III. Ulusal Liman Kongresi
doi: 10.18872/DEU.df.ULK.2017.017

DENİZ TAŞIMACILIĞINDA SİBER GÜVENLİĞİ TEHDİT EDEN UNSURLAR VE KORUMA ÖNLEMLERİ ÜZERİNE BİR ÇALIŞMA

Atalay KELEŞTEMUR[1], Birsen KOLDEMİR[2], Murat YAPICI[3]

ÖZET

Bilgi teknolojilerindeki hızlı gelişmeler her alanda olduğu gibi deniz ticaretinde de kendini göstermiştir. Bilgi teknolojileri, bilgisayar ve iletişim teknolojisiyle beraber kullanıldığında çok önemli olanaklar sağlamaktadır. Limanlarda bilgi teknolojilerinin etkin kullanılması zaman, yer ve maliyet faydaları yaratmaktadır. Gemilerde bilgi teknolojilerinin kullanımı ise özellikle navigasyon ve yükleme/tahliye operasyonları başta olmak üzere, balast operasyonları ve trim hesabı gibi birçok işlemin yerine getirilmesine imkan tanımıştır. Bu durum, zabitlerin iş yükünü hafifletmiş ve aynı zamanda daha hızlı operasyon yapmalarını sağlamıştır. Ancak son yıllarda artarak gerçekleştirilen siber saldırılar; gemilerin, limanların ve deniz taşımacılığı ile uğraşan şirketlerin bilişim sistemlerini olumsuz etkilemektedir.

Liman bilgi teknolojilerinde oluşacak problemler işlerin aksamasına, sonucunda ise ekonomik kayıpların meydana gelmesine neden olacaktır. Dünya'da hızla artan bu saldırılar karşısında bir hukuk oluşturulmaya çalışılırken birçok şirket siber güvenlik konusunda ciddi yatırım yapmaktadırlar. Son birkaç yıldır milyonlarca dolarlık kayıp yaşatan ve seksenden fazla ülkeyi etkileyen fidye yazılımlar tüm sistemleri şifrelemekte, talep edilen dijital paranın ödenmemesi durumunda

---

1 Siber Güvenlik Araştırmacısı, nProt Security, İstanbul atalay.kelestemur@nprot.com

2 Yrd. Doç. Dr., İstanbul Üniversitesi, Mühendislik Fakültesi, İstanbul birsenkoldemir@yahoo.com

3 Doktora Öğrencisi, Piri Reis Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul murat.yapici@pru.edu.tr

verilerin geri dönülemeyecek şekilde yok olması tehdidini oluşturmaktadır. Sadece bu yapıdaki zararlı yazılımlar dahi deniz taşımacılığını ekonomik olarak çökertebilecek bir risk teşkil etmektedir.

Gemiler, özellikle korsan bölgelerinde gerçekleştirilebilecek, GPS ve AIS spoofing gibi yöntemler vasıtasıyla, rotasından saptırılarak, kötü amaçlı kişilerin eline geçmesine sebep olabilecek gelişmiş siber saldırılara maruz kalma tehlikesiyle karşı karşıyadır. Son yıllarda bu konuyla ilgili, güvenlik yazılımcıları çeşitli çalışmalar yapmaktadır. Gemi mürettebatının siber güvenlik farkındalığına sahip olmaması geminin siber güvenliği açısından büyük risk taşımaktadır

Çalışmada Türkiye'de ve Dünya'da deniz taşımacılığına yönelik siber saldırılar ve sonuçları irdelenmiştir. Deniz taşımacılığı paydaşlarının, siber tehditler karşısında izlemesi gereken güvenlik önlemleri konusunda önerilerde bulunulmuştur.

Anahtar Sözcükler: Bilgi Teknolojileri, Deniz Taşımacılığında Güvenlik, Endüstri 4.0, Siber Güvenlik.

1. GİRİŞ

Denizcilik, insanlığın medeniyetle buluştuğu ilk yıllardan beri dünya ticaretinin en önemli öğesi olmuştur. Sadece ticarette değil, aynı zamanda yeni kıtaların keşfedilmesi ve kolonileşme gibi süreçler içerisinde de büyük bir önem arz etmiştir. Günümüzde, ekonomik savaşın önemli bir boyutu haline gelen denizcilik, dünya ticaretinin şekillenmesinde büyük rol oynamaktadır. Son yıllarda bilgi ve iletişim teknolojilerinin, denizcilik ile buluşması sayesinde çok daha hızlı deniz-kara iletişimi gerçekleşebilmektedir. Böylelikle gemi-ofis arasındaki iletişimin hızlanması, şirket içi yönetimin daha verimli ve kazançlı bir hale gelmesini sağlanmıştır. Liman teknolojilerinin gelişimiyle birlikte gemilerin yükleme ve tahliyeleri hızlanmış, doğal sonucu olarak, deniz taşımacılığı da hızlanmıştır. Bu durum az zamanda daha fazla taşımanın gerçekleşmesine olanak sağlamıştır.

Bilgi teknolojileri insan hayatını kolaylaştırmasına karşın kötü amaçlı kişiler tarafından kullanılması ile haksız kazanç yolu olarak görülmektedir. Bu kişiler kişisel bilgisayarlardan, kurumsal firmaların, hatta devlete ait web sitelerin bilgi havuzlarını ciddi tehdit altında bırakmaktadırlar. Son yıllarda özellikle devlete ait sitelerin ele geçirilmesi veya bütünlüğünün değiştirilmesi, elde edilen gizli belgelerin sızdırılması bu korsanlığı gerçekleştirenler için prestij kazanımı gibi görülürken, devletler tarafından ciddi tehdit oluşturmaktadır.

Siber saldırılar ile ilgili ulusal ve uluslararası hukuki yaptırımlar caydırıcılığın sağlanması açısından halen büyük bir sorundur. Özellikle e-ticaretin yaygınlaştığı, insanların evlerinden internet sayesinde kolayca alışveriş yaptığı günümüzde siber korsanlık modern hırsızlık haline gelmiştir.

Günümüzde geniş bant yayın teknolojilerinin gelişimi ve "Big Data" gibi öğelerin önem kazanmasının ardından, denizcilik sektörü siber saldırılara daha fazla maruz kalmaya başlamıştır. Mevcut teknolojiler ve farkındalık seviyesiyle, gerek gemi personelinin gerekse de kara personelinin siber saldırılara karşı çaresiz kalması muhtemeldir. Gemilerde seyir cihazı olarak kullanılan AIS (Automatic Identification System), GNSS (Global Navigation Satellite System) ve ECDIS (Electronic Chart Display and Information System) gibi teknolojiler vardiya zabitleri için büyük bir kolaylık sağlamaktadır. Ancak köprüüstü cihazlarının da siber saldırıların gerçekleştirilmesi ile gemi dışı müdahale ile, kaptan ve zabitleri yanıltabilmesi günümüz şartlarında mümkündür. Gemiye yönelik siber saldırılar, geminin rotasından sapmasına varacak kadar önemli etkilere sahiptir.

1.1. Literatür Özeti

Bilgi teknolojilerindeki hızlı gelişmeler ve siber güvenliğin son yıllarda önemli bir risk haline gelmesi bu yönde bilimsel çalışmaların artmasına neden olmuştur. Bilgi teknolojileri ve siber güvenlik konuları ulusal ve uluslararası literatürde yer almıştır. Özenç çalışmasında kişisel ve kurumsal bilgi güvenliğinin sağlanması kapsamında uluslararası karşılaştırmalar yapmıştır. Bilgi teknolojilerini stratejik sektör olarak tanımlamıştır (Özenç, 2007:183-190).

Baykara. vd. yaptıkları çalışmada bilgi güvenliği için kullanılan araçları incelemişler, son yıllarda artan siber saldırılara dikkat çekilmişler, bilgi güvenliğini gizlilik, erişilebilirlik ve bütünlük olarak üç ana unsurdan oluştuğunu vurgulamışlardır (Baykara, vd, 2013:231-239).

Şentürk. vd. siber saldırı sonucu ortaya çıkan sorunlara karşı uluslararası hukuk kurallarını incelemişlerdir. Siber hukukun yaptırımları ve ülkelerin siber savaşları beşinci bir boyut içerisinde değerlendirdiğine vurgu yapılmıştır (Şentürk, vd, 2013:46-52). Yılmaz. vd., siber güvenlik konusunda risklere dikkat çekmiş hazırlık seviyelerini; siber vandalizm, siber hırsızlık, siber gözetleme, siber casusluk, siber savaş gibi beş temel başlıkta toplamış ve saldırgan tipi, hedef ve amacına göre yöntemlerinin farklılık gösterdiğini vurgulamışlardır (Yılmaz, vd, 2013:158-166).

Hekim ve Başıbüyük Türkiye'nin siber güvenlik politikalarını incelemiş son beş yılda toplam 2000-4000 civarı interaktif dolandırıcılık vakasını vurgulamış risklerin arttığını belirtmiştir (Hekim, Başıbüyük, 2013:135-158).

Göztepe. vd., siber saldırılara karşı ulusal siber güvenlik ajansı organizasyonu tasarımı önerisinde bulunmuşlardır (Göztepe, vd, 2014:1-24). Yılmaz. vd., bilgi toplumuna geçişi siber güvenlik kapsamında incelemişlerdir. Türkiye'nin bilgi toplumu stratejisi konusunda mevcut durumunu değerlendirerek ulusal güvenlik konusunda önerilerde bulunmuşlardır (Yılmaz, vd, 2015:133-146).

1.2. Çalışmanın Amacı ve Kısıtları

Son yıllarda bilgi teknolojilerindeki gelişmelerle beraber siber suç olarak adlandırılan kanunsuz eylemlerinde artmasına neden olmuştur. Kanunsuz bu eylemler tüm sektörleri etkilediği gibi denizcilik sektörünü de etkilemiştir. Her sektörü farklı derecede etkileyen siber suçlara karşı denizcilik sektörünün hangi yollarla, ne şekilde etkilendiği araştırılmış, alınabilecek önlemlere değinilerek sektöre yönelik ileride yapılacak çalışmalara temel teşkil etmesi hedeflenmiştir.

Yapılacak çalışmalarda denizcilik sektörünün armatörlük, liman, acentecilik gibi farklı dinamiklerine yönelik olarak durumsal farkındalık ile mevcut durumuna yönelik detaylı kanitatif ve kalitatif çalışmalara yer

verilmesi gerekmektedir. Bu sayede farklı ölçüde maduriyetlerin en aza indirilmesi sağlanacaktır.

Siber korsanlık faaliyetlerinin son yıllarda artmasına rağmen şirketlerin prestij kaybına uğrama korkusuyla saldırılardan ne derece zarar gördüklerini açıklamaktan kaçınmaları çalışmadaki en önemli kısıtlardan biridir. Çalışmada kurumsal firmaların yaşadıkları vakalar, ikinci kaynaklardan elde edilen bilgiler ve olası saldırılar denizcilik sektörüne yönelik tehditler açısından incelenmiştir.

2. BİLGİ GÜVENLİĞİ VE SİBER SALDIRILAR

Siber tehditler bilgi teknolojilerinin açıklarından yararlanılarak elde edilmiş yasal olmayan aktivitelerdir. Boyutu verdiği zarar ile ölçülen bu faaliyetler kimi zaman dolandırıcılık gibi basit amaçlara hizmet etse de kimi zaman devletlerin kurumsal yapısını hedef alabilmektedir.

2.1. Bilgi Güvenliği Kavramı

Bilgi güvenliği çoğu zaman bilgileri edinmeye yetkili olmayan kişiler tarafından izinsiz olarak kullanılmak, bozulmak, silinmek veya değiştirilme riskine karşı oluşturulması beklenen tedbirler bütünüdür. 1980'li yıllar ile yaygınlaşan TCP/IP ile beraber bilgisayar ile iletişim yaygınlaşmıştır (Baykara, vd, 2013:231-239).

Son kırk yılda siber saldırılar önemli bir gelişim göstermiş, farklı alanlara yönelik farklı şekilde gerçekleşebilir hale gelmiştir. Kimi zaman kişisel maile gelen bir elektronik posta, kimi zaman elektronik veri depo aygıtları, kimi zaman daha karmaşık ve şüphe çekmeyen yöntemler ile gerçekleşmektedir. (Canbek, ve Sağıroğlu, 2007:1-12).

Bilgi güvenliği, bir başka deyişle kurumsal bilgi teknolojilerine erişilebilirlik, bütünlük, gizlilik konularında risklerin azaltılarak ortadan kaldırılmasını amaçlamaktadır (Solms, 2006:166-167).

2.1. Siber Suç Kavramı

Bilgi teknolojilerindeki gelişmeler ve yasa dışı oluşumlar siber suç kavramını beraberinde getirmiştir. Türkçede tam karşılığı bulunmayan siber kelimesi bilgisayar yapısı ve ona bağlı olan interaktif bağlantıları tanımlamada kullanılmaktadır. Siber kelimesinin sonuna gelen güvenlik,

alan gibi kelimelerle soyut kavramlar tanımlanmaktadır (Klimburg, 2012).

Siber suç beraberinde güvenlik ihtiyacını getirmektedir. Sanal güvenliğin sağlanması için gizliliğin, bütünlüğün ve erişilebilirliğin tam anlamıyla hakim olunması gerekmektedir. Bu üç kavramın sağlanması siber güvenliğin sağlanması demektir (Goodrich ve Tamassio, 2010).

3. HARBİN BEŞİNCİ BOYUTU VE SİBER SAVAŞ ÖĞELERİ

Harbin kara, deniz, hava ve uzaydan sonra beşinci boyutu olarak adlandırılan siber uzay, sadece bilgi paylaşımının yapıldığı bir alan olmaktan çıkıp, konvensiyonel savaşlarla paralel olarak operasyonların düzenlendiği ve hatta tamamen bağımsız olarak savaşların yapıldığı bir alan haline gelmiştir. İsrail Eski Başbakanı Benjamin Netanyahu'nun Siber Güvenlik danışmanı Itzhak Ben-Israel, "Siber Savaşlar konvansiyonel savaşlardaki gibi bir etki verebilecek türdedir. Bir ülkeyi vurmak istiyorsanız, o ülkenin enerji ve su kaynaklarına karşı siber saldırılar düzenlemek gerekmektedir. Siber teknoloji bunu tek mermi kullanmadan yapabilme yeteneğine sahiptir." demektedir (Israel, Röportaj, The Times of Israel 2012).

Günümüzde "toprak", iş gücü" ve "sermaye" gibi üretim faktörlerinden daha değerli olarak "bilgi" ortaya çıkmıştır. Dünya üzerindeki emek-yoğun, sermaye-yoğun ya da enerji-yoğun üretim faktör etkisi bilgi-yoğun faktör etkisinin daha fazla önem kazanması şekline dönüşmektedir. Günümüzde hemen hemen tüm işlemler elektronik ortamda yapılabilmektedir. 2010 yılında 206,956,723 adet web sayfası yayındayken, 2017 yılı rakamlarına göre internet üzerinde 1,767,964,429 adet web sayfası bulunmaktadır (NetCraft, 2017). Bu veriler internet üzerinden hizmet sağlayıcıların sayısının yanı sıra kullanıcılarında yıldan yıla öngörülerin çok üzerinde katlanarak arttığını göstermektedir.

Bilgisayar ve iletişim teknolojilerinin sağladığı imkan ve kolaylıklardan daha çok siber suçlar, siber saldırılar ve hatta siber savaş konuşulur olmuş, bunların sonucunda da bilgi ve iletişim sistemlerinin ve yapılarının siber saldırılara karşı korunmasının, yani siber güvenliğin sağlanmasının yolları aranır olmuştur (Şenol, 2016:10-17).

Siber uzay, ABD Savunma Bakanlığı'nın 2010 yılında yaptığı tanıma göre "İnternet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve kontrol birimlerini içeren, birbirine karşılıklı olarak bağımlı olan, bilgi teknolojileri altyapıları tarafından oluşturulan küresel alandır" (ABD Savunma Bakanlığı, 2017).

NATO'nun siber güvenlik terimleri sözlüğünde yer alan, Uluslararası Standartlar Teşkilatı'nın yapmış olduğu tanımda ise "İnsanların, yazılım ve servislerin cihaz ve ağlar üzerinden birbirleriyle etkileşimde bulunduğu, fiziksel bir formda olmayan kompleks ortamdır." ifadesi yer almaktadır (NATO CCDCOE, 2012).

NATO'nun tanımında dikkat edilecek husus; insanlara da yer verilmiş olmasıdır. Bir başka deyişle, siber uzay tamamen bilgisayar sistemlerinden değil, aynı zamanda bunları yöneten insanlardan da oluşmaktadır. Siber uzay, görüldüğü üzere sadece internet ve buna bağlı cihazlardan meydana gelmemektedir. İletişim ağları, bilgi sistem teknolojilerini kullanan personel, askeri ağlar, enerji dağıtım ağları, cep telefonları, IoT cihazlar, elektronik komuta sistemleri, uydu sistemleri, insansız hava araçları, telsizler, SCADA (Supervisory Control And Data Acquisition) sistemler hep birlikte siber uzayın öğeleri arasında yer almaktadır.

Siber Savaş, bir devletin başka bir devlete ait siber uzayda yer alan varlıklarına zarar vermek, manipüle etmek, çıkarları çerçevesinde kullanmak, kesinti yaratmak, tamamen hizmet veremez duruma getirmek üzere gerçekleştirilen saldırı faaliyetlerinin tümüdür. Siber savaşta çok fazla sayıda yöntem kullanarak, hedefe kimi durumda fiziksel hasar dahi verilebilmektedir (Keleştemur, 2015:120-133).

2010 yılı ve öncesinde siber saldırılar genellikle hacking, spam e-posta gönderme, web sitesinin içeriğini değiştirme ya da servis dışı bırakma şeklinde gerçekleşirken, sonraki yıllarda ortaya çıkan APT saldırıları ile birlikte çok daha karmaşık ve büyük hasarlar verebilecek bir hale gelmiştir. Bu saldırı yöntemleriyle birlikte siber savaş dışında siber casusluk, siber istihbarat, siber terör ve siber sabotaj faaliyetleri de ortaya çıkmıştır.

Latince "terrere" kelimesinden türetilmiş olan ve "korkutmak" anlamına gelen terörün, günümüzde hukuki ve politik olarak tarifini yapmak,

devletlerin kendi çıkarlarına göre terör unsurlarını kullanmasından dolayı oldukça zor bir hal almaktadır. Ancak bilimsel olarak terörün tanımını kısaca "hukuk dışı güç kullanarak, amaca ulaşma eylemidir" şeklinde yapmak mümkündür (Çakmak, 2008: 29-30).

Terörizm "genellikle kanundışı siyasi gruplar tarafından güvensiz bir ortam yaratma, bir rejimi zayıflatma bir baskı sistemini başarısızlığa uğratma amacıyla gerçekleştirilen şiddet eylemleridir" (Winock, 2001:76). Siber terörizm ise siber uzay üzerinden, bilgisayar ağlarını ya da ağlara bağlı cihazları kullanılamaz hale getirmeye yönelik, terör maksatlı gerçekleştirilen faaliyetlerdir.

4.DENİZCİLİK SEKTÖRÜNDE SİBER SALDIRININ ETKİLERİ

Denizcilik sektöründe siber saldırılar farklı amaç ve boyutta gerçekleşmektedir. Kimi zaman bir gemiyi, kimi zaman bir denizcilik işletmesini kimi zaman ise bir limanı hedef alabilmektedir.

Gelişmiş siber saldırılar, gemileri rotalarından çıkararak, korsanların olduğu bölgeye yönlendirilebilmektedir. Bu tehlikeli durum farkına varılsa dahi son teknoloji ile donatılmış bir geminin güverte ve makine bileşenlerinin otomasyon sistemleri ile donatılması nedeniyle gemi personeli tarafından müdahale edilemeyebilir. Bu durum maddi zararın yanında insanların hayatını tehlikeye atabilecek seviyededir. Özellikle insansız gemi denemelerinin 2020 yılından itibaren yoğun şekilde deneneceği düşünüldüğünde bilgi teknolojilerinin kullanıldığı gemilerde siber faaliyetlerin daha fazla olacaktır.

Siber saldırılar sadece seyir cihazlarına karşı değil, denizcilik sektörü içinde yer alan diğer paydaşlara karşı da yapılabilmektedir. Yük manifestoları üzerinde değişiklik yapılarak, konteyner içinde taşınan uyuşturucu ve silah gibi yasadışı yüklerin, sıradan ve tehlikesiz bir yükmüş gibi gösterilmesi yine siber saldırılar sayesinde mümkündür. Antwerp Limanı'nda yaşanan yükün kaçırılması ve izinin silinmesi için liman sistemlerinin hacklenerek, yük bilgilerinin disklerden silinmesi hadisesi de oldukça önemli bir örnek teşkil etmektedir. Saldırganların kullandığı yöntemlerin başarısı sebebiyle olay 2011 yılında yaşanmasına rağmen, fark edilmesi bir yıl sürmüş ve 2013 yılında olay medyaya

yansımıştır. Saldırganların yaklaşık bir yıl boyunca kendilerini belli etmeden sisteme sızdıkları ortaya çıkmıştır (Hutchins, International Shipping and Logistics News 2015).

Yük sahibi ve taşıyıcı arasında gerçekleştirilen para akışının da gerek penetre edilerek gerekse de oltalama saldırıları ile üçüncü kişiler tarafından ele geçirildiği de görülmektedir. Tüm bu yaşanan gelişmeler, denizcilik sektörünü olumsuz etkilemekte, dünya genelinde büyük bir ekonomik kayba sebep olmaktadır. Son yılların yoğun saldırılarından siber fidyecilik de yine denizcilik sektörünü yakından ilgilendiren öğelerden biridir. Daha önce Cryptolocker, WannaCry ve Petya gibi dünya genelinde milyonlarca cihazı hedef alan fidye yazılımlar, denizcilik sektörünün hedef alınması halinde, dünya deniz ticareti ekonomisini büyük bir hızla vurabilecek güce sahiptir. Son dönemin en popüler fidye yazılımı WannaCry, dünya genelinde 4 milyar usd'ye yakın bir zarara sebep olmuştur (Berr, 2017).

Özellikle konteyner taşımacılığında zaman kavramının önemli oluşu, siber saldırıların neden olduğu duraksamaların ekonomik zararını arttırmaktadır. 27 Haziran 2017'de gerçekleşen ve denizcilik sektörünü olumsuz etkileyen siber saldırı sonucunda 200 ile 300 milyon Usd'lik bir zararın oluştuğu tahmin edilmektedir (CNBC, 2017).

Endüsrti 4.0 ile beraber liman teknolojileri ve otomaston sistemlerinin bilgi teknolojileri kapsamında gelişmesi beklenmektedir. İşlemlerin ileri teknoloji içeren ekipmanlar ile gerçekleştirilmesi sektörün siber saldırılardan daha fazla etkilenmesine neden olacaktır. Bu nedenle siber koruma önlemlerinin endüstri 4.0 ile gerçekleştirilmesi bir ihtiyaç olarak gözükmektedir.

Denizcilik sektörünün siber güvenlik konusunda yeterli yatırımın yapmadığı göz önüne alındığında, benzer saldırıların denizcilik firmalarına da milyonlarca dolar kayıp yaşatabileceği öngörülmektedir.

5. DENİZ TAŞIMACILIĞINI TEHDİT EDEN SİBER SALDIRI YÖNTEMLERİ

Siber saldırılar eskiden, kendini göstermek ya da para motifi karşılığında bir sistemin hackerlar tarafından ele geçirilmesi ya da kullanılamaz hale getirilmesine yönelik faaliyetler olarak ifade edilmekteyken, bugün

hacktivist gruplar, terör örgütleri ve hatta devletler tarafından gerçekleştirilen ve tesiri oldukça büyük faaliyetler bütünü haline gelmiştir. Böylesine büyük bir alanda gerçekleştirilen saldırılar da gelişen güvenlik teknolojilerini geçebilmek için farklılık göstermekte ve evrimleşmektedir.

Gelişmiş Kalıcı Tehdit ‘‘Advanced Persistant Threat (APT)’’ saldırıları sayesinde, hedefin haberi olmaksızın, arka planda bilgi elde etmek, tüm sistemi ele geçirmek, kullanılamaz hale getirmek ve hatta fiziksel tesir yaratmak mümkün olmaktadır. Ancak sadece APT saldırıları değil Gelişmiş Atlatma Teknikleri ‘‘Advanced Evasion Techniques (AET)’’olarak adlandırılan saldırı yöntemlerine karşılık verebilmek için aynı şekilde güvenlik sisteminin oluşturulması gerekmektedir. Siber saldırılar, siber uzayda çalışmakta olan yazılım, donanım ve altyapıları hedef almaktadır. Siber saldırıların amaçları, saldırı şekilleri ve etkileri farklılık göstermektedir.

Günümüzde sıklıkla kullanılan saldırılardan biri olan Dağıtık Servis Dışı Bırakma ‘‘Distributed Denial of Service (DDoS)’’ saldırılarıdır. Bu saldırıların amacı hedef sistemin belli bir süreliğine hizmet dışı bırakılmasını sağlamaktır. Diğer saldırı türlerine göre gerçekleştirilmesi kolaydır. DDoS saldırıları genellikle sistemin çalışması engellendiğinden, ekonomik kayıpların yaşanmasına sebep olmaktadır. Deniz taşımacılığında kullanılan sistemlere yapılacak DDoS saldırıları, bu sistemlere erişimi durduracak, bu da gemi trafiğinin yönetimini zorlaştıracak ve hatta kimi zaman yönetilemeyecek hale getirecektir. Şu an için bu gibi durumlar birer senaryodan ibaret olsa da bu sistemlerde gerekli siber güvenlik önlemlerinin alınmaması durumunda yaşanması muhtemel birer problemdir.

İnternete bağlanan gemi ve kara personelinin, bilinçsiz kullanımı sonucu ortaya çıkabilecek bir diğer önemli tehlike de oturum çalma saldırılarıdır. Oturum çalma, iki bilgisayar arasındaki oturumun, çeşitli yöntemlerle ele geçirilmesidir. Bu tehlike, özellikle limanlarda ofis bilgisayarını kullanarak internete giren zabitlerin, hatalı davranışları sebebiyle oluşabilmektedir. Oturum çalma saldırıları sayesinde hedef bilgisayara yetkisiz giriş yapılabilmektedir.

Zararlı yazılımlar, sistemde bulunan zafiyetler sonucu sızabileceği gibi, yine kullanıcının siber güvenlik farkındalığına sahip olmamasından dolayı, kullanıcı hatasını kullanarak da sızabilmektedir. Bu durum özellikle, gemi yük planı ve benzeri dosyaların, gemi ofis bilgisayarına yüklenmesi için takılan flashdisklerin, iyi bir güvenlik uygulaması tarafından taranmaması sonucu, tüm gemi ağına yayılması şeklinde yaşanabilmektedir. Etkilenen bilgisayarlar, gemi yükleme/tahliye, stabilite ve benzer yazılımların çalışmamasına, kara departmanı ile internet üzerinden iletişim kurulamamasına ve Voyage Data Recorder (VDR – Sefer Veri Kaydedici) gibi oldukça önemli cihazlarda hatalı verilerin oluşturulmasına kadar varabilmektedir.

Automatic Identification System (AIS – Otomatik Tanımlama Sistemi) gemilerin daha güvenli bir şekilde seyir yapmalarına yardımcı olmak amacıyla geliştirilmiş ve gemilerin izlenmesine olanak sağlayan bir sistemdir. Şu an siber saldırganların yeni gözdesi haline gelen AIS'in, gemilerde kullanımının zorunlu hale geldiği 2002 yılından bugüne 300.000'den fazla gemide kullanıldığı belirtilmektedir. Gemilerin çatışmalarını önlemeye yönelik geliştirilen AIS sayesinde internet üzerinden gemi trafiğini kontrol etmek ve arama kurtarma (SAR) operasyonlarını yönetmek daha kolay ve etkin bir hale gelmiştir.

Güvenlik firması Trend Micro, konuyla ilgili bir çalışma hazırlamış ve AIS cihazlarının, dışarıdan müdahale edilerek kolayca aldatmacaya maruz kalabildiğini sergilemiştir. Yapılan araştırmalar, AIS cihazına yazılımsal müdahale yapılabileceği gibi RF sinyalleri üzerinden de erişilerek, yanıltılabildiğini göstermektedir. Dışarıdan müdahale ile Closest Point of Approach (CPA – En Yakın Yaklaşma Noktası) yanıltma yaparak, zabit ya da kaptanın hatalı manevra yapmasına, dolayısıyla da çatışmaya sebep olabilmektedir. AIS spoofing sebebiyle arama kurtarma operasyonu sırasında geminin mevkiini bulmaya çalışan operasyon ekibi yine hatalı veriler sebebiyle yanıltılabilmektedir (Balduzzi ve Wilhoit, 2014).

Gemilerde kullanılan GPS'ler, RADAR, AIS, VDR gibi diğer pek çok cihaza konum ve hız bilgisi gibi veriler göndermektedir. Bu verilerin manipüle edilebildiği de yine daha önce yapılan araştırmalar sonucu ortaya çıkmıştır. Dahası, GPS'e dışarıdan müdahale ile gemiler rotasından çıkarılabilmektedir. Teksas Üniversitesi tarafından yapılan

araştırmaya göre, 80 milyon dolarlık özel bir yat üzerinde yaptıkları çalışmalar sonucunda, GPS spoofing yöntemi ile yatı rotasından çıkarabilmiş, dışarıdan istedikleri gibi manevra yapmasını sağlayabilmişlerdir. (Teksas Üniversitesi, 2013).

5.1. Siber Saldırı Türleri

Ağ yapılandırmada ya da uygulamalarda kullanıcıların kişisel ve kurumsal düzeyde günün teknolojisine uygun güvenlik önlemlerinin alınması gerekmektedir. Önlemlerin alınmaması kişi veya kurumların veri kaybı ile beraber maddi ya da manevi boyutta kayıpların yaşamasına neden olacaktır. Gerekli güvenlik önlemlerini almak için saldırı çeşitlerini ve nasıl yapıldıklarını bilmek avantaj sağlamaktadır.

Siber saldırılar genel olarak şu süreçleri izlemektedir:

- Bilgi Toplama (Reconnaissance)
- Tarama (Scanning)
- Erişim ve Yetki Yükseltme (Access and Escalation)
- Erişimi Sürdürme (Maintaining Access)
- İzleri Silme (Covering Tracks)

Bu sürecin birinci aşamasındaki bilgi toplama, saldırıların en önemli öğesidir. Dolayısıyla gerek teknik olarak gerekse de çalışanların ketumiyeti gibi konulara eğilmek suretiyle, saldırganlara mümkün olduğunca az bilgi alacak şekilde tedbir alınması gerekmektedir.

Siber saldırı türlerinin en önemli olanları aşağıda yer almaktadır. Bu saldırı yöntemlerinin büyük bir kısmı deniz taşımacılığı içinde yer alan sistemleri de kolaylıkla etkileyebilmektedir. Aşağıda yer alan yöntemler alfabetik sıraya göre listelenmiştir:

- Arka kapı
- Açık mikrofon dinleme
- GSM / VoIP vb. dinleme
- Ağ dinleme
- Ağ tarama ve haritalama
- Hizmet dışı bırakma
- IP aldatmacası

- DNS aldatmacası
- İnternet servis saldırıları
- Kabloya saplama yapma
- Kriptografik saldırılar
- Oturum çalma
- Sosyal mühendislik
- Trafik analizi
- Yemleme
- Yerine geçme
- Yığın e-posta gönderme
- Zamanlama saldırıları
- Zararlı yazılım gönderme

Temel siber güvenlik önlemlerinin alınabilmesi için gerekli olan çeşitli donanımlar, yazılımlar ve protokoller bulunmaktadır. Bugün, her ne kadar gelişmiş ve NG Firewall ya da UTM olarak adlandırılan, komplike güvenlik işlemlerini bir arada yapabilen güvenlik duvarları bulunsa da, bu sistemlerin aşılması mümkün olmaktadır. Diğer taraftan güvenli soket katmanı, taşıma katmanı güvenliği gibi protokoller de zaman zaman çıkan açıkların exploit edilmesiyle kırılabilmektedir (Eyüpoğlu, vd, 2017:177-184).

Tuzak kapı olarak da bilinen ve İngilizce'de backdoor ya da trapdoor terimleri ile ifade edilen saldırı yöntemi sayesinde, hedef sisteme yüklenen bir yazılım ile siber saldırı gerçekleşmektedir. Doğrudan işletim sisteminin kendisinde bulunan bir açık ya da sistemde çalışmakta olan bir yazılımda bırakılan açık kapı vasıtasıyla, kimlik doğrulama mekanizması aşılarak sisteme gizli ve yetkisiz erişim sağlanabilmektedir. Arka kapılar, limanlarda ve gemilerde flashdisk aracılığıyla uygulama, dosya paylaşımı sırasında otomatik olarak çalışacak bir yazılım sayesinde sistemde oluşturulabilmektedir. Bu noktadan sonra hedefin kontrolü tamamen siber saldırıların eline geçebilmektedir. Hedef sisteme sızan saldırganlar, liman ya da gemideki tüm sistem ya da dosyalara erişebileceği gibi, seyir cihazları üzerinde de çeşitli kontrolleri ele geçirebilecek yetkiye sahip olabilmektedir.

Hizmet Dışı Bırakma (Denial of Service – DoS) hedef sistemin işleyişini engellemeye yönelik bir saldırı türüdür. Bu saldırıların daha etkili olabilmesi için Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service – DDoS) saldırıları yapılmaktadır. Bu saldırılar kullanılarak

sunucunun çalışması kısmen ya da tamamen engellenebilmektedir. DDoS saldırılarının çalışma prensibi büyük oranda veri paketlerinin sunucuya gönderilmesi üzerinedir. Hedef sisteme gönderilen karmaşık paketler, sunucudan yanıt beklemektedir. Sunucu, gönderilen paketlerin işlemci, bellek ve bant genişliği gibi sistem kaynaklarının tüketmesinden ötürü çalışamaz hale gelmektedir.

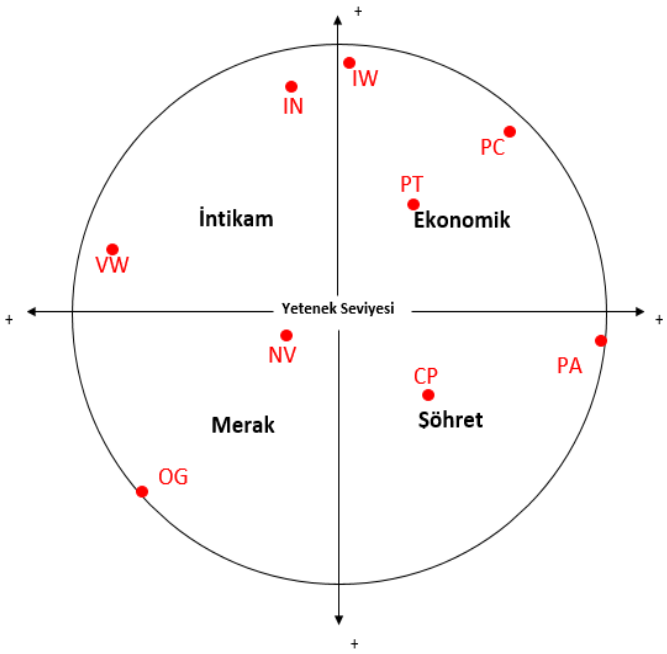
DDoS'un temel olarak DoS'tan en önemli farkı, saldırının birden fazla noktadan tek bir merkeze yapılmasıdır. Bu saldırı türünde saldırılar yüzlerce, hatta binlerce makineden tek bir hedefe yönelik olabilmektedir. Saldırgan, daha önceden ele geçirilmiş cihazları kullanarak saldırıları gerçekleştirmektedir. DDoS saldırısı için kullanılmakta olan zombi bilgisayar topluluklarına Botnet adı verilmektedir. Çeşitli durumlarda bilgisayarlar, sahibinin rızasıyla DDoS saldırısı elemanı haline gelebilmektedir. WikiLeaks destekçileri tarafından büyük kredi kartı şirketleri aleyhine 2010 yılında düzenlenen DDoS saldırıları buna iyi bir örnek teşkil etmektedir (The Guardian, 2010).

Hizmet dışı bırakma saldırıları dışında, daha tehlikeli sonuçlar doğruabilecek Sürekli Hizmet Dışı Bırakma (Permanent Denial of Service – PDoS) saldırıları da bulunmaktadır. Bu saldırıların neticesinde, hedefteki donanımın değiştirilmesi ya da yeniden kurulması gerekmektedir. PDoS saldırıları sayesinde çalışmakta olan uygulama ve servisler yerine router, printer ya da ağdaki herhangi bir donanım hedef alınabilmektedir. Temel olarak amaç, donanımın firmware'ini değiştirmek, bozmak ve silmektir. PDoS saldırıları, donanımın yönetimsel arayüzüne erişmeyi sağlayan güvenlik açıkları üzerine kurulmuştur. Gemideki cihazların, bu saldırıların hedefi haline gelmesi durumunda çalışamaz hale gelmeleri kaçınılmazdır. Bu durum seyir emniyeti açısından büyük bir risk oluşturabilmektedir.

Siber silah olarak da nitelendirilen zararlı yazılımlar sayesinde gelişmiş saldırılar düzenlemek mümkündür. Sisteme virüs, bakteri, solucan, truva atı gibi zararlı yazılımlar yükleyerek, çok daha basit bir şekilde bilgi hırsızlığı yapılabilmektedir. Ayrıca sistemi tamamen kullanılamaz hale getirmek gibi büyük çaplı hasarlar da verilebilmektedir.

5.2. Siber Saldırgan Profili

Saldırganların motivasyonuna göre; intikam, ekonomik, merak ve şöhret olmak üzere 4 farklı tür belirlenmiştir. Şekil 1'de merkezden uzağa gidildikçe saldırganın teknik kabiliyeti artmakta ve dairenin her bir çemberi bir motivasyon kategorisini göstermektedir. (Irmak ve Erkek, 2016:10-15). Şekil 1'de yer alan saldırgan tanımlamaları aşağıdaki gibi ifade edilebilir:



Şekil 1: Saldırganların Gelişiminde 2 Boyutlu Çember Modeli

- Acemi: NV (Novice)
- Siber-acemi: CP (Cyber-punks)
- Kurum içi Çalışan: IN (Internal)
- Acemi Hırsız: PT (Petty Thieves)
- Virüs Yazılımcısı: VW (Virus Writers)
- Eski Kafalı Hacker: OG (Old Guard Hacker)
- Profesyonel Suçlu: PC (Professional Criminals)
- Bilgi Savaşçıları: IW (Information Warriors)

Siber saldırganların en güçlü yanı aslında teknik bilgilerinden ziyade, zekalarını ve iletişim becerilerini etkin bir şekilde kullanabilmeleridir. Hiçbir teknik bilgisi olmadan hedef sisteme sızmayı başarmış birçok

hacker bulunmaktadır. İyi bir saldırgan, insan psikolojisini ve kurum yapısını çözümleyebilmelidir. Sadece bu yeteneği ile bir kurumun içine sızmak mümkün olabilmektedir. İnsanlar arasındaki iletişimdeki açıklardan faydalanarak ikna etme, etkileme, aldatma gibi öğelerin kullanılması ile güvenlik süreçlerini atlatma ve sıradan kullanıcı yetkileriyle hedef sistem hakkında elde edilemeyecek bilgilerin ele geçirilmesine sosyal mühendislik denilmektedir (Keleştemur, 2015;55-60).

Siber saldırıların büyük bir kısmı, personelin siber güvenlik farkındalığına sahip olmamasından kaynaklanmaktadır. Gerekli güvenlik önlemlerinin alınmamasına ek olarak, insan siber güvenlik açısından belki de en büyük öneme sahip faktördür. İnsan faktörü kullanılarak gerçekleştirilen bir diğer önemli saldırı tipi de sosyal mühendisliktir.

Sosyal mühendislik aracılığıyla hedefteki kişiyi kandırmayı başaran bir saldırgan, sistemle ilgili tüm yetkiye sahip olabilmektedir. Yapılacak saldırı neticesinde sadece kuruma ait verilere değil, kurumla iş yapan tedarikçiler, çözüm ortakları, müşteriler vb. de etkilenebilmektedir. Klasik güvenlik donanım ve yazılımlarının, bu saldırı yönetimine karşı koruma sağlaması bugünkü teknolojiler ile pek mümkün değildir.

6. SİBER SALDIRILARA KARŞI ALINAN ÖNLEMLER

Eskiden sadece virüs gönderme ve DDoS gibi yöntemler üzerine kurulu siber saldırılar, bugün sayıca çok daha fazla, çok daha etkin yöntemler ile gerçekleştirilmektedir. Gelişmiş parola saldırıları sayesinde, gemilerde kullanılan sefer planı, yükleme planı, mürettebat yönetim sistemi gibi birçok yazılıma erişmek mümkün olmaktadır. Aynı şekilde deniz sektöründe yer alan firmaların kara departmanlarındaki sistemlerin de gelişmiş parola saldırıları ile ele geçirilmesi mümkündür.

Kara departmanlarında görevli personeli tehdit edebilecek bir diğer önemli saldırı türü de Ortadaki Adam (MITM – Man in the Middle) yöntemidir. Bu yöntemde, bir ağ üzerinde kurban bilgisayar ile diğer ağ araçları (yönlendirici, modem, switch ya da sunucu gibi) arasına girerek verileri yakalama ve görebilme imkanı sağlanmaktadır. Bu saldırıya karşı gelebilmek için HTTPS protokolünün kullanılması gerekmektedir. SSL (Secure Socket Layer) sayesinde veri şifrelenecek, böylelikle verinin ele geçirilmesi halinde anahtarlar bilinmediğinden, saldırganın faaliyeti

başarısızlıkla sonuçlanacaktır. Ancak son zamanlarda HTTPS bağlantılarına karşı da gelişmiş MITM saldırıları yapıldığı görülmektedir.

Şirket ağlarını tehdit edebilecek bir başka saldırı türü de Drive-by Downloads yöntemidir. Firmalarda özellikle ISO 27001 standartlarına uygun bir bilgi güvenliği yönetim sisteminin uygulanmaması halinde, kullanıcıların kişisel cihazları ile aynı ağ üzerinden internete bağlanmaları büyük sorunlara yol açabilmektedir. Drive-by Downloads saldırı yönteminde kullanıcı, belli bir linke yönlendirilerek, buradaki zararlı yazılımın sisteme indirilmesi ve kullanıcının bu yazılımı çalıştırması sağlanır. Yazılımın içine gömülmüş olan zararlı kodlar da sistem içerisinde büyük açıklara sebep olabilmektedir. Bu yazılımlar kimi zaman ana sunucuya veya yönlendirici gibi cihazlara dahi bulaşabilmektedir. Böyle durumlarda sistemin eski haline döndürülmesi oldukça zahmetli ve zaman alan bir işlem olduğundan, iş akışı da olumsuz etkilenmektedir.

Web yazılım güvenliği ise ele alınması gereken bir başka konudur. Zira bugün artık hemen her işlem web teknolojileri üzerinden gerçekleştirilmektedir. Şirketlerin sadece internet üzerinden yayınlanan web siteleri değil, aynı zamanda yerel ağları üzerinden çalışan çeşitli portal ve benzeri web uygulamaları da SQL Injection, Cross-Site Scripting (XSS) ve Cross-Site Request Forgery (CSRF) saldırılarından etkilenebilmektedir. Bu saldırılardan korunmak için web uygulamalarının güvenli kod yazımı ilkelerine göre kodlanması gerekmektedir. Mevcut yazılımlarda ise güvenli kod denetimi uygulanmalıdır. Güvenli kod denetimi, bir yazılımdaki güvenlik problemlerinin tespit edilmesi için uygulanan analizdir. Bu analizin elle yapılması halinde Kod Gözden Geçirme işlemi gerçekleştirilmektedir. Analizin, çeşitli uygulamalarla otomatik olarak yapılması ise Statik Kaynak Kod Analizi olarak adlandırılmaktadır (Demir, 2015: 9).

Bu süreçler dışında ayrıca web uygulamalarına da penetrasyon testleri uygulanmalıdır. Penetrasyon testleri ise çalışan uygulamalar üzerinde dinamik olarak yapılan güvenlik zafiyetlerini bulmak için gerçekleştirilen testlerdir.

Sosyal mühendislik aracı olarak kullanılabilecek önemli bir yöntem olan Yemleme sayesinde başta kredi kartı bilgileri olmak üzere birçok önemli

veri toplanabileceği gibi, satın alma departmanındaki yetkili kişilerin kandırılması sonucu, para transferinin yapılması da sağlanabilmektedir. Yemleme için genellikle orijinal banka siteleri, siteleri, açık artırma siteleri, sosyal ağ siteleri ve deniz taşımacılığında önemli olan tedarikçi vb. firmalara ait sitelerin benzerleri yapılmaktadır. Kurbanlar, bu sitelere yönlendirilerek, kişisel bilgilerinin ve çoğu zaman kredi kartı bilgilerinin girilmesi sağlanmaktadır. Son yıllarda piyasada bulunan güvenlik uygulamaları, yemlemeye karşı başarılı çözümler üretmektedir. Özellikle son kullanıcıları bu konuda uyaran, whitelist'te bulunmayan sitelere girişi engelleyen yazılımlar oldukça etkili olmaktadır.

Şirketler için büyük bir tehlike oluşturan, belki de en önemli konu ise Insider Threat, yani iç hulul tehlikesidir. Insider tehlikesi, kurum içinde çalışan kişilerin farklı motifler sebebiyle şirket bilgilerini dışarı sızdırmak, satmak ya da rakip firmalara sunmak gibi faaliyetler bütününe verilen isimdir. Bilgilerin, Insider tehlikesine karşı korunması için firmaların, mevcut verilerini bilgi güvenliği standartlarına göre tasnif etmesi gerekmektedir. Tasnif işleminin ardından, çeşitli yazılım uygulamaları ve eğitimlerle şirket içi eğitimler ve uygulamaları sağlanmalı, böylelikle herhangi bir sızdırma operasyonuna karşı bilgilerin maksimum seviyede korunması sağlanmalıdır.

Çalışmada yer alan siber tehditlere karşı güvenlik önlemlerinin alınabilmesi için gerekli yazılım, donanım ve diğer unsurların tesis edilmesi, doğru ayarların yapılması ve şirket güvenlik politikaları doğrultusunda bilgi güvenliğinin sürdürülmesi gerekmektedir. ISO 27001 standartlarına uyumlu şirketlerin, bilgi güvenliği konusunda çok daha başarılıdır. Bu standartlar doğrultusunda bilgi güvenliğini sağlamak ve siber güvenlik önlemlerini almak için siber güvenlik ile ilgili çalışmalar yapan firmalardan profesyonel destek almak ya da firma içinde ilgili bir birimlerin oluşturulması gerekmektedir.

7.SONUÇ VE ÖNERİLER

Çalışmada yer alan saldırıların dışında daha farklı siber saldırılar da bulunmaktadır. Tüm siber saldırı yöntemlerinin, oldukça hassas ve zafiyetlerle dolu, eski teknoloji ile donanmış deniz taşımacılığının hedef alınması durumunda, gerek deniz trafiğinin olumsuz etkilenmesi gerekse

de maddi kayıplar sebebiyle deniz ticaretini büyük ölçüde sekteye uğratması kaçınılmazdır.

Yapılacak saldırılar neticesinde sadece firmaya veya kuruma ait verilere değil, firmayla iş birliğinde olan limanlar, tedarikçiler, çözüm ortakları, müşteriler vb. hassas bilgiler de elde edilebilmektedir. Tek bir saldırı sonucunda bu firmaların sistemlerine de sızmak mümkün olmaktadır. Siber saldırıların gerçekleştiği deniz taşımacılığı yapan gemi, firma ya da kurumun yanında etkileşim içinde bulunduğu diğer firmaları da risk altına alabildiğinden karşılaşılan ticari zarar yelpazesi de genişlemektedir. Bu yönde alınacak önlemler:

- Saldırıya maruz kalabilecek şirketlerin karşılaşabilecekleri risklerin ve yaratacağı zararın boyutların hakkında farkındalıkların artırılması. Konuyla ilgili olarak risk analiz ve değerlendirmelerinin yapılması, güvenlik politikalarının oluşturulması,
- Çalışanların siber saldırılar ve bilgi güvenliği konusunda bilgilendirilmesi, çeşitli aralıklarla siber güvenlik farkındalığı konusunda eğitilmesi,
- Kullanılan sistemde bulunan zafiyetlerin ortaya çıkması için zafiyet taraması ve penetrasyon testleri gibi faaliyetlerin belirli zaman dilimlerinde yapılması,
- Siber güvenlik konusunda eğitim veren ve/veya faaliyetlerde bulunan firmalardan danışmanlık ya da diğer hizmetlerin profesyonel olarak alınması gerekmektedir.

Bilgi Teknolojileri sektörü farklı alanlara ayrılmış olup, siber güvenlik konusunda ihtisas sahibi olabilmek için çok fazla alanda uzmanlaşmış olmak gerekir. Bu uzmanlaşmanın, sıradan bilgi işlem çalışanlardan beklenmesi problemin belki de en büyük kaynağıdır. Bir başka deyişle, siber güvenlikle ilgili profesyonel kişi/kurumlardan hizmet alınması, konuyla ilgili gerekli yatırımların yapılması gerekmektedir.

Denizcilik sektöründe siber güvenlik konusuna yapılabilecek her türlü yatırım, siber saldırı sonrasında karşılaşılacak ekonomik kayıptan kat ve kat az olacaktır.

KAYNAKÇA

ABD Savunma Bakanlığı, (2017). http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf , Erişim Tarihi: 20.06.2017.

Balduzzi ve Wilhoit, (2017) *"A Security Evaluation of AIS"*. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf, Erişim Tarihi: 08.06.2017.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013). *"Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi".* 1st International Symposium on Digital Forensics and Security (ISDFS'13). 20-21 Mayıs 2013. Elazığ, Türkiye.

Berr, (2017), "CBS News". https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ , Erişim Tarihi: 20.06.2017.

Canbek, G. ve Sağıroğlu, Ş. (2007) "Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23:(1-2) 1 – 12.

CNBC News (2017). https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html, Erişim Tarihi: 05.10.2017.

Çakmak, H. (2008), *Terörizm*, Barış Platin Kitap, Ankara.

Demir, B. (2015), *Yazılım Güvenliği Saldırı ve Savunma,* Dikeyseksen, İstanbul.

Eyüpoğlu C., Aydin M.A., Sertbaş A., Zaim A.H., Öneş O. (2017) *"Büyük Veride Kişi Mahremiyetinin Korunması",* International Journal Of Informatics Technologies, 10:177-184.

Goodrich, M. ve Tamassio, R. (2010). *Introduction to computer security*. Addison-Wesley.

Göztepe, K., Kılıç, R. ve Kayaalp, A. (2014). *"Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey"*. Journal of Naval Science and Engineering. 10(1):1-24.

Hekim, H. ve Başıbüyük, O. (2013). *"Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları"*. Uluslararası Güvenlik ve Terörizm Dergisi. 4(2):135-158.

International Shipping and Logistics News (2017). https://www.joc.com/maritime-news/container-lines/carriers-threatened-cyber-attacks-experts-warn_20150303.html, Erişim Tarihi: 08.06.2017.

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

Keleştemur, A. (2015), *Siber İstihbarat*, Level Kitap, Kocaeli.

Klimburg, A. (2012). *National cyber security framework manua*l. NATO CCD COEPublication,Tallinn. Erişim tarihi: 03.06.2017, http://www.ccdcoe.org/369.html

NATO Cooperative Cyber Defence Centre of Excellence, (2017). https://ccdcoe.org/cyber-definitions.html, Erişim Tarihi: 08.06.2017.

Netcraft Internet Security Service, (2017). https://news.netcraft.com/archives/2017/07/20/july-2017-web-server-survey.html, Erişim Tarihi: 20.06.2017.

Özenç, K. (2007). *"Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması"*. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı. 13-14 Aralık 2007. Anakara, Türkiye.

Solms, B., (2006). "Information Security—The Fourt Wave", Computers & Security, 25(3):166-167.

Şenol, M. *"Siber Güçle Caydırıcılık Ama Nasıl?*" (2016). Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(2):10-17.

Şentürk, H., Çil, C.Z. ve Sağıroğlu, Ş. (2013). *"Siber Güvenliğin Taarruzi Boyutu ve Uluslararası Hukuk Kurallarının Uygulanabilirliği".* 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. 20-21 Eylül 2013. Ankara, Türkiye.

Teksas Üniversitesi Austin Cockrell Mühendislik Okulu, (2017). http://www.engr.utexas.edu/features/superyacht-gps-spoofing, Erişim Tarihi: 15.07.2017.

The Times of Israel Gazetesi (2012). Cyber Atack Hits a Minute http://www.timesofisrael.com/israel-fights-off-1000-cyber-attack-hits-a-minute, Erişim Tarihi: 08.06.2017.

The Guardian News, (2017). https://www.theguardian.com/media/2010/dec/08/anonymous-4chan-wikileaks-mastercard-paypal, Erişim Tarihi: 15.07.2017.

Winock, M. (2001) *"Terrorisme, l'histoire d'un mot"*.

Yılmaz, E.N., Ulus, H.İ. ve Gönen S. (2015). *"Bilgi Toplumuna Geçiş ve Siber Güvenlik".* Bilişim Teknolojileri Dergisi. 8(3):133-146.

Yılmaz, S.ve Sağıroğlu, Ş. (2013). *"Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri".* 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.20-21 Eylül 2013. Ankara, Türkiye.