Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi • Cilt 25, Sayı 2, Prof. Dr. Ferit Hakan Baykal Armağanı, Aralık 2019, ISSN 2146-0590, ss. 1131-1137 • DOI: 10.33433/maruhad.665513

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

Siber Tehlikelerin Denizcilik Sektörüne Etkisi

Effects of Cyber Risks in Maritime Sector

Didem ALGANTÜRK LIGHT*

Öz

Uluslararası taşımacılığın %90' fazlası deniz yoluyla gerçekleştiği nazara alındığında deniz yolu taşımacılığının dünya ekonomisinin önemli bir parçası olduğu tartışılmazdır. Tarımsal ürünlerin, enerjinin, üretilen eşyanın ve diğer bir çok malın dünyanın bir yanından diğer yanına emniyetli ve güven içinde taşınması önemli bir faaliyettir. Teknik gelişmeler ile birlikte deniz taşımacılığı, bilgisayar sistemine bağlı ve elektronik bağlantı yollarıyla faaliyetlerini sürdürmekte olduğundan bu faaliyetlerin güvenli bir şekilde devam ettirilebilmesi için emniyetli siber sistemlerinin kurulması önemli bir ihtiyaçtır. Çalışmamızda, son dönemlerde siber risklerin denizcilik sektörüne olan etkileri ve uluslararası alanda bu konuda yapılan yasal çalışmalar genel olarak değerlendirilecektir.

Anahtar Kelimeler: Denizcilik, siber tehlikeler, siber risk yönetimi

Abstract

It is unquestionable that maritime transport is an important part of the world trade economy when it receives more than 90% of the international transport by sea. "Secure and safe transportation is an important issue when transporting agricultural products, energy, manufactured goods and many other goods from one part of the world to another part . Since maritime transport is rely on to the computer system and is in operation via electronic connection, the establishment of safe cyber systems is an important in order to ensure that these activities can be secure and safely maintained.
In this paper, the effects of cyber risks in the maritime sector and the legal works in the international arena will be generally evaluated.

Keywords: Shipping, cyber risks , cyber risk management

* Prof. Dr., York Üniversitesi Osgoode Hall Law School,Kanada Misafir Öğretim Üyesi,
E-Mail: didemlight@gmail.com

Makale Gönderim Tarihi: 10.06.2018
Yayına Kabul Tarihi: 26.12.2018

I. DENİZCİLİKTE SİBER RİSKLER

Dünyada, 52.000 ticaret gemisi faaliyet göstermekte olup[1], dünya ticaretinin %90 fazla deniz taşımacılığıyla gerçekleştirilmektedir[2]. Modern dünya çağında her türlü emteanın ithalat ve ihracaatının deniz taşımacılığı olmadan gerçekleşmesi mümkün değildir. Teknolojinin gelişmesi ile birlikte gemilerin teknik yapısı bu gelişim ve değişime uygun olarak digitalleşme, entegrasyon ve otomasyon sistemlerine bağlı kalarak ilerlemektedir.

Denizcilik sektörüne genel olarak baktığımızda liman idareleri, gemilerin tüm operasyon ve yönetimi, gemi klas kuruluşları, gemi acenteleri, gemi ekipman üreticileri, limanlar, terminaller, lojistik faaliyetler, yükün elden geçirilmesi ve yükün yönetimi sistemleri, marina tesis işletmecileri (örneğin yakıt, ikmal, yıkama/temizlik, tamir firmaları, dükkanlar, restaurantlar) yolcu servis ve yönetim sistemleri ve haberleşme gibi tüm faaliyetler bilgisayar sistemi üzerine kurulmuştur ve tüm organizasyon siber saldırılara her an maruz kalma tehlikesi ile karşı karşıyadır. Özelikle ileriki yıllarda gemi müretteabatı olmaksızın (insansız) yolcu ve yük taşımacılığının (autonomus ships) yaygınlaşması ihtimalinde but tür risklerin kapsamı daha da artacaktır[3].

Gemi ekipmanları ve faaliyetleri açısından, örneğin GPS (global konumlandırma sistemleri), otomatikleştirilmiş donatım, fiziksel güvenlik sensörleri, elektronik sertifikalar, kargo takibi, elektronik seyir cihazları, otomatik tanıma sistemleri, kayıt tutma, varış öncesi işlemlerin kaydı gibi tüm denizcilik faaliyetleri için güvenli bilgisayarlara ve bu bilgisayarları yönetecek güvenli internet bağına ihtiyaç vardır. Bu sistemlerin tamamı, internet bağı ile her an siber saldırılara hedef olabilir.

Denizcilik sektöründe, gerçekleşen siber saldırı örneklerini şu şekilde sıralamak mümkündür[4]:

geminin GPS sistemini kontrol altına alarak, geminin yönünü değiştirilmesi,

Bilgisayar korsanları olarak adlandırılan "hackerler, Afrika sahillerinde yüzen petrol platformunu bir yana eğerek sistemin 19 gün kapanması,.

2011 yılında Hackerlar, Antwerp limanının siber sistemine girerek, yasa dışı uyuşturucu yüklü konteynerin yerini tespit edere, yükün çalınması olayı[5]*,*

Somalili korsanların, hackerlar ile anlaşarak, bir denizcilik şirketinin siber ağına girmesi ve ardından değerli yük taşıyan ve gemi bordasında güvenliği az düzeyde olan Şirket gemisini tespit ederek, Gullf Aden geçişi sırasında yükün çalınması,

1 Bu rakkam Ocak 2008 – Ocak 2017 tarihleri için tespit edilmiştir. https://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/, 27.12.2017

2 http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade, 13.11.2017.

3 UK Automated Ships Ltd ve Norveç Kongsberg Maritime birlikteliği ile 2017 yılında inşasına başlanılan Hrönn isimli gemidir, http://gcaptain.com/first-unmanned-and-fully-automated-offshore-vessel-planned-for-2018/ , 8.10.2018

4 *Cyber Security, Managing the threat, www. gard.no/web/topics/article, 9.11.2017.*

5 www.bbc.com/news/world-europe-24539417, 8.10.2018.

2015 yılında Norveç enerji, petrol ve gaz sektöründe 50 den fazla siber saldırı olayı gerçekleşti.

2017 yılı içinde ise, denizcilikte en önemli siber saldırıları, Wannacry/ NotPetya, isimleriyle gerçekleşen fidye saldırılarıdır [6]. Bu tür siber saldırlar bilgisayara veya onun datasına girerek, bilgisayarın kontrolünü ele geçirmekte ve yeniden açmak için Bitcoin[7] ile ödeme talep edilmektedir. Dünyanın en büyük konteyner taşımacılığını yapan firmalardan biri olan AP Moller-Maersk, Notpetya isimli siber saldıraya maruz kaldı ve Temmuz /Ağustos 2017 aylarında yaklaşık 250 milyon Amerikan Doları ticari zarara uğradı[8].

II. DENİZCİLİKTE SİBER GÜVENLİK

Siber güvenlik, yönetim, bilgi ve teknoloji bilgisine dayanmaktadır. Dolayısıyla güvenli denizciliği sağlanması bu üçlü ilişkinin ve yapının sağlam bir şekilde anlaşılması ve kurulmasına bağlıdır. Deniz taşımacılığında, siber sisteme bağlı olan tüm operasyonel işlemlerin değerlendirilmesi suretiyle bunların maruz kalabileceği siber saldırıları belirlemek ve bu konuda milli ve milletlerarası yasal önlemler ve düzenlemeler yapılmasına ihtiyaç vardır[9].

Deniz taşımacılığının maruz kalabileceği siber saldırılar sonucunda örneğin *hackerlerin* petrol taşıyan tankerin navigasyon sistemine veya GPS sistemine girerek çatmaya sebebiyet vermesi senaryosunda, karşı karşıya kalabilecek tehlikeler çevre kirliliği, faaliyetlerin kesilmesi nedeni ile kazanç kaybı, liman faaliyetlerinin durması, geminin tam zıyaı veya hasara uğraması, gemi adamlarının veya yolcuların bedeni zarara uğraması veya ölmesi, yükün zıyaı veya hasara uğraması şeklinde sıralamak mümkündür. Internete bağlanabilecek her ortamda örneğin

6 https://www.itproportal.com/features/what-you-need-to-know-about-the-petya-and-wannacry-cyber-attacks/, 27.10.2017.

7 Bitcoin, sanal bir para birimidir.Ayrıntılı bilgi için bkz **Olena Demchenko,** " BITCOIN : Legal Definition and Its Place In Legal Framework", Journal of International Trade, Logistics and Law, Vol.3, Num.1, 2017, sh. 23-42.

8 https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/, 20.10.2017; https://www.reuters.com/article/us-cyber-attack-maersk/maersk-says-it-breakdown-could-be-global-idUSKBN19I1NO, 8.10.2017

9 Milli yasal düzenlemelere emsal olarak, Kanada tarafından yapılan yasal çalışmaları verebiliriz. Kanada'da 15.12.1994 tarihli Deniz Taşımacılığı Güvenlik Kanunu yürürlüğe girmiştir. Bu yasal düzenleme, Kanada deniz taşımacılığının güvenli bir şekilde işleyebilmesinin sağlanması bakımından hazırlanmış çerçeve bir kanundur. Bu Kanun, Kanada'da bulunan gemilere ve denizcilik tesislerine, Kanada dışında bulunan Kanada gemilerine, deniz teçhizatları ve yapılarına uygulanır. Milli Savunma Bakanı'nın yetkisi altında bulunan gemilere veya deniz tesislerine veya yabancı bir ülkede bulunan askeri gemilere uygulanmaz. Deniz Taşımacılığı Güvenlik Kanunun amacı, Kanada Ulaştırma Bakanlığı'na Kanada deniz ulaşım sisteminin güvenliğinin sağlamasına ilişkin yasal düzenlemeler, güvenlik önlemleri ve kurallarını hazırlama yetkisi vermektedir. Bu Kanunun uygulanması bakımından Deniz Taşımacılığı Güvenlik Yönetmeliği ve Yerel Feribotlar Güvenlik Yönetmeliği (Kanada Ulaşımı) hazırlanarak yürürlüğe girmiştir. Bu her iki yönetmelik kapsamında deniz tesislerinin ve gemilerin siber güvenliğe ilişkin güvenlik planları hazırlanır ve bu hazırlık sırasında yapılacak güvenlik değerlendirmeleri kapsamında radyo ve telekomünikasyon sistemleri, bilgisayar sistemleri ve bilgisayar ağları da dahildir,bkz. Marine Transportation Security Act – "*Deniz Taşımacılığı Güvenlik Kanunu*" madde4; https://www.tc.gc.ca/eng/acts-regulations/acts-1994c40.htm,10;http://laws-lois.justice.gc.ca/eng/regulations/SOR-2004-144/,;http://laws-lois.justice.gc.ca/eng/regulations/SOR-2009-321/page-1.html, 11.11.2017;
https://www.tc.gc.ca/eng/marinesecurity/regulations-362.htm, 13.11.2017.;
http://www.cosbc.ca/index.php/files-downloads/transport-canada/455-understanding-cyber-risk/file, 10.11..2017

gemideki bir personelin bilmeden güvensiz bir internet ortamına bağlanması ile birlikte geminin siber saldırıya uğrayarak belirttiğimiz çatma senaryosunun gerçekleşmesi muhtemeldir. Bu nedenle, gemi adamları da dahil olmak üzere denizcilikte siber saldırılara karşı eğitim her zaman olduğu gibi en önemli etkili yöntemdir.

Son dönemlerde artan siber saldırılar ve siber risklerin deniz taşımacılığını bu denli etkileyecek nitelikte olması karşısında uluslararası denizcilik örgütleri ve sektörden girişimciler tarafından çalışmalar başlatılmıştır. Bu çalışmalardan en önemlisi IMO tarafından hazırlanan "Gemilerde Siber Güvenlik Rehberi"dir. *IUMI, BIMCO, ICS, Intertanko, Intercargo,* ve *Cruise Lines International Association* ve *The Oil Companies International Marine Forum* tarafından ortak bir çalışma olarak hazırlanan ve IMO'nun rehberinin temel alındığı "Gemilerde Siber Güvenlik Rehberi" hazırlanmıştır. Bunun yanı sıra uygulamada sektör girişimcileri siber risklerin farkındalığının sağlanması, danışmalık ve bu konuda eğitim olanakları vermeye başlamıştır. "Denizde Siber Farkındalık Kampanyası[10]* ve "CyberSail[11]" isimli kuruluşlar bunlardan bazılarıdır[12].

A. ULUSLARARASI DENİZCİLİK ÖRGÜTÜ'NÜN (IMO) SİBER TEHDİTLER ÜZERİNE ÇALIŞMALARI

BM'e bağlı bir kurum olan IMO[13]nun uzmanlık alanı, denizde emniyet ve güvenliğin sağlanması ve gemi kaynaklı çevre kirlenmesinin önlenmesidir. Deniz taşımacılığına karşı yapılacak siber saldırıların önlenmesi de IMO'nun uzmanlık alanı kapsamında kalmaktadır.

IMO, denizcilikte siber risk yönetiminde mevcut ve ortaya çıkan siber tehditler ve güvenlik zaaflarından denizciliği korumak için üst düzeyde tavsiyeler niteliğinde bir rehber hazırladı. "*Gemilerde Siber Güvenlik Rehberi*" olarak adlandırılan bu kitapçık , IMO kurallarıyla uyum içerisinde olup, siber güvenlik ve siber emniyet risk yönetimi açısından pratik öneriler niteliğindedir. Ayrıca, etkili siber risk yönetimini destekleyen işlevsel esaslara da yer vermektedir[14]. Böylelikle denizcilikte siber tehlikelere karşı siber yönetim planına yönelik belli standartların uluslararası alanda sağlanarak güvenli ve emniyetli denizciliğin yürütülmesi hedeflenmektedir.

10 Bu kampanya denizcilik ve offshore sektörünün girişimi ile oluşturulmuş olup, amacı denizde siber risklere ve yönetimine ilişkin farkındalık yaratmaktır, https://www.becyberawareatsea.com/, 8.1.2018

11 denizcilikte risk analizi, yönetimi e eğitimi vermektedir https://cybersail.org/, benzer eki

12 **Walter, Justers**, AFNI, Cyber Security at Sea , http://www.bvz-abdm.be/sites/default/files/walter_justers_-_cyber_security_-_proteus_presentation.pdf, 12.11.2017

13 Gemicilik sektörüne etki eden her türlü teknik konuyla ilgili olarak, uluslararası ticaretle uğraşan ülkelerin mevzuat ve uygulamaları açısından hükümetler arasında işbirliği sağlamak, denizde güvenlik, seyrüsefer etkinliği ile gemilerden kaynaklanan deniz kirliliğinin önlenmesi ve kontrolü ile ilgili konularda, en üst düzeyde uygulanma etkinliğine sahip standartların genel kabulünü teşvik etmek ve kolaylaştırmak olarak sıralanabilir.

14 *"Guidelines on maritimecyber risk management"*, "*Kolaylaştırma Komitesi' nin* 4 – 7 Nisan 2017 tarihlerinde gerçekleşen 41. Oturumunda ve Deniz Güvenliği Komitesi'nin 7-16 Haziran 2017 tarihlerinde gerçekleşen Oturumunda, ortaya çıkan siber tehditler ve güvenlik zaafları konusunda denizcilik sektörünün bilinçlendirilmesine acil ihtiyaç nedeniyle hazırlanmıştır. MSC-FAL.1/Circ.3 Guidelines on maritimecyber risk management.

B. ULUSLARARASI DENİZCİLİK BİRLİKLERİNİN ORTAK ÇALIŞMASI

BIMCO, IUMI, , ICS, Intertanko, Intercargo, ve Cruise Lines International Association ve "Oil Companies International Marine Forum" bir araya gelerek "Gemilerde Siber Güvenlik Rehberi" adlı bir kitapçık hazırlamıştır[15].

Bu rehber tavsiye niteliğinde olup amacı, donatanlar ve işletenlere, operasyonlarını nasıl değerlendireceği konusunda bilgi sunmak ve gemilerinde bulunan siber sistemlerin güvenliğini sağlamak için gerekli prosedürleri ayrıntılı olarak örneklerle ele almaktadır[16].

C. DENİZCİLİKTE SİBER RİSK YÖNETİMİ

Siber emniyet ve siber güvenlik risklerinin yönetimi denizcilikte güvenli bir çalışma ortamının sağlanması bakımından son derece önemlidir. Denizcilik faaliyetlerinde siber risk yönetimi IMO tarafından hazırlanan "*Gemilerde Siber Güvenlik Rehberi"* madde 3/5 uyarınca, şu unsurları içermelidir[17];

Tanımlama : siber risk yönetiminde yetkili olan kişilerin belirlenmesi ve sorumlulukların tespit edilmesi, sistemi ve sistemin kapsamını ve verileri ve yine sistemin bozulması halinde gemi faaliyetlerine ilişkin doğacak risklerin tanımlanması.

Koruma : risk kontrol süreçleri ve önlemlerinin uygulanması ve bir siber saldıraya karşı korumak için acil durum planlanması, denizcilik operasyonlarının sürekliliğinin sağlama alınması

Belirleme : bir siber olayını zamanında belirlenmesi için gerekli faaliyetlerin geliştirilmesi ve uygulanması.

Karşılık verme: bir siber saldırı karşısında denizcilik hizmetlerinin ve operasyonun bozulması tehlikesine karşı gerekli faaliyetlerin geliştirilmesi, uygulanması direnç sağlanması ve onarılması.

Telafi edilmesi: bir siber saldırı sonucunda denizcilik hizmetlerinin etkilenmesi halinde siber

sistemin yedeklenmesi ve onarılmasına ilişkin gerekli önlemlerin tanımlanması .

IV. DENİZCİLİKTE SİBER RİSKLER VE SİGORTA TEMİNATI

Denizcilikte siber risk yönetiminin bir unsuru olarak siber risklerin sigorta teminatı alınması önemlidir. Siber riskler, siber güvenlik poliçesi ile veya deniz sigorta poliçelerine ek olarak siber güvenlik teminatı almak suretiyle sigortalanabilir[18].

15 http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16, 9.11.2017.

16 http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16, p.1

17 MSC-FAL.1/Circ.3 "Guidelines On Maritimecyber Risk Management", madde. 3.5

18 *BIMCO, IUMI, , ICS, Intertanko, Intercargo, ve Cruise Lines International Association ve "Oil Companies International*

Uygulamada standart siber güvenlik sigortası ile siber saldırının gerçekleşmesi sonucu dijital varlıkların örneğin veri ve programların uğradığı maddi hasar, iş faaliyetinin kesilmesi nedeniyle doğan kayıplar ve bu sebeple ortaya çıkan masraflar, siber gasp nedeniyle sistemin yeniden çalıştırılabilmesi için verilen fidye, gizlilik taahhüdünün ihlalinden doğan sorumluluklar, IT sorumluluğu, idari para cezaları, masraflar ve giderler, kriz yönetimi masrafları (örneğin bildirim masrafları, adli masraflar) teminat altına alınır[19]. Böylelikle, örneğin, siber saldırı sonucu veri tabanının zıyaı veya gemi ekipmanının arızası nedeniyle verilen idari cezalar nedeniyle doğan zararın siber risk sigortası kapsamında tazmini mümkündür. Siber güvenlik sigortası şahısların uğradığı bedeni zararları ve mallara gelen zıya ve hasardan sorumlu değildir.

Her zaman geminin ve/veya yükün uğradığı zıya veya hasar doğrudan siber riskin gerçekleşmesi nedeniyle doğmayabilir, örneğin siber saldırı sonucu bir geminin yanma, batma veya başka bir gemiye çatma sonucunda üçüncü şahıslara karşı doğan sorumluluk, şeklinde de ortaya çıkabilir. Bu durumda ortaya çıkan zararın tazmini deniz sigorta sözleşmeleri kapsamında değerlendirilmesi mümkündür.

Uygulamada standart tekne[20] ve yük[21] sigorta poliçelerinde siber saldırıların teminat kapsamında olmadığına ilişkin "*Siber Saldırı Teminat Dışı Klozu*" "*Kloz CL380*" bulunmaktadır[22]. Siber risklerin teminat kapsamı dışında olduğuna ilişkin bir diğer kloz ise, "*Terrorism Form T3 LMA3030 Exclusion 9"dir.* Bu kloza göre, terörizm amaçlı siber saldırıları teminat dışındadır.

Kulüp Sigorta (P&I) poliçelerinde ise[23], siber risklerin teminat dışı bırakıldığına dair bir kloz yer almamaktadır. Ancak " "Savaş ve Terörizm" klozu ve "*sektörel uygulamaların benimsemesiyle önlenebilir olabileceği ve öngörülebilir riskler kapsamında*" değerlendirilmek suretiyle meydana gelen zarar, Kulübün takdir yetkisine dayanılarak teminat dışında bırakılması mümkündür[24].

Donatanın siber saldırılar sonucu ödediği fidyeler nedeniyle doğan finansal kayıpları kulüp sigortası teminatı kapsamında değildir. Fidye ödemeleriyle d kaybın ancak kulübün takdir

Marine Forum" tarafından hazırlanan "Gemilerde Siber Güvenlik Rehberi" sh.35-36

19 Cyber Risk and Insurance, An Introduction to Cross Class Cyber Liabilities, January, 2016, Norton Rose Fulbright, http://www.maritimelondon.com/wp content/uploads/2016/01/005_Cyber_Risks_ Combined_ – 110116.pdf, .

20 https://www.swedishclub.com/upload/174/18.increased-value-hull-interest.pdf,10.1.2018

21 http://www.allianz-cargo.co.uk/rsrc/PDF/$file/PolicyWording.pdf, 10.12018

22 Institute Cyber Attack Exclusion Clause 1.*1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense, directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system. 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile..*

23 **Didem Algantürk Light** ; Deniz Sigorta Hukukunda Kulüp Sigortası, İstanbul 2006shç 3 vd.

24 **Rupert Banks,**"Cyber risks and P&I insurance implications", https://www.safety4sea.com/wp-content/uploads/2017/10/Standard-Club-Cyber-risks-and-PI-insurance-implications-2017_10.pdf, 10.1.2018 ; https://www.ukpandi.com/knowledge-publications/industry-issues/industry-developments/cyber-security-at-sea/,; https://www.steamshipmutual.com/loss-prevention/cybersecurity.htm, 11.11.2017

yetkisine bağlı olarak veya bir P& I riskini önlemek ya da azaltmak için ya da bir müşterek avarya masrafı olarak taşıma sözleşmesinin ihlali nedeniyle yük ilgililerinden talep edilememesi nedenleriyle sınırlı olmak tazmini mümkündür[25]. Özellikle son dönemlerde gerçekleşen Wannacry/Notpedya gibi siber saldırı nedeniyle yapılan fidye ödemelerinin sigorta teminatı kapsamında tazmin edilebilmesi için sigorta poliçesinde bu tür risklerin teminat kapsamında olduğunun ayrıca belirtilmesi gereklidir ve bu risklerin "*kaçırılma – fidye sigortası"* teminatı kapsamına alınması gereklidir.

Deniz sigorta poliçelerinde veya siber sigorta poliçelerinde teminat altına alınan siber risklerin ve siber risklerin gerçekleşmesi sonucu doğrudan doğrudan ve dolaylı risklerin (örneğin batma, yanma, çatma gibi) poliçede hiçbir tereddütte yer vermeyecek şekilde tek tek tanımlanması sigortalı açısından önemlidir[26]. Sigorta poliçesinde siber riskler teminat dışında bırakılmış ise, siber saldırı sonucu doğacak zıya ve hasarın tazmini bu kloz nedeniyle mümkün olamayacaktır[27].

Deniz sigortalarında yer alan siber saldırıları teminat dışında tutan bu klozlar karşısında denizcilik sektörünün siber risk sigortası yaptırma ihtiyacı vardır [28]. Bu nedenle, siber risklere ilişkin ek teminatların poliçeye dahil edilmesi gereklidir. Bunun yanı sıra, siber riskler ile ilgili sektörel uygulamaların ve tavsiyelerin örneğin IMO ve *BIMCO, IUMI, , ICS, Intertanko, Intercargo, ve Cruise Lines International Association ve "Oil Companies International Marine Forum"* bir araya gelerek hazırladığı "*Gemilerde Siber Güvenlik Rehberi"lerininin takip edilerek* uygulanması önemlidir.

Sigorta sektörünün de, denizciliğin karşı karşıya kaldığı siber tehlikelere ilişkin bu konuda özel olarak siber risk analizini yaparak, prim dengesini sağlamak suretiyle büyük kayıplara yol açacak bu tür riskleri sigortasız bırakmamaya özen göstermesi gereklidir.

25 https://www.westpandi.com/About-Us/Underwriting/Piracy—-Kidnap-Ransom-, http://www.gard.no/web/updates/content/52041/piracy-and-insurance, 11.11.2017

26 Siber tehlikelere ilişkin sigorta teminatı kapsamında olmayan riskleri sigortalayan "cyber gap insurance" "siber boşluk sigortası" ile teminat altına alınabilmesi mümkündür, http://www.oliverwyman.com/content/ dam/marsh/Documents/PDF/UKen/Cyber%20Gap%20Insurance%20Cyber%20Risk%20Filling%20the%20Coverage%20Gap-07-2014.pdf, 11.11.2017

27 https://www.reuters.com/article/us-shipping-insurance-cyber/insurance-gaps-leave-shipping-exposed-to-growing-cyber-threats-idUSKBN14W1EA, 11.11.2017

28 Cyber Risk and Insurance, An Introduction to Cross Class Cyber Liabilities, January, 2016, Norton Rose Fulbright, http://www.maritimelondon.com/wp content/uploads/2016/01/005_Cyber_Risks_ Combined_ – 110116.pdf, , 10.1.2018