon olduğu, ECDIS yazılımına uygun olmadığı ve sistemin bu nedenle çöktüğü anlaşılmıştır. Geminin yeni ECDIS bilgisayarları tedarik etmesine ve Uluslararası Emniyetli Yönetim Kodu (ISM) dahilinde oluşturulan ramak kala (Near Miss) olay raporunun klas nezaretinde kapatılmasına kadar limanda beklemesi gerekmiştir. Tüm gecikmeler armatör tarafından karşılanmak zorunda kalınmıştır (BIMCO, 2020).

8) Pilotlu Seyir Sırasında Seyir Bilgisayarının Çökmesi: Pilotlu seyir sırasında gemi ECDIS bilgisayarı ve seyir bilgilerinin görülebildiği bilgisayar çökmüştür. Arıza, köprüüstündeki seyir zabitlerinde kısa süreliğine bir dikkat dağılması yaratmış olsa da kaptan ve pilot radar ve gözcülük ile seyre devam edebilmiştir. Yapılan incelemede, cihazın işletim sisteminin eski ve desteklenmeyen bir versiyon olduğu, bilgisayarların çökme sorununun daha önceden de yaşandığı ve kaptan tarafından rapor edildiği fakat şirketin durumu önemsemediği anlaşılmıştır (BIMCO, 2020).

9) Uydu Bağlantısı: Gemi kaptanının kullandığı bilgisayar üzerinden yapılan uydu bağlantısı ile geminin ECDIS cihazına zararlı yazılım yüklenmiştir. Gece saatlerinde köprüüstünde vardiya tutan vardiya zabitine durum fark ettirilmeden zararlı yazılım sayesinde gemi rotasından çıkartılmıştır. Tüm olay süresince ECDIS ekranında geminin normal rotası üzerinde gidiyor görülmesi sebebiyle vardiya zabitinin durumun farkında olmadığı rapor edilmiştir (Kessler, 2019).

10) Radar: ECDIS dahil köprüüstü sistemlerinin, haberleşme sistemlerinin, makine kontrol sistemlerinin bağlı olduğu gemi içi ağa radar cihazının da bağlı olduğu bir gemide, makine kontrol sistemine takılan harici bellek içerisindeki zararlı bir yazılım ağ üzerinden radar sistemine yüklenmiştir. Zararlı yazılım, radar ekranındaki tüm hedeflerin silinmesine ve geminin etrafına dair radar farkındalığını kaybetmesine sebep olmuştur (Kessler, 2019).

11) İran Devletine Ait Tankerler: İran devletine ait tanker firması İran Ulusal Tanker Şirketi'ne (NITC) ait 3 adet tanker ülkeye uygulanmakta olan yaptırımları delebilmek amacıyla AIS sinyallerini saptırmıştır. AIS bilgilerinin gemi ismi değiştirilmiş, bayrağı Tanzanya bayrağı yapılmış, sahibi Suriyeli bir şirket olarak gösterilmiş şekilde düzenlendiği rapor edilmiştir. Böylece açık denizde gemilere başka ülkelerin donanmaları tarafından kontrol yapılmasının, yüke ve gemiye el konulmasının önlemesi amaçlandığı belirtilmektedir (URL-2).

12) Elba Adası: 3 Aralık 2019 tarihinde Elba Adası ile Corsica arasında 28x21 deniz millik bir alanda birincisi 3 dakika, ikincisi 2 dakika süren iki adet AIS saldırısı meydana gelmiştir. Yapılan analizler sonucu Elba Adası yakınlarına yerleştirilmiş olan bir AIS yanıltıcısının (Spoofing Generator) 3.742 adet sahte gemi yarattığı tespit edilmiştir (Androjna vd., 2020).

13) RO-RO Gemisi: RO-RO gemisinde çalışmakta olan personel gelen bir e-postanın ekini açmıştır. Bu işlem, gemide askeri amaçlı yükü bulanan bir kiracı için hazırlanmış personel listesi evrağına fidye yazılım yüklenmesine sebep olmuştur. Durum geminin fazladan 3 gün limanda kalmasına ve 30.000 dolar mali kayba neden olmuştur (Di Rollo, 2017).

14) 8.250 TEU'luk Konteyner Gemisi: Sahibi Alman şirketi olan 8.250 TEU'luk konteyner gemisinin, Güney Kıbrıs'tan Dijibutu'ya seyri sırasında Şubat 2017'de siber saldırıya uğradığı ve korsanların geminin seyir sistemlerinin kontrolünü 10 saatliğine ele geçirdiği rapor edilmiştir. Geminin tüm IT sistemini kontrol altına alan korsanların amacının gemiyi istedikleri yere yönlendirmek ve gemiye el koymak olduğu tahmin edilmektedir. Gemi personeli duruma müdahale etmeye çalışmış, seyir sisteminin kontrolünü elde etmeyi başaramamış ve olay sonrasında gemiye IT uzmanları getirilmiş, saatler süren çalışma sonrasında durum düzeltilmiştir (OSM, 2018). Korsanların bu saldırıyı iletişim uyduları üzerinden gerçekleştirdiği tahmin edilmektedir (Dadiani, 2018). Şirket daha sonra gemiye IT sistemlerinin etkilenmesini önlemek amaçlı bir program kurdurmuştur (Silgado, 2018).

15) Amerikan Yük Gemisi: New York ve New Jersey Liman Otoritesi, rıhtıma yanaşması planlanan bir Amerikan gemisini ABD Sahil Güvenlik kurumuna rapor etmiştir. Sahil Güvenlik ve FBI tarafından yapılan incelemede virüs nedeniyle geminin bilgisayar ağ sisteminin ciddi bir şekilde etkilendiği fakat gemi kontrol sistemlerinin normal çalışır durumda olduğu, virüsten etkilenmediği anlaşılmıştır. Gemide herhangi bir siber güvenlik uygulamasının olmadığı, gemi bilgisayar sistemine giriş için herkesin aynı şifreyi kullanmakta olduğu, kullanılan USB belleklerin virüs taramasının yapılmamış olduğu ve bilgisayar sisteminde virüs koruma programı olmadığı raporlanmıştır (URL-3).

16) Dinamik Konumlandırma (DP) Kullanılan Deniz Araçları: Açık deniz yakıt endüstrisinde çalışmakta olan DP sistemli bir deniz aracının sistem yazılımlarında keşfedilen bir virüs, sistemi kontrol altına almış, deniz aracının aniden ve beklenmedik şekilde durmasına yol açmıştır (Tucci, 2017). 2013 yılında Meksika Körfezi'nde 7.000 feet derinlikteki kuyuda çalışmakta olan açık deniz platformu sürüklenmeye başlayınca emniyet amacıyla otomatik olarak delici uç kuyudan ayrılmış ve kuyu girişi kapanmıştır. Olayın sebebi platform personeli tarafından sistem bilgisayarlarına USB ile bağlanan cep telefonu ve diğer elektronik aletlerin internet üzerinden sisteme bulaştırdığı virüs olduğu düşünülmektedir (Silgado, 2018).

17) The Phantom Menace Olayı: Olay 2013 yılında İngiltere'deki bir petrol şirketi bünyesinde çalışan bilişim güvenliği uzmanlarınca fark edilene kadar, anti virüs programları tarafından tespit edilemeyen ve virüs niteliği taşımayan bir kod; 6 ay süresince 8 farklı petrol şirketinin bilgisayarlarında kullanılan Windows dosyalarına yetkisiz erişim sağlanmıştır ve bu şirketlerin bilgisayarlarında bulunan bilgiler çalınmıştır. Her saat başı otomatik olarak çalışan bu kod şirket bilgisayar ağındaki dosyaları bir Dosya Transfer Protokolü (FPT) sunucusuna kopyalamaktadır. Yapılan incelemede, saldırıya uğrayan şirketin sunucusundaki üst üste kopyalanmış dosyalar teke indirildiğinde 860 adet belgenin saldırganlar tarafından elde edilebildiği anlaşılmıştır. Olay petrol firması personeline kimlik hedefli oltalama e posta ile gönderilen taşınabilir belge biçimi formatlı (PDF) bir boş dosyanın açılmasıyla başlamıştır. Personel, PDF evrağın boş olmasından şüphe duymamış, bir yanlışlık olduğunu ve kısa zaman sonra doğru evrağın gönderileceği düşünmüştür (Tucci, 2017; PANDA, 2015).

18) A.P. Moller – Maersk Olayı: Haziran 2017' de bilgisayar korsanları A.P. Moller Maersk'in dünya çapındaki operasyonlarının NotPetya isimli fidye yazılım ile etkilemeyi ve kontrol altına almayı başarmıştır. Virüs birkaç günlüğüne şirketin bilgisayarlarındaki

bilgilere erişimini engellemiş ve korsanlar bilgilere tekrar erişim için 300 dolar karşılığı Bitcoin fidye istemiştir. Siber saldırı sırasında aralarında Rottterdam, Jawaharlal ve ABD'deki birçok konteynır terminali de bulunan yük terminallerinin operasyonları durmuş ve ciddi gecikmeler meydana gelmiştir. Saldırının başarıyla püskürtülüp püskürtülmediği veya fidyenin ödenip ödenmediği bilinmemektedir. Fakat olay yaklaşık 300 milyon dolarlık bir operasyonel ticari kayıp ile sonuçlanmıştır (Daum, 2019). 2018 yılında World Economic Forum'un bir oturumunda A.P. Møller-Maersk yönetim kurulu başkanı Jim Hagemann Snabe; 10 gün içerisinde, virüsten etkilenen 4.000 adet server (Sunucu), 45.000 adet bilgisayar ve 2.500 adet uygulamanın yenilendiğini açıklamıştır.

19) Port Antwerp Olayı: Haziran 2011 ile Ekim 2013 tarihleri arasında bilgisayar korsanları hiç kimseye tespit edilmeden Antwerp Limanı'nın IT sistemlerine erişim sağlamıştır. Uyuşturucu kaçakçıları ile çalışan bilgisayar korsanları, bu süre zarfında Güney Amerika'dan gelen konteynırların nereye gideceği, ne zaman geleceği ve sahiplerine dair bilgilere ulaşmıştır. Liman IT sistemine erişen bilgisayar korsanları, içlerinde bulunan normal yük dışında kokain veya eroin gibi uyuşturucu madde içeren bu konteynırları liman veya gümrük idaresine sezinletmeden başka yerlere yönlendirmiştir ve uyuşturucu şebekesi, konteynır nihai sahibine ulaşmadan uygun yerde içlerindeki kendi malları olan uyuşturucuyu konteynırdan çıkartmıştır (Daum, 2019). Konteynırların tamamen ortadan kaybolmaya başlaması sonrası liman idaresi olayın farkına varmaya başlamıştır (Lagouvardou, 2018).

20) COSCO Olayı: COSCO denizcilik şirketinin Kuzey ve Güney Amerika IT sistemleri Temmuz 2018'de siber saldırıya uğramıştır. COSCO'dan yapılan basın açıklamasına göre şirketin e posta ve telefon sistemlerinin saldırıdan etkilendiği, diğer operasyon bölgeleri ile irtibatın kesildiği, olayın çok kısa bir zaman sürdüğü ve bir zarar ile karşılaşılmadan atlatıldığı bildirilmiştir (Daum, 2019).

21) Danimarka Denizcilik Otoritesi: 2014 yılında, Danimarka Denizcilik Otoritesi 2012 yılında heklendiğini ve önemli bilgilerin başka bir devlet destekli, istenmeyen kişilerin eline geçtiğini fark etmiştir. Olay ekinde PDF formatlı bir evrak bulunan virüslü bir e posta ile başlamıştır. E postanın kurum personeli tarafından açılması sonucu korsanlar tüm sisteme erişim sağlamıştır. Durum fark edildikten sonra sistemin anti virüs yazılımı değiştirilmiştir (Lagouvardou, 2018). Amerikalı bir IT uzmanının, bilgisayar korsanları tarafından kontrol edildiği hali hazırda biliniyor olan Amerika'daki bir sunucuda Danimarka Denizcilik Otoritesine ait dosyaların bulunduğunu fark etmesi sonucu durumdan şüphelenmesi ve

konuyu ilgili kuruma rapor vermesi ile yapılan araştırmada kurumun heklendiği açıklığa kavuşmuştur (URL-4).

22) Avrupa'da Bir Liman: Liman içi konteynır hareketlerinin GPS bağlantılı bir otomasyon sistemi ile yönlendirildiği ismi verilmeyen bir Avrupa limanında "canı sıkılan" bir liman işçisinin GPS sinyallerini karıştırarak (Jamming) otomasyon sistemini heklemiştir. Sonuç olarak liman içi konteynır hareketleri 12 saat süresince yapılamamıştır (URL-5).

23) Aramco: 2012 yılında şirket personeline gönderilen oltalama e postası içerisindeki virüslü bir link personel tarafından açılmıştır. Durum, şirket bünyesindeki 35.000'e yakın bilgisayarın ya tamamen bozulmasına ya da içlerindeki tüm bilgilerin silinmesine neden olmuştur. Dünya genelinde kullanılan petrolün %10'unu arz eden Aramco, bu siber saldırı nedeniyle 17 gün süresince petrol satışı yapamamıştır (Lagouvardou, 2018).

24) Konteyner Gemisi Firması: 2016 yılında bir konteynır gemisi firmasının gemilerine korsan saldırmıştır. Saldırılar sırasında korsanlar, gemi personelini yaşam mahaline hapsetmekte sonrasında bazı konteynırları açıp içindeki yükü çalıp kısa zaman sonra gemiyi terk etmektedir. Olayın tekrarlanması, korsanların gemi personeline zarar vermemesi, gemiyi kaçırma eğilimi göstermemesi, tüm konteynırları açmak yerine sadece içinde değerli yük olan belirli konteynırlara yönelmesi sonucu firma teknik yardım istemiştir. Yapılan incelemelerde, firmanın kendi yaptığı İçerik Yönetim Sistemi (CMS) programını internet üzerinden kullandığı ve kullandıkları sunucuya daha önce kötü amaçlı web katmanı yüklendiği tespit edilmiştir. Korsanların bu katman sayesinde sisteme girebildikleri, hangi gemideki hangi konteynırda hangi yükün olduğunu, konşimento detaylarını, gemilerin ETA'larını öğrenebildiği anlaşılmıştır. Tespitler sonrasında şirketin bilgisayar sistemlerindeki eksiklikler giderilmiştir (Verizon, 2016).

25) Tahliye Operasyonu: 2017 yılında bir denizcilik firmasının gemisi tahliye operasyonu için bir limana girmiştir. Tahliye operasyonu tamamlandıktan sonra korsanlar tarafından tahliye operasyonuna ait gerçek faturalar ele geçirilerek taklitleri yapılmıştır ve gemi sahibi firmaya gönderilmiştir. Gemi sahibi firma faturaları gerçek zannedip korsanların banka hesabına ödemeyi yapmıştır. Firmanın yaklaşık 100.000 dolar zararı oluşmuştur (MDR, 2019).

26) Enrico Levoli Olayı: 27 Aralık 2011 tarihinde Basra Körfezi'nden Akdeniz'e kostik soda taşımakta olan Enrico Levoli isimli tanker korsanların fiziksel saldırısına uğramıştır. Gemide silahlı muhafız bulunmamaktadır (Belmont, 2016). Gemi korsanlar tarafından kaçırılmış ve 6 İtalyan, 5 Ukraynalı, 6 Hintli personel rehin alınmıştır. Olayın

detayları halen tam olarak çözülememiş olup, olayın daha önceki aylarda kaçırılan ve 5 İtalyan personeli bulunan Sarina Caylyn gemisinin 21 Aralık tarihinde serbest bırakılmasından bir hafta sonra gerçekleşmiş olması, ayrıca bu gemiden önce de 21 Nisan'da kaçırılıp 25 Kasımda serbest bırakılan ve 6 İtalyan personeli bulunan Rosalia D'Amato gemisi olayının yaşanmış olması mevcut olay üzerindeki şüpheleri arttırmaktadır (It-Sec-Spy, 2011). Olayın azmettiricisi olarak İtalyan mafyasından şüphelenilmektedir. Resmi olmayan bilgilere göre, İtalyan mafyası İtalyan personel bulunduran bahsedilen bu 3 gemi de dahil gemilerin sistemlerine siber korsanlık yoluyla sızıp, gemilere ait rota, yük, personel, konum ve hatta silahlı muhafız bulundurup bulundurmadığına kadar detaylı bilgiye ulaşmış ve eylem kısmını Somalili korsanlara yaptırmıştır (BIMCO, 2015).

27) Limasol Merkezli Denizcilik Firması: Ağustos 2015'de Limasol merkezli bir denizcilik firması Afrika'da sürekli yakıt tedarik ettiği bir yakıt firmasından, işlettiği bir gemi için yakıt ikmali yapmıştır ve işleme dair resmi faturasını almıştır. İlerleyen günlerde, Polonya'da oldukları düşünülen bilgisayar korsanları denizcilik firmasına bir e posta göndererek yakıt faturası bedelinin bir hesap numarasına yatırılmasını istemiştir. Bu hesap numarası, denizcilik firmasının Afrika'daki yakıt tedarikçisi firma ile her zaman kullandığı banka hesap numarasından farklı olmasına rağmen durumdan şüphelenilmemiştir ve para korsanların hesap numarasına yatırılmıştır. Sonuçta denizcilik firması 644.000 avro zarara uğramıştır (Belmont, 2016).

28) Açık Deniz Platformu: 2010 yılında inşa edildiği Güney Kore'den Güney Amerika'ya seyir yapmakta olan bir açık deniz petrol platformunun sevk ve idare bilgisayar sistemlerini virüs etkilemiştir. Virüsün tespiti ve sorunun giderilmesi 19 gün sürmüştür. Olay günlük 700.000 dolar ticari kayba neden olmuştur (Jones vd., 2016; Kaspersky, 2015).

29) İran Devlet Denizcilik Şirketi (IRISL): Ağustos 2011'de IRISL'e yönelik siber saldırı düzenlenmiştir. Siber saldırı sonucu, günlük ortalama tahliye / yükleme değerleri, konteyner numaraları, konteynerlere dair zaman ve yer bilgileri ile şirketin dahili haberleşme ağı etkilenmiştir. Şirket bu süre içinde konteynerlerin nerede olduğunu, yüklenip yüklenmediğini, hangi konteynırın hangi gemide veya hangi terminalde olduğunu bilemez duruma gelmiştir. Saldırı sonlandığında saldırının etkilediği bilgiler geri yüklenmiştir fakat durum operasyonel anlamda önemli sorunlara yol açmıştır. Yanlış yerlere gönderilen konteynırlar veya kaybolan konteynırlar önemli ticari kayıplara sebep olmuştur (Silgado, 2018).

30) Ice Fog Olayı: 2011 yılında başladığı tahmin edilen olay, Kaspersky şirketi tarafından 2013 Eylül ayında tespit edilmiştir ve Ice Fog adı verilmiştir. Aralarında Güney Kore ve Japonya'daki tersane ve gemicilik sektöründe faaliyet gösteren şirketlerin de bulunduğu kurbanlar durumdan etkilenmiştir. Amaç, şirketlerin belge, e posta hesabı ve parolalarına ulaşmaktır. Bu saldırıları önemli kılan özellik, korsanların saldırıyı şirket tarafından fark edilene kadar sürdürme çabasında olmamalarıdır. Saldırılar birkaç gün veya birkaç hafta sürmektedir. Bu da korsanların ne aradıklarını veya neyin peşinde olduklarını bildiklerini, aradıklarını elde ettikten sonra fark edilmeden sistemden kendilerini temizlediklerinden anlaşılmaktadır (Kaspersky, 2013; CyberKeel, 2014).

31) BW Group Singapore: Temmuz 2017'de dünyanın önde gelen denizcilik şirketlerinden BW Group Singapore siber saldırıya uğramıştır. Bilgisayar sistemleri heklenmiş, internet ve intranet sistemleri geçici süreliğine durmuştur. Olay şirketin başka yerlerle iletişimini ve dolayısıyla tüm şirket, gemi ve deniz operasyonlarını etkilemiştir. Olay bir fidye yazılım ile fidye talebi içermemektedir (Silgado, 2018; URL-6).

32) Somali Korsan Bölgesi: Somali açıklarında ve Aden Körfezinde faaliyet gösteren korsanlar, bilgisayar korsanlarını kullanarak denizcilik şirketlerinin bilgi sistemlerine ve gemi takip sistemlerine erişim sağlayıp değerli yük taşıyan gemileri tespit edebilmiş ve bu gemilere saldırı yapmaya çalışmıştır. Bu yöntemle konumlarının korsanlar tarafından tespit edilmesini önlemeye çalışan gemi personeli ve şirketler gemideki AIS cihazını kapatma yöntemini seçmiş fakat bu da seyir emniyeti açısından bölgede ayrı riskler oluşturmuştur (Muccin, 2016b).

33) Avustralya Gümrüğü: 2012 yılında bir suç şebekesi Avustralya Gümrüğü'nün kullanmakta olduğu elektronik yük sistemine sızmayı başarmıştır. Suç şebekesi böylelikle gemilerle gelip limanda bekleyen yasa dışı madde içeren kendilerine ait konteynerlerin gümrük otoritesi veya polis tarafından şüpheli olarak değerlendirilip değerlendirilmediğini kontrol etmektedir. Eğer konteynır sistemde şüpheli olarak işaretlenmişse suç şebekesi konteynırı teslim almamakta ve böylelikle ifşa olmamaktadır. Olaydan sonra yapılan araştırmalarda gümrük tarafından kullanılan bilgisayar sisteminin dışarıdan kolayca erişime uygun olduğu anlaşılmıştır (CyberKeel, 2014).

34) Fidye Yazılıma Maruz Kalan Gemi Acentesi ve Armatör: Armatörlük şirketi, şirket bilgisayar sisteminin bir e postanın ekinden bulaşan fidye yazılıma maruz kaldığını bildirmiştir. Fidye yazılımın kaynağının ayrı limanlarda ve ayrı zamanlarda çalışılan kasıtsız iki acente olduğu anlaşılmıştır. İlgili e postalardan, e postaların ulaştığı gemiler de

etkilenmiştir fakat seyir veya operasyonel sistemleri zarar görmemiştir. Bahsedilen olayların bir tanesi için armatörlük şirketi miktarı belirtilmeyen fidye ödemek zorunda kalmıştır (BIMCO, 2020).

35) IT ve Operasyonel Teknolojiler (OT) Sistemlerine Solucan Saldırısı: Yeni inşa olan bir gemide güç yönetim sistemi bulunmaktadır. Sistem, internete bağlı çalışması halinde yazılım güncellemesi, yazılım yaması eklemesi, uzaktan arıza tespiti, bilgi toplama ve uzaktan erişim ile işlem yapılabilmesi amaçlı kullanılabilmektedir. Mevcut durumda ise sistem internete bağlı kullanılmamaktadır. Sistemin internete bağlanması için gemiye gelen şirketin IT personeli sistemde herhangi bir zafiyet olup olamadığı konusunda çalışma yaparken, sistem internete bağlanır bağlanmaz aktif hale gelecek bir solucan tespit etmiştir. Durum güç yönetim sistemi üreticisi firmaya bildirilmiştir. Üretici firma kendi içinde yapmış olduğu araştırma sonucu, konu sistemin kullanıldığı tüm sunucularda bu solucanın bulunduğu ve 875 gündür tespit edilemeden tüm sistemlerde var olduğu anlaşılmıştır. Solucan sistemden uygun şekilde tamamen silinmiştir. Kaynağının bir servis tedarikçisi olduğu ve gemi sistemlerine yazılım güncellemesi sırasında bilgisayara bağlanılan USB bellek ile bulaştığı anlaşılmıştır (BIMCO, 2020).

36) Yakıt Sörveyörü**:** Limanda yakıt alım operasyonunu tamamlayan bir kuru yük gemisinde yakıt sörveyörü, operasyona dair evraklarının çıktısını alabilmek amaçlı makine kontrol odasındaki bilgisayarı kullanmıştır. USB belleğini bilgisayara bağlayınca içinde var olduğunu bilmediği virüs gemi sistemlerine bulaşmıştır. Bir süre sonra gemi personeli gemi bilgisayarlarında sorun olduğunu şirkete rapor etmiştir, siber değerlendirme yapılmış ve virüs tespit edilmiştir (BIMCO, 2020).

37) Ana Sunucuya Bulaşan Fidye Yazılım: Geminin ana sunucusuna bulaşan bir fidye yazılım tüm IT altyapısının çökmesine sebep olmuştur. Fidye yazılım, sunucudaki tüm kritik dosyaları şifrelemiş, hassas bilgilerin yitirilmesine ve geminin kullanması gereken uygulamaları kullanamamasına sebep olmuştur. Sunucudaki sorun onarılsa da her defasında sorun tekrarlanmıştır. Yapılan incelemede sorunun zayıf parola uygulaması olduğu ve saldırganın bu zaaf ile sisteme kolayca ve başarıyla erişebildiği anlaşılmıştır. Olayın tekrarlanmaması için IT departmanı gemi sistemine onaylanmamış kişilerin girişini engellemiş ve şifre uygulaması güçlendirmiştir (BIMCO, 2020).

1.11. Literatürdeki Çalışmalar

Denizcilik alanında siber güvenlik konusunda birçok çalışma mevcuttur. Bunlar genel olarak siber güvenlik farkındalığını, risk değerlendirmesini, sistemlerin siber saldırılara karşı durumlarını analiz eden ve saldırılardan korunma amaçlı önerileri içeren teknik çalışmaları konu almaktadır. Tez çalışmasına konu olan gemi seyir yardımcılarına ilişkin teknik ve deneysel çalışmalar aşağıda daha detaylı olarak açıklanmıştır.

Grant vd. (2009), GPS sinyali karıştırma deneyleri gerçekleştirmiştir. GPS L1 frekansının 2 Mhz bant genişliğinin tümünde gönderim yapabilen sinyal karıştırıcı NLV Pole Star isimli gemiye yerleştirilmiştir, seyir sırasında karıştırıcı çalıştırıldığında geminin GPS sinyali kaybolmuş ve bu dinamik deney ile karıştırıcının etkili çalışır olduğu ispatlanmıştır. Statik deneylerde Flamborough Feneri'ne yerleştirilmiş karıştırıcının kapsama alanına giren NLV Pole Star'ın GPS sinyali yitirilmiş, 10 dakika boyunca çeşitli köprüüstü sistemlerinden alarmlar gelmiştir, ECDIS'in donduğu görülmüştür. Bu deney sırasında geminin mevkii eLORAN ile de takip edilmiş ve eLORAN sinyal karıştırma sürecinden etkilenmemiş, hep doğru mevki tespit etmiştir (Şekil 12). İkinci statik deneyde karıştırıcı, DGPS referans istasyonu yakınlarında çalıştırılmıştır. İstasyonun sinyalleri karıştırıcıdan etkilenmiştir, istasyonun görmesi gereken uydu değerleri kullanılacak uydu kalmayana kadar düşmüştür.

Şekil 12. eLORAN sisteminden ve Gps'den alınan mevkilerin karşılaştırılması (Grant vd., 2009).

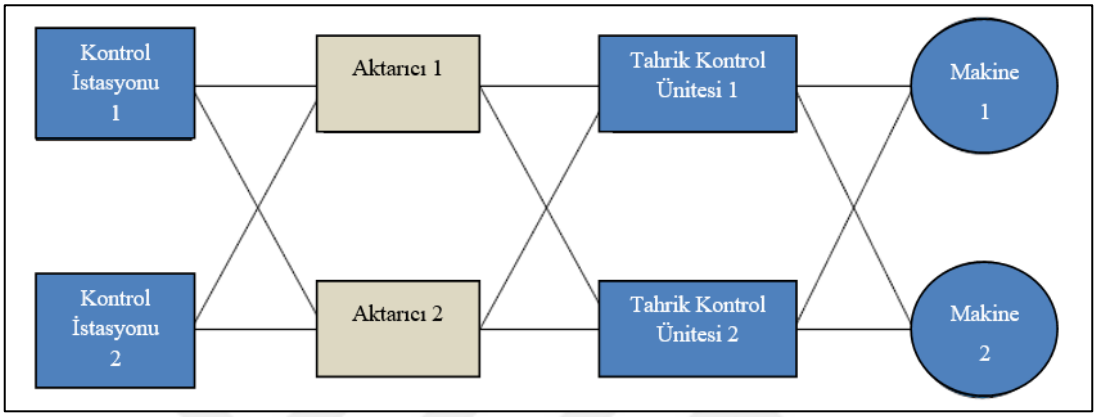
Üçüncü statik deneyde, değişik marka ve model GPS alıcıları test edilmiştir. Karıştırıcı çalıştırıldığında hepsinde sinyal kaybolmuştur. Birbirini takip eden hatalı mevki değerleri nedeniyle bazı gemilerin 100 knotın üzerinde hızları olduğu görülmüştür. GPS üzerinden doğrulama yapan AIS verilerinde de hatalar gözlenmiştir. Radar ekranında gerçek ekosu kare ile işaretli bir geminin daire ile işaretli AIS mevkii radardaki mevkiinin önemli mesafede kuzeyinde görülmüştür. Ayrıca bazı gemilerin mevkileri karada, bazı gemilerin geçmiş AIS izlerini birleştiren çizgilerin ise defalarca kara üzerinden geçmiş olduğu görülmüştür (Şekil 13).

Şekil 13. AIS bilgilerindeki hatalar (Grant vd., 2009).

Sonuç olarak, INS ile seyir yapabilen geminin belirlenmiş seyir planı üzerinde otomatik dümen ile dış müdahaleye ihtiyaç duymadan seyir yaptığı (track mode) durumun en tehlikeli koşul olduğu belirtilmiştir. GPS sinyallerinin karıştırılması sonucu INS'in hiçbir alarm vermemesinin ve karıştırılan sinyalleri doğru kabul edip rota değişikliği yapmasının gemiyi tehlikeye sürükleyebileceği ifade edilmiştir. GPS sinyallerinin karıştırılması sonucunda cihaz verilerinin kullanılamaz duruma gelmesi halinde yedek sistem amaçlı veya herhangi bir durumda GPS verilerinin karşılaştırılması amaçlı gemilerde GPS ile eLORAN veya GALILEO sistemlerinin beraber kullanılması önerilmiştir.

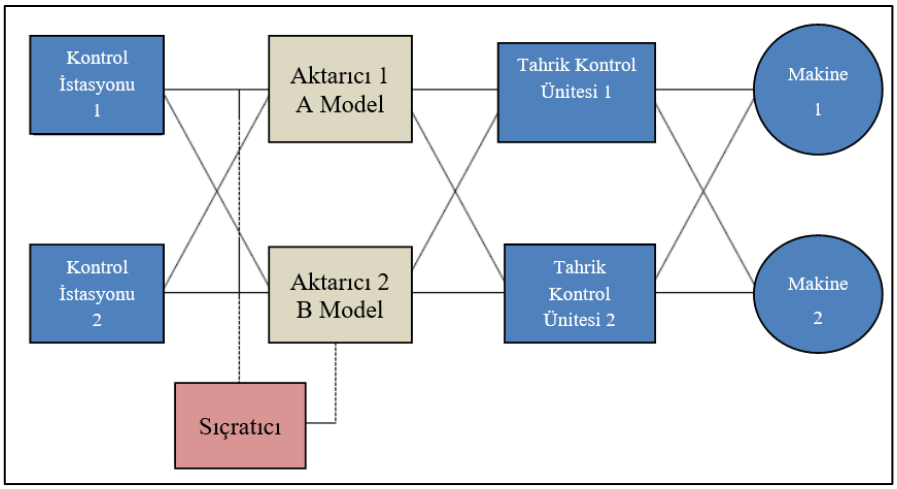
Babineau vd. (2012), gemilerde kullanılmakta olan otomasyon kontrol sistemlerinde siber güvenliği arttıracak bir dizayn modeli önermektedir. Otomasyon sistemleri, daha az personel ve daha düşük bakım masrafları ile ekipmandan yüksek verim alınması amacıyla kullanılmaktadır. Makinelerin uzaktan görüntülenebilmesine ve uzaktan kontrolüne imkan

sağlamak amacıyla günümüzde sistemleri internete bağlı şekilde çalışmakta olan gemi sayısının artmıştı olduğu belirtilmiştir. Bu detay, otomasyonun üstün getirilerinin yanında yüksek siber güvenlik riskleri taşıdığını da gündeme getirmiştir. Çalışmanın temelini 2 adet makineden, 2 adet tahrik kontrol ünitesinden, 2 adet aktarıcıdan ve 2 adet kontrol istasyonundan oluşan sadeleştirilmiş bir kontrol sistemi dizaynı oluşturmaktadır (Şekil 14).



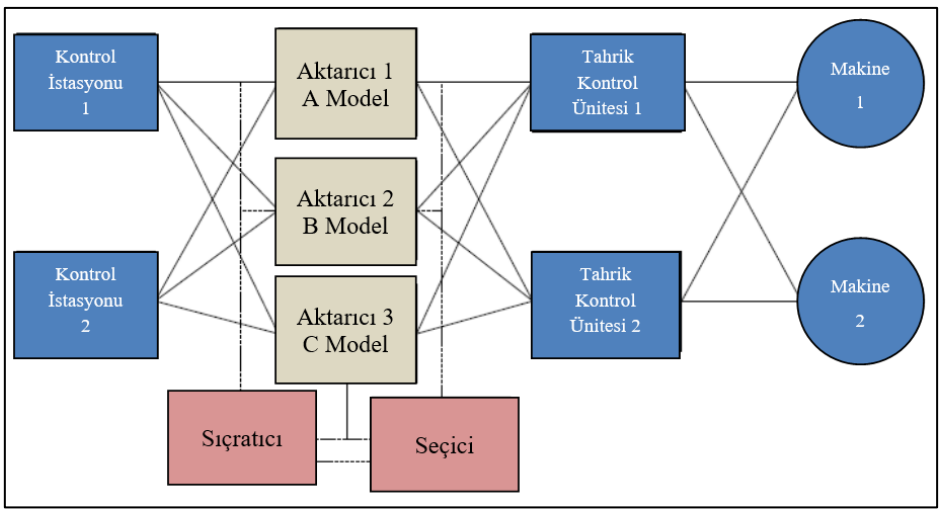
Şekil 14. Sadeleştirilmiş kontrol sistemi dizaynı (Babineau vd., 2012).

Tahrik kontrol sistemi, kontrol istasyonundan verilip aktarıcıdan geçen komutu (makineyi stop et veya çalıştır, devri artır veya azalt gibi) uygulayıp makineyi işleten unsurdur. Bu dizaynda 1 numaralı aktarıcı bir siber saldırı sonucu bilgiyi tahrik kontrol ünitesine aktaramaz duruma gelirse 2 numaralı aktarıcının devreye alınması halinde sistem çalışmaya devam edecektir. Genel uygulama olarak 2 aktarıcının da aynı marka ve model olması yedek parça ve işletim ekonomisi anlamında tercih edilen yöntemdir. Fakat siber saldırı açısından tek bir saldırı ile aynı özellikteki bu 2 eleman da devre dışı bırakılıp sistem kontrol edilemez duruma getirilebilir. Bu nedenle iki farklı marka ve model aktarıcı ile bu aktarıcılardan birinde tehdit algılandığında sinyali diğer aktarıcıya çevirecek bir sıçratıcının (hopper) bulunduğu bir dizayn değerlendirilmiştir (Şekil 15). Bu dizayn üzerinde yapılan testlerde bir aktarıcıdan diğerine geçerken istenmeyen zaman kaybı ve bilgi kaybı yaşandığı tespit edilmiştir.



Şekil 15. Sıçratıcı eklenmiş kontrol sistemi dizaynı (Babineau vd., 2012).

İstenmeyen bu hataların giderilmesi için sıçratıcı yerine seçici (voter) kullanımı değerlendirilmiştir. Tehdit algılanan aktarıcının devre dışı bırakılmasından sonra seçicinin en uygun aktarıcıyı seçebilmesi için en az 2 aktarıcının daha olması gereklidir. Böylelikle sistemde 3 farklı marka ve model aktarıcı ile maliyet olarak ekonomik ve basit bir seçici kullanılmıştır (Şekil 16). Bu seçici ile dizayndan sınırlı verim alınmıştır. Daha karmaşık, programlanabilir bir seçici kullanılması halinde daha fazla tehdidin önlenebileceği fakat bu sistemin maliyetinin çok fazla olacağı değerlendirilmiştir. Sonuç olarak 3 değişik marka ve model aktarıcı, 1 adet sıçratıcı ve 1 adet seçiciden oluşacak sistem oluşturulmuştur.



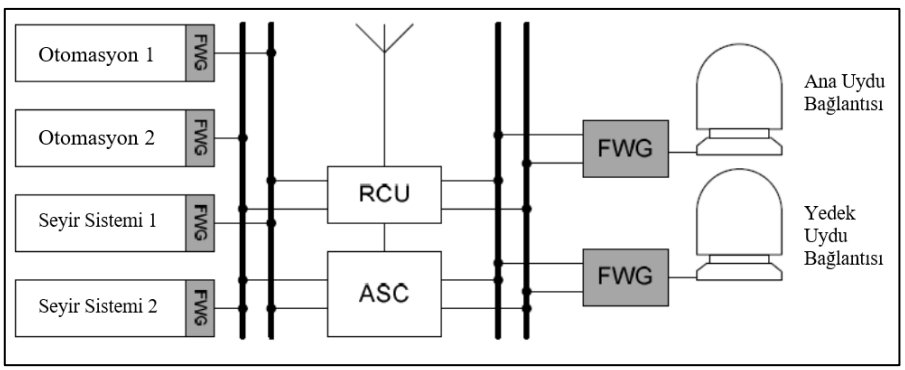
Şekil 16. Sıçratıcı ve seçici eklenmiş kontrol sistemi dizaynı (Babineau vd., 2012).

Yapılan simülasyonlarda bu dizaynın diğerlerine göre maliyet ve verim açısından gemilerde kullanıma en uygun dizayn olduğu değerlendirilmiştir. Tablo 2'de değerlendirme tablosu verilmiştir. Belirlenen 6 kriter kendi içlerinde ağırlıklandırılmış ve 1'den 10'a kadar bir değerle değerlendirilmiştir. Yüksek maliyet faktörü değeri düşük maliyet tutarı, yüksek güvenlik faktörü değeri ise yüksek güvenlik sağlanması anlamındadır.

Tablo 2. Önerilen dizaynların güvenlik ve maliyet açısından değerlendirmesi (Babineau vd., 2012).

	Güvenlik Faktörü			Maliyet Faktörü			Güvenlik Faktörü Toplamı	Maliyet Faktörü Toplamı
	Caydırıcılık	Gerçek Zamanlı Savunma	İyileştirme	Teknik Performans	Kurulum Maliyeti	Kullanım Ömrü Maliyeti		
Ağırlık Çarpanı	0,4	0,4	0,2	0,5	0,25	0,25		
Temel Dizayn	1	1	1	10	10	10	1	10
Sadece Sıçratıcılı Dizayn	5	4	1	4	4	4	3,8	4
Sadece Seçicili Dizayn	4	5	8	8	6	6	5,2	7
Sıçratıcılı ve Seçicili Dizayn	8	7	8	4	3	3	7,6	3,5

Røsdeth vd. (2013), otonom gemilerde kullanılabilecek ve siber güvenlik açısından da verimli bulunan bir gemi içi sistem ağı dizaynı önermiştir. Şekil 17'de önerilen dizayn gösterilmektedir.



Şekil 17. Otonom gemiler için gemi içi ağ dizaynı (Røsdeth vd., 2013).

Çift köprüüstü seyir sistemi ve yine çift makine kontrol sistemi bulunan dizaynda bu sistemlerin yedeklenebilir şekilde birbirine bağlanması ve iki ayrı uydu bağlantı sisteminin oluşturulması önerilmektedir. Ana uydu bağlantısı olarak C, Ku veya Ka bandında VSAT, yedek uydu bağlantısı olarak ise L-band Inmarsat veya Iridium önerilmiştir. Otonom Gemi Deneteleyicisi (ASC) otonom sistemlerin ana işletim sistemidir. Buluşma Kontrol Ünitesi (RCU) ASC ile kara bağlantısı kesildiğinde otonom geminin kara ekibindeki görevliler ile buluşmak için daha önce belirlenmiş bir noktaya giderken kullanılacak işletim sistemidir. FWG, güvenlik duvarı (Firewall) ve ağ geçididir (Gateway), sistemin limitleri içinde güvenliğini ve tutarlılığını sağlamaktadır. Sistemin elektrik enerjisi birbirini yedekleyen ve acil durum güç kaynağını da içeren bir düzende sağlanmaktadır. Bilgi aktarımının, yetkisi olmayan kişilerin erişemeyeceği şekilde şifrelenmiş olması gerekmektedir. Bu amaç için ek gönderimler ile Kullanıcı Veribloğu İletişim Kuralları (UDP) veya ara bellek (Buffer) kapalı şekilde Gönderi Kontrol Protokolü / İnternet Protokolü (TCP/IP) yöntemlerinin kullanılabileceği önerilmiştir. UDP, ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımında kullanılmaktadır. Veri iletim süresini azaltır fakat güvenilir olmayan bir aktarım protokolüdür, paketi gönderir ama gidip gitmediğini takip etmez, paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur. Güvenilir bir akış protokolü kullanılmasının da saldırıların engellenmesi için yararlı olacağı belirtilmiştir.

NCC Group (2014), siber güvenlik konusunda uzmanlaşmış bir bilişim şirketidir. Yapılan çalışmada, gemilerde yaygın olarak kullanılmakta olan ismi belirtilmemiş önde gelen bir ECDIS markasına ait cihazın siber tehditlere karşı güvenlik riskleri araştırılmıştır. Çalışma, Windows 7 işletim sistemiyle çalışan, anti virüs programı bulunmayan, güvenlik duvarı kapalı, sadece temel ayarları yapılmış demo ürün üzerinde yapılmıştır. Sonuç olarak 4 adet önemli zafiyet tespit edilmiştir. Tespit edilen bu zafiyetler doğrultusunda genel siber güvenlik önlemleri önerilmiştir. Bunlar,

- ECDIS üreticilerinin kendilerini güvenlik açıklarına karşı sürekli geliştirmeleri gerektiği,
- Sistem güncellemelerinin zamanında ve belirli prosedürlere uygun yapılması gerektiği,
- ECDIS güncellemeleri için kullanılacak CD veya USB belleğin ECDIS'e sokulmadan önce virüs taramasının yapılması gerektiği,
- Gemi içi bilgisayar ağının güvenlik durumuna göre ECDIS'in bu ağa bağlı olarak mı yoksa ağdan bağımsız olarak mı çalışmasına karar verilmesi gerektiği,

- Sorumlu personel dışındaki personelin ECDIS'e fiziksel erişiminin engellemesi gerektiğidir.

Yüksek hızlı geniş bant (high speed broadband) olan Ka bandı ile 50 Mpds'e varan hızlarla uydu iletişimin mümkün hale geldiği belirtilmiştir. Bunun da, gemilere yönelik güvenlik açıklarını ve tehdidini günümüzde en çok arttıran unsur olduğu vurgulanmıştır.

Balduzzi vd. (2014a, 2014b), AIS sistemini yazılım ve radyo frekansı anlamında donanım özellikleriyle siber güvenlik açısından incelenmiştir. Çalışmada aşağıdaki deneyler yapılmıştır,

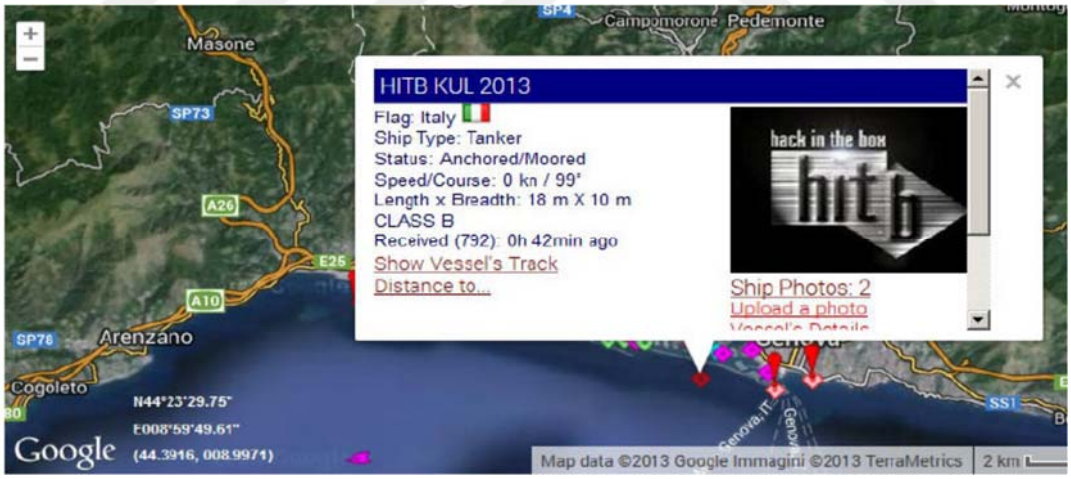
- AIS iletişiminin kesilmesi,
- Mevcut AIS bilgilerinin değiştirilmesi,
- Sahte tehlike alarmı verilmesi,
- Bir deniz alanındaki AIS verilerinin kontrol altına alınması,
- AIS verilerinin yanıltılması ile gemiyi farklı rotada gösterip var olan çatışma riskinin yokmuş gibi gösterilmesi,
- Geminin rota bilgisiyle oynanıp başka bir gemiyle çatışma durumu yaratılması, geminin sakınma manevrası yapması ve böylelikle bir tehlikeye doğru ilerlemesinin sağlanması.

Üretilecek sahte sinyallerden ötürü herhangi bir kazaya sebebiyet vermemek adına denize 200 km mesafede karada gerçekleştirilen deneylerde, değişik anten tipleri test edilerek 16,5 kilometreye kadar hatalı AIS sinyali gönderimi sağlanmıştır. AIS cihazının içerisinde, internet ortamında hizmet veren Marine Traffic veya Vessel Finder gibi sitelere bilgi aktarılmasını da sağlayan bir yazılım olduğu belirtilmiştir. Fakat deniz araçlarının AIS bilgilerini internette yayınlayan bu sitelerin kendilerine gelen sinyalleri doğrulayacak bir mekanizma kullanmıyor olduklarını belirtilmiştir. Yapılan deney ile var olan bir geminin ilk mevkii karada olacak şekilde seyre başlatılmış, "PWNED" harflerinin birleştirilmesiyle oluşan bir rotada seyir yaptırılmıştır. Bu yapay işlem internette AIS bilgilerinin paylaşılması hizmetini veren önde gelen 3 sitede normal bir durum gibi görüntülenmiştir (Şekil 18). Başka bir deneyde ise gerçekte olmayan "HITB KUL 2013" isimli gemi oluşturulup Marine Traffic web sayfasında başarı ile yayınlanmıştır (Şekil 19).

Sonuç olarak; AIS siteminin yanıltma, ele geçirme ve DoS saldırılarına karşı hassas olduğu belirtilmiştir. İnternet sitelerinin ve VTS'lerin, gemilerin rota veya statik bilgilerindeki ani ve şüpheli değişiklikler gibi AIS bilgilerindeki gerçeğe aykırılıkları tespit edilebileceği bir yöntem kullanılması gerektiği belirtilmiştir. AIS bilgilerinin uydudan

alınacak bilgiler ile eşleştirilip uyuşmazlıkların tespit edilebileceği, AIS istasyonlarının birbirlerine gönderdikleri mesajları X509 gibi Açık Anahtar Altyapısı (PKI) kullanarak doğrulayabileceği bir sistemin oluşturulabileceği önerilmektedir.

Şekil 18. Var olan bir geminin AIS bilgilerine etki edilmesi (Balduzzi vd., 2014a).



Şekil 19. Var olmayan bir geminin AIS sisteminde oluşturulması (Balduzzi vd., 2014a).

IOActive (2014) isimli teknoloji şirketi, gemilerde kullanılmakta olan uydu haberleşmesi sistemlerinde (SATCOM) siber tehdit oluşturabilecek unsurlara ilişkin bir araştırma yapmıştır. Çalışma kapsamında Inmarsat C, Çok Küçük Açıklıklı Terminal (VSAT), Geniş Bant Küresel Alan Ağı (BGAN), BGAN M2M, FleetBroadband,

Swiftbroadband, Classic Aero Service sistemleri incelenmiştir. Çalışmanın sonucunda incelenen tüm sistemlerde siber güvenlik açığı tespit edilmiştir. Tüm cihazların uzaktan erişime açık oldukları hatta bazı cihazların SMS veya özel bir mesaj ile dahi kontrol altına alınabileceği tespit edilmiştir. Gemilerde sıklıkla kullanılmakta olan FleetBroadband sisteminde tespit edilen güvenlik açıklarının, içerisinde ECDIS'in de bulunduğu seyir sistemlerinin uzaktan kontrol edilebilmesine, saptırılabilmesine imkan verdiği belirtilmiştir. Sailor 6000 gibi sistemlere zararlı yazılım yüklenebileceği ve haberleşme sisteminin uzaktan kontrol altına alınabileceği, hatta güvenlik açısından önemli bir rolü olan Gemi Güvenlik Uyarı Sistemi'nin (SSAS) dahi Inmarsat Mini-C üzerinden saldırganlar tarafından kontrol altına alınabileceği açıklanmıştır. Sonuç olarak aşağıdaki zafiyetleri tespit edilmiştir,

- Başka kullanıcılara ait parolaların kolaylıkla resetlenebilmesi,
- Kullanıcıların amacına uygun olmayan kayıt dışı protokollerin güvenlik riski oluşturuyor olması,
- Kayıtlı protokollerin güvenlik riski oluşturuyor olması,
- Kullanıcı etkileşimi için mevcut olması gereken kayıtlı ara yüz doğrulama işlemi için kayıt dışı protokollerinin kullanılıyor olması,
- Kullanıcıların amacına uygun olmayan kayıt dışı özelliklere ve ara yüzlere erişiminin mümkün olması.

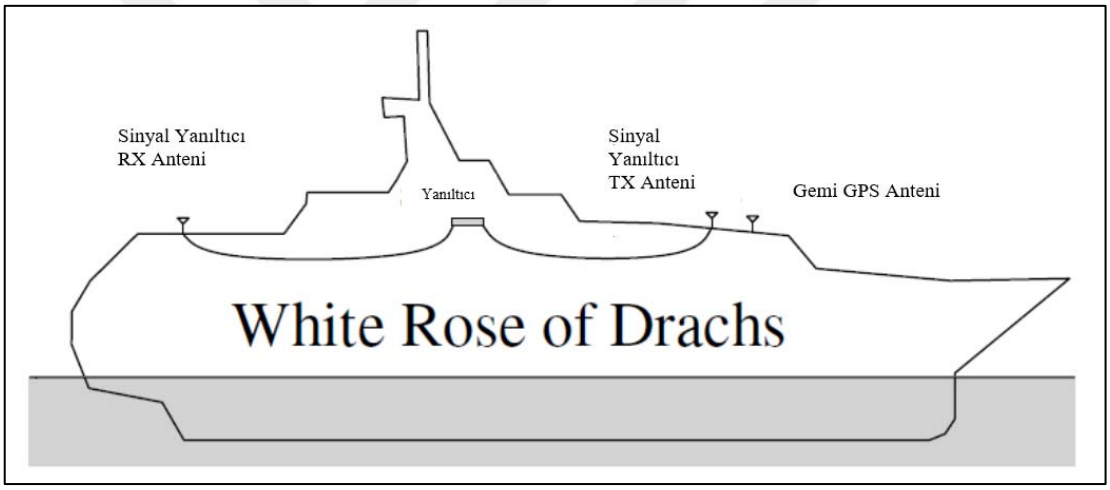
Bolat vd. (2016), Türk denizcilik sektöründeki 249 katılımcı ile 5 soru içeren, siber güvenlik farkındalığını ölçmeyi amaçlayan anket çalışması gerçekleştirmiştir. Yöneltilen sorular şunlardır,

- Denizcilik sektörü bilgi ve haberleşme teknolojilerine aşırı derecede bağımlı mıdır?
- Güverte sistemlerinden hangisi siber saldırılara karşı ne kadar zayıftır?
- Gemi kaptanları ve sistem operatörleri edindikleri bilgi içerisinde hata olduğunu ne derecede ayırt edebilir ve sorgulayabilir?
- Gemi personeli online işlemlere dair güvenlik protokollerini anlayabilir ve uygulayabilir mi?
- Gemi elektronik ekipmanlarının bakım ve güncelleme konusunu engelleyen faktörler nelerdir?

Birinci soruya 167 katılımcı evet cevabı vermiştir, ikinci soruya 101 katılımcı ECDIS, 92 katılımcı AIS, 85 katılımcı Küresel Uydu Seyir Sistemi (GNSS), 76 katılımcı da GPS orta düzeyde siber saldırılara karşı korunmasızdır cevabı vermiştir. Üçüncü soruya 114

katılımcı hataların genelde fark edildiğini, 31 katılımcı ise hataların çoğunun farkına varılmadığını belirtmiştir. Beşinci soruya 115 katılımcı masraflar, 58 katılımcı farkındalık eksikliği, 47 katılımcı ise eğitim cevabını vermiştir. Sonuç olarak, kural eksikliklerinin düşük siber güvenlik bilincine sebebiyet verdiği ve taşımacılık endüstrisi için siber güvenlik eğitiminin önemli bir konu olduğu belirtilmiştir.

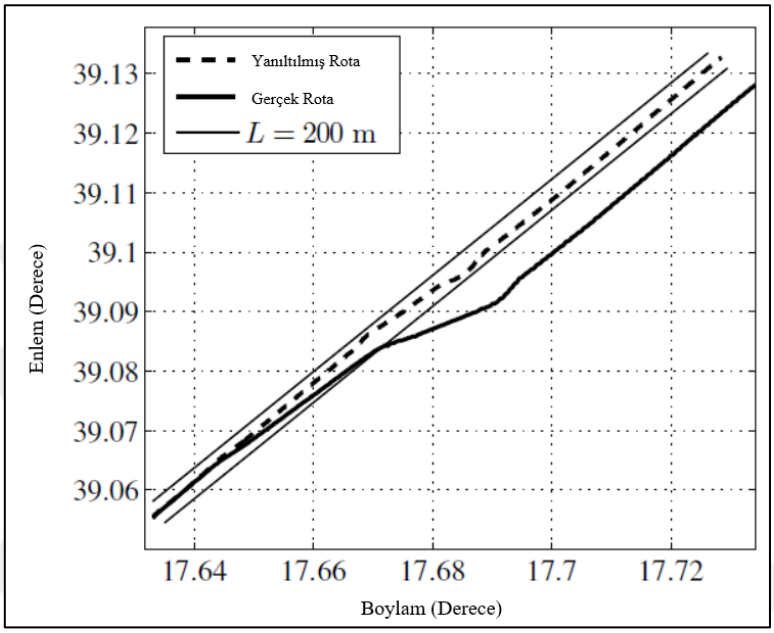
Bhatti ve Humphreys (2016), yaptıkları deney ile sivil denizcilik taşımacılığının yanıltılmış GPS sinyallerine karşı hassaslığını göstermeye çalışmıştır. Ayrıca, modern gemilerde hali hazırda mevut olan sensörlerin kullanılmasıyla bu yanıltmayı tespit edebilecek bir teknik geliştirmek amaçlanmıştır. Deney sırasında kullanılan ekipman, toplam değeri yaklaşık olarak 2.000 dolar olan laptop, Texas Üniversitesi tarafından geliştirilmiştir el yapımı taşınabilir GPS sinyali yanıltıcısı ait verici ve yazılımdır (Şekil 20).



Şekil 20. Deney için kullanılan sinyal karıştırıcı düzeneği (Bhatti ve Humphreys, 2016).

Deney için, Monako'dan Rodos'a seyri sırasında 80 milyon dolar değerinde, 65 metre uzunluğundaki süperyat White Rose of Drach kullanılmıştır. Yanıltma saldırısı manevralarının şiddeti, gemi personelinde, geminin akıntı veya rüzgar nedeniyle rotasından düşüyor izlenimi yaratacak şekilde ayarlanmıştır. Saldırı üç aşamada planlanmıştır. Birinci aşama yumuşak bir manevra, ikinci aşama sert bir manevra üçüncü aşama ise mevcut rotaya paralel bir seyir olarak planlanmıştır. Saldırı boyunca gemi kaptanı yatı rotasında tutmak için ±200 metrelik koridor içinde dümen manevraları yapmıştır. Şekil 21'de deneyin aşamaları grafiklenmiştir, deney süresince yatın ilerlediği gerçek rota düz kalın çizgidir, yanıltılmış GPS sinyallerinin oluşturduğu, harita üzerinde görünen rota ise kesikli çizgidir.

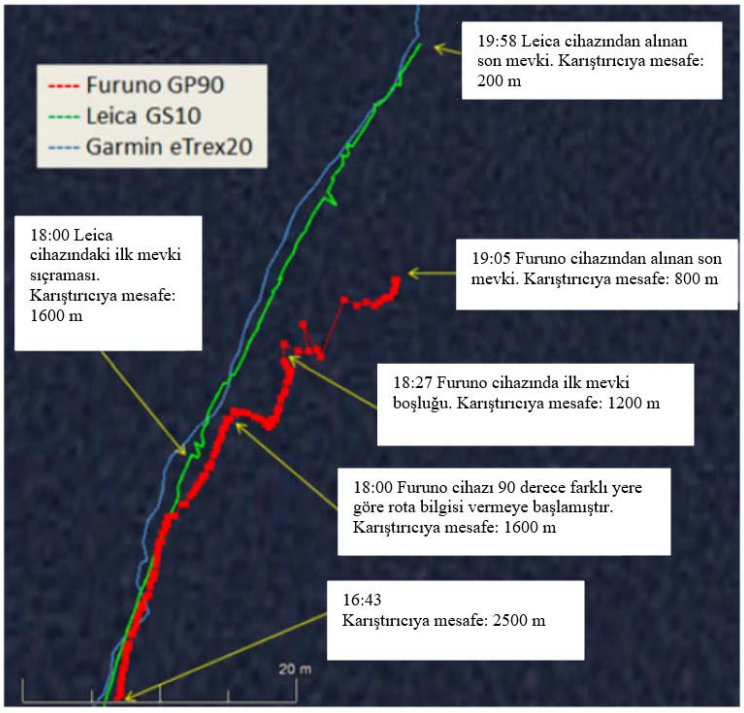
GPS sinyallerinin yanıltıldığının tespiti için, çevresel etmenler olan akıntı ve rüzgar değerlerini temel alan, doopler parakete, gyro pusula ve GNSS sinyallerinin ölçümünün kullanıldığı, istenildiğinde gemide mevcut ECDIS yazılımına da entegre edilebilecek dinamik bir model oluşturulmuştur. Deney sırasında bu model Monte-Carlo simülasyonu ile başarılı şekilde test edilmiş ve uygulanabilir olduğu görülmüştür.



Şekil 21. Deney sırasında yatın izlediği gerçek rota ve yanıltılmış rota (Bhatti ve Humphreys, 2016).

Heymann vd. (2016), dünya ticaretinde önemli yere sahip olan denizcilik sektöründe kullanılan bilişim teknolojilerindeki potansiyel güvenlik açıklarının kötü sonuçlar doğurabileceğini belirtmiştir. Bu sonuçların önlenebilmesi amaçlı kullanılmakta olan MITIGATE, MEDUSA, CYSM gibi klasik risk değerlendirme modellerinin riskin tanımlanmasından öteye geçemediğini, bilgi iletişim teknolojilerine yönelik değil de liman operasyonlarına yönelik olmalarından dolayı yetersiz olduklarını savunmuştur. İlk İlke Güvenlik Açığı Değerlendirmesi'nin (FPVA) sektör için daha uygun bir seçim olacağını belirtmiştir. FPVA'nın en önemli avantajı, mevcut güvenlik açıklıkları dışında yeni güvenlik açıklarını da keşfetmesi ve keşfedilen bu güvenlik açıkları için kontrol yöntemlerini kullanıcıya sunmasıdır. Siber güvenlik konusunda bu yöntemle yapılacak risk değerlendirmelerinden sektörün daha verimli yararlanabileceği açıklanmıştır.

Glomsvoll ve Bonenberg (2016), modern gemilerin üst seviyede otomasyona sahip olduklarını, insan etkileşimi olmadan gemi ağına bağlı seyir ve operasyon sistemleri ile idare edilebileceklerini belirtmiştir. Gemilerin bu özellikleri itibariyle seyir sistemlerinin temel mevki belirleme unsuru olan GPS sinyalinin karıştırılması veya yanıltılması durumları dahil siber saldırılara karşı çok hassas oldukları açıklanmıştır. Bu amaçla, piyasada mevcut olan tek uydu sistemli ve tek frekanslı alıcıları sinyal karıştırma dayanıklılığı açısından çok uydulu ve çok frekanslı alıcılar ile uygulamalı olarak karşılaştırıp, sinyal karıştırma sorununa en dayanıklı çözümü bulmaya çalışmışlardır. İlk önce, birbirine çok yakın frekans değerleri bulunan L1 ve G1'den L1 frekans değerine daha yakın bir frekansta çalışan karıştırıcı ile kullanılacak alıcının tespiti için deney yapılmıştır. Garmin eTrex20 alıcısının, Furuno GP90 ve Leica GS10 alıcılarına göre sinyal karıştırılmasında daha dayanıklı olduğu tespit edilmiştir (Şekil 22).



Şekil 22. Test edilen alıcıların sinyal karıştırmaya karşı direnci (Glomsvoll ve Bonenberg, 2016).

Asıl deneylerde ise karada sabit duran alıcıya göre hareketli botun içerisindeki karıştırıcının mesafesi değiştirilerek farklı GPS uyduları ile L1 ve L2 frekanslarından, ayrıca farklı GLONASS uyduları ile G1 ve G2 frekanslarından ölçümler yapılmıştır. Sonuç olarak, sivil kullanıma açık GLONASS G1 frekansının GPS L1 frekansına göre sinyal

karıştırılmasına karşı daha dayanıklı olduğu tespit edilmiştir. GLONASS'ın sinyal karıştırma açısından GPS'e olan üstünlüğü nedeniyle tek frekanslı ve çok uydu sistemli alıcıların daha emniyetli olacağı savunulmuştur. Gemilerde şu an yaygın olarak kullanılmakta olan tek frekanslı (L1) tek uydulu (GPS) alıcılar yerine gemiler için siber güvenlik ve maliyet anlamında en kullanılabilir çözümün, tek frekanslı (L1 + G1) ve çok uydulu (GPS + GLONASS) alıcılar olacağı belirtilmiştir. Bunun dışında, hali hazırda G1 ve G2 frekanslarını beraber kullanan GLONASS alıcıları veya gelecekte yaygınlaşması planlanan L1 ve L5 veya L1 ve L2C frekanslarını beraber kullanabilen GPS alıcıları gibi çok frekanslı tek uydu sistemli çözümlerin de verileri birbiriyle karşılaştırma olanağı sunacağı için kullanılabileceği vurgulanmıştır.

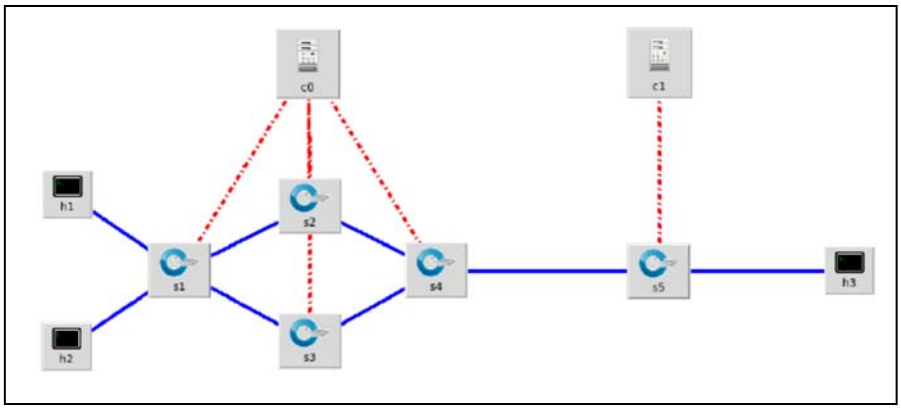
Koldemir vd. (2017), gemilerde ve limanlarda kullanılan bilişim teknolojilerinin genel olarak özetini yapmıştır. Bu teknolojilerin maruz kalabileceği siber saldırıları ve bu saldırıların sonuçlarını irdelemiştir. Gemilere, limanlara ve işletmelere yönelik siber saldırıların, deniz trafiğinin olumsuz etkilenmesi, maddi kayıpların oluşması veya hassas bilgilerin ele geçirilmesi gibi çeşitli sonuçlarının olabileceği belirtilmiştir. Siber güvenlik farkındalığının arttırılması, siber güvenlik politikasının oluşturulması gerektiği, siber güvenlik risk analizinin yapılması gerektiği, çalışanlara siber güvenlik eğitimi verilmesi, kullanılan sistemlerdeki zafiyetlerin belirlenmesi amaçlı sızma testlerinin yapılması, siber güvenlik konusunda faaliyet gösteren firmalardan danışmanlık hizmeti alınabileceği gibi unsurlar saldırının önlenmesi veya etkisinin en aza indirilmesi adına önerilmiştir.

Lee vd. (2017), gemide kullanılmakta olan AIS, GPS, ECDIS gibi siber saldırıya maruz kalabilecek cihazlara dair riskleri belirtmiştir. Sektörde meydana gelen siber saldırı olaylarının sonuçlarını paylaşmış ve bu saldırılara dair istatistiki verileri sunmuştur. Gemiadamlarının siber güvenlik konusundaki yeterlilikleri konusunu incelemişlerdir. BIMCO, JWC International, ASPIDA, CBS gibi gemiadamlarına yönelik siber güvenlik eğitimi veren kurumların eğitimlerinin içeriği irdelenmiş, gemiadamlarının eğitim ve göreve aşinalıkları açısından siber güvenlik ile ilgili Gemiadamlarının Eğitimi, Vardiya Tutma ve Sertifikalandırılması Hakkında Uluslararası Sözleşmesi'ne (STCW) eklenmesi gereken detaylar önerilmiştir.

Hassani vd. (2017), GNSS içerisinde en çok tercih edilen GPS'i temel seyir yardımcısı olarak kullanmakta olan günümüz gemilerinde GPS sinyallerinin dışarıdan müdahale edilip edilemeyeceğini ve bunun yaratacağı etkileri Nomoto ismi verilen bir model ile matematiksel olarak incelemişlerdir. İncelemede 3 ayrı senaryo üzerinde durulmuştur.

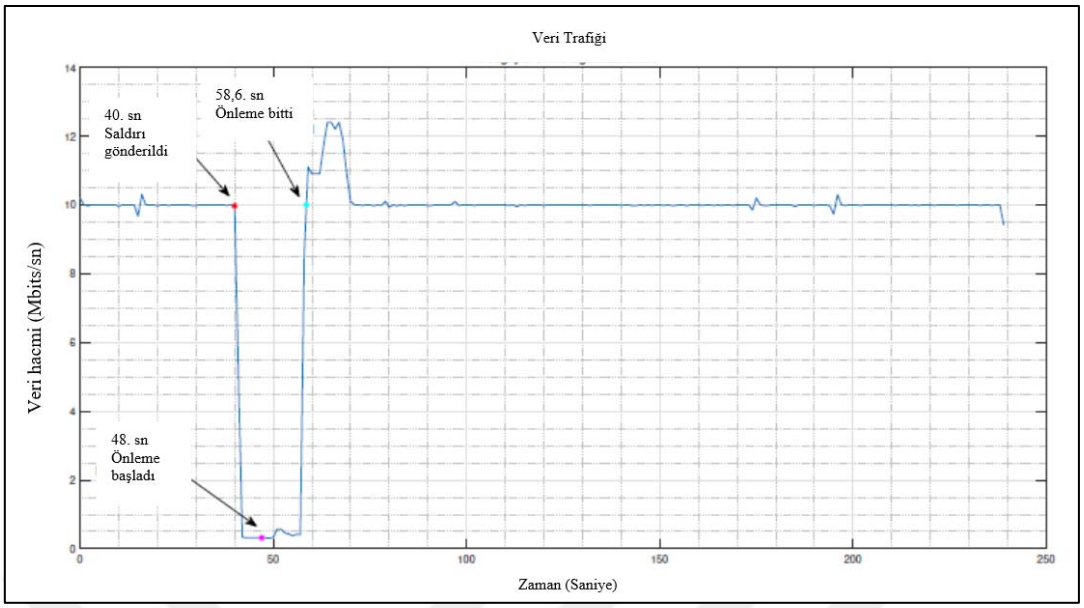
Birinci senaryoda geminin sadece GPS verisi ile seyir yaptığı ve otomatik dümenin bu verileri kullandığı varsayılmıştır. İkinci senaryoda geminin GPS'in yanı sıra bir de pusula ile seyir yaptığı ve otomatik dümenin her ikisi tarafından desteklendiği varsayılmıştır. Üçüncü senaryoda ise geminin gyro pusula ve GPS'den oluşan basit bir INS ile seyir yaptığı varsayılmıştır. 3 senaryo için de siber korsanların GPS sinyallerini saptırarak geminin pruva değerini istedikleri gibi kontrol edebilecekleri Nomoto modeli ile matematiksel olarak ispat edilmiştir. Üçüncü senaryo için yapılan simülasyonda, normal GPS sinyalleri ile ilk 200 saniye 10 derece rotasına ilerleyen gemide 200. saniyede GPS sinyalleri ile oynanmaya başlandığında 600 saniye sonra geminin pruva değerinin -20 derece olduğu belirtilmektedir. Çalışmanın sonucu olarak önleyici herhangi mekanizmanın olmadığı sistemlerde GPS sinyali ile oynanıp geminin pruva değerinin değiştirilebileceğinin matematiksel olarak ispatlandığı açıklanmaktadır.

Lagouvardou (2018), gemilerde kullanılmakta olan bilgisayar sistemlerinde karşılaşılabilecek siber saldırıları hafifletmek ve önlemek için Yazılım Tabanlı Ağlar (SDN) teknolojisini önermiştir. SDN, esnek programlanabilme özelliği itibariyle otomatik ve dinamik şekilde savunma mekanizması oluşturmaktadır. SDN, yeni geliştirilmekte olan bir bilgisayar modeli olup bilgi paketlerinin iletimi ve yönlendirilmesi ile açık ve programlanabilir ağların kullanılabilmesini sağlamaktadır. SDN ile oluşturulan modelde, Python, Ryu Controller, Mininet ve Open Flow Protocol kullanılmıştır. Python programlama dilidir. Ryu Controller, ağı yönetmekte ve kontrol etmektedir. Mininet, SDN'nin unsurları olan bilgisayar, aktarma ve kontrol elemanlarının oluşturulmasını, düzenlenmesini ve ayarlanmasını sağlamaktadır. Open Flow Protocol, aktarma elemanı ve kontrol elemanı arasındaki iletişimi sağlar, her bir aktarma elemanını SDN ile tek tek programlamaktansa hepsini bütüncül şekilde programlamaya yaramaktadır. Oluşturulan gemi bilgisayar ağı modelinde 3 adet bilgisayar (Host), 5 adet SDN aktarma elemanı (Switch), 2 adet SDN kontrol elemanı (Controller) bulunmaktadır. 1 numaralı bilgisayar köprüüstünde bulunan INS, 2 numaralı bilgisayar siber saldırının başlatılacağı bilgisayar, 3 numaralı bilgisayar ise makine kontrol bilgisayarıdır (Şekil 23).



Şekil 23. Önerilen gemi bilgisayar ağ modeli (Lagouvardou, 2018).

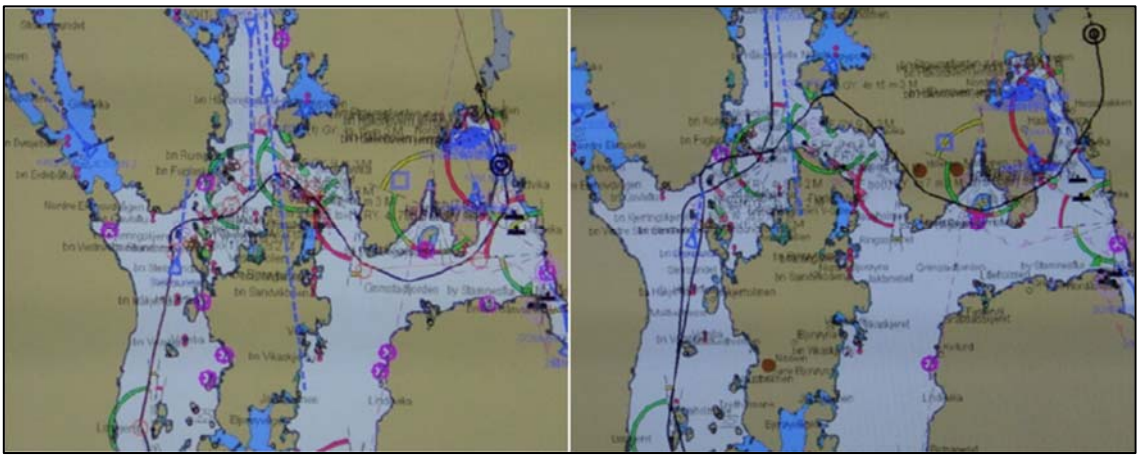
DDoS saldırısına karşı bu sistemin işlevselliğinin simülasyonu yapılmıştır. Bir siber saldırı yöntemi olana DDoS, ağ üzerindeki normal bilgi akışı trafiğini bozmak için hedeflenen unsuru yoğun bilgi akışına maruz bırakarak bilgi akışı trafiğinin boğulmasıdır. Makine kontrol bilgisayarı sunucu (Server) olarak seçilmiştir. Tehdit algılandığında oluşturulan modelin ilk amacı sunucuyu korumak, saldırıyı tanımlamak ve hafifletmektir. Kullanılmakta olan 2 SDN kontrol elemanı ağın işletilmesi ve savunma hareketinin uygulanabilmesi, saldırıyı durdurmak için aktarım elemanlarının yapılandırılması görevi görmektedir. C1 kontrol elemanı kritik unsur olan h3 bilgisayarına gelen bilgi akışını, 5 numaralı aktarıcıdan alınan trafik istatistiklerini analiz ederek denetlemektedir, trafik akışının saldırı niteliği taşıdığı anlaşılınca güvenlik alarmı vermektedir. C0 kontrol elemanı alarmı aldıktan sonra saldırıyı bloke ederek ağa sızılmasını engellemektedir. INS bilgisayarından makine kontrol bilgisayarına gönderilen bilgi akışına yönelik saldırı olduğu senaryosu için simülasyon yapılmıştır. 10 Mbps hız ile h3 bilgisayarına gelen bilgi akışına sisteme sızma amaçlı 40. saniyede 200 Mbps ile müdahale edilmiş ve bilgi akışı hızı yoğun trafik nedeniyle düşmeye başlamıştır. 8 saniye sonra C1 kontrol elemanı alarm vermiş ve C0 kontrol elemanı savunma hareketini yapmıştır. 58,6. saniyede durum düzelmiş ve bilgi akışı hızı tekrar 10 Mbps'e dönmüştür (Şekil 24). Modelin başarı ile simüle edilmiş olması itibariyle gemilerde kullanılabileceği savunulmaktadır.



Şekil 24. Saldırı ve önleme hareketine dair veri hızı, zaman grafiği (Lagouvardou, 2018).

Haraide vd. (2018), güncel bir eğilim olan uzaktan görüntüleme veya uzaktan kontrol amaçlı otomasyon sistemlerinin ve bunlara entegre edilmiş sensörlerin kullanımının yakın gelecekte başarı ile neticelenebilecek siber saldırılara işaret ettiğini belirtmiştir. INS'e aşırı derecede güvenmenin tehlikeli durumlara yol açabileceğine, seyir sistemlerine yönelik siber saldırılara hazırlıklı olmamanın da ciddi sonuçlara sebebiyet verebileceğine vurgu yapmışlardır. Yapılan çalışmada, herhangi bir geminin karşılaşabileceği siber saldırıyı deneysel olarak gerçekleştirmiş ve bunun sonuçlarının durumsal farkındalığı gözetilerek vardiya zabitinin etkinliğinin nasıl arttırılabileceği araştırılmıştır. Gemi ECDIS'ine yüklenmek üzere bir virüs oluşturulmuştur. Bu virüs piyasada kullanılmakta olan 60 anti virüs programında test edilmiş ve sadece 2 tanesi tarafından tespit edilmiştir. Deney için Bergen, Norveç açıklarında seyir yapacak olan bir gemide çalışma yapılmıştır. Gemide Windows 7 işletim sistemine sahip ismi belirtilmeyen, piyasada yaygın bulunan bir ECDIS cihazı ve INS mevcuttur. INS'e gerekli olan bilgiler, ilgili sensörlerden yerel ağ bağlantısı (LAN) ile ulaşmaktadır. Seyir sırasında, hazırlanan virüsün yüklü olduğu USB bellek ECDIS cihazına bağlanmıştır. Virüs bilgisayar tarafından tespit edilememiştir. Virüs kendisini bilgisayar işletim sistemine bilgisayar faresi ve klavye olarak tanıtıp Windows sistemine giriş yapmıştır, bilgisayarı yeniden başlatmıştır. ECDIS bilgisayarı çalışmaya başladığında virüs de görevine ve sisteme gelen GPS verilerini değiştirmeye başlamıştır. Gemi ECDIS ekranında gerçekte olduğu mevkide değil de hatalı bir mevkide görünmektedir (Şekil 25).

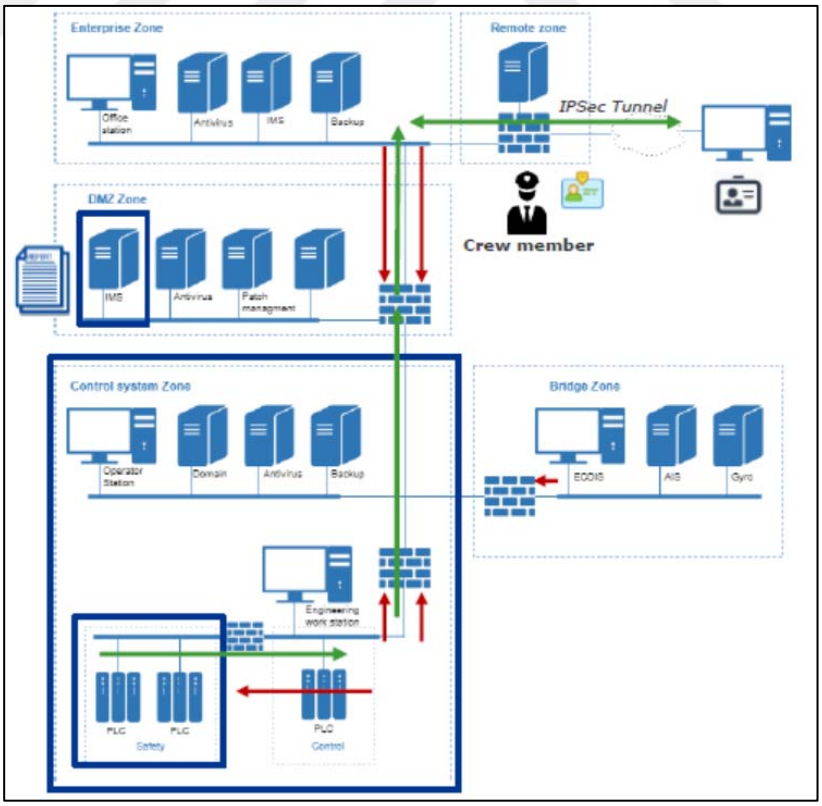
Gemi seyrine devam ettikçe virüs içerisine tanımlanmış belirli bir mevkiye gelindiğinde ECDIS ekranında gemi dakikada yaklaşık 0,8 metre hızla 45 derece sancağına doğru rota değiştiriyormuş gibi görünür, halbuki gerçekte gemi aynı rotasında devam etmektedir. Virüs içerisine tanımlanmış ikinci mevkide ise virüs programı ECDIS bilgisayarını kapatmıştır ve vardiya zabiti harita bilgilerini göremez duruma gelmiştir. ECDIS yeniden başlatıldığında ise virüs, bilgisayarın mavi ekran hatası vermesini sağlamıştır ve yine harita bilgilerine erişilememiştir. Aynı senaryolar gemi "track mode" yani INS'e girilmiş rota bilgilerinin otomatik dümen ile vardiya zabitinin müdahalesine ihtiyaç duyulmadan yapılan seyir sırasında test edilmiştir. GPS verileri değiştirilip GPS'in gerçekte bulunulan mevki yerine hatalı mevki gösterdiği zaman otomatik dümen rotayı düzeltmek için manevra yapmıştır, gemiyi gerçekte olması gereken rotasından çıkarmış ve tehlikeli bir duruma sokma potansiyeli oluşturmuştur. Sonuç olarak, siber güvenlik zincirinde insan kapasitesini en güçlü halka olarak kullanabilmek için, siber güvenliğin denizcilik eğitim ve staj sürecinin bir parçası haline getirilmesi, sistem farkındalığının arttırılması ile vardiya zabitinin etkinliğinin de arttırılması gerektiği belirtilmiştir. Sistemdeki, burada INS'tir, kısıtların ve siber güvenlik tehdit olasılıklarının anlaşılmasının sistem farkındalığının artması anlamına geleceği, böylelikle durumsal farkındalığın arttığı bir ortamda daha emniyetli ve etkin bir seyir yapılabileceği belirtilmiştir.



Şekil 25. Gerçek ve değiştirilen GPS verileri ile rota görüntüleri

DNV-GL (2018), gemilerde siber güvenlik uygulamaları konusunda yaptığı çalışmalarda gemi bilgisayar ağ sistemleri için bölgelere ayrılmış ve kanallar ile

birleştirilmiş bir model önermektedir. Modelde, köprüüstü seyir sistemleri, makine kontrol sistemleri, ofis bilgisayarları, personel kullanımı için ayrılmış bilgisayarlar ayrı ayrı bölgeler oluşturmaktadır (Şekil 26). Her bir bölge birbirine kanallar ile bağlanmıştır. Ağın içerisinde çevre ağı veya sivil bölge (DMZ) olarak adlandırılan bir bölge de bulunmaktadır. DMZ, bir kuruluşun dış servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa (genellikle internet) maruz bırakan fiziksel veya mantıksal bir alt ağdır. DMZ'nin amacı bir kuruluşun yerel alan ağına (LAN) ek bir güvenlik katmanı eklemektir; dışarıdaki bir saldırganın ağın herhangi başka bir bölümünden ziyade yalnızca DMZ içindeki ekipmana erişimi vardır. Sistem ayrıca güvenlik duvarları, anti virüs programları ile de siber güvenlik anlamında desteklenmektedir. Böylelikle hem sistem içi haberleşme hem de dışarıdan izinsiz erişimin kontrolünün sağlanması amaçlanmıştır. Çalışmada mevcut siber güvenlik zaaflarının belirlenebilmesi amaçlı bazı gemilerin bilgisayar sistemlerine sızma testi yapılmış ve önemli derecede birçok zafiyet tespit edilmiştir. Bu nedenle özellikle şirketlerin ağ sistemleri için hem de gemiler için düzenli aralıklarla sızma testi yapılmasının yararı vurgulanmıştır.



Şekil 26. Gemi içi ağ modeli şeması

Güneş (2019), Endüstri 4.0 ile siber fiziksel sistemlerin kritik altyapılarda sıklıkla kullanılmaya başlandığını belirtmiştir. Dünya ticaretinde önemli bir yere sahip olan ve giderek yaygınlaşan konteynır terminallerinde de siber fiziksel sistemlere örnek olabilecek uzaktan kontrollü ekipmanlar, otomasyon sistemleri gibi ekipmanlar kullanıldığı ve bu sistemlerin siber riskler oluşturduğu açıklanmıştır. Örnek bir konteynır terminalinin siber varlık haritası çıkarılmıştır. Bu varlıkların etkilenebileceği siber güvenlik açıkları belirlenmiş ve varlıkların bu açıklara karşı ne derece dirençli olduğu ölçülmüştür. Alınması gereken önlemlere dair anahtar performans göstergeleri belirlenmiştir. Bunlara dair bir risk değerlendirme modeli Bütünleşik Siber Güvenlik Risk Yönetimi metodu kullanılarak oluşturulmuştur. 4 adet senaryo bu modelde uygulanmıştır ve terminal için risk hesabı yapılmıştır.

Kozan (2019), GPS tabanlı konum belirleme sistemlerinin güvenliği ve sinyal geliş doğrultusu kestirimi ile saldırı tespiti konulu çalışmasında GPS sinyallerinin aldatılmasının tespiti için bazı yöntemler önermiştir. Çoklu sensör kullanımının mevki verisini karşılaştırma olanağı sağlaması nedeniyle yararlı olacağı belirtilmiştir. Bunun için GPS / GLONASS kullanımın yaygın olduğu belirtilmiştir ayrıca GALILEO ve Hindistan merkezli IRNSS ve Çin merkezli COMPASS'dan (BEIDOU) da bahsedilmiştir. İkinci olarak anten tabanlı çözümler önerilmiştir. GPS aldatma sinyallerinin özgün GPS sinyallerinden en az 2 veya 3 db fazla olması gerektiği gerçeğine istinaden adaptif maksimum sinyal seviyesi filtresi kullanılarak aldatma sinyalinin temizlenebileceğini belirtmiştir. Ayrıca GPS sinyal seviyesi gücündeki ani değişimlerin kullanıcıya alarm olarak bildirilmesinin yararlı olacağını söylemektedir. Üçüncü olarak, doopler etkisi ve analizi yöntemi önerilmiştir. Doopler etkisi gözlemci ve kaynak arasındaki değişikliklerin frekans değişimine neden olması ve bunun matematiksel olarak yorumlanmasıdır. GPS alıcıları konum çözümüne ve uyduların konumuna sahiptir, böylelikle alıcı her bir GPS uydusuna göre göreceli hızını hesaplayabilmektedir. Doopler kayması taşıyıcı frekansını değiştirdiğinden tek bir verici kullanılarak yapılan saldırılarda saldırı kaynağı tüm uyduların hareketini taklit edemeyeceğinden aldatma saldırısının bu yöntemle tespit edilebileceğini belirtmiştir.

Yüksel (2019), dünya ekonomisinde önemli bir yere sahip olan deniz taşımacılığında kullanılan kritik altyapıların siber saldırı sonucu tüm tedarik zincirini etkileyecek derecede zarar görmesinin istenmeyecek bir durum olduğunu belirtmiştir. Kritik ekipmanın bir parçası olan siber fiziksel sistemlerin güvenliğinin sağlanmasının ve korunmasının son kullanıcı durumundaki çalışanların siber güvenlik farkındalıklarına bağlı olduğunu açıklamıştır. Bu

amaçla 186 tane denizcilik çalışanı ile Beş Noktalı Likert Tipi Anket metodu kullanılarak Türk denizcileri arasındaki siber güvenlik bilincinin öncül faktörleri ve sonuçları araştırılmıştır. Eğitimin ve deneyimin çalışanların siber güvenlik bilincini ve davranışlarını etkilediği, siber güvenlik bilincinin de güvenli kullanıcı davranışını etkilediği saptanmıştır.

Sakar vd. (2019), önde gelen 14 Türk denizcilik firması yetkilileri ile Kolayda Örneklem Yöntemi kullanılarak anket çalışması yapmıştır. Çalışmada, 12 firmanın siber güvenlik konusunda politika ve strateji geliştirmekte olduğu, 1 firmanın henüz konu hakkında planlama aşamasında olduğu, diğerinin ise konu hakkında bir hazırlığının bulunmadığı belirtmiştir. Türk denizcilik sektöründe son yıllarda siber güvenlik konusundaki yatırımların artmakta olduğu fakat konuya dair ilginin halen istenilen seviyede olmadığı belirtilmiştir.

Svilicic vd. (2019), Kobe Üniversitesi Deniz Bilimleri Fakültesi'nin eğitim gemisi Fukae-maru'nun ECDIS cihazı üzerinde siber güvenlik değerlendirme çalışması yapmışlardır. Doğrudan internete bağlı olmayan, IMO standartlarına uygun, Windows XP işletim sistemiyle çalışmakta olan, gyro pusula, doopler parekete, GPS, Navtex, iskandil, ARPA radar, AIS ve otopilot bağlantısı yapılmış olarak kullanılan JRC Jan-901B cihazının risk değerlendirmesinin sayısal verileri için Nessus Proffesional isimli program kullanılmıştır. Program, gemide kullanılan ECDIS'de 7'si kritik, 2'si yüksek, 4'ü orta, 1'i düşük seviyede toplam 14 açıklık tespit etmiştir. Yapılan değerlendirmede, en üst seviye siber risk olarak fiziksel erişim (Physical Access) değerlendirilmiştir. Elektronik cihazlar için fiziksel erişim cihazın izinsiz kullanımı veya sorumlu olmayan personel tarafından kullanımı anlamındadır. Cihaz internete bağlı olarak kullanılmıyor olduğu, gemiyi eğitim amaçlı kullanan öğrenciler köprüüstünde kontrol altında tutulabildiği için cihaz internete bağlı olarak çalıştırılıncaya kadar fiziksel erişimin sınırlı kalacağı belirtilmiş ve cihaz, orta risk seviyesinde değerlendirilmiştir. Kullanılan risk değerlendirme yönteminin tüm gemiler için uygulanabilir olduğu vurgulanmıştır.

Sivilicic vd. (2019b), Rijeka Üniversitesi Deniz Bilimleri Fakültesi ECDIS simülatöründe bulunan 6 adet ECDIS bilgisayarı üzerinde siber güvenlik değerlendirmesi yapmıştır. Simülatör bilgisayarlarında Transas Navi-Sailor 4000 programı, Microsoft Windows 7 işletim sistemi kullanılmaktadır, bilgisayarların internet bağlantısı bulunmamaktadır. Değerlendirme için Nesus Professional 8.0.1 isimli program kullanılmıştır. Yapılan değerlendirme sonucunda aralarında işletim sistemi ve Sunucu İleti Bloğu'na (SMB) dair 24 adet siber güvenlik açığı tespit edilmiştir. Simülatör

bilgisayarlarında SMB v1. protokolünün tespit edilmiş olması ilginç bir sonuç olarak değerlendirilmiştir çünkü konteynır şirketi Maersk'in maruz kaldığı NotPetya siber saldırısı SMB v1. üzerinden yapılmış olan bir fidye yazılım saldırısıdır. Bilenen bu açıklığa dair simülatör bilgisayarlarında halen bir önlem alınmadığı anlaşılmıştır. İşletim sistemi güncellemelerinin yapılması ve anti virüs programı kullanılması gerekliliğinin yanında SMB v1. protokolünün devre dışı bırakılacağı şekilde uygun işletim sistemi ayarlarının yapılması gerektiği önerilmiştir.

Topal (2020), Türk gemi işletmecilerinin siber güvenlik konusundaki çalışmalarının analizini yapmıştır. 14 denizcilik şirketinin bilişim departmanı yetkililerine ve 31 ayrı denizcilik şirketine bilişim desteği veren özel bir kuruluşun yetkilisi olmak üzere toplam 15 uzmana konu hakkında belirli sorular yöneltilmiştir. Gemilere yönelik mevcut tehditler doğrultusunda, kurumsal işletmecilerin kendi bilişim departmanlarının ve bilişim politikalarının olduğu, dışarıdan bilişim desteği alan firmaların ise siber politikalarının olmadığı ve bunun da onları siber saldırılara karşı daha açık hale soktuğu belirlenmiştir. Şirketlerin ve gemilerin güvenlik konusunda yeterince önlem almadığı, kaynak ayırmadığı, konuya dair personel eğitiminde eksiklikler olduğu, yazılım yetersizliğinin olduğu tespit edilmiştir.

Oruç (2020), her türlü teknolojik gelişmenin uygulama alanı bulduğu gemilerde kullanılan cihazların siber saldırıya maruz kalabilme potansiyeline göre seyir halindeki bir tankerin köprüüstü, makine dairesi ve kargo kontrol dairesindeki ekipmanların siber saldırı risklerini değerlendirilmiştir. Yapılan değerlendirmede 31 risk belirlenmiş ve bunlar için 37 prosedürel ve teknik önlem içeren bir risk değerlendirme modeli Bulanık Fine-Kinney metodu kullanılarak oluşturulmuştur. Oluşturulan modelin tanker tipi gemilerde kullanılabileceği önerilmiştir.

2. YAPILAN ÇALIŞMALAR

2.1. Çalışmanın Kapsamı

Bu çalışmada, gemilere yönelik siber saldırı olaylarını modelleyen bir ağ yapısı ortaya konulmuştur. Son yarım yüzyılda kaza analizi de olmak üzere birçok alanda kullanılan Bayes Ağı metodunun modelleme için uygun olacağı düşünülmüştür (Ekici, 2005). Bayes Ağı ile olayı meydana getiren faktörler arası ilişki, düğümler ve kenarlar kullanılarak kolay anlaşılır bir grafik yapısında incelenmektedir. Ayrıca Bayes Ağı bu ilişkiyi koşullu olasılık yaklaşımı kullanarak nicel, gerçeğe en yakın şekilde ortaya koyma imkanı da sağlamaktadır (Cai vd., 2013). Çalışma 5 aşamadan oluşmaktadır. Birinci aşamada, Konum Belirleme Sistemi, AIS, ECDIS ve Haberleşme, Otomasyon, Bilgisayar Sistemi temel alınarak akademik yayınlara, deneysel ve laboratuvar çalışmalarına, gerçekleşmiş siber olaylara, ilgili kurum ve kuruluşların önerilerine göre Bayes Ağı'nın düğümleri oluşturulmuştur. İkinci aşamada denizcilik sektörünün farklı kollarında çalışmakta olan siber güvenlik, bilgisayar ve elektronik teknolojileri konularında uzman 8 kişi belirlenmiştir. Hazırlanan Bayes Ağı'ndaki düğümlerin değişkenleri istatistiksel verilere ve uzman görüşlerine göre, her bir düğümün değişkenlerinden meydana gelen koşullu olasılık tabloları ise uzman görüşlerine göre değerlendirilmiştir. Üçüncü aşamada koşullu olasılık sonuçları bulanık mantık (FUZZY) aşamalarından geçirilerek her bir düğümün oluşma olasılığı hesaplanmıştır. Dördüncü aşamada ise Genie programı kullanılarak hassasiyet analizi yapılmıştır. Son olarak, belirtilen 4 sistem için gemilerde kullanılabilecek siber güvenli seçeneklere dair değerlendirme ve öneriler yapılmıştır.

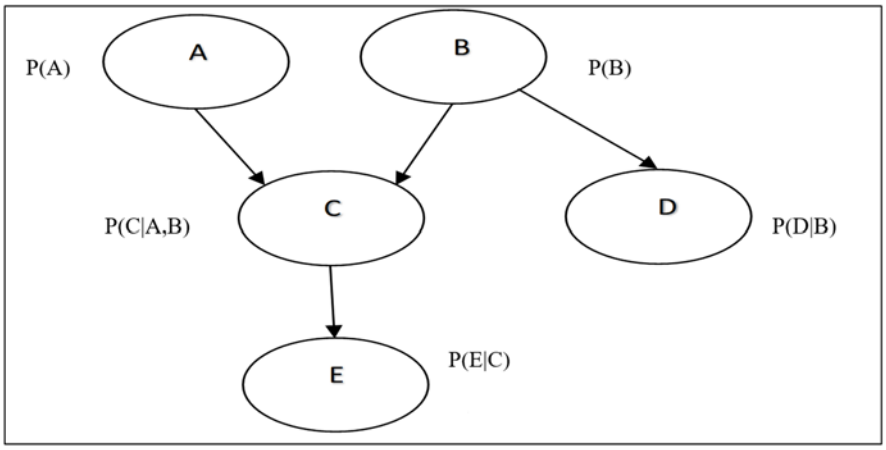
2.2. Bayes Ağları ve Koşullu Olasılık Yaklaşımı

Bayes yaklaşımının temelleri, 1763 yılında yayımlanan, İngiliz matematikçi Thomas Bayes tarafından yazılan "Şanslar Doktrinindeki Bir Problemi Çözmeye Yönelik Bir Deneme" adlı makale ile ortaya çıkmıştır (Link ve Barker, 2010; Savchuk ve Tsokos, 2011). Teoremin literatürde tanınması 1930'larda olmuştur. 1970'lerden itibaren ise birçok sektörde bilinmezlik içeren olay dizilerinin modellenmesi, sonuçlarının yorumlanması ve bir

sonuç olayını meydana getiren ilişkili durumların değerlendirilmesi amaçlarıyla kullanılmıştır (Demirel ve Bodur, 2004; Yang vd., 2008).

Bayes ağları, düğümler ve oklar vasıtasıyla değişkenler arası ihtimallerin gösteriminin yapıldığı grafiksel kısım ve düğümlere ait koşullu olasılık tabloları olmak üzere iki kısımdan oluşmaktadır. Düğümler, ana soruna katkıda bulunan faktörlerdir. Yönlendirilmiş oklar doğrudan etkiyi göstermekte ve rastgele değişkenler arasında tutulması gereken bağımsızlık varsayımlarını belirtmektedir (Rausand, 2011). Kendilerine oklar yönlendirilmiş düğümlere "çocuk" düğüm (Child Nodes), okların kendilerinden çıktığı düğümlere "ebeveyn" düğüm (Parent Nodes) ve kendilerine hiç ok yönlendirilmemiş düğümlere de "kök" düğüm (Root Nodes) denilmektedir (Trucco vd., 2008). Ağın sahip olabileceği ebeveyn ya da çocuk düğüm sayısı bakımından bir kısıtlama bulunmamaktadır. Tek kısıt, herhangi bir düğümden başlayarak yönlendirilen okları takip etmek suretiyle yine aynı düğüme ulaşılmamasıdır (Korb ve Nicholson, 2004). Bayes Ağ yapısındaki düğümlerin olasılık değerleri hesaplanırken iki ana yaklaşım söz konusudur. Bunlardan biri istatistiksel veri veya önceki çalışmaları kullanarak koşullu olasılık değerlerini belirlemektir. Diğeri, incelenen vakalar üzerinde daha önce hiç çalışma yapılmadığı, ölçülmesi mümkün olmadığı ve istatistiksel verilerin mevcut olmadığı durumda koşullu olasılıkların uzman yargıları kullanılarak belirlenmesidir (Pristrom vd., 2016; Matellini vd., 2013).

Şekil 27'de A, B, C, D ve E değişkenlerinden oluşan örnek bir Bayes Ağı'nın gösterimi bulunmaktadır. Bu ağda A ve B değişkenleri C değişkeninin ebeveyni, C değişkeni ise E değişkeninin ebeveynidir. Ayrıca şekilde görüldüğü üzere D değişkeni B değişkeninin çocuk değişkenidir.



Şekil 27. Örnek Bayes Ağı şeması

Şekilde değişkenlerin sahip oldukları koşullu olasılık dağılımları, P(A), P(B), P(C|A,B), P(D|B) ve P(E|C) olarak belirtilmektedir. Ağda yer alan bir değişkenin, başka bir değişkenle arasında herhangi bir ok bulunmaması o değişkenin ağda yer alan diğer değişkenlerle arasında olasılıksal bir bağın olmadığını ifade eder (Çinicioğlu vd., 2013).

Koşullu olasılık kavramı, bir olayın gerçekleşme olasılığının hesaplanmasında, o olayla ilişkili ek bilgilerin kullanılması gerektiğini ve nasıl kullanılacağını ifade etmektedir (Loughney ve Wang, 2018; Trucco vd., 2008). Bayes Ağı koşullu olasılık mantığına göre, herhangi A ve B gibi iki olay için;

B olayı bilindiğinde A'nın olma olasılığı;

$$P(A|B) = P(A \cap B) / P(B),\ P(B)>0 \quad (1)$$

A olayı bilindiğinde B'nin olma olasılığı;

$$P(B|A) = P(A \cap B) / P(A),\ P(A)>0 \quad (2)$$

A ve B'nin birlikte görüldüğü olasılıkların kesişim kümesi;

$$P(A \cap B) = P(A|B) \,.\, P(B) = P(B|A) \,.\, P(A) \quad (3)$$

Koşullu olasılık genelleştirildiğinde; B olayı bilindiğinde A_i olayının olma olasılığı; (B olayının birbirinden ayrık A olaylarından (A_1,A_2,A_3,…,A_k) biriyle birlikte gerçekleşebileceği durum veya başka bir ifadeyle B olayıyla kesişen ve karşılıklı birbirini etkileyen k tane A olayı olması durumu).

$$P(A_i|B) = P(A_i) \,.\, P(B|A_i) / P(B) \quad i=1,2,3,\ldots.k \quad (4)$$

Eşitlik (3)'te ki P(B)'nin açılımı aşağıda verilmiştir.

$$P(B) = P(A_1).P(B|A_1)+\ldots..+P(A_k).P(B|A_k) = \sum_{j=1}^{k} P(A_j).P(B \mid A_j) \quad (5)$$

Eşitlik 4 ile değişkenlerin sahip oldukları koşullu olasılıkların çarpımı ağın birleşik olasılık dağılımını oluşturur (Trucco vd., 2008; Akhtar ve Utne, 2014; Kragt, 2009). Aynı zamanda bu eşitlik, Bayes Teoremi'nin istatistiki olarak kabul edilebilen mantıklı ve tutarlı ilişkisini de ifade etmektedir. Sübjektif olasılık yaklaşımı acısından değerlendirildiğinde Bayes Teoremi, yeni kanıtlar ışığında olasılık değeri ile önceki verilerin güncelleştirilip değiştirilmesine olanak sağlayan bir araç olarak kullanılabilir (Jones vd., 2010).

2.2.1. Bayes Ağının Tesisi

Bayes Ağı'nda toplam 25 düğüm bulunmaktadır. Düğümlerin oluşturulmasına ilişkin detaylar aşağıda verilmiştir.

2.2.1.1. Konum Belirleme Sistemi Bölümüne Ait Düğümler

Cihaz çifti düğümünde, yaygın ve en etkin şekilde kullanılan uydu tabanlı 2 sistem olan GPS ve GLONASS ile uydu tabanlı olmayan, karasal bir sistem olan eLORAN seçeneklerinden oluşmaktadır. Bunlara istinaden, 2 GPS, GPS ve GLONASS, eLORAN ve GLONASS değişkenleri belirlenmiştir.

Sistemlerin siber güvenlik anlamında değerlendirilmesinde çeşitli yayınlardan yararlanılmıştır. Rodriguez (2008), CDMA kodu kullanılan ve hepsi aynı frekansta yayın yapan GPS uydularına dar bant üzerinden sinyal karıştırma saldırısı yapıldığında tüm uydu sisteminin kullanılmaz duruma geleceğini belirtmiştir. FDMA kodu kullanılan ve hepsi farklı frekanslarda yayın yapan GLONASS uydularında ise sadece saldırı yapılan frekanstaki uydunun devre dışı kalacağını, sistemin geri kalanının ise çalışmaya devam edeceğini ayrıca FDMA kodlama sisteminin CDMA'ya göre bazı açılardan daha siber güvenli olduğunu belirtilmiştir. Glomsvoll ve Bonenberg (2016) yapmış oldukları deneylerde GLONASS sisteminin GPS'e göre sinyal karıştırma saldırısına karşı daha dirençli olduğunu belirtmiştir. eLORAN sisteminde yüksek güçte vericiler ve düşük frekanslı sinyaller kullanılıyor olması sebebi uydu temelli mevki sistemleri gibi sinyal etkilemesi veya karıştırması saldırısına maruz kalma riski bulunmamaktadır (ILA, 2007). Tam vd. (2019b), düşük frekansta çalışan uzun menzilli seyir sistemi olan uydudan bağımsız eLORAN'ın sinyal karıştırma veya etkileme saldırısına maruz kalmasının zor olduğunu fakat gelecekte bu sistemin de siber korsanların ilgisini çekip siber saldırıya maruz kalma

durumunun olabileceğini belirtmiştir. eLORAN teknolojisi konusunda uzmanlaşmış Hellen Systems şirketi, eLORAN'ın uydu tabanlı sistemlere göre en az 3 milyon kat güçlü olduğunu ve ilave edilmiş güvenlik özellikleriyle sinyal etkileme veya karıştırma saldırısına maruz kalmayacağını belirtmektedir (URL-7). Grant vd. (2009), yapmış oldukları deneylerde GPS sinyallerinin dışarıdan yapılacak müdahale ile etkilendiğini fakat deney süresince eLORAN sisteminden hep doğru mevki alındığını belirtmiştir. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

Coğrafi konum düğümü için, detayları verilen gerçekleşmiş siber saldırıların yoğunlukla Karadeniz ve Kore Yarımadası çevresinde meydana gelmesi nedeniyle "Karadeniz – Kore Yarımadası" ve "Diğer" değişkenleri oluşturulmuştur. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

Sinyal seviyesi filtresi düğümü, Kozan (2019) tarafından yapılan çalışmada adaptif maksimum sinyal seviyesi filtresi kullanımının aldatma sinyalinin temizlenmesinde yararlı olacağı görüşüne göre belirlenmiştir. Aynı amaçla Oroli Maritime tarafından geliştirilen bir cihaz gemilerde kullanılmak üzere piyasada mevcuttur (OM, 2019). Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

Tablo 3'de ağın Konum Belirleme Sistemi bölümünün yapısı verilmiştir. Konum Belirleme Sistemleri bölümündeki düğümlerin değişkenlerinin oluşturduğu koşullu olasılık tabloları uzmanlar tarafından belirlenmiştir.

Tablo 3. Ağın Konum Belirleme Sistemi bölümünün yapısı

Düğüm Adı	Değişkenler	Olasılık		Ebevyn Düğüm	Çocuk Düğüm	Çocuk Düğüm Olumsuzluk İfadesi
Cihaz Çifti	GPS + GPS	%25	Uzmanlar Tarafından Değerlendirilmiştir	Kök Düğüm	Konum Belirleme Sistemi	Güvenli Değil
	GPS + GLONASS	%35				
	eLORAN + GLONASS	%40				
Coğrafi Konum	Karadeniz – Kore Yarımadası	%46	Uzmanlar Tarafından Değerlendirilmiştir	Kök Düğüm		
	Diğer	%54				
Sinyal Seviyesi Filtresi	Var	%63	Uzmanlar Tarafından Değerlendirilmiştir	Kök Düğüm		
	Yok	%37				

2.2.1.2. AIS Bölümüne Ait Düğümler

Cihaz çeşidi düğümü, gemilerde kullanılmakta olan AIS cihazı çeşitlerinden uydu AIS ve VHF AIS seçenekleri ile oluşturulmuştur. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir. Sinyal doğrulama ekipmanı düğümü, Balduzzi vd. (2014) tarafından yapılan çalışmada X509 gibi PKI ekipmanları kullanılarak AIS sinyallerinin doğrulanabileceği görüşüne göre belirlenmiştir. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir. Tablo 4'de ağın AIS bölümünün yapısı verilmiştir. AIS bölümündeki düğümlerin değişkenlerinin oluşturduğu koşullu olasılık tabloları uzmanlar tarafından belirlenmiştir.

Tablo 4. Ağın AIS bölümünün yapısı

<table>
<tr><th>Düğüm Adı</th><th>Değişkenler</th><th colspan="2">Olasılık</th><th>Ebevyn Düğüm</th><th>Çocuk Düğüm</th><th>Çocuk Düğüm Olumsuzluk İfadesi</th></tr>
<tr><td rowspan="2">Cihaz Çeşiti</td><td>Uydu AIS</td><td>%61</td><td rowspan="3">Uzmanlar Tarafından Değerlendirilmiştir</td><td>Kök Düğüm</td><td rowspan="3">AIS</td><td rowspan="3">Güvenli Değil</td></tr>
<tr><td>VHF AIS</td><td>%39</td><td rowspan="2">Kök Düğüm</td></tr>
<tr><td rowspan="2">Sinyal Doğrulama Ekipmanı</td><td>Var</td><td>%69</td></tr>
<tr><td>Yok</td><td>%31</td><td></td></tr>
</table>

2.2.1.3. ECDIS Bölümüne Ait Düğümler

Kullanıcı prosedürleri düğümü için çeşitli yayınlardaki önerilerden yararlanılmıştır (BIMCO, 2020; NCC, 2014; MAYAICT, 2019; Svilicic vd., 2019; 2019b; 2020). Ayrıca gerçekleşmiş siber olaylardan elde edinilen yanlış uygulamalardan da yararlanılmıştır. Bunlara istinaden aşağıdaki prosedürler hazırlanmıştır. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

- ECDIS'e kişisel tablet, cep telefonu gibi cihazlar bağlamamak.
- Yazılım koruma kilidi (USB Dongle Key) kullanmak.
- Kritik ekipman olan ECDIS'e fiziksel erişimi sınırlamak, sadece yetkili kişilerin köprüüstüne girebilmesini ve cihazı kullanabilmesini sağlamak (Köprüüstü giriş kapısına şifreli veya kartlı elektronik kilit sistemi koymak gibi).
- Harita düzeltmeleri veya sistem güncellemeleri USB bellek ile yapılıyorsa bu iş için her zaman belirli bir belleği kullanılmak.

- Kullanılacak her harici belleğe önce virüs taraması yapmak.
- Güvenlik duvarı gibi yazılım ayarlarını en üst seviyede kullanmak, işletim sistemi ayarlarını en uygun şekilde yapmak (SMB v1. protokollerinin kapatılması gibi).
- İşletim sistemi ve virüs programı güncellemelerinin şirket tarafından gemiye düzenli olarak gönderilmesi veya geminin bu işlemleri internet üzerinden yapması gerektiğine dair talimatların var olması.

Yazılım ile onun kök düğümleri olan işletim sistemi, virüs programı ve güncellemeler düğümleri için çeşitli yayınlardaki önerilerden yararlanılmıştır (BIMCO, 2020; NCC, 2014; MAYAICT, 2019). Güncellenmemiş veya güncellemesi artık yayınlanmıyor olan eski yazılım veya sistemlerin kullanılmasının çok büyük güvenlik zafiyetleri yaratıyor olması bilgisi değerlendirilmiştir. Denizcilik şirketlerinin %37'sinin kullandığı Microsoft yazılımlarını güncellemek için doğru dosyaları indirmedikleri istatistiğinden yararlanılmıştır (Jones vd., 2016). Haraide vd. (2018) tarafından yapılan çalışma ve gerçekleşmiş siber olayların analizi de değerlendirilmiştir. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir. Harita düzeltme yöntemleri düğümü için ECDIS'de harita düzeltmeye dair uygulamadaki mevcut 3 yöntem seçenek olarak sunulmuştur. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir. Tablo 5'de ağın ECDIS bölümünün yapısı verilmiştir. ECDIS bölümündeki düğümlerin değişkenlerinin oluşturduğu koşullu olasılık tabloları uzmanlar tarafından belirlenmiştir.

Tablo 5. Ağın ECDIS bölümünün yapısı

<table>
<tr><th>Düğüm Adı</th><th>Değişkenler</th><th colspan="2">Olasılık</th><th>Ebevyn Düğüm</th><th>Çocuk Düğüm</th><th>Çocuk Düğüm Olumsuzluk İfadesi</th></tr>
<tr><td rowspan="2">Kullanıcı Prosedürleri</td><td>Var</td><td>%74</td><td rowspan="7">Uzmanlar Tarafından Değerlendirilmiştir</td><td rowspan="2">Kök Düğüm</td><td rowspan="7">ECDIS</td><td rowspan="7">Güvenli Değil</td></tr>
<tr><td>Yok</td><td>%26</td></tr>
<tr><td rowspan="3">Harita Düzeltme Yöntemi</td><td>Orijinal Düzeltme CD'si</td><td>%45</td><td rowspan="3">Kök Düğüm</td></tr>
<tr><td>Harici Bellek</td><td>%22</td></tr>
<tr><td>İnternet Bağlantısı</td><td>%33</td></tr>
<tr><td rowspan="2">Yazılım</td><td>Sistemi Korur</td><td>%65</td><td rowspan="2">İşletim Sistemi, Virüs Programı, Güncellemeler</td></tr>
<tr><td>Zafiyet Yaratır</td><td>%35</td></tr>
</table>

Tablo 5'ün devamı,

Düğüm Adı	Değişkenler	Olasılık		Ebevyn Düğüm	Çocuk Düğüm	Çocuk Düğüm Olumsuzluk İfadesi
İşletim Sistemi	Desteklenen Versiyon	%71	Uzmanlar Tarafından Değerlendirilmiştir	Kök Düğüm	Yazılım	Zafiyet Yaratır
	Desteklenmeyen Versiyon	%29				
Virüs Programı	Kullanılıyor	%83		Kök Düğüm		
	Kullanılmıyor	%17				
Güncellemeler	Yapılıyor	%82		Kök Düğüm		
	Yapılmıyor	%18				

2.2.1.4. Otomasyon, Haberleşme ve Bilgisayar Sistemleri Bölümüne Ait Düğümler

Ağ altyapısı düğümünün kök düğümleri şu şekilde oluşturulmuştur. İnternet bağlantısı düğümü, gemi içi ağda internet bağlantısının varlığı seçenek olarak sunulmuş ve belirlenen değişkenlerin olasılık yüzdesi uzmanlar tarafından belirlenmiştir. Ağın bölgelere ayrılması düğümü çeşitli evraklarda gemi içi ağın bölgelere ayrılması gerektiği önerilerine göre belirlenmiştir (DNV-GL, 2018; MAYAICT, 2019; Class NK, 2020; BIMCO, 2020). Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir. Tespit edici ekipman düğümü, Lagouvardou (2018) ve Babineau vd. (2012) tarafından yapılan çalışmalardaki görüşlere göre belirlenmiştir. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

Kullanıcı prosedürleri düğümü için çeşitli evraklardaki önerilerden yararlanılmıştır (ENISA, 2019; BIMCO, 2020; MAYAICT, 2019; DNV-GL, 2018; Class NK, 2020; IOActive, 2014; Koç Sistem, 2019; Jones Walker LLP, 2018; Sağıroğlu vd., 2018). Rider (2018) ve Sakar vd. (2019) tarafından yapılan çalışmalar ile gerçekleşmiş siber olayların analizi de değerlendirilmiştir. Bunlara istinaden aşağıdaki prosedürler hazırlanmıştır. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

- Gemi bilgisayarlarına ve sistemlerine kişisel tablet, cep telefonu gibi cihazların bağlanmaması.
- Sisteme bağlanılan tüm harici medyalara virüs taraması yapılması.
- Bilgisayarların USB portlarının fiziki olarak kapatılması ve harici bellek kullanımıyla oluşabilecek tüm risklerin bertaraf edilmesi. Veya bilgisayara

yüklenecek yazılım ile sadece belirli harici belleklerin kullanımına imkan vererek diğer harici belleklerin kullanımının engellenmesi.

- Güvenlik duvarı gibi yazılım ayarlarının en üst seviyede kullanılması, işletim sistemi ayarlarının en uygun şekilde yapılması (SMB v1. protokollerinin kapatılması gibi).
- Personel ve yolcular için sosyal ağlara giriş kuralları belirlenmesi, ağ ayarlarının en emniyetli ve uygun şekilde yapılması.
- Bulut tabanlı depolama yöntemleri kullanılıyorsa bunlara dair kurallar belirlenmesi.
- Bilinmeyen e posta adreslerinden gelen e postaların açılmaması, bu e postaların eklerini açılmaması gibi e posta yönetimi uygulamaları belirlenmesi.
- Tüm kullanıcılar için parola ve şifre kullanımı zorunluluğu olması, şifre veya parolaların başkaları ile paylaşılmasının yasaklanması, parola kaydetme özelliğinin kullanılmaması, kullanılan parolaların başkaları tarafından tahmin edilemeyecek şekilde kullanıcılar tarafından belirlenmesi.
- Kritik ekipmana fiziksel erişimin sınırlanması, laptop veya bilgisayar kasası gibi ekipmanların bulundukları yerden başka yere kontrolsüz taşınmasının engellenmesi için bulundukları yere sabitlenmesi.
- Sistem / veri yedeklerinin düzenli olarak alınması.
- İşletim sistemi ve virüs programı güncellemelerinin şirket tarafından gemiye düzenli olarak gönderilmesi veya geminin bu işlemleri internet üzerinden yapması gerektiğine dair talimatların var olması.
- Sistemdeki zafiyetlerin tespit edilebilmesi için düzenli olarak sızma (Penetrasyon) testlerinin yapılması, bulunan zafiyetlere göre ek tedbirler alınması.
- Şirketin, gemi personeli de dahil tüm personeline siber güvenlik konusunda eğitim, bilgi vermesi, güncel gelişmelere dair personelin farkındalığını arttırıcı uygulamaların geliştirilmesi.
- Siber güvenlik konusunda yetkin bir şirketten Yönetilen Uç Nokta Atak Tespiti ve Yanıtlama (EDR) gibi hizmet alınarak uç nokta kullanıcısı olarak değerlendirilebilecek gemiye yönelik siber saldırıların veya veri ihlallerinin engellenmesi.

- Bilgi teknolojileri acil durum planının oluşturulması, siber risk değerlendirmesinin etkin şekilde yapılması, siber tehditler konusunda bilgi alışverişinin arttırılması.
- Macroların devre dışı bırakılması.
- Gemi ofis arası internet bağlantılarında sanal özel ağ (VPN) kullanımının tercih edilmesi.
- Gereksiz yazılım, protokol ve portalların bilgisayara yüklenmemesi, yüklü ise uygun şekilde silinmesi.

Tablo 6'de ağın Otomasyon, Haberleşme, Bilgisayar Sistemi bölümünün yapısı verilmiştir. Otomasyon, Haberleşme ve Bilgisayar Sistemleri bölümündeki düğümlerin değişkenlerinin oluşturduğu koşullu olasılık tabloları uzmanlar tarafından belirlenmiştir.

Tablo 6. Ağın Otomasyon, Haberleşme, Bilgisayar Sistemi bölümünün yapısı

Düğüm Adı	Değişkenler	Olasılık		Ebevyn Düğüm	Çocuk Düğüm	Çocuk Düğüm Olumsuzluk İfadesi
Kullanıcı Prosedürleri	Var	%74	Uzmanlar Tarafından Değerlendirilmiştir	Kök Düğüm	Otomasyon, Haberleşme, Bilgisayar Sistemi	Güvenli Değil
	Yok	%26				
Ağ Altyapısı	Güçlü	%65		İnternet Bağlantısı, Ağ Bölgelere Ayrılmış, Tespit Edici Ekipman		
	Zayıf	%35				
İnternet Bağlantısı	Var	%43		Kök Düğüm	Ağ Altyapısı	Zayıf
	Yok	%57				
Ağ Bölgelere Ayrılmış	Evet	%71		Kök Düğüm		
	Hayır	%29				
Tespit Edici Ekipman	Var, aynı Marka	%36		Kök Düğüm		
	Var, farklı Marka	%45				
	Yok	%19				
Yazılım	Sistemi Korur	%65		İşletim Sistemi, Virüs Programı, Güncellemeler	Otomasyon, Haberleşme, Bilgisayar Sistemi	Güvenli Değil
	Zafiyet Yaratır	%35				
İşletim Sistemi	Desteklenen Versiyon	%71		Kök Düğüm	Yazılım	Zafiyet Yaratır
	Desteklenmeyen Versiyon	%29				
Virüs Programı	Kullanılıyor	%83		Kök Düğüm		
	Kullanılmıyor	%17				
Güncellemeler	Yapılıyor	%82		Kök Düğüm		
	Yapılmıyor	%18				

2.2.1.5. Tespit Edici, Önleyici Eylem ve Sonuç Düğümleri

Yedek Ekipman düğümü, siber saldırı olduğu anlaşıldığında siber zararın oluşmaması veya zararın en aza indirilmesi için önleyici eylem seçeneğidir. Røsdeth vd. (2013) tarafından otonom gemiler için oluşturulmuş model günümüz ticari gemileri için çok maliyetlidir. Buna rağmen kritik cihazların, kullanımda olan mevcut sistemden bağımsız ve farklı modelde yedeklerinin bulunması, uydu bağlantı sisteminde değişik modelde bir yedek sistemin varlığı, ağ bağlantıları ve uygulanacak protokoller açısından ticari gemilerde de uygulanabilir. Değişkenlerin olasılık yüzdeleri uzmanlar tarafından belirlenmiştir.

Dijital verinin doğrulanması siber saldırının tespit edilebilmesi eylemi anlamındadır. Fitton vd. (2015), siber saldırıları önlemek, tespit etmek ve savunmak için eğitimin gerekli olduğunu, böylelikle personelin saldırıya etkili şekilde direnç gösterip operasyonlara devam edebileceğini belirtmiştir. Köprüüstü seyir ekipmanlarındaki cihazlardan elde edilen dijital verilere aşırı güven tehlikeli durumlar doğurabilmektedir, ayrıca seyir sistemlerine yönelik bir siber saldırıya hazırlıksız olmak da ciddi sonuçlara sebep olabilir (Haraide vd. 2018). Her türlü dijital verinin farklı bir yöntemle doğrulaması yapılarak siber saldırının varlığı tespit edilebilir, böylelikle siber zararı önlemek veya azaltabilmek mümkün olur. Karşılaştırılan iki değerin anlamlı bir farkı bulunuyorsa bunun yorumlanması, siber saldırı ihtimali için farkındalık oluşturup geminin emniyetini sağlayacak asgari düzeltici harekettir (Shaikh, 2017). Değişkenlerin olasılık yüzdesi uzmanlar tarafından belirlenmiştir. Bu amaçla yapılabilecek bazı uygulamalar şunlardır,

- Uydu tabanlı konum belirleme cihazlarından elde edilen mevkinin; hedefe / kerteriz, radar, astronomik seyir, LOP (line of position), manually fix position, parekete / tahmini mevki (DR / EP) gibi yöntemlerle doğrulanması.
- AIS hedeflerinin ARPA radarda plotlanarak takip edilmesi, şüpheli durumlarda VHF teması sağlanması.
- Harita bilgilerinin düzenli olarak iki ECDIS'den kontrol edilip doğrulanması.
- Otomasyon sistemi el verdiği ölçüde parametrelerin (basınç, sıcaklık vs.) doğrudan kontrolü.

Bayes Ağı'nın sonuç düğümleri siber zarar ve başarısız girişimdir. Siber saldırı olma durumda tespit edici ve önleyici eylemlerin varlığı ve uygulanması siber zararın ne derecede olacağını belirlemektedir. Başarısız girişim, siber korsanlar tarafından gerçekleştirilen bir siber saldırı girişiminin hem alınmış mevcut önlemler hem de siber korsanların becerileri

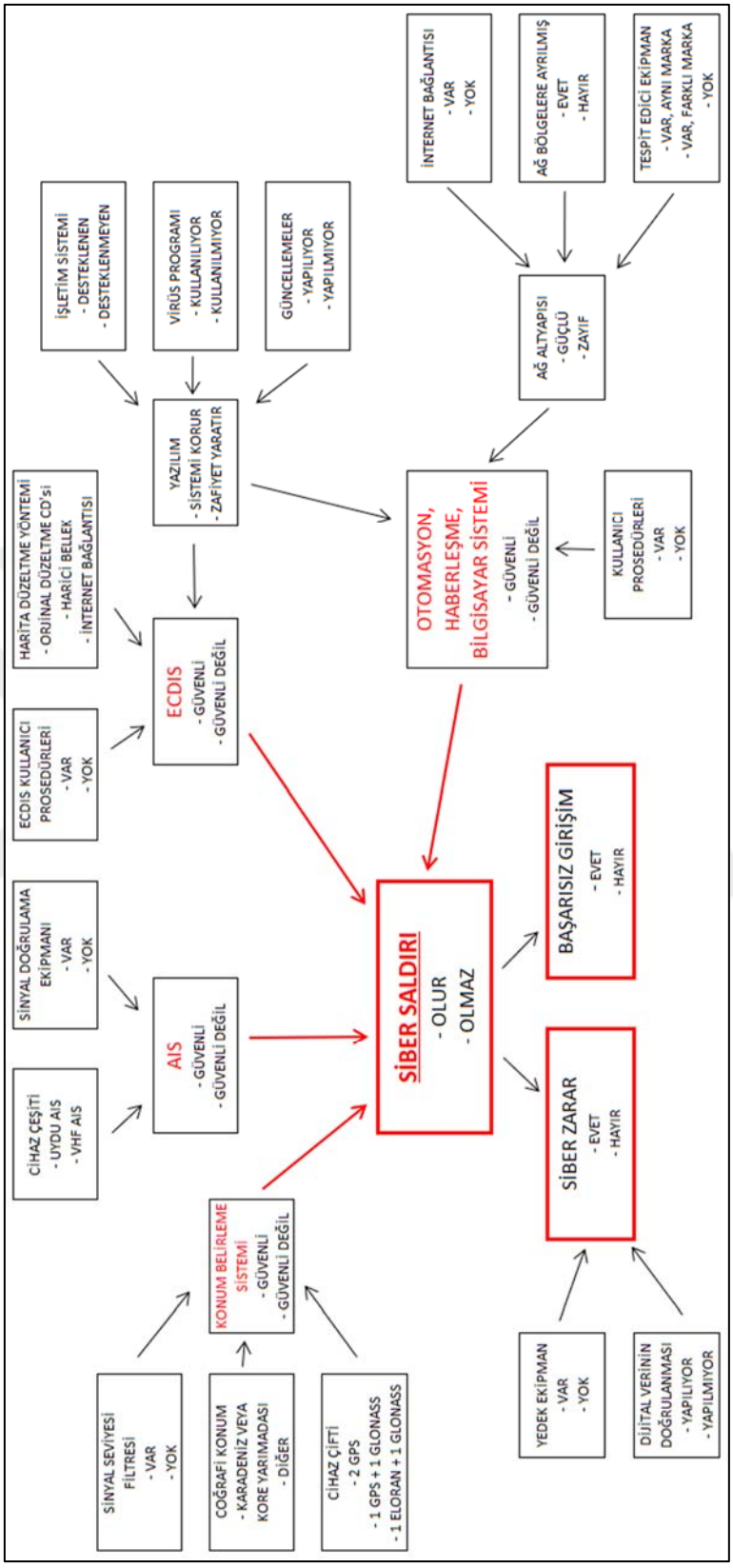
ölçüsünde başarısız olma ihtimalidir. Siber saldırı "olmaz" ise başarısız girişim "evet" olacak anlamındadır. Bu düğüm için, çalışmamızda yaralandığımız uzmanların bir olasılık değeri bildirmeleri, konu hakkında derin bir bilgi ve araştırma gerektirdiği için zordur. Denizcilik sektörü için de bu anlamda sayısal bir değer mevcut değildir.

Başarısız girişim düğümü olasılık değerleri için Harvard Business Review – Dijital Dönüşüm Siber Güvenlik (2020) kitabından yararlanılmıştır. Buna göre, bir sektördeki siber ihlal vakalarının oranı, o sektördeki siber kırılganlık hakkında fikir vermektedir. Konaklama ve gıda sektörü en kırılgan hedeflerin başında gelmektedir. Bu sektörde, her 1 başarısız saldırıya karşılık ortalama 11 başarılı ihlal vardır (%8 başarısız girişim). Halka açık sektörlerde her 74 başarısız saldırıya karşılık 1 sızma gerçekleşmektedir (%98 başarısız girişim). Verizon 2018 yılı Veri İhlalleri Soruşturma Raporu'nda, 65 ülkede 53.000'in üzerinde siber güvenlik vakasından 2.216 tane ihlal analiz edilmiştir (%96 başarısız girişim). Verizon'un 2019 yılı raporundaki rakamlar ise 41.686 siber güvenlik vakasında 2.013 başarılı girişim mevcuttur (%95 başarısız girişim). Accenture 2018 yılı Siber Dayanıklılık Durumu Raporu 15 ülkedeki 19 sektörde piyasa değeri 1 milyar dolar üzerinde olan şirketlerin 4.600 idarecisi ile gerçekleştirilmiştir. 2018 yılında yapılan araştırmada 232 siber olaydan 30 tanesi başarı ile sonuçlanmıştır (%87 başarısız girişim). Aynı çalışmanın 2017 rakamları ise 106 siber olayda 32 başarılı sonuçtur (%70 başarısız girişim). Başarısız girişim rakamlarının büyüklüğü siber saldırılara karşı güvende olduğumuz düşüncesi yaratabilir fakat unutulmamalıdır ki saldırgan ve saldırı sayısı her geçen gün artmayı sürdürmektedir. Siber saldırının başarısız olma girişimi için yukarıda belirtilen değerler kullanılmıştır. 6 değerden ilki olan %8, birbirlerine yakın değerler olan diğer 5 değerden (%98, %96, %95, %87, %70) olumsuz yönde ayrışıyor olması nedeniyle ilk değer hesaba katılmayarak diğer 5 değerin ortalaması alınmış ve başarısız girişim olasılığı %89 olarak değerlendirilmiştir.

Tablo 7'de ağın Tespit Edici, Önleyici Eylem ve Sonuç Düğümleri bölümünün yapısı verilmiştir. Belirtilen düğümlerle hazırlanmış Bayes Ağı Şekil 28'de gösterilmiştir.

Tablo 7. Ağın Tespit Edici ve Önleyici Eylem Düğümler bölümlerinin yapısı

Düğüm Adı	Değişkenler	Olasılık		Ebevyn Düğüm	Çocuk Düğüm	Çocuk Düğüm Olumsuzluk İfadesi
Siber Saldırı	Olur	%57	Uzmanlar Tarafından Değerlendirilmiştir	Konum Belirleme Sistemi, AIS, ECDIS, Otomasyon Haberleşme Bilgisayar Sistemi	Siber Zarar	Olur
	Olmaz	%43			Başarısız Girişim	Hayır
Yedek Ekipman	Var	%60		Kök Düğüm	Siber Zarar	Olur
	Yok	%40				
Dijital Verinin Doğrulanması	Yapılıyor	%63		Kök Düğüm		
	Yapılmıyor	%37				



Şekil 28. Bayes Ağı

2.3. Uzman Değerlendirmesi

Uzman görüşlerinden faydalanmak, Bayes Ağı ile yapılan çalışmalarda sıkça kullanılan bir yöntemdir fakat bir kişiden alınacak görüş hatalı ya da eksik olabilmektedir. Bu sorunun üstesinden gelmenin etkili ve sıkça kullanılan yolu bir kişi yerine çok sayıda kişinin görüşlerinin alınmasıdır. Bu çalışmada da farklı özelliklerde uzman görüşleri, bu özelliklerine göre ağırlıklandırılarak kullanılmıştır. Uzman *i*'nin görüşü x_i olmak üzere ve her ω_i (*i*=1,2, ….6) normalleştirilmiş uzman *i* ağırlık değeri iken

($\sum_{i=1}^{6} \omega_i = 1$) bu işlem şu denklem uyarınca yapılmıştır:

$$x = \omega_1 \times x_1 + \omega_2 \times x_2 + \omega_3 \times x_3 + \omega_4 \times x_4 + \omega_5 \times x_5 + \omega_6 \times x_6 = \sum_{i=1}^{6} w_i x_i \quad (6)$$

Çalışma kapsamında değerlendirme yapan uzmanların özellikleri aşağıda verilmiştir. Uzmanlar bu özelliklerine göre 6 numaralı formül kullanılarak ağırlıklandırılmıştır (Tablo 8 ve Tablo 9).

- Aktif olarak denizde çalışan gemiadamları,
- Aktif deniz hayatını tamamlamış, denizcilik şirketinde üst düzey yönetici,
- Gemi adamı ehliyetine sahip, deniz tecrübesi bulunan, siber güvenlik konusunda doktora seviyesinde lisans üstü çalışma yapmakta olan öğretim elemanları,
- Elektronik konusunda doktora seviyesinde lisansüstü çalışmak yapmakta olan öğretim elemanı,
- Siber güvenlik konusunda yüksek lisansını tamamlamış, askeri gemide görevli muvazzaf subay,
- Askeri gemilerde ve tesislerde elektronik konusunda görev yapmış, günümüzde ticari gemilerin elektronik ve teknik gereksinimlerini karşılamak üzere kurduğu kendi şirketinde görev yapan yetkili.

Tablo 8. Uzman değerlendirme etkisi

UZMAN DEĞERLENDİRME									
No	Meslek	Öğrenim	Çalışma Alanı	Deneyim Süresi	Ağırlık Faktörü			Toplam Ağırlık	Değerlendirme Etkisi
1	Araştırma Görevlisi	C	J	M	3	5	3	11	0,150685
2	Doktora Öğrencisi	E	J	L	5	5	2	12	0,164384
3	Araştırma Görevlisi	E	J	K	5	5	1	11	0,150685
4	Elektroteknik Zabiti	A	F	K	1	1	1	3	0,041096
5	DPA	D	H	M	4	3	3	10	0,136986
6	Uzakyol Kaptan	D	G	M	4	2	3	9	0,123288
7	Deniz Subayı	E	G	M	5	2	3	10	0,136986
8	Şirket Sahibi	B	I	K	2	4	1	7	0,095890
				TOPLAM				73	1,000000

Tablo 9. Değerlendirme kriterleri ve ağırlıkları

Kriter	Kod	Açıklama	Ağırlık
Öğrenim	A	Lisans / Diğer	1
	B	Lisans + Yüksek Lisans, Doktora / Diğer	2
	C	Lisans + Yüksek Lisans, Doktora / Elektronik, Haberleşme	3
	D	Lisans / Denizcilik	4
	E	Lisans + Yüksek Lisans, Doktora / Denizcilik, Siber Güvenlik	5
Çalışma Alanı	F	Gemi Personeli / Güverte zabiti, Elektro Teknik Zabiti	1
	G	Gemi Personeli / Kaptan, Subay	2
	H	Armatör Şirketi Görevlisi / DPA - Teknik Müdür	3
	I	Deniz, Gemi Elektronik Sistemleri / Şirket Sahibi, Teknisyen	4
	J	Araştırma - Öğretim Görevlisi / Denizcilik - Siber Güvenlik	5
Deneyim Süresi	K	0 - 5 Yıl	1
	L	6 - 10 Yıl	2
	M	10 Yıldan Fazla	3

2.4. Bulanık Mantık Metodu

Prof. Dr. Lütfi A. Zadeh bulanık mantığın modern anlamda kurucusu olarak gösterilmektedir (Bih, 2006). Bulanık mantık yönteminde, kesin değerlere dayanan düşünce sistemi yerine, yaklaşık düşünce sistemi ve terimleri kullanılmaktadır (Zadeh, 1965). Bulanık mantığı klasik mantık sistemlerinden ayıran farklılık dilsel değişkenlerin

kullanımına izin vermesidir. Bulanık mantık yaklaşımına uygun gelen modelleme problemlerinde, genellikle bir uzmanın tecrübe ve bilgisinden yararlanılmaktadır. Uzman kişi; sözlü değişkenler olarak ifade edilen "uygun, uygun değil, alçak, biraz alçak, az, çok az, kısa, çok kısa" gibi günlük yaşantıda sıkça kullanılan kelimelerle derecelendirme yaparak, esnek bir denetim mekanizması oluşturmaktadır. Böylece sözlü ifadeler yani değişken değeri olan sözcükler kullanılarak, net olarak ifade edilemeyen karar ve kavramların yaklaşık olarak nitelenebilmesi sağlanır (Zadeh, 1975). Bir başka ifadeyle bulanık mantık, belirsiz durumlar için kullanılan sözel ifadeleri insan düşünce yapısına uygun durumda matematiksel bir temele dayandırarak bilgisayar ortamına aktarılmasını sağlamaktadır (Akıllı ve Atıl, 2014).

Bulanık küme, sürekli dizi halindeki üyelik derecelerine sahip nesnelerden oluşan bir sınıf olarak ifade edilmektedir (Zadeh, 1965). Bu tip bir küme, bir üyelik fonksiyonu ile tanımlanmış olup her bir nesneye 0 ile 1 arasında üyelik derecesi atar. Zadeh, klasik mantıktan farklı olarak ara değerlerin de göz önünde bulundurulması gerektiğini ifade etmiştir (Zadeh, 1965). Buradaki 0 sayısı, ilgili nesnenin kümeye ait olan bir üye olmadığını, 1 sayısı ilgili nesnenin kümenin tam üyesi olduğunu, 0 ile 1 arasındaki herhangi bir sayı ise ilgili nesnenin kümeye üyelik derecesini veya kısmi üyeliğini gösterir (Zimmermann, 1993). Eğer A $R \in (-\infty, +\infty)$' da, söz konusu kümenin bir elemanı ise $\mu A(x)$ üyelik fonksiyonu $R \rightarrow [0, 1]$ aralığında oluşur. Üyelik fonksiyonları genellikle, üçgen üyelik fonksiyonları ve yamuk üyelik fonksiyonları olmak üzere iki başlık altında incelenmektedir. Bu çalışmada üçgen üyelik fonksiyonları kullanılmıştır.

Rajakarunakaran vd.'nin (2015) çalışmasından yararlanılarak bulanık yaklaşımın aşamaları şu şekilde açıklanabilir:

1. Bulanıklaştırma: Bulanıklaştırma, bulanık kümelerin sisteme uyum sağlayacak şekilde oluşturulmasıdır. Bu aşamada; veri setlerinin, sistemin çıkarım mekanizması ile bulanık kural tabanındaki kayıtlı olan veriler kullanılarak işlenmesi için gerekli hazırlıklar yapılmaktadır (Wang, 1997).

Bu çalışmada üçgen bulanık sayıları (TFN) siber saldırının koşullu olasılık hesaplaması için kullanılmıştır. TFN, a_1, a_2, a_3 gibi bulanık olasılık değerlerinin üçlü setini temsil etmektedir. A bir bulanık sayı, aralık R→ [0,1], xϵA olmak üzere $\mu_{\check{A}}(x)$, A bulanık sayı kümesinin üyelik (membership) fonksiyonudur. A kümesinin $[a_1, a_3]$ aralığında olduğu kabul edilirse $\mu_{\check{A}}(x)$ üyelik fonksiyonu aşağıdaki gibi hesaplanır (Wang, 1997).

$$\mu_{\tilde{A}}(x) = \begin{cases} 0 & x \le a_1 \\ (x-a_1)/(a_2-a_1) & a_1 \le x \le a_2 \\ (a_3-x)/(a_3-a_2) & a_2 \le x \le a_3 \\ 0 & x \ge a_3 \end{cases} \quad (7)$$

2. Birleştirme: Heterojen bir grup içerisindeki uzmanların farklı deneyimleri temel olaylara (BE) ilişkin çeşitli fikirlerin çıkmasını sağlamaktadır. Önemli olan uzmanların tüm yargılarını bir araya getirmek ve düşüncelerini uzlaştırmaktır. Hsu ve Chen (1994) bu konuda bir algoritma önermiştir.

$\widetilde{R1}, \widetilde{R2}$: Bir çift uzman görüşü

$S_{UV}(\widetilde{R1}, \widetilde{R2})$: İki farklı uzman görüşünün benzerlik derecesi

$S(\tilde{A}_1, \tilde{A}_2)$: İki bulanık sayı kümesi arasındaki benzerlik derecesi

$AA(E_u)$: Uzmanların ortalama anlaşma dercesi

$RA(E_u)$: Uzmanların değişken anlaşma dercesi

$CC(E_u)$: Uzman Konsensus Katsayısı

$\tilde{R}_{AG}$: Uzman kararlarının toplam sonucu olarak ifade edilmektedir.

1. Adım: Her bir uzman E_U (u =1,2,3 … M) şeklinde ifade edilir. Bir çift uzmanın $\widetilde{R1}$ ve $\widetilde{R2}$ görüşlerinin arasındaki $S_{UV}(\widetilde{R1}, \widetilde{R2})$ benzerlik derecesi hesaplanacaktır.

Bu yaklaşıma göre, $\tilde{A}_1 = (a_{11}, a_{12}, a_{13})$ ve $\tilde{A}_2 = (a_{21}, a_{22}, a_{23})$ iki standart üçgen bulanık sayılar kümesini oluşturmaktadır. Bu iki bulanık sayı kümesi arasındaki benzerlik derecesi benzerlik fonksiyonu ile hesaplanır.

$$S(\tilde{A}_1, \tilde{A}_2) = 1 - (1/3) \sum_{i=1}^{3} | a_{1i} - a_{2i} | \quad (8)$$

2. Adım: M tane uzmanın ortalama anlaşma (AA) derecesi aşağıdaki gibi hesaplanır.

$$AA(E_u) = \frac{1}{M-1 \sum_{\substack{U \neq V \\ V=1}}^{M} S(\tilde{A}_1, \tilde{A}_2)} \quad (9)$$

3. Adım: M tane uzmanın değişken anlaşma (RA) derecesi aşağıdaki gibi hesaplanır.

$$RA(E_u) = \frac{AA(E_U)}{\sum_{1}^{M} AA(E_U)} \quad (10)$$

4. Adım: M tane uzmanın konsesus katsayısı (CC) aşağıdaki gibi hesaplanır.

$$CC(E_U) = \beta . w(E_U) + (1 - \beta) . RA(E_U) \quad (11)$$

β (0≤β≤1) önerilen yöntemin gevşetme faktörüdür ve bu w (E_u) 'nin (weight factor of expert) RA (E_u) üzerindeki önemini göstermektedir. β = 0 olduğunda uzmanın ağırlık faktörüne önem verilmez, uzmanlar arasında homojen bir dağılım mevcuttur. β = 1 olduğunda ise uzmanın konsesus katsayısı derecesi ile ağırlık önemi aynıdır. Bu çalışmada β = 0.5 olarak alınmıştır (Lavasani vd., 2015; Rajakarunakaran vd., 2015).

5. Adım: Uzman görüşlerinin birleştirilmiş sonucu $\tilde{R}_{AG}$ değeri aşağıdaki gibi hesaplanır.

$$\tilde{R}_{AG} = CC(E_1) \times \tilde{R}_1 + CC(E_2) \times \tilde{R}_2 + \ldots + CC(E_M) \times \tilde{R}_M \quad (12)$$

3. Durulaştırma: Durulaştırma işleminin amacı bulanık mantıkta ölçülebilir sonuçlar elde etmektir. Yani durulaştırma, bulanık sayı veya bulanık küme elemanlarının gerçek sayıya dönüştürüldüğü süreç olarak ifade edilmektedir (Bayram vd., 2002). Bulanık sayıların netleştirilmesi, belirsiz konularda karar vermek için oldukça önemlidir. Bulanık derecelendirmeler Bayes Ağı'na ait bir probleme dahil edildiğinde sonuçta elde edilen derecelendirme yine bulanık sayıdır. Bu sayılar arasındaki ilişkiyi belirlemek için bulanık sayının bulanık olasılık puanına (FPS) dönüştürülmesi gerekmektedir. Temel olay FPS sayısı, uzman görüşü birleştirme aşamasında hesaplaması yapılan son üyelik fonksiyonundan elde edilmektedir. Durulaştırma yöntemleri arasında "mean – max membership, centroid method, weighted average method, centre of largest area, and centre of sums" gibi yöntemler yer almaktadır (Wang, 1997). Bu çalışmada; her bir temel olayın bulanık olasılık değeri, en çok tercih edilen durulaştırma yöntemi olan merkezi alan durulaştırma (centre of area) yöntemi ile hesaplanmıştır. Bu yöntem 1985 yılında Sugeno tarafından geliştirilmiştir.

Durulaştırma denklemi: $X^* = \frac{\int \mu_i(x)\, dx}{\int \mu_i(x)}$ (13)

Üçgen bulanık sayı $\widetilde{A} = (a_1, a_2, a_3)$ için formül aşağıdaki gibidir.

$$X = \frac{\int_{a_1}^{a_2} \frac{x-a_1}{a_2-a_1} x\,dx + \int_{a_2}^{a_3} \frac{a_3-x}{a_3-a_2} x\,dx}{\int_{a_1}^{a_2} \frac{x-a_1}{a_2-a_1} dx + \int_{a_2}^{a_3} \frac{a_3-x}{a_3-a_2} dx} = \frac{1}{3}(a_1 + a_2 + a_3) \quad (14)$$

2.4.1. Bulanık Mantık Hesaplamalarından Elde Edilen Veriler

Yapılan çalışmada uzmanların değerlendirme kriterlerini oluşturan sözel ifadeler ve bunlara karşılık gelen üçgen bulanık sayılar Tablo 10'da verilmiştir.

Tablo 10. Sözlü ölçüm terimleri ve üçgen bulanık sayı değeri karşılıkları (Rajakarunakaran, 2015).

		Üçgen Bulanık Sayılar		
Ölçüm Terimi	Ölçüm Terimi Kısaltması	A	B	C
Very Low (Çok Düşük)	VL	0	0,04	0,08
Low (Düşük)	L	0,07	0,13	0,19
Reasonable Low (Biraz Düşük)	ML	0,17	0,27	0,37
Medium (Orta)	M	0,35	0,5	0,65
Reasonable High (Biraz Yüksek)	MH	0,63	0,73	0,83
High (Yüksek)	H	0,81	0,87	0,93
Very High (Çok Yüksek)	VH	0,92	0,96	1,0

İlk 5 koşullu olasılık durumu için uzmanların sözlü değerlendirmesi ve bu sözlü değerlendirmelerin üçgen bulanık sayılara çevrildiği bulanıklaştırma aşamasına dair veriler Tablo 11, Tablo 12 ve Tablo 13'de verilmiştir. Diğer koşullu olasılık durumları için uzmanların sözlü değerlendirme verileri Ek Tablo 1'de verilmiştir.

Tablo 11. İlk 5 koşullu olasılık durumu için uzman sözlü değerlendirme verileri

Koşullu Olasılık No	Cihaz Çifti Düğümü	Coğrafi Konum Düğümü	Sinyal Seviyesi Filtresi Düğümü	Uzman Numarası ve Uzman Sözlü Değerlendirme Konum Belirleme Sistemi GÜVENLİ							
				1	2	3	4	5	6	7	8
1	2 GPS	KARADENİZ-KORE YA.	VAR	M	ML	H	MH	M	L	H	H
2	2 GPS	KARADENİZ-KORE YA.	YOK	L	VL	ML	M	ML	VL	L	H
3	2 GPS	DİĞER	VAR	MH	ML	MH	H	H	M	H	H
4	2 GPS	DİĞER	YOK	L	L	M	MH	MH	ML	L	H
5	GPS + GLONASS	KARADENİZ-KORE YA.	VAR	H	M	VH	MH	MH	H	VH	MH

Tablo 12. İlk 5 koşullu olasılık durumu için üçgen bulanık sayı verileri, Uzman 1~4

Koşullu Olasılık No	Uzman 1			Uzman 2			Uzman 3			Uzman 4		
	A	B	C	A	B	C	A	B	C	A	B	C
1	0,35	0,50	0,65	0,17	0,27	0,37	0,81	0,87	0,93	0,63	0,73	0,83
2	0,07	0,13	0,19	0,00	0,04	0,08	0,17	0,27	0,37	0,35	0,50	0,65
3	0,63	0,73	0,83	0,17	0,27	0,37	0,63	0,73	0,83	0,81	0,87	0,93
4	0,07	0,13	0,19	0,07	0,13	0,19	0,35	0,50	0,65	0,63	0,73	0,83
5	0,81	0,87	0,93	0,35	0,50	0,65	0,92	0,96	1,00	0,63	0,73	0,83

Tablo 13. İlk 5 koşullu olasılık durumu için üçgen bulanık sayı verileri, Uzman 5~8

Koşullu Olasılık No	Uzman 5			Uzman 6			Uzman 7			Uzman 8		
	A	B	C	A	B	C	A	B	C	A	B	C
1	0,35	0,50	0,65	0,07	0,13	0,19	0,81	0,87	0,93	0,81	0,87	0,93
2	0,17	0,27	0,37	0,00	0,04	0,08	0,07	0,13	0,19	0,81	0,87	0,93
3	0,81	0,87	0,93	0,35	0,50	0,65	0,81	0,87	0,93	0,81	0,87	0,93
4	0,63	0,73	0,83	0,17	0,27	0,37	0,07	0,13	0,19	0,81	0,87	0,93
5	0,63	0,73	0,83	0,81	0,87	0,93	0,92	0,96	1,00	0,63	0,73	0,83

İkinci aşama olan birleştirmenin 4 adımı mevcuttur. İlk 5 koşullu olasılık durumu için; Tablo 14, Tablo 15 ve Tablo 16'da birinci adım olan Benzerlik Fonksiyonu, Tablo 17'de ikinci adım olan Ortalama Anlaşma, Tablo 18'de üçüncü adım olan Değişken Anlaşma, Tablo 19'da ise dördüncü adım olan Konsesus Katsayısı verileri belirtilmiştir.

Tablo 14. İlk 5 koşullu olasılık durumu için Benzerlik Fonksiyonu verileri S(1-2)~S(2-5)

Koşullu Olasılık No	Benzerlik Fonksiyonu Verileri									
	S(1-2)	S(1-3)	S(1-4)	S(1-5)	S(1-6)	S(1-7)	S(1-8)	S(2-3)	S(2-4)	S(2-5)
1	0,77	0,63	0,77	1,00	0,63	0,63	0,63	0,40	0,54	0,77
2	0,91	0,86	0,63	0,86	0,91	1,00	0,26	0,77	0,54	0,77
3	0,54	1,00	0,86	0,86	0,77	0,86	0,86	0,54	0,40	0,40
4	1,00	0,63	0,40	0,40	0,86	1,00	0,26	0,63	0,40	0,40
5	0,63	0,91	0,86	0,86	1,00	0,91	0,86	0,54	0,77	0,77

Tablo 15. İlk 5 koşullu olasılık durumu için Benzerlik Fonksiyonu verileri S(2-6)~S(4-5)

Koşullu Olasılık No	Benzerlik Fonksiyonu Verileri								
	S(2-6)	S(2-7)	S(2-8)	S(3-4)	S(3-5)	S(3-6)	S(3-7)	S(3-8)	S(4-5)
1	0,86	0,40	0,40	0,86	0,63	0,26	1,00	1,00	0,77
2	1,00	0,91	0,17	0,77	1,00	0,77	0,86	0,40	0,77
3	0,77	0,40	0,40	0,86	0,86	0,77	0,86	0,86	1,00
4	0,86	1,00	0,26	0,77	0,77	0,77	0,63	0,63	1,00
5	0,63	0,54	0,77	0,77	0,77	0,91	1,00	0,77	1,00

Tablo 16. İlk 5 koşullu olasılık durumu için Benzerlik Fonksiyonu verileri S(4-6)~S(7-8)

Koşullu Olasılık No	Benzerlik Fonksiyonu Verileri								
	S(4-6)	S(4-7)	S(4-8)	S(5-6)	S(5-7)	S(5-8)	S(6-7)	S(6-8)	S(7-8)
1	0,40	0,86	0,86	0,63	0,63	0,63	0,26	0,26	1,00
2	0,54	0,63	0,59	0,77	0,86	0,40	0,91	0,17	0,26
3	0,63	1,00	0,96	0,63	1,00	1,00	0,63	0,63	1,00
4	0,54	0,40	0,82	0,54	0,40	0,86	0,86	0,40	0,26
5	0,86	0,77	0,93	0,86	0,77	1,00	0,91	0,86	0,770

Tablo 17. İlk 5 koşullu olasılık durumu için Ortalama Anlaşma verileri

Koşullu Olasılık No	Ortalama Anlaşma Verileri							
	AA(E1)	AA(E2)	AA(E3)	AA(E4)	AA(E5)	AA(E6)	AA(E7)	AA(E8)
1	0,72286	0,59143	0,68286	0,72286	0,72286	0,47143	0,68286	0,68286
2	0,77571	0,72429	0,77571	0,63857	0,77571	0,72429	0,77571	0,32143
3	0,82143	0,49286	0,82143	0,81571	0,82143	0,69000	0,82143	0,81571
4	0,65000	0,65000	0,69000	0,61857	0,62429	0,69000	0,65000	0,49857
5	0,86143	0,66429	0,81000	0,85190	0,86143	0,86143	0,81000	0,85190

Tablo 18. İlk 5 koşullu olasılık durumu için Değişken Anlaşma verileri

Koşullu Olasılık No	Değişken Anlaşma Verileri							
	RA(E1)	RA(E2)	RA(E3)	RA(E4)	RA(E5)	RA(E6)	RA(E7)	RA(E8)
1	0,13690	0,11201	0,12933	0,13690	0,13690	0,08929	0,12933	0,12933
2	0,14075	0,13142	0,14075	0,11586	0,14075	0,13142	0,14075	0,05832
3	0,13466	0,08080	0,13466	0,13372	0,13466	0,11311	0,13466	0,13372
4	0,12817	0,12817	0,13606	0,12197	0,12310	0,13606	0,12817	0,09831
5	0,13107	0,10107	0,12324	0,12962	0,13107	0,13107	0,12324	0,12962

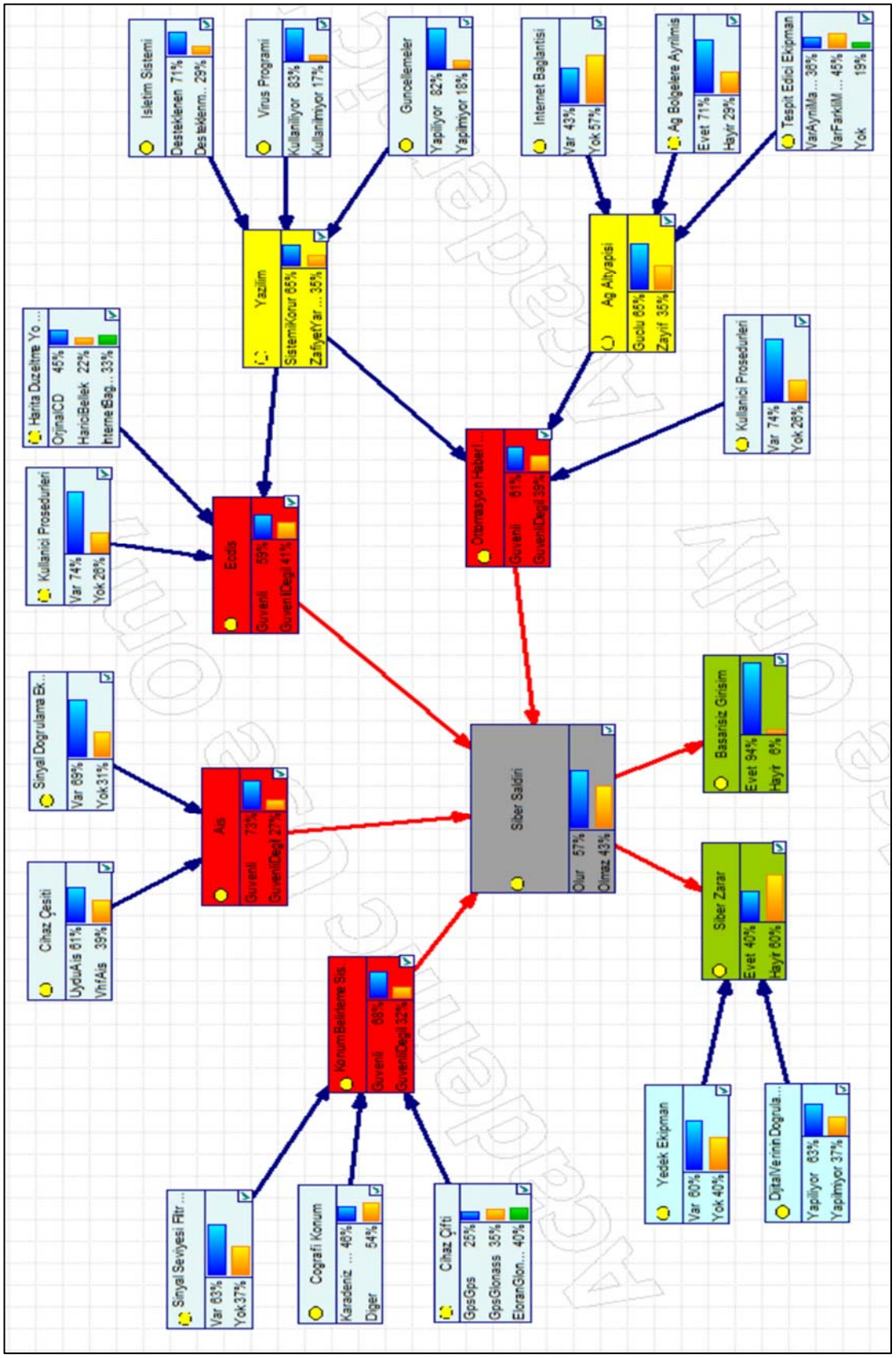
Tablo 19. İlk 5 koşullu olasılık durumu için Konsensus Katsayısı verileri

Koşullu Olasılık No	Konsensus Katsayısı Verileri							
	CC(E1)	CC(E2)	CC(E3)	CC(E4)	CC(E5)	CC(E6)	CC(E7)	CC(E8)
1	0,14379	0,13820	0,14001	0,08900	0,13695	0,10629	0,13316	0,11261
2	0,14572	0,14790	0,14572	0,07848	0,13887	0,12735	0,13887	0,07711
3	0,14267	0,12259	0,14267	0,08741	0,13582	0,11820	0,13582	0,11481
4	0,13943	0,14628	0,14337	0,08153	0,13004	0,12967	0,13258	0,09710
5	0,14088	0,13273	0,13696	0,08536	0,13403	0,12718	0,13011	0,11275

İlk 5 koşullu olasılık durumu için üçüncü aşama olan durulaştırma ve ona bağlı olarak bulanık olasılık değeri verileri Tablo 20'de verilmiştir. 25 adet düğümün oluşturduğu 82 adet koşullu olasılık durumu için belirlenen bulanık olasılık değerleri Genie programına girilmiş ve sonuç düğümlerin olasılıkları elde edilmiştir (Şekil 29). Diğer koşullu olasılık durumlarına ait bulanık olasılık değerleri Ek Tablo 1'de verilmiştir.

Tablo 20. İlk 5 koşullu olasılık durumu için Durulaştırma ve Bulanık Olasılık verileri

Koşullu Olasılık No	Durulaştırma Değerleri			Bulanık Olasılık Değeri
1	0,49774	0,59209	0,68645	0,592094897
2	0,15822	0,23116	0,30411	0,23116433
3	0,62581	0,71276	0,79972	0,712763258
4	0,31345	0,40000	0,48655	0,4000011
5	0,71854	0,79843	0,87832	0,798428255



Şekil 29. Bulanık olasılık değeri girilmiş durumu ile Bayes Ağı.

2.5. Hassasiyet Analizi

Bu çalışmada tüm hesaplamalar ve analizler için hassasiyet analizi yöntemi uygulanmıştır. Diğer düğümlerin olasılık değerleri sabit tutularak hassasiyet analizi uygulanacak düğümün olasılık değeri ilk önce 0 sonra 100 yapılarak etkinin ilgili çoçuk düğümün olasılık değerlerindeki değişimi yani sonuca etkisi incelenmiştir.

Hassasiyet analizi için Genie adlı yazılım programı kullanılmıştır. Genie, kolay ve anlaşılır arayüzü nedeniyle seçilmiştir (Fusion, 2017). Genie'nin grafiksel arayüzü benzer amaçlı programlara göre önemli bir avantajdır (Murphy, 2007).

İlk önce incelenen 4 sistemin her birinin kök ve ebeveyn düğümleri teker teker değerlendirilmiştir. Sonrasında siber saldırı düğümünün ebeveyn düğümleri olan bu 4 sistem düğümlerinin olasılıkları değerlendirilmiştir. En son olarak da siber zarar; 2 adet kök düğümü ve siber saldırı ebeveyn düğümü ile hassasiyet analizine tabi tutulmuştur. Hassasiyet analizi sonuçları Tablo 21'de verilmiştir.

Tablo 21. Hassasiyet analizi sonuçları

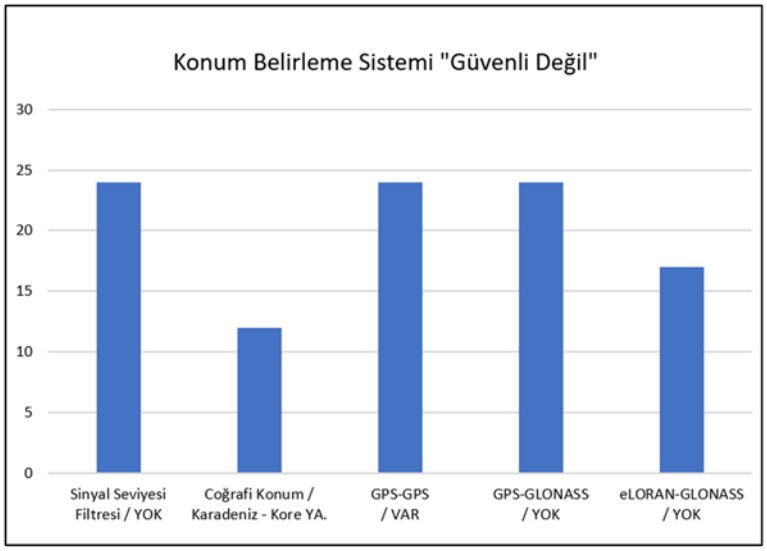
Değişken	Olumsuzluk	Kötü Durum	İyi Durum	Fark	Çocuk Düğüm ve Orijinal Yüzdesi		3 Değişkenli Düğümler İçin Not
Sinyal Seviyesi Filtresi	Yok	47	23	24	Konum Belirleme Sistemi Güvenli Değil	32	
Coğrafi konum	Karadeniz – Kore Yarımadası	36	28	12			
GPS – GPS	***Var***	47	23	24			İyi durumda: GPS – GLONASS var
GPS – GLONASS	Yok	47	23	24			Kötü durumda: GPS – GPS var
eLORAN – GLONASS	Yok	47	30	17			Kötü durumda: GPS – GPS var
Cihaz Çeşiti	VHF AIS	43	16	27	AIS Güvenli Değil	27	
Sinyal Doğrulama Ekipmanı	Yok	44	19	25			
İşletim Sistemi	Desteklenmeyen	71	20	51	Yazılım Zafiyet Yaratır	35	
Virüs Programı	Kullanılmıyor	62	29	33			
Güncellemeler	Yapılmıyor	57	30	27			

Tablo 21'in devamı

Değişken	Olumsuzluk	Kötü Durum	İyi Durum	Fark	Çocuk Düğüm ve Orijinal Yüzdesi		3 Değişkenli Düğümler İçin Not
Kullanıcı Prosedürleri	Yok	59	34	25	ECDIS Güvenli Değil	41	
Yazılım	Zafiyet Yaratır	68	26	42			
Harici Bellek	***Var***	52	27	25			İyi durumda: Orj CD ile
İnternet Bağlantısı	***Var***	51	27	24			İyi durumda: Orj CD ile
Orijinal Düzletme CD'si	Yok	52	27	25			Kötü durumda: Harici Bellek ile
İnternet bağlantısı	***Var***	46	26	20	Ağ Altyapısı Zayıf	35	
Ağ bölgelere ayrılmış	Hayır	61	24	37			
Tespit Edici Ekipman Yok	***Var***	53	27	26			İyi durumda: Var Farklı Marka
Tespit Edici Ekipman Var Aynı marka	Yok	53	35	18			Kötü durumda: Yok
Tespit Edici Ekipman Var Farklı marka	Yok	53	27	26			
Yazılım	Zafiyet Yaratır	66	24	42	Otomasyon Haberleşme Bilgisayar Sistemi Güvenli Değil	39	
Ağ altyapısı	Zayıf	58	28	30			
Kullanıcı Prosedürleri	Yok	56	33	23			
Konum Belirleme Sistemi	Güvenli Değil	65	50	15	***Siber Saldırı Olur***	55	
AIS	Güvenli Değil	65	51	14			
ECDIS	Güvenli Değil	74	41	33			
Otomasyon Haberleşme Bilgisayar Sistemi	Güvenli Değil	78	44	34			
Siber Saldırı	***Olur***	61	12	49	***Siber Zarar Evet***	39	
Yedek Ekipman	Yok	49	32	17			
Dijital Verilerin Doğrulanması	Yapılmıyor	50	33	17			

3. BULGULAR VE İRDELEME

Deniz ulaştırma sistemleri, dünya ekonomisinin sürdürülebilirliği için kritik süreçleri içine alan bir yapıya sahiptir. Uluslararası ticaretinin önemli bir bölümü deniz taşımacılığı ile yapılmaktadır. Deniz ulaştırma sistemlerindeki olası bir aksaklık tüm tedarik zincirini etkileyecek ve yüksek maliyetli zararlara neden olabilecektir. Bu açıdan bakıldığında denizcilik sektörü, siber güvenlik farkındalığı az fakat siber güvenlik riskleri yüksek olan bir sektör olarak karşımıza çıkmaktadır (Yüksel ve Uygur, 2016). Gemilere yönelik siber risklerin artmış olması dijital bağlantıların ve küresel seyir sistemlerine bağımlılığın artmış olmasının bir sonucudur. Bu nedenle siber güvenlik; bilgi sistemlerinin kendisinin, içerisindeki bilginin, sistemin sağladığı hizmetlerin izinsiz erişimden, zarardan ve yanlış kullanımdan korumak anlamındadır (Shaikh, 2017). Bu çalışmada, akademik çalışmalardan ve gerçekleşmiş siber olaylardan yararlanılarak daha siber güvenli seyir yardımcı sistemlerinin oluşturulabilmesi amaçlı hazırlanan Bayes Ağının düğümlerinin meydana getirdiği koşullu olasılık durumları hassasiyet analizi ile değerlendirilmiştir. Dijital cihazların kullanımının ve onlara bağımlılığın arttığı denizcilik alanında siber güvenlik farkındalık kısıtlarının yarattığı siber riskler belirlenmeye çalışılmıştır, elde edilen bulgular aşağıda sunulmuştur.



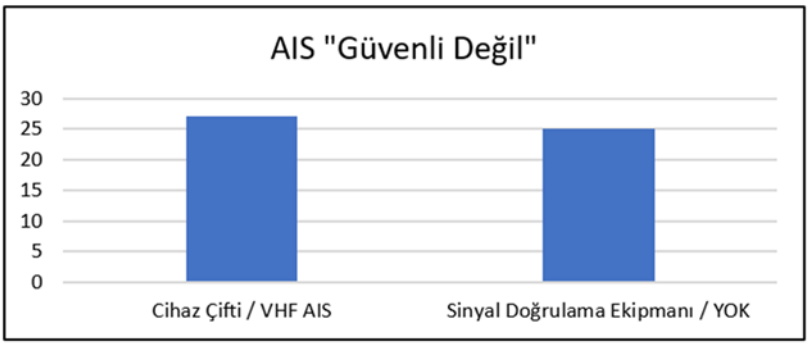
Şekil 30. Konum Belirleme Sistemi'nin siber güvenli olma durumunu etkileyen faktörler

Konum Belirleme Sistemi'nin güvenli olması durumunu Sinyal Seviyesi Filtresi %24, Coğrafi Konum %12 oranında etkilemiştir. Cihaz çifti seçeneklerinden GPS – GPS %24, GPS – GLONASS %24, eLORAN – GLONASS ise %17 oranında Konum Belirleme Sistemi'nin siber güvenli olması durumunu etkilemiştir (Şekil 30).

Sinyal seviyesi filtresi gemilerdeki mevcut uygulamalarda yaygın olarak kullanılmamaktadır. Fakat kullanılmasında siber güvenliği arttıracağı için yarar görülmüştür. Coğrafi Konumun ise sistemin güvenliğine çok fazla bir etkisi yoktur. Her ne kadar gerçekleşmiş siber saldırılar Karadeniz ve Kore Yarımadası çevresinde meydana gelmişlerse de değerlendirme yapan uzmanların doğrudan bu konuyu deneyimlememiş olmaları bu sonucu doğurmuştur. En yaygın kullanılan konum belirleme sistemi olan GPS'in hem tek sisteme bağlı kalmanın yarattığı risk hem de diğer sistemlere nazaran siber anlamda daha zayıf olması nedeniyle GPS – GPS cihaz çiftinin kullanılması %24 oranı ile riskli görülmüştür. En güvenli sistem olan eLORAN'a ise kullanıcı gözüyle yaklaşılmıştır. Hem dünya genelinde yaygın kullanımının olmaması, hem eriminin şu an için sınırlı olması, hem de hali hazırda geliştirilmekte olan bir sistem olması sebebiyle uydu tabanlı sistemlere nazaran %17 ile daha olumsuz görülmüştür. Uydu tabanlı sistemler kullanıcı gözüyle değerlendirildiğinde yaygın kullanım ve sisteme aşinalık, en az güvenli sistem olan GPS'i de içinde barındırıyor olmasına rağmen sistem çeşitliliğinin getireceği güvenlik artısı nedeniyle GPS – GLONASS cihaz çiftini %24'lük oran ile ön plana çıkarmıştır.

Sinyal Seviyesi Filtresinin "VAR" olduğu, Coğrafi Konumunun "DİĞER" olduğu, Cihaz Çiftinin "GPS – GLONASS" olduğu düzende Konum Belirleme Sistemi %86 ile en güvenli durumdadır. Sinyal Seviyesi Filtresinin "YOK" olduğu, Coğrafi Konumunun "KARADENİZ – KORE YARIMADASI" olduğu, Cihaz Çiftinin "GPS – GPS" olduğu düzende Konum Belirleme Sistemi %23 ile en az güvenli durumdadır. Üçlü koşullu olasılık değerlendirmesinde değişkenler %63 oranında sistemin güvenliğine etkide bulunmaktadır.

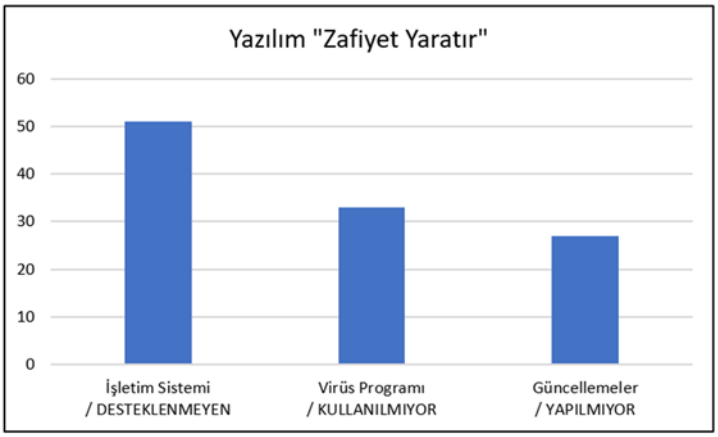
AIS sisteminin güvenli olma durumunu Cihaz Çifti %27, Sinyal Doğrulama Ekipmanı ise %25 oranında etkilemektedir (Şekil 31). Gemilerdeki mevcut uygulamalarda yaygın olarak kullanılmayan uydu AIS ve sinyal doğrulama ekipmanı kullanımı siber güvenliğin arttırılması anlamında olumlu değerlendirilmiştir.



Şekil 31. AIS'in siber güvenli olma durumunu etkileyen faktörler

Cihaz Çeşidinin "UYDU AIS", Sinyal Doğrulama Ekipmanının "VAR" olduğu düzende AIS %90 ile en siber güvenli durumdadır. Cihaz Çeşidinin "VHF AIS", Sinyal Doğrulama Ekipmanının "YOK" olduğu düzende AIS %33 ile en az siber güvenli durumdadır. İkili koşullu olasılık değerlendirmesinde değişkenler %57 oranında sistemin güvenliğine etkide bulunmaktadır.

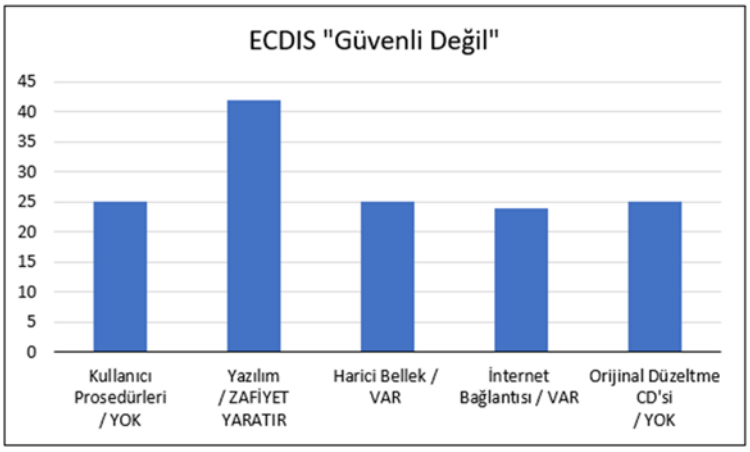
Yazılım konusunda siber güvenliği en çok etkilen faktör %51 ile işletim sistemidir. Virüs programı %33, güncellemeler ise %27 oranında yazılımı etkilemektedir (Şekil 32). Bu düğümdeki değişkenlerin sonucu etkilemedeki oranlarının yüksek olmasının nedeni uzmanların bilgisayar teknolojileri konusundaki bilgilerinin fazla olmasına ve küçük çaplı dahi olsa bilgisayar teknolojileri ile alakalı bir siber olayı deneyimlemiş olmalarına bağlıdır.



Şekil 32. Yazılım'ın siber güvenli olma durumunu etkileyen faktörler

İşletim Sisteminin "DESTEKLENEN" olduğu, Virüs Programının "KULLANILIYOR" olduğu, Güncellemelerin "YAPILIYOR" olduğu düzen Yazılım için %92 ile en siber güvenli durumdur. İşletim Sisteminin "DESTEKLENMEYEN" olduğu, Virüs Programının "KULLANILMIYOR" olduğu, Güncellemelerin "YAPILMIYOR" olduğu düzende Yazılım %8 ile en az siber güvenli durumdadır. Üçlü koşullu olasılık değerlendirmesinde değişkenler %84 oranında sistemin güvenliğine etkide bulunmaktadır.

ECDIS'in siber güvenli olma durumunu Kullanıcı Prosedürleri %25, Yazılım ise %42 oranında etkilemiştir. Harici Bellek %25, İnternet Bağlantısı %24, Orijinal Düzeltme CD'si ise %25 oranında ECDIS'in siber güvenli olması durumunu etkilemektedir (Şekil 33).



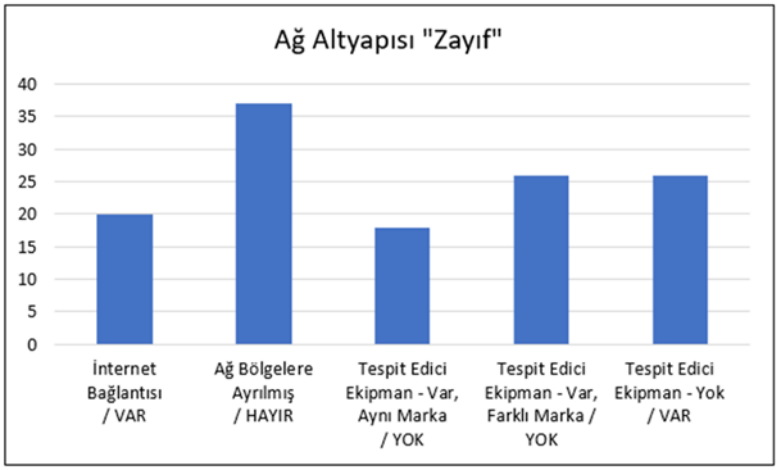
Şekil 33. ECDIS'in siber güvenli olma durumunu etkileyen faktörler

Siber güvenlik; yönetim, bilgi ve teknoloji bilgisine dayanmaktadır. Güvenli denizciliğin sağlanması bu üçlü ilişkinin ve yapının sağlam bir şekilde anlaşılmasına ve kurulmasına bağlıdır. Bu nedenle, gemi adamları da dahil olmak üzere denizcilikte siber saldırılara karşı eğitim her zaman olduğu gibi en önemli etkili yöntemdir (Algantürk Light, 2019). Siber güvenlik eğitimlerinin verilmesi ve siber güvenlik konusunda prosedürlerin, politikaların geliştirilip bilinçli kullanıcı profilinin oluşturulmasının önemi uzmanlar tarafından üst seviyede değerlendirilmiştir. Ayrıca uzmanların bilgisayar teknolojileri konusundaki bilgi ve deneyimleri de diğer düğümlerim içeriklerine göre fazladır. Bu iki etken yukarıda belirtilen oranlarda etkili olmuştur.

Kullanıcı Prosedürlerinin "VAR" olduğu, Yazılımın "SİSTEMİ KORUR" olduğu, Harita Düzeltme Yönteminin "ORJİNAL CD" olduğu düzen %92 ile ECDIS için en siber

güvenli durumdur. Kullanıcı Prosedürlerini "YOK" olduğu, Yazılımın "ZAFİYET YARATIR" olduğu, Harita Düzeltme Yönteminin "HARİCİ BELLEK" olduğu düzende ECDIS %13 ile en az siber güvenli durumdadır. Üçlü koşullu olasılık değerlendirmesinde değişkenler %79 oranında sistemin güvenliğine etkide bulunmaktadır.

Ağ Altyapısının siber güvenli olması durumunu, İnternet Bağlantısı %20, Ağın Bölgelere Ayrılması %37 oranında etkilemiştir. Tespit Edici Ekipman; Yok %26, Var-Aynı Marka %18, Var-Farklı Marka ise %26 oranında Ağ Altyapısının siber güvenli olması durumunu etkilemektedir (Şekil 34).



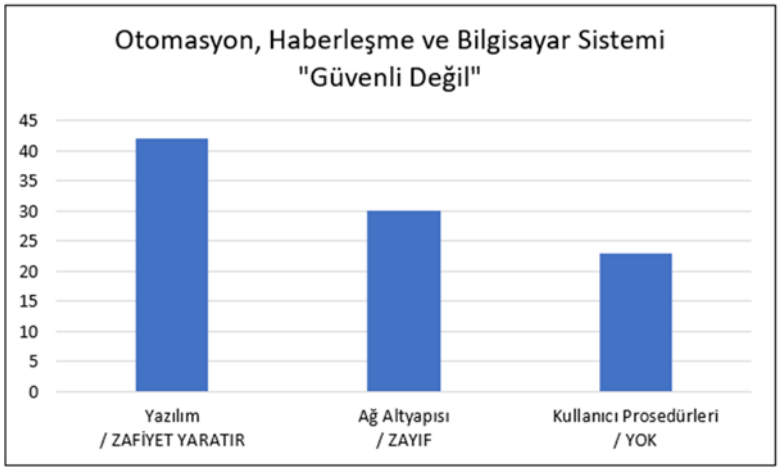
Şekil 34. Ağ Altyapısı'nın siber güvenli olma durumunu etkileyen faktörler

Farklı markada tespit edici ekipman kullanılması siber güvenliği arttıracak bir uygulama olarak değerlendirilmiş olsa da tespit edici ekipman gibi karmaşık ve maliyet arttırıcı çözümler yerine ağın bölgelere ayrılması gibi daha basit ve düşük maliyetli aynı zamanda kullanıcı kolaylığı da sağlayan çözümlere yönelik bakış açısı sonuçlarda etkili olmuştur. Günümüzde internet bağlantısı olmadan işletilebilecek modern bir gemi düşünülemez, buna rağmen ağın internete bağlantısı olması siber anlamda riskli değerlendirmiştir.

İnternet Bağlantısının "YOK" olduğu, Ağ Bölgelere Ayrılmış "EVET" olan, Tespit Edici ekipman "VAR, FARKLI MARKA" olan düzen Ağ Altyapısı için %93 ile en güvenli durumdur. İnternet Bağlantısının "VAR" olduğu, Ağ Bölgelere Ayrılmış "HAYIR" olan, Tespit Edici ekipman "YOK" olan düzende Ağ Altyapısı %9 ile en az siber güvenli

durumdadır. Üçlü koşullu olasılık değerlendirmesinde değişkenler %82 oranında sistemin güvenliğine etkide bulunmaktadır.

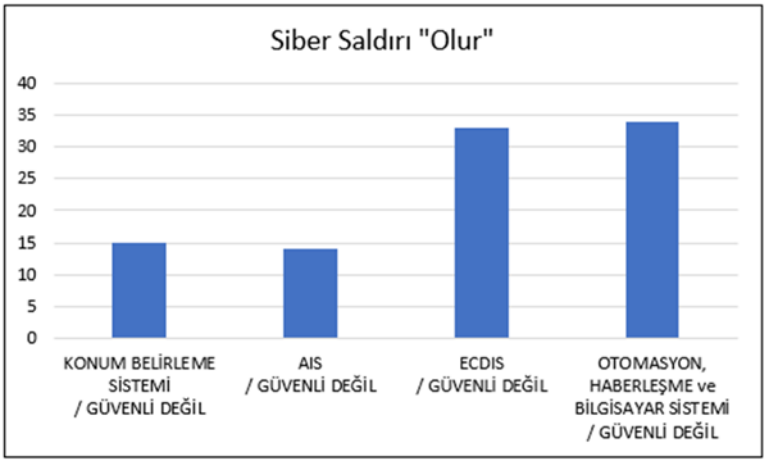
Otomasyon, Haberleşme ve Bilgisayar Sisteminde siber güvenliği en çok etkileyen faktör %42 ile Yazılım'dır. Ağ Altyapısı %30, Kullanıcı Prosedürleri %23 oranında sonucu etkilemektedir (Şekil 35). Uzmanların bilgisayar teknolojileri konusundaki bilgi ve deneyimleri sonuçlar üzerinde etkili olmuştur.



Şekil 35. Otomasyon, Haberleşme, Bilgisayar Sistemi'nin siber güvenli olma durumunu etkileyen faktörler

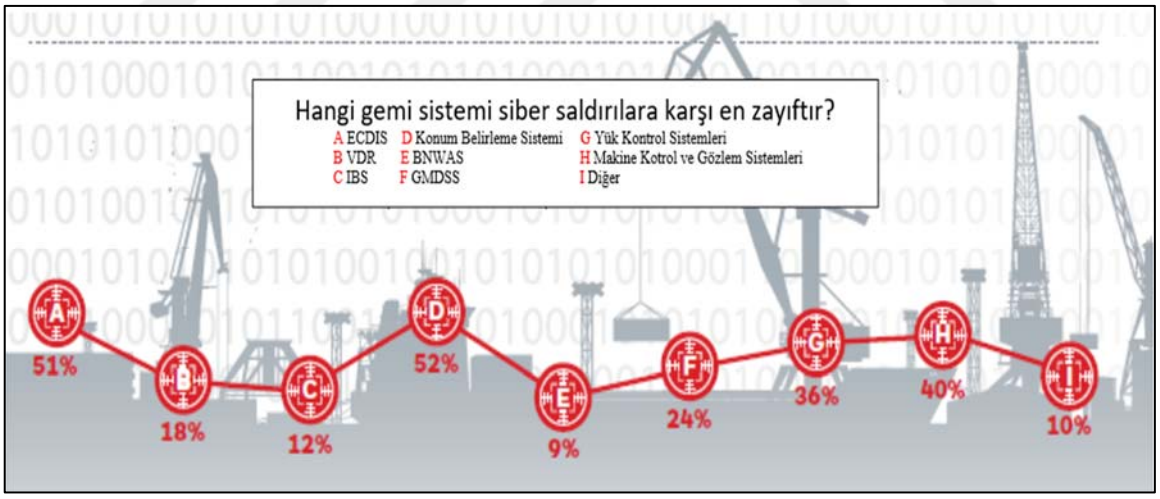
Yazılımın "SİSTEMİ KORUR", Ağ Altyapısının "GÜÇLÜ", Kullanıcı Prosedürlerinin "VAR" olduğu düzen Otomasyon, Haberleşme ve Bilgisayar Sistemleri için %93 ile en siber güvenli durumdur. Yazılımın "ZAFİYET YARATIR", Ağ Altyapısının "ZAYIF", Kullanıcı Prosedürlerinin "YOK" olduğu düzende Otomasyon, Haberleşme ve Bilgisayar Sistemleri %7 ile en az siber güvenli durumdadır. Üçlü koşullu olasılık değerlendirmesinde değişkenler %86 oranında sistemin güvenliğine etkide bulunmaktadır.

Siber Saldırı düğümünü; Konum Belirleme Sistemi %15, AIS %14, ECDIS %33, Otomasyon, Haberleşme ve Bilgisayar Sistemleri %34 oranında etkilemektedir (Şekil 36). Bu oranlarda uzmanların, uydu tabanlı ve uzun zamandır kullanılmakta olan seyir sistemlerine kullanıcı gözüyle güven duyma içgüdüsü, bilgisayar tabanlı sistemlerde az dahi olsa siber bir olay yaşamış olmanın getirmiş olduğu risk öngörüsü etkili olmuştur.



Şekil 36. Siber saldırı durumunu etkileyen faktörler

IHS Markit ve BIMCO tarafından 2016 yılında siber güvenlik anketi yapılmıştır. Anketin sonuçlarına göre, Konum Belirleme Sistemleri %52 ile en riskli unsurdur, ikinci sırada %51 ile ECDIS, üçüncü sırada %40 ile makine kontrol sistemleri bulunmaktadır (Şekil 37).



Şekil 37. Siber saldırıya karşı en zayıf gemi sistemine ilişkin sonuçlar (IHS Markit, 2016)

Çalışmanın yukarıda belirtilen sonuçları ile bu anketin sonuçları arasında benzerlik mevcut olup herhangi bir zıtlık görülmemektedir. GPS ve AIS gibi sistemler sadece dış saldırganların saldırılarına açıktırlar. İç saldırgan olarak görülebilecek gemi personelinin istemsiz saldırıları bu iki sistem üzerinde pek mümkün değildir. Buna rağmen, ECDIS veya Otomasyon, Haberleşme, Bilgisayar Sistemleri amaçları değişiklik göstermekle beraber dış

saldırganların hedefinde olabilecekleri gibi aynı zamanda gemi personelinin istemsiz, yanlış uygulamaları neticesinde de siber zafiyet gösterebilirler. Önceki bölümlerde detayları verilmiş denizcilik sektöründeki siber olaylardan gemilere yönelik olan 20 olay incelendiğinde de benzer sonuç çıkmaktadır (Tablo 22 ve Tablo 23). Olay sayısı açısından bakıldığında, iki yönden de tehlike altında olan bilgisayar tabanlı sistemlerin tek yönden tehlike altında olan GPS veya AIS gibi sistemlere göre daha riskli bulunmuş olması daha rasyoneldir.

Tablo 22. GPS ve AIS'e yönelik siber saldırı detayları

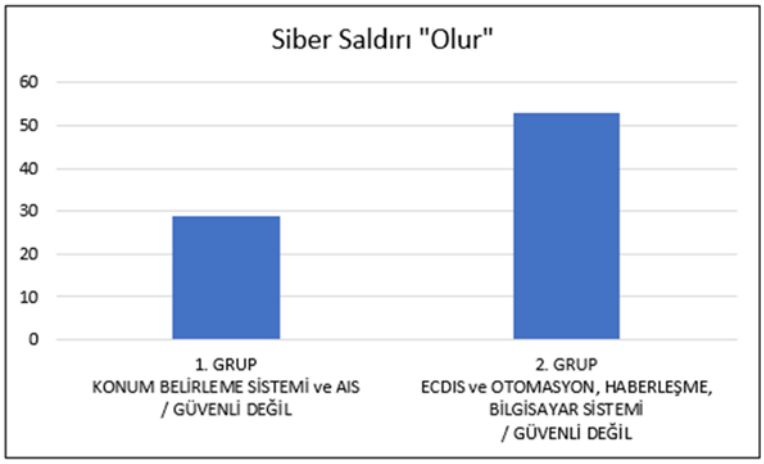
Sistem	Saldırı Sayısı	Saldırı Yöntemi	Saldırgan Çeşidi	
		Sinyal Karıştırma / Saptırma	İç Saldırgan	Dış Saldırgan
GPS	2	2	---	2
AIS	2	2	1	1

Tablo 23. ECDIS ve Bilgisayar, Otomasyon, Haberleşme Sistemlerine yönelik siber saldırı detayları

Sistem	Saldırı Sayısı	Saldırı Yöntemi		Saldırgan Çeşidi		
		Uydu Bağlantısı, Harici Bellek veya ePosta ile Zararlı Yazılım Bulaştırma	Yazılım, Güncelleme Eksiklikleri	İç Saldırgan	Dış Saldırgan	Belirsiz
ECDIS	8	6	2	5	2	1
Bilgisayar, Otomasyon, Haberleşme Sistemleri	8	7	1	4	2	2

Konum Belirleme Sistemi ve AIS birlikte birinci grup, ECDIS ve Otomasyon, Haberleşme, Bilgisayar Sistemleri de birlikte ikinci grup olarak değerlendirilebilir. Birinci gruptakiler "GÜVENLİ" seçilip ikinci grubun değerleri sabit tutulduğunda Siber Saldırı "OLUR" %48 olarak hesaplanmaktadır. Birinci gruptakiler "GÜVENLİ DEĞİL" seçilip ikinci grubun değerleri sabit tutulduğunda Siber Saldırı "OLUR" %77 olarak hesaplanmaktadır. Birinci gruptaki değişiklik %29 oranında sonuca etki yapmaktadır. İkinci gruptakiler "GÜVENLİ" seçilip birinci grubun değerleri sabit tutulduğunda Siber Saldırı "OLUR" %32 olarak hesaplanmaktadır. İkinci gruptakiler "GÜVENLİ DEĞİL" seçilip

birinci grubun değerleri sabit tutulduğunda Siber Saldırı "OLUR" %85 olarak hesaplanmaktadır. İkinci gruptaki değişiklik %53 oranında sonuca etki yapmaktadır (Şekil 38).

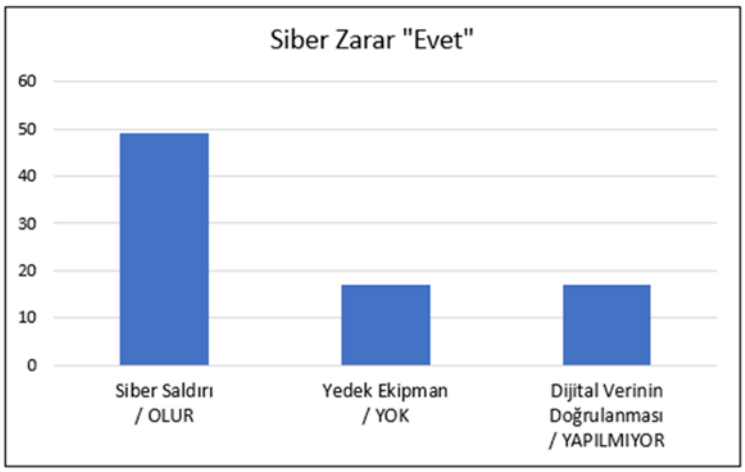


Şekil 38. İkili grupların siber saldırı durumuna etkisi

İkinci grupta bulunan bilgisayar tabanlı sistemlerin sonucu daha fazla etkiliyor olmasının sebebi uzmanlar gözünde bilgisayar teknolojilerinin ve buna dayalı sistemlerin daha fazla siber tehdit potansiyeline sahip olduğu düşüncesidir. 1. grup ve 2. grup arasındaki farkın büyük olması 2. gruba dair önlemlerin daha hızlı ve etkin bir şekilde alınması gerektiği anlamındadır.

Kullanılan 4 sistemin (Konum Belirleme Sistemi, AIS, ECDIS, Otomasyon, Haberleşme ve Bilgisayar Sistemi) hepsi "GÜVENLİ" seçildiğinde Siber Saldırı "OLUR" %18 olarak, 4 sistem "GÜVENLİ DEĞİL" seçildiğinde ise Siber Saldırı "OLUR" %95 olarak hesaplanmaktadır. Dörtlü koşullu olasılık değerlendirmesinin sonuca etkisi %77 oranındadır. Siber güvenlik anlamında doğru yani güvenli sistem detaylarının oluşturulmaması halinde güvenli olmayan bir sistem ile siber saldırıya uğrama potansiyeli yüksektir.

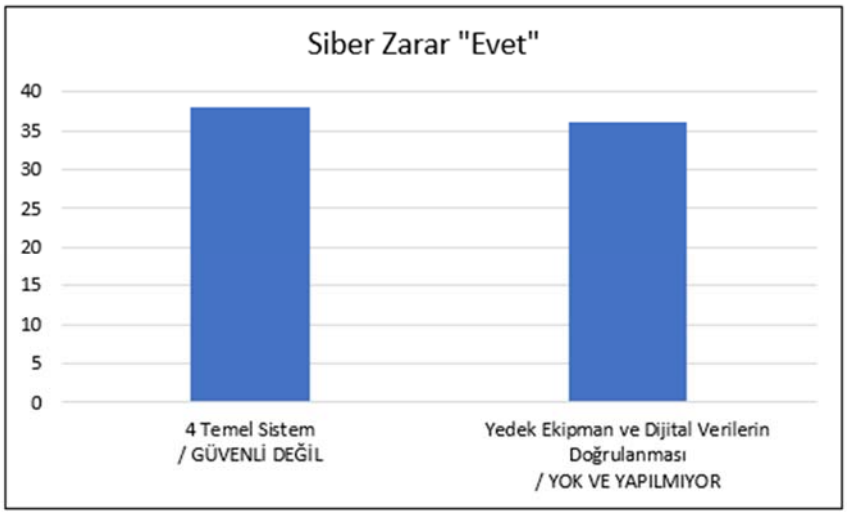
Siber Zarar düğümü için, Siber Saldırı %49, Yedek Ekipman %17, Dijital Verilerin Doğrulanması %17 oranında sonucu etkilemektedir (Şekil 39). Siber Saldırı diğerlerine göre daha yüksek yüzdeye sahiptir. Bunun nedeni; uzmanlar açısından, siber saldırganların planlı ve etkin bir saldırısı neticesinde gemide alınabilecek tedbirlerin veya düzeltici faaliyetlerin yetersiz olabileceği düşüncesi vardır.



Şekil 39. Siber zararı etkileyen faktörler

Yedek Ekipman ve Dijital Verilerin Doğrulanması bir grupta değerlendirilebilir. Siber Saldırı değeri sabit tutulduğunda (OLUR %57), Yedek Ekipman "VAR" ve Dijital Verilerin Doğrulanması "YAPILIYOR" düzeninde Siber Zarar "EVET" %28'dir, Siber Saldırı değeri sabit tutulduğunda (OLUR %57), Yedek Ekipman "YOK" ve Dijital Verilerin Doğrulanması "YAPILMIYOR" düzeninde Siber Zarar "EVET" %64'dür. İkili koşullu olasılık değerlendirmesinde tedbir ve düzeltici faaliyetlerin sonuca %36 oranında etkisi vardır. Siber Saldırı "OLUR" %100, Yedek Ekipman "VAR" ve Dijital Verilerin Doğrulanması "YAPILIYOR" düzeninde Siber Zarar "EVET" %43'dür, Siber Saldırı "OLUR" %100, Yedek Ekipman "YOK" ve Dijital Verilerin Doğrulanması "YAPILMIYOR" düzeninde Siber Zarar "EVET" %94'dür. Bu koşullu olasılık değerlendirmesinde ise tedbir ve düzeltici faaliyetlerin sonuca %51 oranında etkisi vardır.

4 sistem "GÜVENLİ" seçilip Yedek Ekipman ve Dijital Verilerin Doğrulanması değerleri sabit tutulursa Siber Zarar "EVET" %21, 4 sistem "GÜVENLİ DEĞİL" seçilip Yedek Ekipman ve Dijital Verilerin Doğrulanması değerleri sabit tutulursa Siber Zarar "EVET" %59 hesaplanmaktadır, yani 4 sistemin sonuca etkisi %38'dir. 4 sistemin değerleri sabit tutulup Yedek Ekipman "VAR" ve Dijital Verilerin Doğrulanması "YAPILIYOR" seçilirse Siber Zarar "EVET" %28, 4 temel sistemin değerleri sabit tutulup Yedek Ekipman "YOK" ve Dijital Verilerin Doğrulanması "YAPILMIYOR" seçilirse Siber Zarar "EVET" %64 hesaplanmaktadır, yani tedbir ve düzeltici faaliyetlerin sonuca %36 etkisi vardır (Şekil 40).



Şekil 40. Yedek ekipmanın siber zarar üzerindeki etkisi

Her iki değer birbirine çok yakındır yani sonucu benzer oranda etkilemektedir. Bu nedenle, yedek ekipman veya yedek sistemin temini gibi yüksek maliyetli ve geniş hacim kaplayabilecek çözümler yerine mevcut sistemlerin en güvenli şekilde oluşturulması ve dijital verilerin uygun yöntemlerle doğrulanması gibi düzeltici faaliyetlerin varlığının siber zararı etkin şekilde düşüreceği söylenebilir.

Her organizasyon potansiyel bir siber kurbandır ve tüm organizasyonların başkaları için değerli olabilecek bir şeyleri bulunmaktadır. Eğer siber güvenlik konusunda temel işler yerine getirilmeyip açıkça bir zaaflık ortaya koyulursa, herhangi şekilde bir siber saldırı deneyimi geçirilmesi kaçınılmazdır (GCHQ, 2015). Jones Walker LLP tarafından Ekim 2018'de ABD'deki denizcilik şirketleri ile yapılan siber güvenlik konulu ankette, katılımcıların %69'u denizcilik sektörünün bütün olarak yıkıcı bir siber saldırıya karşı hazırlıklı olduğunu düşünürken sadece %36'sı kendi şirketlerinin siber saldırıya karşı hazırlıklı olduğunu belirtmiştir. Bu sonuçlardan hazırlıklı olmaya dair sektörde önemli büyüklükte yanlış bir algının mevcut olduğu anlaşılmaktadır (Jones Walker LLP, 2018). Dolayısıyla, siber güvenlik konusunda tedbir almakta gecikmek, saldırıya uğrama potansiyelini hafife almak veya siber saldırganların başarısız olmalarını ümit etmek yanlış davranış şekilleri olacaktır. Başarısız girişim olasılık yüzdesi yüksek görünse de siber saldırganların yeteneklerinin, saldırı yöntemlerinin her geçen gün daha da arttığı göz ardı edilmemelidir.

Denizcilik sektöründe kullanılmakta olan sistemler genel olarak hizmet yılına veya kullanım şekline bağlı materyal yorgunluğu gibi öngörülebilir hataları içerecek şekilde dizayn edilmektedir, akıllı aktörlerin etkilerini barındırmamaktadır. Denizcilik sektöründeki siber sistemlerin bir merkezden yönetilmesi, işletilmesi de mümkün değildir. Bu nedenle sektördeki her aktörün kendi sistem ağını yönetmesi, bilgisayarlarını, sunucularını, mobil cihazlarını, kontrol sistemlerini ve diğer dijital cihazlarını siber güvenlik zafiyetleri ile ilgili tehditlerden korumak için siber güvenlikle ilgili politikalar ve prosedürler geliştirmesi, kendilerini başkalarından koruması gereklidir (Kessler, 2019). Bu amaçla, Tablo 24'de çalışmamız dahilinde kullanılmış olan Bayes Ağı düğümleri ile oluşturulabilecek teorideki en siber güvenli durum, günümüzde mevcut bir gemideki asgari durum ve tez çalışması sonuçları ışığında pratikte kurulabilecek en siber güvenli gemiye dair durum belirtilmiştir. Pratikte kurulabilecek en siber güvenli durum için yukarıda bahsedilen değerlendirmelere ilave olarak geminin internet bağlantısı olmadan ve Karadeniz, Kore Yarımadası gibi günümüzde siber olaylar adına riskli bölgelere gitmeden ticaret yapamayacağı gerçekleri de göz önünde bulundurulmuştur.

Tablo 24. Pratikte kurulabilecek en siber güvenli gemi için sistem önerisi

	Değişken	Teoride En Siber Güvenli Durum	Mevcut Bir Gemideki Durum	Pratikte Kurulabilecek Durum
Konum Belirleme Sistemi	Sinyal Seviyesi Filtresi	Var	Yok	Var
	Coğrafi Konum	Diğer	Karadeniz – Kore Yarımadası	Karadeniz – Kore Yarımadası
	Cihaz Çifti	eLORAN – GLONASS	GPS – GPS	GPS – GLONASS
AIS	Cihaz Çeşiti	Uydu AIS	VHF AIS	Uydu AIS
	Sinyal Doğrulama Ekipmanı	Var	Yok	Var
Yazılım	İşletim Sistemi	Desteklenen	Desteklenen	Desteklenen
	Virüs Programı	Kullanılıyor	Kullanılıyor	Kullanılıyor
	Güncellemeler	Yapılıyor	Yapılıyor	Yapılıyor

Tablo 24'ün devamı

	Değişken	Teoride En Siber Güvenli Durum	Mevcut Bir Gemideki Durum	Pratikte Kurulabilecek Durum
Ağ Altyapısı	İnternet Bağlantısı	Yok	Var	Var
	Ağ Bölgelere Ayrılmış	Evet	Evet	Evet
	Tespit Edici Ekipman	Var, Farklı Marka	Yok	Yok
ECDIS	Kullanıcı Prosedürleri	Var	Var	Var
	Harita Düzeltme Yöntemi	Orijinal CD	İnternet Bağlantısı	İnternet Bağlantısı
	Yazılım	Sistemi Korur	Sistemi Korur	Sistemi Korur
Otomasyon, Haberleşme, Bilgisayar Sistemi	Yazılım	Sistemi Korur	Sistemi Korur	Sistemi Korur
	Ağ Altyapısı	Güçlü	Güçlü	Güçlü
	Kullanıcı Prosedürleri	Var	Var	Var
	Yedek Ekipman	Var	Yok	Yok
	Dijital Verilerin Doğrulanması	Yapılıyor	Yapılıyor	Yapılıyor
	Siber Saldırı – OLUR	**%34**	**%64**	**%45**
	Siber Zarar - EVET	**%19**	**%47**	**%36**

Pratikte Kurulabilecek Durum için siber saldırı ve siber zarar olasılık değerleri, en iyi koşul olan Teoride En Siber Güvenli Durum ve en kötü durum olabilecek Mevcut Bir Gemideki Durum'a ait değerlerin yaklaşık ortalaması kadardır. Bu açıdan önerilen sistemin siber güvenliği arttırıcı etkisi olacaktır.

4. SONUÇ VE ÖNERİLER

Gelişen teknoloji ile denizcilik sektörü ve onun en önemli parçalarından biri olan gemi için siber tehlikeler en önemli risk unsurlarından bir tanesi durumuna gelmiştir. Çalışmanın sonucu olarak, Konum Belirleme Sistemi ve AIS gibi uydu ya da telsiz tabanlı seyir sistemlerinin doğurabilecekleri sonuçlar itibariyle önemli derecede siber risk barındırıyor olduğu, fakat mevcut olan asıl risk unsurunun ECDIS ve Otomasyon, Haberleşme, Bilgisayar Sistemi gibi bilgisayar teknolojilerinin ve bilgisayar temelli sistemlerin olduğu anlaşılmaktadır.

Gemilere yönelik siber güvenliğin sağlanmasında iki önemli nokta bulunmaktadır. Birincisi sürdürülebilir sistem çözümlerinin hayata geçirilebilmesidir. Bu çözümlerin aşağıdaki özellikleri içerecek şekilde seçilmesi önemlidir,

- İlk kurulum veya gemide mevcut olan düzenin modifikasyonu, bakım tutumu veya meydana gelebilecek arızaların giderilmesi konularının en ekonomik şekilde planlanması ve tamamlanması,
- Oluşturulacak bu çözümlerin kaplayacakları hacimlerin gemilerin köprüüstü, yaşam mahali ve makine kontrol odası dahil makine dairesi koşullarının göz önüne alınarak planlanması. Gemiadamlarının yaşam kalitesini ve çalışma koşullarını olumsuz yönde etkilemeyecek şekilde dizayn edilmesi,
- Sistem veya marka çeşitliliği sağlanması,
- Olabildiğince doğrulama veya karşılaştırma yapılabilmesi imkanı vermesi,
- Zamanın teknolojik ihtiyaç ve risklerine göre geliştirilmeye müsait olması.

İkinci nokta ise, kullanıcı açısından işletim kolaylığı sağlayan çözümlerinin hayata geçirilebilmesidir. Bu çözümlerin aşağıdaki özellikleri içerecek şekilde seçilmesi önemlidir,

- Karmaşıklıktan uzak, her seviyede gemiadamının kullanabileceği basit bir düzene oturtulması,
- Kullanıcı kaynaklı hataların en aza indirgenmesi,
- Devreden çıkartılabilip mümkün olduğunca elle (manuel) kullanıma imkan vermesi,
- Elektronik arıza riskini veya bakım gereksinimini en aza indirgemesi ve mevcut gemiadamı yeterlilikleri ile (Deniz Ulaştırma İşletme Mühendisi, Gemi Makinesi

İşletme Mühendisi ve Elektrik / Elektroteknik Zabiti) potansiyel arızaların denizde giderilebilmesi.

IHS Markit ve BIMCO tarafından yapılan siber güvenlik anketinde "Şirketiniz, çalışıyor olduğunuz gemiyi operasyonel teknolojilerden (OT) koruyor mu?" sorusuna, 2018 yılında %7 "evet", %93 "hayır" yanıtı verilmiştir, 2019 yılında ise %42 "evet", %26 "hayır", %32 "bilgim yok" yanıtı verilmiştir. Rakamlardan anlaşıldığı kadarıyla her türlü olumsuzluğa rağmen denizcilik sektöründe siber güvenlik konusunda zaman ilerledikçe olumlu tedbirler alınmaya çalışılmaktadır (IHS Markit, 2019). Bununla birlikte siber güvenlik bilincinin gelişiyor olması da olumlu gelişmedir.

Kimyasal Madde Dağıtım Enstitüsü (CDI), Petrol Şirketleri Uluslararası Denizcilik Forumu (OCIMF) ve RightShip denetimleri siber güvenlik konusunda detaylar da içermektedir. Bu denetlemeleri geçiren tanker ve kuru yük gemileri siber güvenliğe dair bazı önemli unsurları şu ana kadar tamamlamış olmaları itibariyle bu denetlemeleri geçirmemiş diğer gemilere göre bir adım önde sayılabilirler (Oruç, 2020). Fakat IMO kararıyla, 1 Ocak 2021 tarihinden itibaren tüm gemiler için, ilk Şirket Uygunluk Belgesi (DoC) onayından önce siber güvenlik risk değerlendirmesi, siber tehditlere dair alınan önlemler ve prosedürler ile ilgili detaylar ISM dahilinde hazır olmalıdır (IMO, 2017b). Amerikan Sahil Güvenlik Kurumu (USCG) Amerika limanlarına uğramakta olan gemilere artık siber güvenlik konusunda da denetim yapmaktadır. USCG'ın gemi denetimi yapacak personeli için hazırlamış olduğu kılavuzda, bilgisayarlarda şifre veya parola kullanılıp kullanılmıyor olduğu kontrolünden, harici bellek kullanımı alışkınlığına, hatta gemi personelinin siber güvenlik konusundaki şikayetlerine kadar birçok denetim konusu bulunmaktadır. Tespit edilen olumsuzlukların büyüklüğüne göre denetleme, geminin tutuklanması ile dahi sonuçlanabilmektedir (USCG, 2020). Bunların ışığında denizcilik sektörünün kısa zaman içerisinde tamamlanması gereken birçok konu bulunmaktadır. Çalışma sonucunda belirlenen öneriler aşağıdaki gibidir;

- Siber güvenlik konusunda personelin eğitilmesi ve geliştirilecek prosedürler ile siber güvenlik farkındalığının arttırılması, bilinçli teknoloji kullanıcısı profilinin oluşturulması.
- IMO tarafından da zorunlu hale getirilen siber güvenlik risk değerlendirmesinin, siber saldırıların sonuçlarının ne denli büyük olabileceği göz önünde bulundurularak en uygun şekilde yapılması.

- Sistem altyapısındaki siber güvenlik zafiyetlerinin gerekliyse profosyonel kuruluşlardan yardım alarak uygun risk değerlendirmesi ile tespit edilmesi, çalışmada belirtilenler de dahil en uygun çözümler ile iyileştirmelerin yapılması ve sistemin siber güvenli duruma getirilmesi. Nesnelerin İnterneti (Internet of Things), Dijital İkiz (Digital Twins) veya Blok Zincir (Block Chain) gibi gelişen teknolojilere ve siber saldırı yöntemlerine göre sistem altyapısının sürekli güncellenmesi. Dijital bağımlılığın ve dijital verilere aşırı güvenin önüne geçilmesi, özellikle seyir bilgilerine ait dijital verilerin en uygun yöntemlerle doğrulanabileceği uygulamaların teşvik edilmesi.

Çalışmada, gemilere yönelik siber saldırı olaylarını modelleyen ağ içerisindeki kısıtlı sayıda teknolojik unsur kısıtlı sayıda uzman tarafından değerlendirilmiştir. Bu çalışma, siber güvenli gemiler için iki konuda gelecekteki çalışmalara ve araştırmalara zemin oluşturabilir. Birincisi, teknolojik unsurlar genişletilip daha da detaylandırılarak oluşturulacak yeni bir ağ, daha geniş ve daha çeşitli uzmanlar tarafından değerlendirmeye tabi tutulabilir. İkincisi, mevcut ağın veya genişletilerek hazırlanacak yeni bir ağın siber güvenlik durumu yazılım, bilgisayar ve elektronik mühendisleri de dahil edilerek deneysel olarak uygulamalı test edilebilir.

5. KAYNAKLAR

Adamson, K., D., 2016. Knowledge is Power, The Navigator, 12, 4-5.

Akhtar, M., J. ve Utne, I., B., 2014. Human Fatigue′s Effect on The Risk of Maritime Groundings - A Bayesian Network Modeling Approach. Safety Science, 62, 427–440.

Akıllı, A., ve Atıl, H., 2014. Süt Sığırcılığında Yapay Zekâ Teknolojisi: Bulanık Mantık ve Yapay Sinir Ağları. Hayvansal Üretim, 55, 1, 39-45.

Allen, J., H., 2001. The CERT Guide to System and Network Security Practices, Addison-Wesley Professional, 447 s.

Allianz, Allianz Global Corporate and Specialty, https://www.agcs.allianz.com/content/dam/ onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf, Allianz Risk Barometer Top Business Risks for 2019, 21 Aralık 2020.

Algatürk Light, D., 2019. Siber Tehlikelerin Denizcilik Sektörüne Etkisi, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 25, 2, 1131-1137.

Altunok T. ve Çakmak, H., 2009. Suç Terör ve Savaş Üçgeninde Siber Dünya, Barış Platin Basımevi, Ankara, 232 s.

Androjna, A., Brcko, T., Pavic, I. ve Greidanus, H., 2020. Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8, 21, 776-796.

Ashby, W. R., 1957. An Introduction to Cybernetics, Chapman and Hall Ltd., London, 156 s.

Aslay, F., 2017. Siber Saldırı Yöntemleri ve Türkiye′nin Siber Güvenlik Mevcut Durum Analizi, International Journal of Multidisciplinary Studies and Innovative Technologies, 1, 1, 24-28.

Babineau, G., L., Jones, R., A. ve Horrowitz, B., 2012. A System-Aware Cyber Security Method for Shipboard Control Systems With a Method Described to Evaluate Cyber Security Solutions, 2012 IEEE Conference on Technologies for Homeland Security (HST), Kasım, Waltham, Bildiri Kitabı: 99-104.

Balduzzi, M., Wilhot, K. ve Pasta, A., 2014. A Security Evaluation of AIS, A Trend Micro Research Paper, Irving, 33 s.

Balduzzi, M., Pasta, A. ve Wilhot, K., 2014b. A Security Evaluation of AIS, Automated Identification System, 30th Annual Computer Security Applications, Aralık, New Orleans, Proceedings: 436–445.

Bayram, H., Uğur, A.,F. ve Danışman, K., 2002. FPGA (Field Programmable Gate Array) Tabanlı Bulanık Kontrolör Tasarımı ve Bir Uygulama, ELECO.

Becrypt, Becrypt, Protecting IP in the Oil, Gas & Minerals Sector, https://cybersail.org/wp-content/uploads/2017/02/Becrypt-Protecting-IP-in-the-Oil-Gas-Minerals-sector.pdf, 21 Aralık 2020.

Belmont, K., B. ve Caponi, S., L., 2014. Old Dogs, New Tricks: Bunker Fuel Industry Facing Growing Cyber Threat, Bunkerspot, Aralık 2014 - Ocak 2015 Sayısı, 5-7.

Belmont, K., B., 2016. Maritime Cybersecurity: Cyber Cases in the Maritime Environment, Blank Rome Llp, 43 s.

Betz, D. ve Stevens, T., 2011. Chapter One: Power and Cyperspace, Adelphi Series, 51(424), 35-54.

Bhatti, J. ve Humphreys T., E., 2016. Hostile Control of Ships via False GPS Signals: Demonstration and Detection, Navigation, 64, 1, 51-66.

BIMCO, 2015. Shipping Must not Underestimate the Threat to its Cyber Security, BIMCO Bulletin, 110, 4, 54-55.

BIMCO, 2020. The Guidelines on Cyber Security Onboard Ships Version 4, Baltic and International Maritime Council, 56 s.

Bih, J., 2006. Paradigm Shift - An Introduction to Fuzzy Logic, Potentials, IEEE, Transactions, 25, 1, 6- 21.

Bolat, P., Yüksel, G. ve Uygur, S., 2016. A Study for Understanding Cyber Security Awareness Among Turkish Seafarers, The Second International Conference on Global International on Innovation, Ekim, Muğla, Bildiriler Kitabı: 278.

Boyes, H., 2013. Maritime Cyber Security – Securing the Digital Seaways, Engineering & Technology Reference Resilience, Security & Risk in Transport, 2013, 56-63.

Brasington, H. ve Park, M., 2016. Cybersecurity and Ports Vulnerabilities, Consequences and Preparation, Ausmarine, 38, 4, 23-24.

Brčić, D. ve Žuškin, S., 2018. Towards Paperless Vessels: A Master's Perspective, Pomorski Zbornik, 55, 183-199.

Brettel, M., Friederichsen, N., Keller, M. ve Rosenberg, M., 2014. How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 Perspective, International Journal of Mechanical, Industrial Science and Engineering, 8, 1, 37-44.

Broadhurst, P., Inmarsat Takes Mature Approach to Maritime Cyber Security, https://safety4sea.com/inmarsat-takes-mature-approach-maritime-cyber-security/, 21 Aralık 2020.

Broadhurst, P., Shipping: Making the Connection on Cyber Security, https://www.inmarsat.com/en/insights/maritime/2019/shipping-making-the-connection-on-cyber-security.html, 22 Aralık 2020.

BTK, Bilgi Teknolojileri ve İletişim Kurumu, https://www.btk.gov.tr/siber-guvenlik-genel-bilgi, Genel Bilgi, 20 Aralık 2020.

Buchan, R., Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?, Journal of Conflict & Security Law, 17, 2, 219.

C4ADS, 2019. Above Us Only Stars, 66 s.

Cai, B., Liu, Y., Zhang, Y., Fan, Q., Liu, Z. ve Tian, X., 2013. A Dynamic Bayesian Networks Modeling of Human Factors on Offshore Blowouts, Journal of Loss Prevention in the Process Industries, 26, 4, 639-649.

Can, Ö. ve Akbaş M., F., 2014. Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Durum Çalışması, TÜBAV Bilim Dergisi, 7, 2, 16-31.

Canbek, G. ve Sağıroğlu, Ş., 2007. Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23, 1, 1-12.

Cojocaru, S., 2009. GPS-GLONASS-GALILEO: A Dynamical Comparison, The Journal of Navigation, 62, 135-150.

Caprolu, M., Pietro, R., Raponi, S., Sciancalepore, S. ve Tedeschi, P., 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. IEEE Communications Magazine, 58, 90-96.

Chen, J., Su, C., Yeh, K. H. ve Yung, M., 2018. Special Issue on Advanced Persistent Threat, Future Generation Computer Systems, 79, 1, 243-246

Clarke, R. ve Knake R., 2010. Siber Savaş, İstanbul Kültür Üniversitesi Yayını, No.148, İstanbul, 154 s.

Class NK, 2020. Guidelines for Designing Cyber Security Onboard Ships, Second Edition, Class Nippon Kaiji Kyokai, Tokyo, 64 s.

CFCS, 2017. Threat Assessment: The Cyber Threat Agaist the Maritime Sector, Danish Defence Intelligence Service's Centre for Cyber Security, 7 s.

Çelik, Ş., 2013. Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan kaçınma İlkesi Çerçevesinde Bir Değerlendirme, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 15, 1, 137-175.

Challamel, R., Calmettes, T. ve Gigot, C., N., 2012. A European Hybrid High Performance Satellite- AIS System, 6th Advanced Satellite Multimedia Systems Conference (ASMS), Ekim, Baiona, 246-252.

Charney, S., 2009. Rethinking the Cyber Threat: A Framework and Path Forward, Microsoft Corp., 13 s.

Chen, Y., 2014. Satellite-based AIS and its Comparison with LRIT, The International Journal on Marine Navigation and Safet of Sea Traansportation, 8, 2, 183-187.

Çinicioğlu, E. N., Atalay, M. ve Yorulmaz, H., 2013. Trafik Kazaları Analizi için Bayes Ağları Modeli, Bilişim Teknolojileri Dergisi, 6, 2, 41.

CyberKeel, 2014. Maritime Cyber-Risks, CyberKeel, Copenhagen, 26 s.

Dadiani, D., 2018. Cyber-Security and Marine Insurance, World Maritime University Dissertations, 607, 63 s.

Daum, O., 2019. Cyber Security in the Maritime Sector, Journal of Maritime Law and Commerce, 50, 1, 1-20.

Dashora, K., 2011. Cyber Crime in the Society: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences, 3, 1, 240-259

Dawoud, S., 2012. GNSS Principles and Comparison, Potsdam University, 10s.

Demirel, S. ve Bodur, S., 2004. Application of Bayes Theorem In Genetic Counseling, Erciyes Medical Journal, 26,2, 81-85.

DHS, 2016. Consequences to Seaport Operations From Malicious Cyber Activity, U.S. Department of Homeland Security, 17 s.

Di Rollo, J., 2017. Cyber Tsunami, Breakbulk Magazine, 3, 2017, 59-60.

DNV-GL, 2018. Maritime Cyber Security Webinar 1 Cyber Security Threats for the Maritime Industry–Are you prepared?, Det Norske Veritas–Germanischer Lloyd, Kopenhag, 51 s.

EGM, Emniyet Genel Müdürlüğü, https://www.egm.gov.tr/siber/sibersucnedir, Siber Suç Nedir, 20 Aralık 2020.

Eğilmez, M., 2018. Endüstri 4.0, Accounting and Financial History Research Journal, 2018, 15, 264-271.

Ekici, O., 2005. Bayesyen Regresyon ve WinBUGS ile Bir Uygulama, Yüksek Lisans Tezi İstanbul Üniversitesi, İstanbul.

ENISA, 2019. Port Cybersecurity Good Practices for Cybersecurity in the Maritime Sector, European Union Agency for Cybersecurity, Atina, 61 s.

EUROSTAT,https://ec.europa.eu/eurostat/statistics-explained/index.php/International_trade_ in_goods_by_mode_of_transport International, Trade in Goods by Mode of Transport. 20 Aralık 2020

Fitton, O., Prince, D., Germond, B. ve Lacy, M., 2015. The Future of Maritime Cyber Security, Lancester University, 36 s.

Garba, F., A., 2019. Proposed Framework for Effective Detection and Prediction of Advanced Persistent Threats Based on the Cyber Kill Chain, Scientific and Practical Cyber Security Journal, 3, 3, 1-11.

GCHQ, 2015. Common Cyber Attacks: Reducing The Impact, Government Communications Headquarters, Londra, 17 s.

Global Security, 2015. Somebody's Watching You!, 13 s.

Glomsvoll, O. ve Bonenberg, L., K., 2016. GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea, The Journal of Navigation, 2017, 70, 33-48.

Grant, A., Williams P., Ward, N. ve Basker, S., 2009. GPS Jamming and the Impact on Maritime Navigation, The Journal of Navigation, 2009, 62, 173-187.

Guinchard A., 2011. Between Hype and Understatement - Reassessing Cyber Risks as a Security Strategy, Journal of Strategic Security, 4, 2, 87.

Güneş, B., 2019. Siber Fiziksel Sistemler Üzerinde Bütünleşik Siber Güvenlik Risk Değerlendirmesi: Bir Konteyner Limanı Uygulaması, Yüksek Lisans Tezi, İstanbul Teknik üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Gürses, B., 2013. E-Seyir, E-Seyrin Bileşenleri ve Ülkemizdeki E-Seyir Kullanıcı İhtiyaçlarının Belirlenmesi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Han, C. ve Dongre, R., 2014. Q&A. What Motivates Cyber-Attackers, Technology Innovation Management Review, 4, 10, 40–42.

Hareide, O., S., Jøsok, Ø., Lund, M., S., Ostnes, R. ve Helkala, K., 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security, TheJournal of Navigation, 71, 5, 1-15.

Harvard Business Review, 2020. Dijital Dönüşüm Siber Güvenlik, Optimist Yayın Grubu, İstanbul, 200 s.

Hassani, V., Crasta N. ve Pascoal, A., M., 2017. Cyber Security Issues in Navigation Systems of Marine Vessels From a Control Perspective, 36th International Conference on Ocean, Offshore and Arctic Engineering, Haziran, Trondheim, Bildiriler Kitabı 7B: 1-6.

Hayes, C., R., 2016. Maritime Cybersecurity: The Future of National Security, Yüksek Lisans Tezi, Naval Postgraduate School, Monterey.

Heymann, E., Miller, B., P., Alghazzawi, M., J. ve Incertis, D., Addressing The Cyber-Security Of Maritime Shipping, https://ftp.cs.wisc.edu/par-distrys/papers/ETC_2016_Heymann_ Miller.pdf, 22 Aralık 2020.

Ho, T., D., Hagaseth, M., Rialland, A., Rødseth, Ø., J., Criado, R., G. ve Ziaragkas, G., Internet of Things at Sea: Using AIS and VHF over Satellite in Remote Areas, 7th Transport Research Arena TRA, Nisan, Viyana, Proceedings:

Hogg T. ve Ghosh, S., 2016. Autonomous Merchant Vessels: Examination of Factors That Impact the Effective Implementation of Unmanned Ships, Australian Journal of Maritime and Ocean Affairs, 8, 3, 206-222.

Hsu, H., M. ve Chen, C., T., 1996. Aggregation of Fuzzy Opinions Under Group Decision Making. In Fuzzy Sets and Systems, 79.

IHO, 2019. Current IHO ECDIS and ENC Standards, International Hydrographic Organization.

IHS Markit, 2016. IHS-BIMCO-Survey-Findings, Story in Numbers, IHS Markit, 1 s.

IHS Markit, 2018. Maritime Cyber Survey 2018 - The Results, IHS Markit, 11 s.

IHS Markit, 2019. Safety at Sea and BIMCO Cyber Security White Paper, IHS Markit, 24 s.

ILA, 2007. Enhanced Loran (eLoran) Definition Document, International Loran Association, 17 s.

IMO, 2006. MSC.232(82) Adoptation of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS), International Maritime Organization

IMO, 2016. MSC 96/WP.9, Measures to Enhanced Maritime Security, International Maritime Organization.

IMO, 2017. MSC.1/Circ.1503/Rev.1 ECDIS—Guidance for Good Practice, Resolution, International Maritime Organization.

IMO, 2017b. MSC 98/23, Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems, International Maritime Organization.

IOActive, 2014. A Wake-up Call for SATCOM Security, IOActive, Seattle, 25 s.

Irmak, E. ve Erkek, İ., 2016. Çok Nitelikli Fayda Teorisiyle Saldırgan Profiline Yeni Parametrelerin Eklenmesi, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2, 2, 1-9.

It-Sec-Spy, 2011. 2011 Report on Security Intelligence Policy, İtalya Başbakanlığı, 79 s.

İçen, E., 2018. Global and Regional Positining Satellite Systems and a Proposal for Turkey, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Jackson, J., C., 2012. Satellite AIS – Developing Technology or Existing Capability?, The Journal of Navigation, 2012, 65, 303-321.

Jakobsson, M., Finn, P. ve Johnson, N., 2008. Why and How to Perform Fraud Experiments, IEEE Security and Privacy, Mart/Nisan 2008, 66-68.

Jakobsson, M. ve Ratkiewicz, J., 2006. Designing Ethical Phishing Experiments: A Study of (ROT13) rOnl Query Features, 15th International Conference on World Wide Web, Mayıs, Edinburgh.

Jensen, L., 2015. Challenges in Maritime Cyber-Resilience, Technology Innovation Management Review, Nisan 2015, 35-38.

Jensen, L., 2015b. Maritime Cyber Risks What is Real, What is Fiction?, https://www.ciffa.com/wp-content/uploads/2015/04/Maritime-Cyber-Risks-Jensen.pdf, 21 Aralık 2020.

Jones, B., Jenkinson, I., Yang, Z. ve Wang, J., 2010. The Use of Bayesian Network Modelling for Maintenance Planning in a Manufacturing Industry, Reliability Engineering & System Safety, 95,3, 267-277.

Jones, K., D., Tam, K. ve Papadaki, M., 2016. Threats and Impacts in Maritime Cyber Security, Engineering and Technology Reference, 22 Nisan 2016, 5 s.

Jones Walker LLP, 2018. Maritime Security Survey.

Justers, W., Cyber Security at Sea, https://www.bvz-abdm.be/sites/ default/files/walter _justers_-_cyber_security_-_proteus_presentation.pdf, 21Aralık 2020.

Kaspersky, 2013. https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-exposes--icefog--a-new-cyber-espionage-campaign-focusing-on-supply-chain-attacks, Kaspersky Lab Exposes "Icefog": A New Cyber-espionage Campaign Focusing on Supply Chain Attacks, 22 Aralık 2020.

Kaspersky, 2015. https://www.kaspersky.com/blog/maritime-cyber-security/8796/, Maritime Industry is Easy Meat for Cyber Criminals, 22 Aralık 2020.

Katsikas, S., K., 2017. Cyber Security of the Autonomous Ship, CPSS,17, 56-57.

Kessler, G., C., 2019. Cybersecurity in the Maritime Domain, USCG Proceedings of the Marine Safety and Security Council, 76, 1, 34-39.

Kobylinski, L., 2016. Maritime Transport and the Fourth Industrial Revolution, Oficyna Wydawnicza Politechniki Warszawskiej, 111, 269-278.

Koç Sistem, 2019. Siber Güvenlik Bülteni, No:1, Koç Sistem, İstanbul, 10 s.

Koldemir, B., Yapıcı, M. ve Keleştemur, A., 2017. Deniz Taşımacılığında Siber Güvenliği Tehdit Eden Unsurlar ve Koruma Önlemleri Üzerine Bir Çalışma, Üçüncü Ulusal Liman Kongresi, Kasım, İzmir.

Korb, K. B. ve Nicholson A. E., 2004. Bayesian Artifical Intelligence, A CRC Press Company, London, UK.

Kozan, M., H., 2019. GPS Tabanlı Konum Belirleme Sistemlerinin Güvenliği ve Sinyal Geliş Doğrultusu Kestirimi ile Saldırı Tespiti, Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Kragt, M., E., A Beginners Guide to Bayesian Network Modelling for Integrated Catchment Management. https://search.utas.edu.au/s/search.html?query=A+Beginners +Guide+to+Bayesian+Network+Modelling+for+Integrated+Catchment+ Management &collection=utas-search, 22 Aralık 2020.

Kramek, J., The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities, https://www.brookings.edu/research/the-critical-infrastructure-gap-u-s-port-facilities-and-cyber-vulnerabilities/, 21 Aralık 2020.

Krutz, R., L., Vines, R., D., 2007. The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking. Indianapolis, IN: Wiley Publising Inc.

Langner,R., 2011. Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE Security & Privacy, 9, 3, 49-51.

Lavasani, M. R., Zendegani, A., Celik, M., 2015. An Extension to Fuzzy Fault Tree Analysis (FFTA) Application in Petrochemical Process Industry, Process Safety and Environmental Protection, 93,75–88.

Limba, T., Pleta, T., Agafonov, K. ve Damkus, M., 2017. Cyber Security Management Model for Critical Infrastructur,. Entrepreneurship and Sustainability Issues, 4, 4, 559-573.

Lindsay, J., R., 2013. Stuxnet and the Limits of Cyber Warfare, Security Studies, 22, 3, 365-404.

Link, W. A. ve Barker, R. J., 2010. Bayesian Inference: With Ecological Applications, Academic Press, 0123748542, Boston, 400 s.

Loughney, S. ve Wang, J., 2018. Bayesian Network Modelling of an Offshore Electrical Generation System for Applications Within an Asset Integrity Case for Normally Unattended Offshore Installations, Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment, 232,4, 402-420.

Lagouvardou, S., 2018. Maritime Cyber Security: Concepts, Problems and Models, Master Thesis, Technical University of Denmark, Department of Management Engineering, Lyngby.

Lee, Y., C., Park, S., K., Lee, W., K. ve Kang, J., 2017. Improving Cyber Security Awareness in Maritime Transport : A Way Forward, Journal of the Korean Society of Marine Engineering, 41, 8, 738-745.

Lo, S., C., Peterson B., B. ve Enge, P., K., 2009. Assessing the Security of a Navigation System: A Case Study using Enhanced Loran, http://citeseerx.ist.psu.edu/viewdoc /download?doi=10.1.1.299.202&rep=rep1&type=pdf, 22 Aralık 2020.

Matellini, D., B., Wall, A., D., Jenkinson, I., D., Wang, J. ve Pritchard, R. 2013. Modelling Dwelling Fire Development and Occupancy Escape Using Bayesian Network. Reliability Engineering and System Safety. 114, 75-91.

MAYAICT, Son Kullanıcı Siber Güvenlik Bilgilendirme Dokümanı, MayaICT Bilgisayar Hizmetleri Ltd. Şti., İstanbul, 5 s.

McAfee, 2019. McAfee Labs Threats Report, August 2019, McAfee, 42 s.

MDR, 2019. Stormy Seas Ahead Cyber-Security Guidance for the Maritime Industry, Mishcon de Reya Group, 23 s.

Mileski, J., Clott, C. Ve Galvao, C., B., 2018. Cyberattacks On Ships: A Wicked Problem Approach, Maritime Business Review, 3, 4, 414-430.

Muccin, E., 2016. Cyber World Safer Seas via Phatom Ships, Maritime Reporter and Engineering News, 1,78, 20-21.

Muccin, E., 2016b. Cyber Security at Sea, https://www.maritime-executive.com/blog/cyber-security-at-sea, 22 Aralık 2020.

Murphy, K., 2007. Software Packages for Graphical Models/Bayesian Networks. International Society for Bayesian Analysis.

Nachenberg, C., 1997. Computer Virus-Antivirus Coevolution, Communications of the ACM, 40, 1, 46-51

NCC, 2014. Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, NCC Group, 10 s.

Nickolov, E., Modern Trends in the Cyber Attacks Against the Critical Information Infrastructure, https://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolov-modern-trends-sofia-oct-08.pdf, 20 Aralık 2020.

Ning, H., Dhelim, S., Bouras, M. A., Khelloufi A. ve Ullah, A., 2018. Cyber-Syndrome and its Formation, Classification, Recovery and Prevention, IEEE Access, 6, 35501-35511

OM, 2019. Navigation Cyber Security with M-SecureSync, Orolia Maritime, OM 07.19 v3, 2 s.

Oruç, A., 2020. Cybersecurity Risk Assessment for Tankers and Defence Methods, Yüksek Lisans Tezi, Piri Reis Üniversitesi, Lisansüstü Eğitim Enstitüsü, İstanbul.

OSM, 2018. Cyber Security Fleet Protection, OSM Maritime Group, 42 s.

Özen, A., 2014. Yüzer araçlarda Dinamik Konumlandırma Sistemlerinde Bileşen Seçiminin Sistemin Çalışmasına Etkisi Bakımından Önemi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Pajunen, N., 2017. Overview Of Maritime Cybersecurity, Bachelor's Thesis Marine Technology, South Eastern Finland University.

PANDA, 2015. Operation "Oil Tanker" The Phantom Menace, PANDA Labs, 11 s.

Pang, K., Maritime Cyber Security: The Emerging Virtual Threat to Shipping, https://ciltuk.org.uk/LinkClick.aspx?fileticket=kFlgRMm5X9w%3D&portalid=0, 21 Aralık 2020.

Patel, S., Zaveri J., 2010. A Risk Assessment Model for Cyber Attack on Information Systems, Journal of Computers, 5, 3, 352-359.

Pristrom, S., Yang, Z., Wang, J. ve Yan, X., 2016. A Novel Flexible Model for Piracy and Robbery Assessment of Merchant Ship Operations. Reliability Engineering and System Safety, 155, 196-211.

Rajakarunakaran, S., Maniram, K., A. ve Arumuga P., V., 2015. Applications of Fuzzy Faulty Tree Analysis and Expert Elicitation for Evaluation of Risks in LPG Refuelling Station. Journal of Loss Prevention in the Process Industries, 33, 109–123.

Rausand, M. 2011. Risk Assessment Theory, Methods, and Applications.: John Wiley & Sons, inc. New Jersey.

Rider, D., 2018. Cyber Security at Sea: The Real Threats, Northern California Area Maritime Security Committee Cyber Security News Letter, 2018, 4, 5-8.

Rodrigez, J., A., A., 2008. On Generalized Signal Waveforms for Satellite Navigation, Doktora Tezi, FAF University of Munich, Münih.

Rolls-Royce plc, 2016. Autonomous Ships the Next Step, 8s.

Røsdeth, Ø., Kvamstad, B., Porathe, T. ve Burmeister, H., C., 2013. Communication Architecture for an Unmanned Merchant Ship, Oceans 2013 MTS/IEEE: The Challenges of the Northern Dimension, Haziran, Bergen, 1-9.

Røsdeth, Ø., 2016. Sustainable and Competitive Cyber-Shipping through Industry 4.0, Singapore Maritime Sustainability Forum 2016: Smart Maritime Solutions and Overcoming Challenges April 19th 2016, Suntec City.

Saeed, I. A., Selmat, A. ve Abugoub, A. M. A., 2013. A Survey on Malware and Malware Detection Systems, International Journal of Computer Applications, 67, 16, 25-31

Safar, J., Lebekwe, C., K. ve Williams, P., 2010. Accuracy Performance of ELoran for Maritime Applications, Annual of Navigation, 16/2010, 109-121.

Sağıroğlu, Ş., Alkan, M., Samet, R., Ulutaş, G., Yalman, Y., Şengül, G., Paşaoğlu, C., Bostan, A., Doğru, A., Dörtler, M., efe, A., Vural, Y., Şenol, M., Terzi, D., S., Aslan, Ö., Sümer, Ç. ve Urfalıoğlu, R., 2018. Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınları No: 287, Ankara, 400 s.

Sakar, C., Köseoğlu, B., Büber, M. ve Toz A., C., 2019. Are The Ships Fully Secured Against the Cyber-Attacks?, III. Global Conference on Innovation in Marine Technology and the Future of Maritime Transportation, Nisan, İzmir, Bildiriler Kitabı: 276-288.

Savchuk, V. ve Tsokos, C. T., 2011. Bayesian Theory and Methods with Applications,9789491216138, Atlantis Press, Paris, 318 s.

Shah, S., K., 2004. The evolving Landscape of Maritime Cybersecurity, Review of Business, New York, 25, 3, 30-36.

Shaikh, S., A., 2017. Future of the Sea: Cyber Security, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf.

Shaw, N. ve Ayerst C., The UK's Cyber Security Code of Practice for Ships, https://www.reedsmith.com/en/perspectives/2017/10/the-uks-cyber-security-code-of-practice-for-ships, 21Aralık 2020.

Shin, M. Y., Cho, S. L., Kim, J. O., Song, K. W. ve Lee S. J., 2010. Analysis of GPS Spoofing Characteristics and Effects on GPS Receiver, Journal of the Korea Institute of Military Science and Technology, 13, 2, 296-303.

Silgado, D., M., 2018. Cyber-Attacks; A Digital Threat Reality Affecting the Maritime Industry, Yüksek Lisans Tezi, Dünya Denizcilik Üniversitesi, Malmö.

Skrlec, Z., Bicanic, Z. ve Tadic, J., 2014. Maritime Cyber Defense, 6th International Maritime Science Conference, Nisan, Split, Bildiriler Kitabı: 19-25.

SMI, 2017. Hackers Wage a Cyber War at Sea, Ship Management International, 65, 12-13.

Son, P., Rhee, J., H., Hwang, J. ve Seo, J., 2019. Universal Kriging for Loran ASF Map Generation, IEEE Transactions on Aerospace and Electronic Systems, 55, 4, 1828-1842.

Sophos, 2013. Threatsaurus The A-Z of Computer and Data Security Threats, Sophos Ltd., 100 s.

Soylu, A., 2018. Endüstri 4.0 ve Girişimcilikte Yeni Yaklaşımlar, Pamukkale Üniversitesi Sosyal Bililmler Enstitüsü Dergisi, 32, 43-57, Denizli.

Svilicic, B., Kamahara, J., Rook, M. ve Yano, Y., 2019. Maritime Cyber Risk Management: An Experimental Ship Assessment, The Journal of Navigation, 72, 5, 1-13.

Svilicic, B., Brčić, D., Žuškin, S. ve Kalebić. D., 2019b. Raising Awareness on Cyber Security of ECDIS, The International Journal on Marine Navigation and Safety of Sea Transportation, 13, 1, 231-236.

Svilicic, B., Miho, K., Srđan, Ž. ve David, B. 2020. Paperless Ship Navigation: Cyber Security Weaknesses, Journal of Transportation Security, 13, 203-214.

Symantec, 2011. W32.Stuxnet Dossier, Symantec, Cupertino, CA, 69 s.

Tam, K., Forshaw, K. ve Jones, K., D., 2019. Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities, ICMET, Ekim, Oman, Bildiriler Kitabı: 129-135.

Tam, K. ve Jones, K., 2019b. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment, WMU Journal of Maritime Affairs, 18, 129-163.

Thompson, P., 2019. Smart Ships and Smart Navigation Using Intelligent Data Fusion for Safe Navigation, The Journal of Ports and Terminals, 89 Ed., 124-125.

Topla, O., 2020. Denizcilikte Siber Güvenlik: Türk Gemi İşletmecileri Üzerine Bir İnceleme, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, İzmir.

Trucco, P., Cagno, E., Ruggeri, F., ve Grande, O., 2008. A Bayesian Belief Network Modelling of Organisational Factors in Risk Analysis, A Case Study in Maritime Transportation, Reliability Engineering and System Safety, 93, 823-834.

Tucci, A., E., 2017. Cyber Risks in the Marine Transportation System, Cyber-Physical Security. Protecting Critical Infrastructure, 3, 113-131.

Turgut, B., S., 2019. Potential Benefits of Satellite-Based Automatic Identification System in the Context of Intelligent Transportation Systems, Yüksek Lisans tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Turhan, M., 2010. Siber Güvenliğin Sağlanması, Dünya Uygulamalar ve Ülkemiz İçin Çözüm Önerileri, Bilgi Teknolojileri ve İletişim Kurumu, 42 s.

UAB, 2016. Ulaştırma ve Altyapı Bakanlığı, https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, 2016-2019 Ulusal Siber Güvenlik Stratejisi.

Uma, M. ve Padmavathi, G., 2013. A Survey on Various Cyber Attacks and Their Classification, International Journal of Network Security, 15, 5, 390-396.

UNCTAD, Review of Maritime Transport 2018, Paper presented at the United Nations Conference On Trade And Development (UNCTAD), New York and Geneva, https://unctad.org/system/files/official-document/rmt2018_en.pdf., 4 Ocak 2021.

UNCTAD, Review of Maritime Transport 2019, Paper presented at the United Nations Conference On Trade And Development (UNCTAD), New York and Geneva, https://unctad.org/system/files/official-document/rmt2019_en.pdf., 4 Ocak 2021.

URL-1, https://www.bbc.com/news/technology-40685821, How Hackers Are Targeting the Shipping Industry, 22 Aralık 2020.

URL-2, https://www.reuters.com/article/us-syria-iran-tracking/exclusive-iran-shipping-signals-conceal-syria-ship-movements-idUSBRE8B50KX20121206, Exclusive: Iran Shipping Signals Conceal Syria Ship Movements, 22 Aralık 2020.

URL-3, https://www.hellenicshippingnews.com/ll-hands-on-deck-malware-is-infecting-cargo-vessels-arriving-in-the-united-states/, All Hands on Deck: Malware Is Infecting Cargo Vessels Arriving in the United States, 22 Aralık 2020.

URL-4, https://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies, State-sponsored Hackers Spied on Denmark, 22 Aralık 2020.

URL-5, https://mariners.coastguard.dodlive.mil/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/, 6/15/2015: Coast Guard Commandant on Cyber in the maritime domain, 22 Aralık 2020.

URL-6, https://lloydslist.maritimeintelligence.informa.com/LL111889/BW-Group-computers-hit-by-cyber-attack-in-July, BW Group Computers Hit by Cyber Attack in July, 22 Aralık 2020.

URL-7, www.hellensystems.com, Hellen Systems, 24 Aralık 2020

USCG, 2020. Vessel Cyber Risk Management Work Instruction, USCG Office of Commercial Vessel Compliance (CG-CVC), 7s.

Verizon, 2016. Data Breach Digest, Verizon, 84 s.

Wall, D., 2007. Cybercrime: The Transformation of Crime in the Information Age, Polit Press, Cambridge, 94 s.

Wang, J., Pillay, A., Kwon, Y., Wall, A. ve Loughran, C., 2005. An analysis of fishing vessel accidents, Accident Analysis & Prevention, 37,6, 1019-1024.

Watkins, M. ve Wallace, K., 2008. CCNA Security Offical Exam Certification Guide, Cisco Press, Indianapolis, 637 s.

Weintrit, A., 2018. Clarification, Systematization and General Classification of Electronic Chart Systems and Electronic Navigational Charts Used in Marine Navigation. TransNav the International Journal on Marine Navigation and Safety of Sea Transportation, 12, 471–482.

Wen, H., Huang, P. Y., Dyer, J., Archinal, A. ve Fagan, J., 2005. Countermeasures for GPS Signal Spoofing, Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), Long Beach, 1285-1290

Wylie, J., Cyber Security Offshore; The New Virtual Battlefield?, https://cybersail.org/wp-content/uploads/2017/02/JWC-International-Cyber-Security-Offshore-The-New-Virtual-Battlefield.pdf, 21 Aralık 2020.

Yang, Z., Bonsall, S. ve Wang, J., 2008. Fuzzy Rule-Based Bayesian Reasoning Approach for Prioritization of Failures in FMEA, IEEE Transactions on Reliability, 57,3, 517-528.

Yaşar, H., Çakır, H., 2015. Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3, 488-507.

Yiğit, T., Akyıldız M., A., 2014. Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 18, 1, 14-21.

Yüksel, G., 2019. Antecedents and Consequences of Cyber Security Awareness: A Case Study for Maritime Sector, Yüksek Lisans Tezi, İstanbul teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Yüksel, G., Uygur, S., 2016. Denizcilik Alanında Siber Güvenlik Tehdit Analizi (Limanlar ve/veya Gemiler), Lisans Bitirme Tasarım Projesi, İstanbul Teknik Üniversitesi, Deniz Ulaştırma İşletme Mühendisliği Bölümü, İstanbul.

Zadeh, L., A., 1965. Fuzzy Sets. Information And Control, 8, 3, 338-353.

Zadeh, L., A., 1975. The Concept of a Linguistic Variable and Its Application to Approximate Reasoning , II. Information Sciences, 8, 4, 301-357.

Zimmermann, H., J., 1993. Fuzzy Sets, Decision Making and Expert Systems. Kluwer Academic Publishers.

6. EKLER

Ek Tablo 1. Koşullu olasılık durumlarına ait uzman sözlü değerlendirme verileri ve bulanık olasılık değerleri

Koşullu Olasılık No	Cihaz Çifti Düğümü	Coğrafi Konum Düğümü	Sinyal Seviyesi Filtresi Düğümü	Uzman Sözlü Değerlendirme Konum Belirleme Sistemi GÜVENLİ								
				1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
6	1 GPS + 1 GLONASS	KARADENİZ - KORE YA.	YOK	ML	MH	M	H	M	MH	VH	MH	0,651803787
7	1 GPS + 1 GLONASS	DİĞER	VAR	VH	MH	VH	H	MH	VH	VH	MH	0,86478286
8	1 GPS + 1 GLONASS	DİĞER	YOK	M	H	M	MH	M	H	MH	MH	0,674382145
9	1 ELORAN + 1 GLONASS	KARADENİZ - KORE YA.	VAR	H	H	VH	M	L	H	VH	M	0,750777551
10	1 ELORAN + 1 GLONASS	KARADENİZ - KORE YA.	YOK	ML	MH	M	ML	L	MH	MH	M	0,496830464
11	1 ELORAN + 1 GLONASS	DİĞER	VAR	VH	VH	VH	MH	ML	VH	VH	M	0,822179299
12	1 ELORAN + 1 GLONASS	DİĞER	YOK	M	H	M	M	ML	H	MH	M	0,597510293

Ek Tablo 1'in devamı

Koşullu Olasılık No	Cihaz Çeşidi Düğümü	Sinyal Doğrulama Ekipmanı Düğümü	Uzman Sözlü Değerlendirme AIS GÜVENLİ								
			1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
13	UYDU AIS	VAR	VH	H	VH	H	H	VH	MH	VH	0,898953018
14	UYDU AIS	YOK	H	M	H	MH	MH	H	L	H	0,713498985
15	VHF AIS	VAR	H	MH	MH	ML	ML	MH	H	MH	0,683309915
16	VHF AIS	YOK	MH	L	M	L	L	M	VL	M	0,333813271

Ek Tablo 1'in devamı

Koşullu Olasılık No	İşletim Sistemi Düğümü	Virüs Programı Düğümü	Güncellemeler Düğümü	Uzman Sözlü Değerlendirme Yazılım SİSTEMİ KORUR								
				1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
17	DESTEKLENEN	VAR	YAPILIYOR	H	VH	VH	H	VH	VH	H	H	0,918424348
18	DESTEKLENEN	VAR	YAPILMIYOR	MH	ML	H	MH	ML	M	H	M	0,590453667
19	DESTEKLENEN	YOK	YAPILIYOR	M	ML	H	MH	ML	M	MH	M	0,535989665
20	DESTEKLENEN	YOK	YAPILMIYOR	ML	L	ML	M	ML	L	M	ML	0,279581596
21	DESTEKLENMEYEN	VAR	YAPILIYOR	L	ML	MH	MH	ML	M	ML	L	0,356189928
22	DESTEKLENMEYEN	VAR	YAPILMIYOR	L	ML	L	M	VL	L	ML	L	0,182876019
23	DESTEKLENMEYEN	YOK	YAPILIYOR	VL	L	L	M	VL	L	L	L	0,129619578
24	DESTEKLENMEYEN	YOK	YAPILMIYOR	VL	VL	VL	ML	VL	VL	L	L	0,078977369

Ek Tablo 1'in devamı

Koşullu Olasılık No	Yazılım Düğümü	Harita Düzeltme Yöntemi Düğümü	Kullanıcı Prosedürleri Düğümü	Uzman Sözlü Değerlendirme ECDIS GÜVENLİ								
				1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
25	SİSTEMİ KORUR	ORJİNAL CD	VAR	H	VH	VH	VH	H	VH	H	H	0,914075342
26	SİSTEMİ KORUR	ORJİNAL CD	YOK	MH	MH	H	VH	MH	L	H	M	0,707066598
27	SİSTEMİ KORUR	HARİCİ BELLEK	VAR	MH	H	H	MH	M	H	M	M	0,702504701
28	SİSTEMİ KORUR	HARİCİ BELLEK	YOK	ML	ML	M	M	ML	L	M	ML	0,331875504
29	SİSTEMİ KORUR	İNTERNET BAĞLANTISI	VAR	M	VH	H	M	H	MH	M	VH	0,75104315
30	SİSTEMİ KORUR	İNTERNET BAĞLANTISI	YOK	L	MH	MH	ML	M	L	ML	M	0,41711825
31	ZAFİYET YARATIR	ORJİNAL CD	VAR	MH	M	M	H	ML	M	MH	L	0,51997704
32	ZAFİYET YARATIR	ORJİNAL CD	YOK	M	L	ML	H	L	L	MH	L	0,314074728
33	ZAFİYET YARATIR	HARİCİ BELLEK	VAR	M	ML	ML	M	VL	ML	M	VL	0,293520051
34	ZAFİYET YARATIR	HARİCİ BELLEK	YOK	L	VL	L	ML	VL	VL	M	VL	0,134446234
35	ZAFİYET YARATIR	İNTERNET BAĞLANTISI	VAR	L	M	L	ML	L	ML	L	L	0,205993887
36	ZAFİYET YARATIR	İNTERNET BAĞLANTISI	YOK	VL	L	VL	L	VL	VL	L	L	0,082965728

Ek Tablo 1'in devamı

Koşullu Olasılık No	İnternet Bağlantısı Düğümü	Ağ Bölgelere Ayrılması Düğümü	Tespit Edici Ekipman Düğümü	Uzman Sözlü Değerlendirme Ağ Altyapısı GÜÇLÜ								
				1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
37	VAR	EVET	VAR, AYNI MARKA	MH	MH	M	H	MH	MH	ML	H	0,67804168
38	VAR	EVET	VAR, FARKLI MARKA	H	H	MH	H	H	ML	ML	H	0,722234052
39	VAR	EVET	YOK	M	M	M	MH	M	ML	ML	M	0,461339983
40	VAR	HAYIR	VAR, AYNI MARKA	M	L	VL	MH	L	ML	L	ML	0,23850675
41	VAR	HAYIR	VAR, FARKLI MARKA	MH	ML	M	MH	ML	L	L	ML	0,356803956
42	VAR	HAYIR	YOK	VL	VL	VL	M	VL	VL	L	L	0,091105186
43	YOK	EVET	VAR, AYNI MARKA	H	H	M	VH	MH	VH	H	H	0,826216345
44	YOK	EVET	VAR, FARKLI MARKA	VH	VH	VH	VH	VH	H	H	H	0,926408174
45	YOK	EVET	YOK	MH	MH	M	H	ML	MH	H	M	0,646720899
46	YOK	HAYIR	VAR, AYNI MARKA	MH	ML	ML	H	L	MH	MH	ML	0,4782027
47	YOK	HAYIR	VAR, FARKLI MARKA	H	M	H	H	L	ML	MH	ML	0,563213009
48	YOK	HAYIR	YOK	ML	L	ML	M	L	M	MH	L	0,311956876

Ek Tablo 1'in devamı

Koşullu Olasılık No	Yazılım Düğümü	Ağ Altyapısı Düğümü	Kullanıcı Prosedürleri Düğümü	Uzman Sözlü Değerlendirme Otomasyon, Haberleşme, Bilgisayar Sistemi GÜVENLİ								
				1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
49	SİSTEMİ KORUR	GÜÇLÜ	VAR	H	VH	VH	VH	VH	VH	H	H	0,925175297
50	SİSTEMİ KORUR	GÜÇLÜ	YOK	MH	MH	H	H	MH	M	MH	M	0,705667734
51	SİSTEMİ KORUR	ZAYIF	VAR	M	MH	MH	MH	MH	MH	M	M	0,642270648
52	SİSTEMİ KORUR	ZAYIF	YOK	ML	ML	M	M	M	L	ML	ML	0,331875504
53	ZAFİYET YARATIR	GÜÇLÜ	VAR	MH	M	M	H	ML	M	M	L	0,486338356
54	ZAFİYET YARATIR	GÜÇLÜ	YOK	M	L	ML	MH	ML	VL	ML	L	0,26244883
55	ZAFİYET YARATIR	ZAYIF	VAR	ML	L	L	M	ML	L	L	L	0,191904836
56	ZAFİYET YARATIR	ZAYIF	YOK	VL	VL	VL	ML	VL	VL	VL	L	0,067655584

Ek Tablo 1'in devamı

Koşullu Olasılık No	Konum Belirleme Sistemi Düğümü	AIS Düğümü	ECDIS Düğümü	Otomasyon Haberleşme Bilgisayar Sistemleri Düğümü	Uzman Sözlü Değerlendirme Siber Saldırı OLMAZ								
					1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
57	GÜVENLİ	GÜVENLİ	GÜVENLİ	GÜVENLİ	H	VH	VH	M	M	VH	H	MH	0,818126088
58	GÜVENLİ	GÜVENLİ	GÜVENLİ	GÜVENLİ DEĞİL	VL	MH	M	ML	ML	M	MH	L	0,404362154

Ek Tablo 1'in devamı

Koşullu Olasılık No	Konum Belirleme Sistemi Düğümü	AIS Düğümü	ECDIS Düğümü	Otomasyon Haberleşme Bilgisayar Sistemleri Düğümü	Uzman Sözlü Değerlendirme Siber Saldırı OLMAZ								
					1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
59	GÜVENLİ	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ	L	ML	ML	ML	ML	H	H	L	0,357912844
60	GÜVENLİ	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	VL	ML	L	L	L	ML	MH	VL	0,204385425
61	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ	L	ML	M	ML	ML	H	MH	L	0,380977887
62	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	VL	L	L	L	L	L	ML	VL	0,123981559
63	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ	MH	L	H	M	M	MH	MH	ML	0,566989098
64	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ DEĞİL	VL	ML	ML	ML	ML	L	ML	L	0,205862562
65	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ	GÜVENLİ	M	MH	MH	ML	ML	MH	MH	M	0,579747793
66	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ	GÜVENLİ DEĞİL	VL	ML	M	ML	ML	L	ML	L	0,233805835
67	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ	L	ML	M	ML	ML	M	M	L	0,322043202
68	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	VL	L	VL	L	VL	L	ML	VL	0,099368481
69	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ	L	L	L	L	VL	ML	M	L	0,177252218
70	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	VL	VL	VL	L	VL	VL	VL	VL	0,046915383
71	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ	M	L	MH	L	ML	M	M	ML	0,387848375
72	GÜVENLİ DEĞİL	GÜVENLİ DEĞİL	GÜVENLİ	GÜVENLİ DEĞİL	VL	L	L	L	ML	L	L	L	0,135275135

Ek Tablo 1'in devamı

Koşullu Olasılık No	Siber Saldırı Düğümü	Yedek Ekipman Düğümü	Dijital Verilerin Doğrulanması Düğümü	Uzman Sözlü Değerlendirme Siber Zarar HAYIR								
				1	2	3	4	5	6	7	8	Bulanık Olasılık Değeri
73	OLUR	VAR	EVET	M	M	MH	ML	H	H	ML	M	0,574174282
74	OLUR	VAR	HAYIR	L	L	M	L	MH	MH	L	M	0,369107591
75	OLUR	YOK	EVET	ML	ML	L	L	MH	M	L	M	0,329500799
76	OLUR	YOK	HAYIR	VL	VL	VL	VL	L	VL	VL	L	0,06238972
77	OLMAZ	VAR	EVET	VH	VH	VH	H	VH	VH	MH	VH	0,925396693
78	OLMAZ	VAR	HAYIR	VH	MH	VH	H	VH	MH	MH	VH	0,863340046
79	OLMAZ	YOK	EVET	VH	H	H	H	VH	H	MH	VH	0,887908788
80	OLMAZ	YOK	HAYIR	VH	ML	H	H	VH	M	M	VH	0,741964255

81 nolu koşullu olasılık durumu için uzman değerlendirmesi kullanılmamıştır, istatistiki veri kullanılmıştır.
82 nolu koşullu olasılık durumu: Siber saldırı olmaz ise başarısız girişim de olmaz, yani olasılık sıfırdır.

ÖZGEÇMİŞ

Denizcilik Fakültesi Güverte Bölümü'nden mezun oldu ve Uzakyol Vardiya Zabiti ehliyeti ile kuru yük gemilerinde görev yapmaya başladı. Uzakyol Birinci Zabit, 2011 yılında Uzakyol Kaptan yeterliliğini aldı, sonunda aktif deniz çalışma sürecini bitirdi. Trabzon Limanı'nda stajer kılavuz kaptan, KTÜ Sürmene Deniz Bilimleri Fakültesi Araştırma Gemisi KTÜ DENAR-1'de kaptan olarak görev yaptı. Halen, Giresun Limanı'nda Kılavuz Kaptan olarak görev yapmaktadır.