Siber Güvenlik ve Hukuki Boyutu

Nilüfer ÖZMEN
Avukat

Bu yazımızda özellikle deniz sektörüne yönelik gerçekleştirilen siber saldırılar karşısında Türkiye ve Dünya'da var olan tehdit algılamasını ve bu duruma karşı mücadele yöntemleri ile hukuki aksiyonlar konusunda sizlere bilgi aktaracağız.

Bilgisayar ve ağ sistemlerinin sağladığı efektif ve hızlı çalışma imkanı tüm sektörlerde olduğu gibi deniz taşımacılığı sektöründe de internet tabanlı iş akışı ve kontrolünü etkin derecede arttırmıştır. Bu etkinlik internetin kendi içerisinde barındırdığı tehlikeleri de doğal olarak sektörün sorunlarının önemli bir parçası haline getirmiştir.

Günümüzde özellikle deniz taşımacılığına ilişkin iş akışları gerek gemi acenteleri, gerek konteyner firmaları, gerekse donatanlar ve ayrıca da müşteriler tarafından kullanılmaktadır. Sektördeki iş emirlerinin yüzde 90'dan fazlası elektronik talimat ile gerçekleşmekte, bu elektronik talimatlar daha sonrasında yazılı belgeye dönüş-

mektedir. Gemilere ulaşan yazılı belgelerin birçoğunun temelinde elektronik talimat yer almaktadır. Ayrıca önemli bir husus da, uzun yol deniz taşımacılığında gelişen gemi teknolojisinin gemilerin yönetim sisteminin elektronikleşmesinde de arttırıcı bir etkisinin olduğunu gözden kaçırmamak gerekir.

Bu anlamda tehdit algılamasının 3 ayaklı olduğundan bahsetmek yanlış olmaz. Bunlar gemiye ulaşan elektronik talimatlar, geminin yönetimi ve gemide saklanan elektronik verinin korunmasıdır. Deniz taşımacılığını hedef alan elektronik saldırılar iş akışının bu 3 ayağına odaklanmaktadır. Saldırı çeşitlerini ise yine 3 çeşitle sayabiliriz. Bunlar verinin değiştirilmesi, verinin kilit altına alınması veyahut verinin tamamen yok edilmesidir.

Seyir halindeki bir geminin karşılaşacağı en tehlikeli siber saldırılar da birkaç farklı şekilde gerçekleşmektedir.

Uzun yol taşımacılığı esnasında en tehlikeli ve güncel tehdit gemi tarafından kullanılan GPS cihazlarının hacklenerek gemilerin güvensiz (korsan) sulara çekilmesi olarak gösterebiliriz. Bu saldırı tekniğinde hedef olarak belirlenen geminin elektronik harita ve GPS sistemine yaklaşan yüksek frekanslı ufak bir tekne vasıtasıyla yanlış veriler yüklenerek gemi rotadan çıkartılmakta ve özellikle NATO koruması dışındaki sulara gemi yönlendirilmektedir. Bu saldırıların temel olarak tehlikeli sulara yakın seyreden gemilerde yaşandığı tespit edilmiştir. Özellikle tehlikeli sulara yakın rota izleyen gemilerde geminin seyrinin bizzat kademe kademe seyredilmesi ve geminin önceden izlediği rotalarla uyumlu olup olmadığının anlık olarak denetlenmesi gerekmektedir. Bu durum özellikle 2016-2017 yılları arasında Kuzey Kore yakınlarında seyahat eden ABD li ve Japon gemilerinde yansımış olup, ABD ve Japon gemileri Kuzey Kore yakınlarında GPS yerine radyo sinyalleri ile yön tespitine girişmiştir.

Diğer önemli bir tehdit ise geminin elektronik sistemlerinin kilitlenmesi ve rehin alınması olayıdır. Bu saldırılarda genellikle gemi personelinin gemi sistemine bağladığı (tablet, usb, cep telefonu vb) gibi aletler önceden ele geçirilmekte. Casus yazılım gemi sistemine bağlandığı esnada aktif hale gelerek, geminin elektronik sistemini ele geçirerek gemiyi durdurmaktadır. Sistemin yeniden aktif hale gelmesi ancak yazılım korsanı tarafından sağlanacak bir kod ile mümkün olup, yazılım korsanı geminin taşıdığı yüke ve bulunduğu sulara göre belirli bir fidye karşılığında bu kodu iletmektedir.

Önemle bahsetmek gerekir ki fidye verildiğinde geminin yeniden aktif hale getirilmesi tamamen kesin olmamakla birlikte, yazılım korsanları para karşılığında aktif hale getirme güvencelerini kaybetmek istemediklerinden parayı alıp ortadan kaybolmamaktadırlar. Bu saldırıların temel hedefi Voyage Data Recorder (VDR – Sefer Veri Kaydedici) ve Automatic Identification System (AIS – Otomatik Tanımlama Sistemi) lerdir. Kara yönetim merkezi ile olan internet bağlantısının bloke edilmesi de bu saldırı türleri arasında sayılabilir.

Uzun yol taşımacılığına ilişkin güncel olarak en tehlikeli husus ise gemi manifestolarının ve yük çeşitlerinin değiştirilmesidir. Bu saldırılar güncel operasyon akışına herhangi bir müdahale de bulunmadıkları için de oldukça geç fark edilmektedir. 2013 ve 2014 yıllarında Antwerp limanında uyuşturucu yüklü tam 252 konteyner farklı konteyner bilgileri kopyalanarak çeşitli ülkelere gönderilmiştir. Olayın ortaya çıkışı ise ancak 2016 yılının sonunda olmuştur.

2017 yılının Ocak ayından Haziran ayına kadar deniz taşımacılığına yönelik az önce bahsettiğimiz siber saldırıların sektöre verdiği zarar (kaçakçılık haricinde) 350.000.000 USD'nin üzerindedir.

Yukarıda bahsedilen saldırı türlerine karşı hukuki koruma yöntemlerinin ne yazık ki çok etkili olduğu söylenemez.. Bunun temel sebebi gemi seyir halindeyken saldırıların uluslararası sularda yapılması yahut ulusal sularda olsa bile saldırının başka bir ülkeden gerçekleştirilmesidir. Önemle üzerinde durulması gereken diğer bir konu ise yapılan saldırıların genellikle hangi ülkeden yapıldığının tespit edilmesinde imkan bulunmamaktadır. Bu kapsamda ulusal ve uluslararası düzenlemelere değinilmelidir..

Konumuz açısından Türk Hukuku'nda yer alan düzenleme Türk Ceza Kanunu'nun 244. maddesinde yer almaktadır. Az önce bahsettiğimiz saldırı şekillerine göre maddenin ilgili fıkrası hüküm ifade etmektedir. Bu madde şu şekildedir:

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

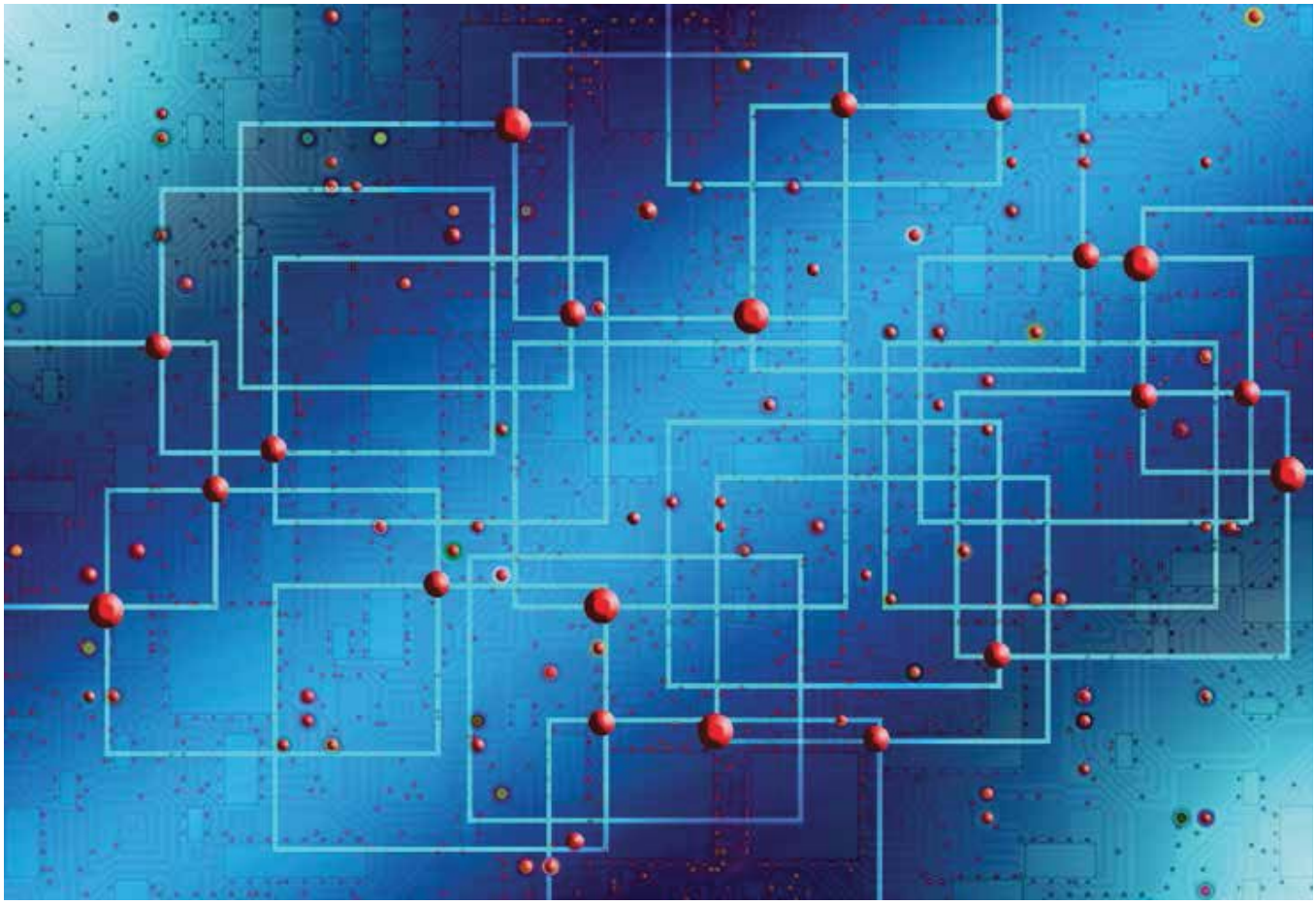
(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

Bu madde kapsamında uluslararası bir suda yapılan saldırının Türkiye'de soruşturulması mümkün dür.

Nitekim Türk Ceza Kanunu'nun 8. maddesinin düzenlemesi şu şekildedir:



"(2) Suç;

a) Türk kara ve hava sahaları ile Türk karasularında,

b) Açık denizde ve bunun üzerindeki hava sahasında, Türk deniz ve hava araçlarında veya bu araçlarla,

c) Türk deniz ve hava savaş araçlarında veya bu araçlarla,

d) Türkiye'nin kıta sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı,

İşlendiğinde Türkiye'de işlenmiş sayılır."

Ayrıca Türk Ceza Kanunu'nun 13. maddesinin i fıkrası da "deniz, demiryolu veya havayolu ulaşım araçlarının kaçırılması veya alıkonulması (madde 223, fıkra 2, 3) ya da bu araçlara karşı işlenen zarar verme (madde 152) suçları. vatandaş veya yabancı tarafından, yabancı ülkede işlenmesi halinde, Türk kanunları uygulanır" hükmü uygulanır

Görüldüğü üzere bir Türk gemisinde (Türk donatı tarafından yönetilen bir gemi de olabilir) suçun işlenmesi halinde Türk makamları da soruşturmaya yetkilidir.

Fakat bu hususta dikkat edilmesi gereken, Türk gemilerindeki saldırıyı soruşturan Türk makamlarının gerekli bilgi ve belgeleri yabancı ülkelerden isteyip isteyemeyeceği noktasıdır Buradaki temel sebep, uyuşturucu ve silah kaçakçılığı, banka dolandırıcılığı ve çocuk pornosu dışındaki siber suçlarda ulusal makamların isteksiz tavırları gösterilebilir.

İlgili suçun incelenmesine ve güvenlik güçlerinin müdahale hakkını tanıyan Birleşmiş Milletler Deniz Hukuku sözleşmesine de değinilmelidir. Bu durum ulusal karasularına komşu uluslararası sularda bir gemi kaynaklı siber saldırı halinde ortaya çıkmaktadır.

Sözleşmenin 109. Maddesi, ulusal devletlerin komşu uluslararası sulardan yapılan izinsiz radyo yayınları karşısında, radyo yayını yapan gemiye müdahale edebileceğini öngörmektedir. Özellikle GPS hack müdahaleleri sırasında karasuyu en yakın ulusal makamlara izinsiz radyo yayını kapsamında bildirim yapılabilir.

Siber güvenlik alanında henüz nihayete ermese de Türkiye'de de yasal çalışmaların temeli atılmış bulunmaktadır. Ulaştırma, Denizcilik ve Haberleşme Başkanlığı koordinesinde birçok strateji belgesi yayınlanmış ve yasal düzenleme çalışmalarına başlanmıştır.

2016 Ulusal Siber Güvenlik Stratejisinde yer alan Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması" kapsamında Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi

Siber Güvenlik Kurumu ve Deniz ve İç sular Düzenleme Genel Müdürlüğü de çalışmalarını yürütmektedir.

Ulusal Siber Güvenlik Yasa tasarısı Bakanlık tarafından Başbakanlığa gönderilmiş ve redaksiyon çalışmalarının sonuna gelinmiştir. Yakın zamanda meclise sevk edilecek tasarıda her bir işyerinde siber güvenlik uzmanı istihdamı zorunlu hale gelecektir. Düzenleme içeriği netleştiğinde hem gemide hem de karadaki merkezde düzenli bir bilişim uzmanı istihdamı söz konusu olabilecektir.

Siber saldırılar genel olarak INTERPOL aracılığı ile birlikte adi suçlar kapsamında işbirliği halinde soruşturulduğu gibi aynı zamanda Avrupa Konseyi Siber Suçlar Kapsamı altında Avrupa Konseyi ülkelerde kurulan özel birimler tarafından incelenmekte ve bu sözleşme daha etkin sonuçlar vermektedir. Deniz taşımacılığı açısından dikkate değer hususlardan birinin ise deniz taşımacılığına yönelik saldırıların büyük bölümünün Çin ve Afrika kaynaklı olmasından dolayı ve bu ülkelerin uluslararası suç anlaşmalarına imza atma konusundaki isteksizlikleri nedeniyle bir etkinlik problemi olduğu tartışmasızdır. Nitekim deniz güvenliğine karşı yapılan ticari saldırılardan siber tehdit kategorisine girenlerin %95'inin faili bulunamamaktadır.

Siber saldırılara ilişkin Birleşmiş Milletler nezdinde bir yardımlaşma anlaşması gündeme gelmişse de Rusya ve Çin'in vetosu nedeniyle imzalanamamıştır. Bu nedenle BM Anlaşmaları siber saldırılar karşısında kullanıma elverişsizdir.

NATO bünyesinde NATO Bilgisayar Olayları Müdahale Gücü Teknik Merkezi'yle (NATO Computer Incident Response Capability Technical Centre-NCIRC), NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE) nin devreye girmesi ile NATO üyesi ülkeler arasında sadece ulusal güvenliği değil aynı zamanda siber hırsızlığa karşı da bilgi paylaşımı ve müdahale ortaklığı geliştirilmiştir. Siber saldırılara karşı özellikle batı bloğu ülkeleri arasında ayrıca NATO gözetiminde Talinn Protokolü çalışmaları başlamıştır. Talinn protokolünün temel amacı siber soruşturmalarda ve müdahalelerde ortak bir müdahale timi kurulmasını öngörmektedir.

Uluslararası düzlemde siber saldırılara karşı ortaklığı ilk geliştiren Avrupa Konseyi üyesi ülkeler olmuştur. Daha 2001 yılında Avrupa Siber Suçlar Protokolü ortaya konulmuştur. Bu sözleşmenin en önemli özelliği Avrupa Konseyi olmayan ülkelere de açık olması ve ABD'nin de bu protokole taraf olmasıdır. Protokol ile taraflar verilerin izlenmesini, veri kaynaklarının bulunmasını ve veri kaynaklarına el konulmasını karşı devletlerden isteyebilmektedir.

Avrupa Konseyi'nin bu girişimine müteakip Amerikan Devletleri Birliği bir Siber Güvenlik Birlikteliği Protokolü yayınlamıştır. Hemen ardından da Shangai İşbirliği Örgütü

de kendi üyeleri arasında bir siber güvenlik yardımlaşması anlaşması olan Yekatirinburg Deklarasyonu'nu hayata geçirmiştir.

Bahsedilen bu uluslararası hukuki metinler dikkat edileceği üzere daha çok saldırı sonrası işbirliğine yöneliktir. Temel amaç suç soruşturmasının ulusal sınırlara bağlı kalmaksızın yürütülmesidir. Fakat bir ülke tarafından verinin izlenmesi ve el koyulması talepleri ülkelerin ulusal hukuklarında sıkı şartlara bağlandığı için birçok talep geri çevrilmekte veya saldırı kaynağı sözleşme tarafı olmayan devletlerdir.

Yukarıda bahsedilen uygulamaların hepsi saldırı sonrasındaki durumu belirtmektedir. Oysa asıl dikkat edilmesi gereken husus bu saldırıların önlenmesinin hukuki temelidir. Saldırılara ilişkin yapılan çalışmalar saldırıların özellikle gemi personelinin elektronik cihazları (özellikle kişisel cihazlarını) gemiye entegre etmesi sayesinde gerçekleştirildiğini ortaya koymaktadır. Bu nedenle ilk başta gemi personeline yönelik çeşitli önlemlerin alınması gerekmektedir.

Deniz İş Kanunu'muzun 6. maddesi gereğince iş şartlarının açık bir biçimde iş sözleşmesinde belirtilmesi ve gemi adamının da iş sözleşmesinde yer alan şartların altına imza atması gerekmektedir.

Maddenin bu kapsamına özellikle gemi adamlarına elektronik cihazları (ister gemiye ait olsun ister kendilerinin olsun) nasıl kullanacağına dair kapsamlı ve adım adım halinde ilerleyen bir yönerge imzalatılması zorunluluğu unutulmamalıdır. Bu yönergede özellikle gemi adamlarının kendi elektronik cihazlarını hangi şartlar dahilinde gemide kullanabilecekleri belirtilmelidir. Örneğin şirket tarafından sağlanan bir yazılımla sürekli olarak virüs taraması yapılması gerektiği, bazı cihazların kullanımının yasaklanması vb. gibi.

Gemilerin güvenliği meselesi hukuki alanda oldukça ayrıntılı düzenlenerek belirli hükümlere bağlanmıştır. Konumuzla ilgisi olan en önemli sözleşme 1980 yılından itibaren yürürlükte olan Denizde Can Emniyeti Uluslararası Sözleş-

mesi (Solas 1974)'dir. Solas'ın temel amacı Uluslararası Denizcilik Odası tarafından denetlenen bir can ve seyir güvenliği sağlanmasıdır. Güncellenerek mevcut sorunlara karşı belirli standartların oturmasını sağlamaktadır.

1988 protokolü ile birlikte artık IV. Bölümde düzenlenen telsiz haberleşmesi, V. Bölümde düzenlenen Seyir Güvenliği ve IX. Bölümde düzenlenen Gemi Güvenliği kapsamında standartlar belirlenmektedir.

Bu kapsamda başka bir örnek verilecek olursa; 11 Eylül Saldırıları sonrasında deniz güvenliğinin sağlanması için IMO içerisinde Deniz Güvenlik Komitesi (MSC) kurulmuştur. En son Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından 10.10.2017 tarihinde deniz ticaret odalarına gönderilen IMO'nun MSC 428 (98) sayılı siber güvenlik bildirgesi gemideki her bir elektronik aletin kimin tarafından kullanılacağını, bu alet üzerindeki aksaklıkların nasıl giderileceğini, gemi personelinin kişisel elektronik cihazlarını nasıl kullanması gerektiği yönünde eğitim almasının gerekliliklerinin önemini çizmiştir. Bu gereklilikler daha sonrasında zorunlu hale gelecektir.

SOLAS'ın diğer önemli bir özelliği de gemilerin elektronik aksamının kullanımı ve yönetimi konusundaki standartlar doğrudan Uluslararası Gemi ve Liman Tesisi Güvenlik Kodunuzu etkileyebilir. Bildiğiniz üzere Dünya üzerindeki çeşitli limanlara ancak bu koda sahipseniz giriş yapabilmektesiniz. ISPS standartlarına göre "elektronik ortamda saklanan hassas güvenlik bilgilerini korumak için gerekli işlem ve uygulamalar;" donatan şirket yükümlülüğünde olup, sertifikasyonun bu işlemlerin yapılmaması halinde iptali veya geçici olarak durdurulması gündeme gelebilir.

ISPS kodlarının geçerliliği için Company Security Officer (CSO) - şirket güvenlik uzmanı- and Company Ship Security Officer (SSO) - gemi güvenlik uzmanı- nın özellikle elektronik saldırılara karşı eğitim alması önemlidir. Bu nedenle uzman bilişim şirketlerinden gemiler ve gemilerle irtibat kuran kara merkezinin siber güvenliği hususunda çalışmalar yapılması hayati önem arz etmektedir.

Siber saldırının kaynağının bulunup cezalandırılması da önemli bir husustur. Ancak diğer önemli bir husus ise saldırı sonrası uğranılan zararın tazminidir. Burada sigorta şirketleri devreye girmektedir. Yukarıda bahsedilen standartlar zararın tazmini hususunda önem arz etmektedir. Belirlenen standartlara uymama durumunda sigorta şirketleri rizikonun ağırlaştırılmasına yönelik Türk Ticaret Kanunu'nun 1444. Maddesini ileri sürerek zarar tazminide indirim hakkı elde edebilir. . Siber saldırı devam ederken bir şekilde merkez ile irtibat kurulabilmesi halinde, kara merkezinin saldırının durumu hakkında derhal sigorta şirketine bildirim yapması gereklidir. Zira sigorta şirketi bu kapsamda çeşitli talimatların izlenmesini isteyebilecektir..

Gemi Türk karasularında ise geminin en yakın olduğu limandaki güvenlik birimlerine suç duyurusunda bulunulacak ve akabinde Suç soruşturması Türkiye'de yürütülecektir.

Gemi başka bir karasuyunda ise o ülkenin ulusal makamlarına aynı zamanda Türkiye'deki liman şehrindeki savcılığa da suç duyurusunda bulunulacak ve Soruşturma çift taraflı yürütülecektir

Ancak gemi uluslararası sularda ve tehdit başka bir gemiden geliyorsa uluslararası sularda bulunan savaş gemilerinden veyahut en yakın ulusal sulardaki güvenlik biriminden Denizde izinsiz radyo yayını kapsamında müdahale talep edilmeli,. Suç soruşturması liman şehrindeki savcılığa yapılmalı ve soruşturma Türkiye'den yürütülmelidir.

Zararın tazmini konusunda ise sigorta şirketi ile yapılmış olan sözleşmeler büyük önem arz etmektedir. Kural olarak tazmine ilişkin davalar Türkiye'de görülebilmekle birlikte sigorta sözleşmelerinde yer alan tahkim şartları nedeniyle yabancı ülke/ulusal organizasyon tahkimlerinde de görülebilmektedir. Siber saldırı faillerinden tazmin ise bu faillerin mal varlığına sahip olmaması nedeniyle sonuçsuz kalmaktadır.

Son olarak önemli üç kısmın altını çizilmelidir.:

1- Saldırı sonrası değil saldırı öncesi etkinliğin arttırılması amacıyla Deniz İş Kanunu kapsamında elektronik cihaz kullanım şartlarının belirlenmesi ve Gemi adamlarının kendi elektronik cihazlarını kullanma konusunda kısıtlanması, bu kapsamda bir yönerge hazırlanması

2- Gemi ve kara merkezi arasındaki haberleşmenin alternatif yollarının oluşturulması. Aynı zamanda gemi seyrüsefer ve elektronik yönetim sistemlerinin mekanik yedeklerinin bulundurulması.

3- Mümkünse gemi manifestolarının yazılı ve kara merkezi tarafından onaylı suretlerinin elde bulunması. Nihai limanda ve yükleme limanında bu verilerin bilgisayar verileri ile karşılaştırılması.