بیمه مخاطرات سایبری دریایی: مسائل نوظهور و راهکارها

منصور امینی*
مریم آقاسی جاوید**

تاریخ دریافت: ۱۴۰۳/۰۹/۱۴ تاریخ پذیرش: ۱۴۰۴/۰۹/۱۷

چکیده

گسترش استفاده از فناوری‌های نو در حوزه حمل‌ونقل دریایی و اجتناب‌ناپذیر اتصال بخش‌های مختلف به یکدیگر، مخاطرات سایبری را به یکی از تهدیدهای جدی این حوزه مبدل کرده است. ازاین‌رو تحت پوشش بیمه قرار دادن این مخاطرات امری ضروری تلقی می‌گردد. اما از آنجا که ابعاد مختلف این نوع مخاطرات برای بیمه‌گرها چندان مشخص نیست، آنان نسبت به ارائه این نوع پوشش بیمه‌ای مردد بوده‌اند؛ حتی اغلب در بیمه‌نامه‌های معمول دریایی نیز سعی دارند تا با استفاده از شروط خاصی، این دسته از مخاطرات را از گستره شمول این بیمه‌نامه‌ها مستثنا سازند. این وضعیت مبهم، بر حقوق بیمه‌گذارها و تصمیمات آنان نیز اثرگذار است. از همین رو لازم است نسبت به مفهوم مخاطره سایبری دریایی، خسارات ناشی از آنها که معمولاً تحت پوشش قرار می‌گیرند، وضعیت حقوقی بیمه‌های معمول دریایی درخصوص پوشش این قسم از مخاطرات و نیز ابزارهای حقوقی تعیین و مدیریت چنین مخاطراتی شناخت حاصل شود تا بیمه‌گر و بیمه‌گذار با کسب اطلاعات بیشتر درخصوص حقوق و تعهدات خود، با اطمینان بیشتری وارد رابطه قراردادی شوند. ازاین‌رو، پژوهش حاضر با رویکرد توصیفی و تحلیلی، ضمن ارائه شناخت درخصوص مفاهیم مرتبط با مخاطره سایبری دریایی و بررسی گستره پوشش‌های بیمه‌ای معمول دریایی در خصوص مخاطرات سایبری؛ سعی کرده است با ارائه تحلیلی نو از نهادهای حقوقی بیمه دریایی موجود و چگونگی اِعمال این نهادها در وادی مخاطرات سایبری دریایی و به‌طورکلی از طریق ایجاد قطعیت حقوقی، زمینه را برای تحت پوشش قرار گرفتن این دسته از مخاطرات فراهم نماید.

کلیدواژگان:

افزایش ریسک، پوشش بیمه‌ای مسکوت، تعهد به افشا، شرط استثنا، مخاطرات سایبری دریایی.

---

* دانشیار، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.

** دانشجوی دکتری، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران. (نویسنده مسئول)
m_aghasijavid@sbu.ac.ir

مقدمه

امروزه استفاده از سامانه‌های پیشرفته ناوبری و پایش دریایی به رکن جدایی‌ناپذیر صنعت حمل‌ونقل دریایی مبدل شده است و سامانه‌های ارتباطی[1] مانند نمایشگر نمودار الکترونیکی و سامانه اطلاعات،[2] سامانه‌های شناسایی خودکار[3] و سامانه موقعیت‌یابی جهانی (جی‌پی‌اِس)[4] اغلب مورد استفاده قرار می‌گیرند. این سامانه‌ها درعین‌حال که در کشتی تعبیه می‌شوند، به سامانه‌های دیگری متصل‌اند که متعلق به شرکت مالک کشتی‌اند و برای پایش و کنترل کشتی و محموله مورد استفاده قرار می‌گیرند و همچنین بنادری که برای انجام عملیات لجستیکی مجهز به سامانه‌های رایانه‌ای‌اند. به‌علت رابطه متقابل میان سامانه‌ها، اختلال در هریک از آنها می‌تواند منجر به اختلال در دیگر سامانه‌ها شود و در نهایت، خسارات اقتصادی قابل توجهی به بار آورد. بنابراین، استفاده از سامانه‌های رایانه‌ای در حمل‌ونقل دریایی، موجب ایجاد نوعی از مخاطرات می‌شوند که از آن با عنوان مخاطره سایبری در حوزه حمل‌ونقل دریایی یاد می‌شود. تحمل خسارات ناشی از مخاطرات سایبری دریایی ازسوی شرکت‌های حمل‌ونقل، از منظر تحلیل اقتصادی بسیار هزینه‌بر و گاه خارج از توان آنهاست. به همین دلیل، استفاده از نهاد بیمه، گزینه جذابی پیش‌روی این شرکت‌ها محسوب می‌شود. اما، ازسوی دیگر، بیمه‌گرها به‌دلیل ناشناخته بودن مفهوم و گستره مخاطرات سایبری دریایی، در دسترس نبودن اطلاعات کافی درخصوص حدوث این نوع مخاطرات و همچنین مخاطرات اخلاقی، تمایلی به ورود به این بازار ندارند. مضاف بر این، به‌علت شکل‌گیری اغلب قواعد و مقررات ناظر بر حقوق و تعهدات بیمه‌گر و بیمه‌گذار بر مبنای مخاطرات دریایی مرسوم، عدم قطعیت حقوقی در جنبه‌های مختلف تحت پوشش قرار دادن مخاطرات سایبری موجب شده است که بیمه‌گرها نتوانند پوشش بیمه‌ای مناسب را برای این مخاطرات ارائه دهند و حتی به‌دلیل عدم شناخت کافی و عدم پیش‌بینی تمهیدات مناسب قراردادی، گرفتار جبران خساراتی شوند که منشأ آن مخاطرات سایبری است که در پوشش بیمه‌ای مسکوت گذارده شده است.

بنابراین، شناخت ابعاد این نوع مخاطره و نیز ارائه پوشش بیمه‌ای مناسب، به موضوعی اجتناب‌ناپذیر مبدل شده است. از همین رو پژوهش حاضر نیز سعی داشته است تا ضمن ارائه شناخت از مفهوم مخاطره سایبری دریایی، خسارات و بیمه آن، به این سؤالات پاسخ دهد که: ۱. پوشش‌های بیمه‌ای معمول چه

1. Bridge systems
2. Electronic Chart Display and Information System (ECDIS)
3. Automatic Identification Systems (AIS)
4. Global Positioning System (GPS)

رویکردی در خصوص این مخاطره دارند؟ و ۲. چگونه می‌توان با به کار گرفتن ابزارهای حقوقی موجود در بیمه دریایی و حقوق و تعهدات طرفین، چنین مخاطراتی را در پوشش بیمه‌ای قطعیت بخشید؟

در مقاله حاضر با رویکرد مذکور و با استفاده از شیوه توصیفی- تحلیلی، ابتدا مفهوم بیمه مخاطره سایبری دریایی و چالش‌های اصلی تحت پوشش بیمه قرار دادن این مخاطرات بررسی شده، در ادامه، عمده خسارات ناشی از مخاطرات سایبری دریایی برشمرده شده است. همچنین وضعیت پوشش‌های بیمه‌ای معمول دریایی درخصوص تحت پوشش قرار دادن یا مستثنا ساختن این مخاطرات مورد تدقیق قرار گرفته و در نهایت چگونگی استفاده از ابزارهای حقوقی موجود جهت تعیین گستره و مدیریت این نوع مخاطرات تحلیل شده است.

۱. شناخت مخاطره سایبری دریایی و بیمه کردن آن

همان‌گونه که اشاره شد، امروزه بازار بیمه دریایی با نوع جدیدی از مخاطرات تحت‌عنوان «مخاطره سایبری» روبه‌رو است. اما پیش از بررسی جوانب مرتبط با این مخاطره نوظهور، ضروری است که حدود و ثغور آن از گذر ارائه تعریفی مشخص گردد. متأسفانه، تعریف چندان مشخصی نه‌تنها از مفهوم مخاطره سایبری دریایی، بلکه از مفهوم مخاطره سایبری ارائه نشده است. مطابق یک تعریف، مخاطره سایبری چنین تعریف شده است: «احتمال صدمه دیدن و تحمل خسارت و ضرر به‌دلیل در معرض یک عامل الکترونیکی بودن که می‌تواند منجر به ایجاد آثار سوء بر کسب‌وکار شود».[۱] مطابق تعریف انجمن بیمه لوید نیز مخاطره سایبری، «هر گونه رخداد ناگهانی است که نتیجه آن وارد ساختن ضرر سایبری بر دارایی‌های مادی یا غیرمادی بوده و ناشی از افعال مبتنی‌بر سوءنیت (همچون حمله سایبری و نفوذ به سامانه به‌وسیله کد مخرب)[۲] یا غیر آن (همچون از بین بردن داده، افعال اتفاقی یا ترک فعل) باشد».[۳]

تعاریفی که پیش‌تر ارائه شد، تصویر چندان روشنی از مفهوم مخاطره سایبری به‌دست نمی‌دهند؛ چراکه تعریف نخست، به‌جای توجه به خودِ مخاطره، اثر آن (یعنی صدمه و خسارت) را مطمح نظر قرار داده و تعریف دوم نیز اگرچه به نسبت تعریف نخست، تعریف مناسب‌تری است، بدون تشریح مصادیق سایبر، از عبارت «ضرر سایبری» استفاده کرده است. به نظر می‌رسد تعریف مناسب از مخاطره سایبری در عین توجه به اثر آن، باید خودِ مخاطره را محور قرار دهد و درعین‌حال دربردارنده عبارتی که درصدد

۱. السان، مصطفی، **بیمه فضای مجازی: مفاهیم اساسی و برنامه عملیاتی**، تهران: پژوهشکده بیمه. ۱۳۹۵. ص. ۱۹.
2. Malicious code
3. Lloyd's Market Bulletin Y5258 dated 4 July 2019.

تعریف آن هستیم، نباشد. بدین ترتیب مخاطره سایبری را می‌توان به این صورت تعریف نمود: «هرگونه اختلال محتمل، براساس سوءنیت یا غیر آن، در کارکرد متعارف یا از پیش تعیین‌شده هر آنچه مبتنی‌بر رایانه، شبکه رایانه‌ای، فناوری اطلاعات و واقعیت مجازی است؛ به‌طوری‌که نتیجه این اختلال، ورود خسارت بر دارایی‌های مادی یا غیرمادی باشد».

پس از تعریف مخاطره سایبری لازم است مخاطره سایبری دریایی نیز مورد تعریف قرار گیرد تا گستره موضوع مقاله حاضر، وضوح بیشتری یابد. همانند مخاطره سایبری، تعریف مناسبی از مخاطره سایبری دریایی نیز به چشم نمی‌خورد و تنها تعریف ارائه‌شده در این خصوص، تعریفی است که توسط سازمان بین‌المللی دریانوردی[1] ارائه گردیده است. مطابق تعریف مزبور، مخاطره سایبری دریایی عبارت است از: «در معرض تهدید قرار گرفتن دارایی مبتنی‌بر فناوری، به‌واسطه اختلال، مفقودی یا به خطر افتادن اطلاعات یا سامانه‌ها که منجر به ناکارآمدی عملیاتی، ایمنی یا امنیتی مرتبط با حمل‌ونقل دریایی شود».[2]

اگرچه تعریف مزبور تعریف چندان جامع و مانعی نیست، می‌توان با استفاده از آن، مخاطره سایبری دریایی را به این صورت تعریف کرد: «هرگونه اختلال محتمل، براساس سوءنیت یا غیر آن، در کارکرد متعارف یا از پیش تعیین‌شده هر آنچه که در حمل‌ونقل دریایی مبتنی‌بر رایانه‌ها، شبکه‌های رایانه‌ای، فناوری اطلاعات و واقعیت مجازی است؛ به‌طوری‌که نتیجه این اختلال، به ورود خسارت بر دارایی‌های مادی یا غیرمادی مرتبط با حمل‌ونقل دریایی منجر گردد».

لذا، با امعان نظر به این تعریف، می‌توان «بیمه مخاطرات سایبری دریایی» را نیز «تحت پوشش قرار دادن خسارات ناشی از وقوع یا بروز مخاطره سایبری دریایی بر موضوع بیمه از سوی بیمه‌گر، در ازای پرداخت حق بیمه از سوی بیمه‌گذار» تعریف نمود.

شایان ذکر است که موضوع بیمه در بیمه مخاطره سایبری دریایی، می‌تواند شامل طیفی از موضوعات شود که نه‌تنها شامل کشتی و محموله آن می‌شود، بلکه شرکت‌های کشتی‌رانی و بنادر را نیز دربرمی‌گیرد.

۲. چالش‌های بیمه مخاطرات سایبری دریایی

اگرچه اغلب شرکت‌های فعال در زمینه حمل‌ونقل دریایی تجاری، به‌خوبی از آثار بالقوه مخاطره سایبری آگاهی دارند و به‌تازگی نیز تحت پوشش بیمه‌ای قراردادن این نوع مخاطره از سوی شرکت‌های

1. International Maritime Organization (IMO)
2. Guidelines on Maritime Cyber Risk Management, published by the International Maritime Organization (IMO)

بیمه افزایش یافته است؛ بااین‌حال، بیمه مخاطره سایبری دریایی، پوشش بیمه‌ایِ نسبتاً جدیدی است که از ابعاد مختلف برای بیمه‌گران و بیمه‌گذاران چالش‌برانگیز تلقی می‌شود.[۱]

از دیدگاه بیمه‌گران، تحت پوشش بیمه قراردادن این نوع مخاطره از منظر اقتصادی چندان قابل توجیه نیست؛ به‌طوری‌که هزینه‌های ناشی از حدوث چنین مخاطره‌ای می‌تواند به میزان قابل توجهی بالا باشد؛ چراکه به‌علت ارتباط سامانه‌های مورد استفاده در حمل‌ونقل دریایی، ایجاد اختلال و نقض ساختار امنیتی یک سامانه، می‌تواند منجر به اختلال دیگر سامانه‌ها شود و زنجیره اختلالات باعث گردد تا بیمه‌گر در پی هر اختلالی، متعهد به جبران خسارت باشد.[۲] بنابراین، به‌طور مثال، چنانچه موضوع بیمه مخاطره سایبری دریایی محموله یک کشتی باشد که به سامانه‌های ناوبری دریایی متصل بوده و با شرکت کشتی‌رانی و بنادر مرتبط است، ممکن است هرگونه اختلال در سامانه شرکت یا بنادر، موجب اختلال در سامانه‌های کشتی و درنتیجه آسیب به محموله شود. بنابراین، بیمه‌گر به‌طور بالقوه در معرض جبران خساراتی است که سبب حدوث آن در حدود پیش‌بینی وی نبوده است.

همچنین احتمال حدوث اختلال سایبری در هر نقطه‌ای از شبکه، تعیین میزان خطر در محدوده جغرافیایی را برای بیمه‌گران دشوار می‌کند و بیمه‌گران نمی‌توانند با استفاده از شروط تضمینِ (وارانتی)[۳] محدوده جغرافیایی یا شروط استثنا، مخاطره را مدیریت و مسئولیت خود را تحدید نمایند.[۴] مضافاً، به‌دلیل قلّت داده‌های آماری مرتبط با مخاطرات سایبری دریایی، بیمه‌گرها در ورود به این بازار دچار تردید ناشی از عدم کفایت اطلاعات آماری‌اند. تمامی موارد مذکور موجب می‌شوند بیمه‌گرها به‌واسطه مشخص نبودن گستره تعهدات بیمه‌ای خود، برای ورود به این بازار نوظهور چندان راغب نباشند.[۵]

از منظر بیمه‌گذاران نیز مشخص نبودن گستره خسارات تحت پوشش این نوع پوشش بیمه‌ای امکان شانه خالی کردن بیمه‌گرها از تعهدات خود را افزایش می‌دهد و بدین ترتیب بیمه‌گذار برخلاف آنچه مطلوب بوده است، در مقابل پرداخت حق بیمه، معوض دریافت نمی‌کند. به‌عنوان نمونه، مخاطراتی که در زمان جنگ، تهاجم و شورش رخ می‌دهند، به‌موجب بسیاری از بیمه‌نامه‌ها مستثنا می‌شوند؛ از همین رو

1. Marano, Pierpaolo, and Kyriaki Noussia, **InsurTech: A Legal and Regulatory View**, Vol. 1. Switzerland: Springer. 2019. p. 170.

2. Sözer, Bülent, **Unmanned Ships and the Law**, United Kingdom: Routledge, 2023, p.144.

3. Warranty

4. *Ibid*. p. 147.

5. Armstrong, Dean., Shyam Thakerar, and Thomas Steward, **Cyber Risks and Insurance: The Legal Principles**, United Kingdom: Bloomsbury Professional. 2021. p.183.

ممکن است بیمه‌گر با استناد به این شرط استثنا، از جبران خسارات تبعی ناشی از جنگ سایبری بین دو دولت متخاصم در حوزه حمل‌ونقل دریایی، شانه خالی کند.[۱]

مضاف بر این، باتوجه‌به درحال توسعه بودن پوشش بیمه‌ای مخاطره سایبری، محتمل است بیمه‌گذار برای خطری که قبلاً توسط یک بیمه‌نامه جداگانه تحت پوشش بیمه‌ای قرار گرفته است، مجدداً پوشش بیمه‌ای سایبری خریداری کند و این امر موجب حدوث موضوع بیمه مضاعف گردد. برای مثال، ممکن است نرم‌افزاری که برای کنترل دمای کانتینرهای حاوی محموله سریع‌الفساد مورد استفاده قرار می‌گیرد، توسط یک کد مخرب مختل شود. سپس اختلال نرم‌افزار باعث فاسد شدن محموله شود. در چنین فرضی، بسیار محتمل است که بیمه‌گرِ بیمه محموله به‌موجب بیمه نامه مزبور، خسارت وارده را جبران کند و درعین‌حال، بیمه‌گر دیگری نیز مستند به بیمه‌نامه مخاطره سایبری دریایی، خسارت مزبور را مجدداً جبران نماید. بنابراین بیمه مضاعف در چنین مواردی که دو یا چند بیمه‌نامه خسارت واحدی را تحت پوشش قرار دهند، قابل حدوث است. وضعیت ناشی از بیمه مضاعف نه‌تنها از منظر بیمه‌گرها رخدادی نامطلوب قلمداد می‌شود، بلکه به‌دلیل مشخص نبودن ضمانت اجرای بیمه مضاعف ناشی از حسن‌نیت در برخی نظام‌های حقوقی و تسری این عدم قطعیت به منافع بیمه‌گذار، نزد بیمه‌گذاران نیز پدیده مخاطره‌آمیزی محسوب می‌شود.[۲] در چنین فروضی، حتی اگر بیمه‌گذار را مخیر در رجوع به هریک از بیمه‌گرها برای مطالبه جبران خسارت وارده بدانیم، بازهم ممکن است به‌واسطه اطلاع بیمه‌گرها از حدوث وضعیت بیمه مضاعف، با تأخیر در جبران خسارت خود مواجه شود و بدین ترتیب اعطای چنین اختیاری از منظر اقتصادی، آورده چندانی برای او به‌همراه نداشته باشد. به‌علاوه، چنانچه شرط استثنای صریحی در بیمه‌نامه درخصوص بیمه مضاعف گنجانده شده باشد، ممکن است بیمه‌گذار به طورکلی موفق به مطالبه خسارت خود نشود و بدون پوشش بیمه‌ای بماند.[۳]

علاوه‌بر فقدان مقررات قانونی خاص در این حوزه، عامل چالش‌برانگیز دیگری که بر تصمیم بیمه‌گرها و بیمه‌گذران در ورود به ترتیبات بیمه‌ای مخاطرات سایبری اثر سوء دارد، نبود رویه مقتضی درخصوص موضوع است. توضیح آنکه به‌علت نوظهور بودن پوشش‌های بیمه‌ای خطر سایبری، رویه چندانی درمورد کارکرد و آثار این چنین پوشش‌هایی و اصطلاحات فنی مرتبط با آنها وجود ندارد و نیازمند

1. *Ibid*, p.162.

۲. بابایی، ایرج، **حقوق بیمه**، چ ۱۴، تهران: سمت، ۱۳۹۶، صص. ۱۴۸–۱۴۹.

3. The Australian Agricultural Company v Saunders (1874–75) LR 10 CP 668. Available at: https://vlex.co.uk/vid/the-australian-agricultural-company-803513305 (last visited on 16/05/2022).

تصمیم‌گیری و تفسیر مرجع رسیدگی‌کننده در هر پرونده است. همین امر موجب تردید در وضع حقوقی طرفین می‌شود.[1] به‌عنوان مثال، هیچ تعریف و تفسیر مشخصی درخصوص مفاهیم «ناتوانی مکانیکی / الکترونیکی»[2] یا «کد مخرب» که در بسیاری پرونده‌ها ملاحظه می‌گردند، وجود ندارد.

بنابر آنچه بیان شد، ارائه‌دهندگان و متقاضیان دریافت پوشش بیمه‌ای معمولاً درخصوص تحت پوشش بیمه‌ای قرار گرفتن مخاطره سایبری دریایی با چالش‌هایی مواجه‌اند که این امر به‌طور می‌تواند آنها را از مشارکت کامل در بازار بیمه سایبری منصرف کند.

به‌منظور کاهش گستره این چالش‌ها لازم است تا حد امکان با استفاده از نهادهای حقوقی از دامنه تردیدها کاسته شود. به‌عنوان مثال، می‌توان با بازتعریف نهادهای دیرین حقوق بیمه، همچون «افشا» و «معرفی دقیق اطلاعات راجع به موضوع بیمه»، شرط «تضمین قابلیت دریانوردی»، استفاده صحیح‌تر از «شروط استثنا» و نیز نهاد «افزایش ریسک»، تا حد بسیاری از گستره اطلاعات نامتقارن کاست و در نتیجه، محدوده حقوق و تعهدات بیمه‌گر و بیمه‌گذار را مشخص نمود.

۳. خسارات تحت پوشش بیمه مخاطرات سایبری دریایی

هیچ پوشش بیمه‌ای استانداردی درخصوص خسارات تحت پوشش ناشی از مخاطره سایبری دریایی وجود ندارد. پوشش‌های بیمه‌ای که در این خصوص ارائه می‌شوند قصد دارند خلأهایی را که در بیمه‌نامه‌های معمول در ارتباط با خطرات سایبری وجود دارند، پر کنند تا بیمه‌گذاران بتوانند با در نظر گرفتن شرایط و نیازهای خاص خود، بیمه‌نامه سایبری لازم را تحصیل دارند. پوشش بیمه‌ای سایبری دریایی بسته به موضوع بیمه، معمولاً خسارات ذیل را تحت پوشش قرار می‌دهند:

۳.۱. سرقت محموله

سارقان قادرند با دستیابی به شبکه کشتی یا راهبران آن، اظهارنامه بار کشتی را تغییر دهند و با هک کردن سامانه‌های اداره‌کنندهِ امور مربوط به محموله‌ها،[3] موجب شوند محموله کشتی، به‌جای تسلّم به گیرندهِ به‌حق آن به سارقان تحویل داده شود. مثال‌های متعددی در این خصوص وجود دارند، اما شاید

1. De Maurier (Jewels) Ltd v. Bastion Insurance Co Ltd [1967] 2 Lloyd's Rep 550. Donaldson, J, disregarding the technical meaning of the words, held that a car "owned by the insured" included cars held on hire-purchase by the company, as a reasonable assured not fully aware of the niceties of law would describe them as "the company cars". Available at: https://www.i-law.com/ilaw/doc/view.htm?id=146105 (last visited on: 23/05/2022).
2. Mechanical/electronic failure
3. Cargo Handling Systems

بارزترین آن پرونده اِم‌اِس‌سی مدیترنین شیپینگ کو اِس‌اِی علیه گلن کور اینترنشنال آجی (گلن کور)[1] باشد. در این پرونده، شرکت کشتی‌رانی مدیترانه (اِم‌اِس‌سی) به‌عنوان حمل‌کننده، سه کانتینر بار را تحت یک بارنامه از بندر فرمنتل[2] به بندر آنتورپ[3] حمل می‌کرد. طبق بارنامه، شرکت گلن کور به‌عنوان فرستنده، و سی اِشتاینوِگ اِن‌وی (اِشتاینوِگ)،[4] نماینده گلن کور، به‌عنوان «مطلع»[5] تعیین شده بودند. چند روز پیش از رسیدن کشتی به بندر تخلیه، با تسلیم یکی از بارنامه‌ها توسط اِشتاینوِگ به حمل‌کننده، وی از طریق رایانامه، ترخیص‌نامه و کدهای پین[6] سامانه الکترونیکی ترخیص محموله را به اِشتاینوِگ، ارسال نمود. پس از اینکه کشتی به بندر آنتوِرپ رسید و کانتینرها تخلیه و در ترمینال حمل‌کننده انبار شدند، اِشتاینوِگ درصدد ترخیص و تحویل گرفتن محموله برآمد؛ اما مشخص شد محموله این دو کانتینر پیش‌تر توسط گیرندگان ناشناس و غیرمجاز ترخیص شده است. در این پرونده، کاشف به عمل آمد که گیرندگان غیرمجاز به کدهای پین ارسال شده به اِشتاینوِگ دست یافته و محموله را قبل از اینکه مالک قانونی آن این کار را انجام دهد، تحویل گرفته بودند.

از همین رو، در اغلب پوشش‌های بیمه‌ای مخاطره سایبری دریایی، خسارات وارده از قِبلِ سرقت موضوع بیمه با استفاده از اختلالات سایبری، در زمره مخاطرات تحت پوشش ذکر می‌شوند.

۳.۲. خسارات ناشی از وقفه یا تأخیر در عملیات و فعالیت

امروزه اتکای شرکت‌های حمل‌ونقل به رایانه‌ها و ذخیره‌سازی دیجیتالی داده‌ها، امری انکارناپذیر است و بدون استفاده از فناوری اطلاعات، مراودات و مبادلات تقریباً غیرممکن خواهد بود. این شرکت‌ها درصورت حدوث حمله سایبری، معمولاً به‌عنوان یک اقدام احتیاطی، ابتدا سامانه‌های مربوطه را خاموش می‌کنند که این امر موجب تعلیق فعالیت‌های شرکت‌ها و حتی تأخیر در تسلیم محموله‌هایی که توسط کشتی‌های متصل به این سامانه‌اند، می‌شود و در نهایت ممکن است به زیان مالی قابل توجهی بینجامد. از همین رو، پوشش بیمه مخاطره سایبری دریایی، اغلب این قسم از خسارات را تحت پوشش قرار

1. MSC Mediterranean Shipping Co SA v. Glencore International AG [2015] EWHC 1989 (Comm); aff'd [2017] EWCA Civ 365. Available at: https://www.i-law.com/ilaw/doc/view.htm?id=377477 (last visited on: 27/05/2022).
2. Fremantle
3. Antwerp
4. C Steinweg NV (Steinweg)
5. Notify Party
6. Pin Codes

می‌دهد.[1] شایان ذکر است که اگرچه شرایط و ضوابط ثابت و یکنواخت در همه پوشش‌های بیمه‌ای برای پوشش این نوع خسارات ناشی از مخاطره سایبری وجود ندارد، به‌طور کلی برای تحت پوشش گرفتن این خسارات، لازم است شقی از اختلال در عملکرد شبکه رخ دهد. این اختلال می‌تواند ناشی از این عوامل باشد: ۱. استفاده یا دسترسی غیرمجاز به شبکه، ۲. ممانعت از ارائه خدمات یا محرومیت از دسترسی، ۳. دریافت یا انتقال کدهای مخرب ازجمله ویروس‌ها، ۴. آسیب، از دست رفتن یا سرقت داده‌ها، ازجمله داده‌های محرمانه. همچنین، لازم است اختلالات مذکور موجب ایجاد وقفه در عملیات تجاری یا تسلیم محموله شوند.[2]

اغلب، بیمه‌نامه‌های سایبری تمام زیان‌هایی که مستقیماً از چنین رویدادهایی ناشی شوند را تا پایان یک دوره ثابت، معمولاً بین ۶۰ تا ۱۲۰ روز، تحت پوشش قرار می‌دهند که از این دوره با عنوان «حداکثر دوره غرامت»[3] یاد می‌شود.[4] همچنین، به‌طور معمول، خسارات ناشی از وقفه یا توقف، به‌عنوان «از بین رفتن سود ناخالص» یا «سود خالص به اضافه هزینه‌های ثابت مداوم»[5] ذیل خسارت ناشی از «عدم‌النفع»[6] محاسبه و پرداخت می‌شوند.[7]

۳.۳. خسارت ناشی از اخاذی سایبری

تعاریف متعددی درخصوص اخاذی سایبری ارائه شده است، لکن به‌طورکلی می‌توان آن را «دسترسی عمدی به سامانه حفاظت‌شده از طریق ارتباطات داخلی یا خارجی و تهدید برای صدمه زدن به تمام یا بخشی از سامانه، به‌منظور تحصیل اهداف مالی یا غیرمالی تعریف نمود».[8] یکی از ابزارهای ایجاد مخاطره سایبری در حوزه حمل‌ونقل دریایی، استفاده از باج‌افزارها[9] برای اخاذی است. باج‌افزار با استفاده از نوعی بدافزار[10] از یک سامانه رمزگذاری برای قفل کردن داده‌ها در رایانه‌های آلوده استفاده می‌کند و بدین ترتیب، باعث قفل نمودن یا از دسترس خارج کردن کنترل تمام یا برخی از سامانه‌های مرتبط با

1. Tettenborn, Andrew and Barış Soyer, **Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector**, United Kingdom: Routledge, 2020, p. 120.
2. *Ibid*.
3. Maximum Indemnity Period
۴. السان، مصطفی، *منبع پیشین*، ص.۲۷.
5. Net profit plus Continuing fixed costs
6. Loss of Profit
7. Marano, Pierpaolo, Ioannis Rokas, and Peter Kochenburger. *Dematerialized Insurance: Distance Selling and Cyber Risks from an International Perspective*. Switzerland: Springer International Publishing. 2016. p 197.
۸. حسینی، سیده آمنه، محمدرضا زندی و عباس تدین، «بررسی جرم قلدری مجازی در حقوق کیفری ایران و آمریکا»، *پژوهش‌های حقوق تطبیقی*، ش. ۳. ۱۴۰۲. ص. ۹۳.
9. Ransomwares
10. Malware

کشتی می‌شود.[1] فرمانده و کارکنان کشتی تنها در برابر پرداخت مبلغی تحت‌عنوان وجه اخاذی، می‌توانند کنترل دوباره کشتی را به دست آورد. بنابراین، در برخی از بیمه‌نامه‌ها، هزینه‌هایی که بیمه‌گذار برای جلوگیری از عملی ساختن تهدید اختلال سایبری از سوی اخلالگرانِ با سوءنیت پرداخت می‌کند نیز تحت پوشش قرار داده شده است. بدین ترتیب، حتی درصورتی‌که تهدید هیچ‌گاه صورت بالفعل به خود نگیرد، بازهم هزینه پرداختی توسط بیمه‌گذار از سوی بیمه‌گر، قابل جبران خواهد بود.[2]

۳.۴. هزینه‌های مدیریت بحران

پس از حدوث اختلالات سایبری، بیمه‌گذار موظف است در راستای عمل به تعهد مستمر خود مبنی‌بر رعایت حسن‌نیت، پس از حدوث خسارت، اقدامات متعارف و متناسبی برای جلوگیری از گسترش دامنه خسارات[3] اتخاذ نماید.[4] این اقدامات چنانچه مستلزم صرف هزینه باشند، ازسوی بیمه‌گرها به‌عنوان خسارات ناشی از حملات سایبری قلمداد می‌شوند و حتی در فرض عدم تصریح به آنها، تحت پوشش بیمه‌ای قرار می‌گیرند.[5] از همین رو بیمه مخاطره سایبری دریایی معمولاً آن دسته از خسارات بیمه‌گذار را که ناشی از هزینه‌های اطلاع‌رسانی، هزینه‌های روابط عمومی و به‌طورکلی تمام هزینه‌های مصروفه به‌منظور جلوگیری از گسترش دامنه خسارت باشند، تحت پوشش قرار می‌دهد.

۴. مخاطره سایبری و بیمه‌نامه‌های دریایی معمول

بیمه‌نامه‌های دریایی معمول، اغلب درخصوص قابل جبران بودن خسارات ناشی از مخاطره سایبری دریایی ساکت‌اند یا در برخی موارد با گنجاندن شرطی، خسارات ناشی از این مخاطره را مستثنا ساخته‌اند. لذا، بررسی رویکرد پوشش‌های بیمه‌ای مرسوم دریایی درخصوص این نوع مخاطره و شرط استثنای خسارات ناشی از مخاطره سایبری دریایی برای تعیین حقوق و تعهدات طرفین این نوع پوشش بیمه‌ای بسیار حائز اهمیت است.

1. Reetz, Margaret A., Lauren B. Prunty, Gregory S. Mantych, and David J. Hommel, "Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law", *Penn State Law Review*. Vol. 122. Issue 3. 2018. p.736.
2. Davit, Dadiani, **Cyber-security and marine insurance**, PhD diss. World Maritime University. 2019. p.15.
3. Mitigation
4. Dunt, John, Marine Cargo Insurance, United Kingdom: Routledge. 2015. p. 347.
5. Tettenborn, Andrew and Barış Soyer, Op. cit, p.111.

۴.۱. مخاطره سایبری دریایی مسکوت

چنانچه یک بیمه‌نامه معمول دریایی همچون «بیمه بدنه و ماشین‌آلات»،[۱] به‌صراحت خسارات مربوط به مخاطره سایبری را تحت پوشش قرار ندهد یا چنین خساراتی را مستثنا نسازد، چنین فرض می‌شود که بیمه‌نامه مزبور جبران خسارات ناشی از چنین مخاطراتی را نیز دربر می‌گیرد. به این شیوه از پوشش بیمه‌ای مخاطرات سایبری با عنوان پوشش بیمه‌ای مخاطرات سایبری «مسکوت» یا «غیرمصرح»[۲] یاد می‌شود.[۳] در این صورت، به‌عنوان مثال در نظام حقوقی انگلستان، چنانچه مخاطره سایبری، سبب نزدیک و بی‌واسطه خسارت[۴] قلمداد شود، خسارات ناشی از آن را می‌توان تحت پوشش بیمه‌ای محسوب کرد و قابل جبران دانست.[۵] برای مثال، مفروض است محموله کانتینری حاوی تلفن‌های همراه که تحت پوشش بیمه‌ای «بند الف شروط محموله مؤسسه‌ای (آی‌سی‌سی) سال ۲۰۰۹»[۶] قرار گرفته، از چین به بریتانیا در حال حمل است. در همین حین، هکرها در یکی از بنادری که برای انتقال محموله از کشتی به کشتی دیگر معین شده[۷] و دارای دستگاه ردیابی کانتینر رایانه‌ای است، از طریق نصب دستگاه‌های ضبط رمز عبور،[۸] محموله را شناسایی، و با نفوذ در سامانه فناوری اطلاعات ترمینال کانتینری و نصب کدهای ارسال جدید،[۹] آن را به مقصدِ دلخواه خود هدایت نمایند. در این صورت، ادعای بیمه‌گذار برای دریافت خسارت ناشی از چنین انحراف مسیری، احتمالاً موفقیت‌آمیز خواهد بود، زیرا مخاطره سایبری سبب نزدیک و بی‌واسطه خسارت محسوب می‌شود.

البته باید به این موضوع توجه داشت که چنانچه در یک بیمه‌نامه معمول، که نسبت به پوشش مخاطره سایبری مسکوت است، خطر سایبری باعث اِعمال یکی از شروط استثنای مندرج در بیمه‌نامه شود، خسارت ناشی از آن مخاطره، قابل پرداخت نخواهد بود.

برای مثال، تصور کنید در چارچوب بیمه‌نامه بدنه و ماشین‌آلاتی که پوشش بیمه‌ای در برابر خطرات دریایی ارائه می‌کند (مانند شروط بدنه مؤسسه‌ای تایم سال ۱۹۹۵)،[۱۰] کشتی بیمه‌شده به‌علت وجود نقص

1. Marine Hull & Machinery Insurance
2. Silent Cyber Risk
3. McKenzie, Alicia. **Cyber Risks, Potential Liabilities and Insurance Responses in the Marine Sector**, Ph.D. Dissertation: Swansea University. 2022. p.84.
4. The Proximate Cause
5. Gürses, Özlem, **Marine Insurance Law**, United Kingdom: Routledge. 2023. p.205.
6. Institute Cargo Clauses (ICC) 2009 (A)
7. Transshipment
8. Password Capture Devices
9. New dispatch codes
10. Institute Time Clauses Hulls (ITCH) (1995)

در «نمودار الکترونیکی و سامانه اطلاعات»، قادر به شناسایی سایر کشتی‌ها نباشد و با کشتی دیگری که مطابق با قوانین و مقررات در لنگرگاه قرار داشته، تصادم کند، سپس، معلوم شود که علت چنین نقصی، کد یا نرم‌افزار مخربی بوده است که از روی سوءنیت، توسط رقیب تجاری شرکت مالک کشتی روی سامانه رایانه‌ای کشتی بارگذاری شده است، در این مثال، باتوجه‌به اینکه بند ۲۶ شروط بدنه مؤسسه‌ای تایم تصریح می‌کند که این بیمه‌نامه، «فقدان، خسارت، مسئولیت یا هزینه‌هایی را که بر اثر اَعمال از روی سوءنیت[1] اشخاص یا با انگیزه سیاسی صورت گرفته است» تحت پوشش بیمه‌ای قرار نمی‌دهد، اگرچه مخاطره سایبری سبب نزدیک و بی‌واسطه خسارت بوده، ازآنجاکه این مخاطره از پوشش بیمه‌ای مستثنا می‌گردد، خسارت ناشی از آن نیز قابل جبران نخواهد بود.

۴.۲. استثنای مخاطرات سایبری دریایی

بیشتر بیمه‌نامه‌های مرسوم دریایی به‌صراحت، خسارات ناشی از مخاطرات سایبری را از شمول مخاطرات تحت پوشش مستثنا می‌نمایند. بنابراین اگر خسارت به‌واسطه مخاطره سایبری مندرج در شرط ایجاد شود، بیمه‌گر مسئولیتی نخواهد داشت. دراین‌خصوص رابطه سببیت نقش بسیار حیاتی ایفا می‌کند؛ یعنی بیمه‌گر تنها زمانی مسئولیتی ندارد که ریسک سایبری، سبب نزدیک و بی‌واسطه حدوث خسارت باشد.[2]

در بازار بیمه لندن، نمونه‌های متعددی از شروط استثنا مخاطرات سایبری وجود دارند. ازجمله آنها می‌توان به‌شرط مربوط به «مستثنا ساختن حملات سایبری مؤسسه» معروف به (سی‌اِل ۳۸۰) سال ۲۰۰۳[3] و شروط مستثنا ساختن فقدان ناشی از مخاطرات سایبری انجمن بین‌المللی بیمه‌گران لندن (۲۰۱۹)[4] اشاره نمود. از آنجایی که شرط استثنای سی‌اِل ۳۸۰ مهم‌ترین شرط استثنا مرتبط با مخاطرات سایبری در زمینه حمل‌ونقل دریایی است، لذا به بررسی آن می‌پردازیم.

به‌موجب (سی‌اِل ۳۸۰):

«این بیمه به‌هیچ‌وجه فقدان، خسارت، مسئولیت یا هزینه‌ای را که به‌طور مستقیم یا غیرمستقیم به‌واسطه استفاده یا راهبری رایانه، سامانه رایانه‌ای، نرم‌افزار رایانه‌ای، کد مخرب، ویروس یا پردازش یا

1. Malicious
2. Soyer, Barış. *Warranties in Marine insurance*, London: Routledge-Cavendish. 2016. pp. 46-47.
3. The Institute Cyber Attack Exclusion Clause – Cl. 380.
4. IUA Cyber Loss Exclusion Clauses (IUA 09-081 / IUA 09-082) (2019).

هر سامانه الکترونیکی دیگری، به‌عنوان ابزاری جهت وارد کردن آسیب، حادث شود، تحت پوشش قرار نمی‌دهد».[1]

اگرچه این شرط تاکنون محل اختلاف حقوقی نبوده و بدین سبب تحت تفسیر قضایی قرار نگرفته است، با به‌کارگیری اصول عام تفسیر، به‌راحتی می‌توان به این نتیجه رسید که گستره این شرط استثنا بسیار عام است؛ چراکه اسباب ایجاد رابطه سببیت[2] که با استفاده از عبارت «به‌طور مستقیم یا غیرمستقیم به‌واسطه استفاده یا راهبری» تعیین شده‌اند، این قابلیت را دارند که دامنه این شرط را به میزان قابل‌توجهی گسترش دهند.[3] در واقع، به‌موجب این شرط، احراز هرگونه رابطه سببیت بین خسارت و استفاده از رایانه یا عملیات رایانه‌ای، سامانه رایانه‌ای، نرم‌افزار رایانه‌ای، کد مخرب، ویروس یا پردازش یا هر سامانه الکترونیکی دیگری، برای مستثنا ساختن مسئولیت بیمه‌گر کافی است؛ حتی اگر این ارتباط در سیر عادی امور چندان منطقی به نظر نرسد و منجر به نتایج غیرمعقول گردد.[4]

با طرح مثالی می‌توان بهتر به اثر سوء چنین شرط بی‌حدومرزی پی‌برد. اگرچه، معمولاً مخاطرات دریایی ازجمله زمین‌گیر شدن کشتی، در اکثر بیمه‌نامه‌های بدنه و ماشین‌آلات تحت پوشش قرار می‌گیرند، در فرضی‌که یک هکر غیرحرفه‌ای بدافزاری را به‌طور تصادفی و بدون قصدِ وارد ساختن خسارت به کشتی یا محموله موضوع بیمه، ایجاد و منتشر نماید و این بدافزار در نتیجه انتشار و گردش، به‌طور اتفاقی منجر به اختلال «نمودار الکترونیکی و سامانه اطلاعات» کشتی موضوع بیمه و در نهایت زمین‌گیری آن شود، بیمه‌گر می‌تواند با استناد به‌شرط مزبور، خود را از مسئولیت برهاند. بنابراین، اگر این تحلیل درست باشد، دامنه سی‌ال ۳۸۰ به‌قدری گسترده می‌شود که گنجاندن آن در بیمه‌نامه، حتی می‌تواند کاربرد بیمه‌نامه‌های دریایی مرسوم را نیز متأثر سازد یا استفاده از آنها را بی‌فایده نماید.

آثار سوء شرط سی‌ال ۳۸۰ باعث شده است تا شرط جدیدی با عنوان «بیمه بدنه سی‌ال ۳۸۰ اصلاح‌شده»[5] ارائه شود. به‌موجب این شرط اصلاحی:

1. International Underwriting Association, "Institute Cyber Attack Exclusion Clause" (IUA, 10 November 2003). Available at: www.iua.co.uk/IUA_Member/Clauses/IUA_Member/Clauses/eLibrary/Clauses.aspx?hkey=6f7dd1a36ab34b10-94c2-5a8c644b1c32 (last visited on: 09/05/2022).
2. Causation Triggers
3. Coxe v. Employers' Liability Assurance Corp Ltd, [1916] 2 KB 629. Available at: https://casetext.com/case/cox-v-emps-liability-assur-corp-et-al (last visited on: 24/07/2022).
4. Tektrol Ltd v International Insurance Co of Hanover Ltd [2005] EWCA Civ 845; [2006] 1 All ER 780 (Comm Ct). Available at: https://www.i-law.com/ilaw/doc/view.htm?id=153089 (last visited on: 28/07/2022).
5. CL380 Hull amended 2019.

«درصورتی‌که این شرط به بیمه‌نامه‌هایی که مخاطرات دریایی را تحت پوشش قرار می‌دهند، الحاق شود، بند ۱,۱ موجب مستثنا شدن فقدان یا خسارت یا هزینه‌های ناشی از:... مخاطرات دریا،...، آتش‌سوزی یا انفجار،...، غفلت فرمانده، افسر، خدمه و نیز جبران خسارت ناشی از تصادم نخواهد شد».

بنابراین، پس از الحاق این شرط به قرارداد، مخاطرات معمول دریا، حتی در فرض مداخله رایانه و سامانه‌های رایانه‌ای در بروز آنها، تحت پوشش بیمه‌ای قرار می‌گیرند.[1]

۵. ابزارهای تعیین و مدیریت ریسک در بیمه مخاطرات سایبری دریایی

اغلب بیمه‌گرها به‌دلیل ماهیت مخاطره سایبری و دغدغه‌های ناشی از آن، سعی می‌کنند با درج یک شرط استثنا، خسارات ناشی از این مخاطره را مستثنا سازند. اما چنین رویکردی باتوجه‌به گسترش استفاده از ابزارهای مبتنی‌بر فناوری اطلاعات و تقاضا برای تحت پوشش قرار دادن این خسارات، چندان مطلوب نیست. بنابراین، بیمه‌گرها می‌توانند با استفاده متناسب از ابزارهای تعیین و مدیریت گستره ریسک، پوشش بیمه‌ای مناسبی برای این نوع از مخاطره ارائه دارند. از همین رو در ادامه، «تعهد به افشا و معرفی اطلاعات»[2] و نیز شرط تضمین و تعهد به اعلام افزایش ریسک به‌عنوان مهم‌ترین این ابزارها، مورد بررسی قرار می‌گیرند.

۵.۱. تعهد به افشا و معرفی

به‌دلیل ماهیت معوض قرارداد بیمه و نیز بنیان آن بر حسن‌نیت کامل، برای این‌که بیمه‌گر بتواند ارزیابی درستی نسبت به میزان تعهد خود و عوض آن داشته باشد، لازم است تا بیمه‌گذار طیفی از اطلاعات مرتبط با موضوع بیمه را در اختیار او قرار دهد.

ذیل ماده ۳ قانون بیمه ۲۰۱۵ انگلستان، بیمه‌گر موظف است به‌طور منصفانه، ریسک موضوع بیمه را نزد بیمه‌گر معرفی نماید. فی‌الواقع به‌موجب این تعهد، بیمه‌گر باید تمام اطلاعات مرتبط با ریسک را که «نسبت به آن آگاه بوده یا آگاه فرض می‌شود» افشا دارد. شق دیگری از این تعهد را می‌توان در قوانین بیمه سایر کشورها ازجمله قانون بیمه ۱۳۱۶ ایران نیز یافت.[3]

1. Mukherjee, Proshanto K., Maximo Q. Mejia, Jr., and Jingjing Xu., **Maritime Law in Motion. Part: Soyer, Barış. Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems**, Switzerland: Springer. 2020. p. 640.
2. Duty of Disclosure
۳. مواد ۱۲ و ۱۳ قانون بیمه ایران.

اطلاعات سایبری‌ای که بیمه‌گذار در حمل‌ونقل دریایی، متعهد به افشای آن در زمان انعقاد قرارداد به بیمه‌گر است، شامل این موارد است: اطلاعاتی که به آنها عالم بوده یا موظف به آگاهی از آنها فرض می‌شود و همچنین اطلاعاتی که با انجام جست‌وجوی متعارف می‌توان به آنها پی برد. بنابراین، بیمه‌گذار باید در راستای عمل به تعهد خود دراین‌خصوص، هر گونه عدم کفایت ظاهری و اساسی موجود در تجهیزات و ترتیبات امنیت سایبری و نیز نقض موارد مقرر در دستورالعمل صادره توسط سازمان بین‌المللی دریانوردی در خصوص مدیریت مخاطرات سایبری دریانوردی[1] و کد مدیریت امنیت بین‌المللی[2] را که باید آگاه به آنها باشد، معرفی نماید.

چنانچه بیمه‌گذار تعهد خود را دراین‌خصوص نقض نماید، بسته به قانون حاکم بر قرارداد بیمه، ضمانت اجراهای مختلفی برای آن تعیین شده است. به‌عنوان مثال، به‌موجب قانون بیمه ۲۰۱۵ انگلستان، در فرض نقض این تعهد، بیمه‌گر بسته به عامدانه یا از روی غفلت بودن نقض تعهد ازسوی بیمه‌گذار، از ضمانت اجرای متناسب برخوردار است.[3] چنانچه نقض، عامدانه یا از روی غفلت باشد، بیمه‌گر محق به ابطال قرارداد با اثر به گذشته است و ممکن است محق به مطالبه حق بیمه نیز باشد. اما چنانچه نقض نه عامدانه و نه از روی غفلت باشد، ضمانت اجرای موجود برای بیمه‌گر بسته به میزان غرور او در ورود به رابطه قراردادی متفاوت خواهد بود.[4]

در نظام حقوق بیمه ایران نیز بسته به عمدی یا غیرعمدی بودن عدم افشا و اظهار نکردن اطلاعاتی که باید نزد بیمه‌گر افشا می‌شدند، حسب مورد موجب بطلان قرارداد بیمه (در فرض عمدی بودن آن و تغییر موضوع خطر یا کاستن از اهمیت آن نزد بیمه‌گر)، دریافت اضافه حق بیمه یا فسخ قرارداد (در فرض غیرعمدی بودن عدم اظهار اطلاعات و معلوم شدن این موضوع قبل از حدوث حادثه) و تقلیل خسارت به نسبت وجه بیمه پرداختی (در فرض غیرعمدی بودن عدم اظهار اطلاعات و معلوم شدن این موضوع بعد از حدوث حادثه) می‌گردد.[5]

1. IMO Guidelines - MSC-FAL.1/Circ.3.
2. International Standard for the Safe Management and Operation of Ships (ISM code).
۳. خروشی، عبدالعظیم، حبیب‌الله رحیمی، عباس قاسمی حامد و جلیل مالکی، ««معرفی منصفانه» جایگزین «تعهد به افشا» در بیمه‌های تجاری»، *فصلنامه علمی – پژوهشی پژوهشنامه بیمه*، د. ۳۴، ش. ۲، ۱۳۹۸، ص. ۹۱.
4. Clarke, Malcolm., and Barış Soyer, **The Insurance Act 2015: A new regime for commercial and Marine insurance law**. United Kingdom: Routledge. 2017. pp. 35-36.
۵. بابایی، ایرج، *منبع پیشین*، صص. ۷۷–۸۵.

۵.۲. شرط تضمین و افزایش ریسک مخاطرات سایبری دریایی

نهاد تضمین در نظام حقوق بیمه انگلستان و اغلب نظام‌های حقوقی مبتنی‌بر رویه قضایی و نهاد افزایش یا تغییر ریسک در نظام‌های حقوق بیمه مبتنی‌بر نظام حقوقی نوشته، دو نهادی‌اند که به‌منظور کنترل مدیریت ریسک در اختیار بیمه‌گر قرار گرفته‌اند تا از این طریق همواره تعادل میان دو تعهد متقابل حفظ شود.[۱] مطابق نهاد تضمین، مسئولیت بیمه‌گر منوط به متابعت بیمه‌گذار از تعهداتی است که باید در دوره زمانی خاص یا به‌صورت مستمر رعایت شوند. یکی از بنیادین‌ترین این تعهدات، تعهد بیمه‌گذار مبنی‌بر تضمین قابلیت دریانوردی کشتی[۲] است. براساس این تعهد که مختص بیمه‌نامه‌های سفر معین[۳] است، بیمه‌گذار متعهد است کشتی را در زمان «عزیمت»،[۴] جهت مقابله با مخاطرات دریا مهیا کند.[۵]

امروزه باتوجه‌به استفاده بیش از پیش فناوری اطلاعات در حوزه حمل‌ونقل دریایی و نیز پدیدار گشتن مخاطره سایبری، مفهوم قابلیت دریانوردی نیز دستخوش تغییر شده است و بدین ترتیب «قابلیت سایبری»[۶] کشتی را نیز دربر می‌گیرد. یعنی فقدان، عدم کفایت یا ناکارآمدی تدابیر حفاظتی در برابر اختلالات سایبری در کشتی، منجر به عدم قابلیت دریانوردی کشتی می‌شود.[۷] به‌دلیل صعوبت پیش‌بینی زمان، مکان، منشأ، ماهیت و هدف اختلال سایبری؛ تعیین وظایف بیمه‌گذار برای تمهید قابلیت سایبری کشتی، بسیار دشوار است. برای حل این مشکل باید گفت درصورتی‌که بیمه‌گذار اقدامات ضروری و متعارف را برای مقابله با مخاطره سایبری احتمالی اتخاذ نموده باشد، به تعهد خود دراین‌خصوص عمل نموده است. برای این منظور، لازم است نرم‌افزار یا سخت‌افزار مناسب انتخاب و نصب شود. همچنین، در همین رابطه، همسویی اقدامات بیمه‌گذار با برخی دستورالعمل‌ها ازجمله دستورالعمل سازمان بین‌المللی دریانوردی درخصوص مدیریت ریسک سایبری و دستورالعمل امنیت سایبری بر روی عرشه کشتی[۸] منتشره توسط شورای دریانوردی بین‌المللی و بالتیک، می‌تواند اماره‌ای بر این باشد که بیمه‌گذار به تعهد

---

۱. امینی، منصور و محمدرضا حاذقی اقدم، «تعهد بیمه‌گذار مبنی بر مطلع ساختن بیمه‌گر در فرض افزایش ریسک: مطالعه تطبیقی حقوق بیمه ایران، چین و اصول قراردادهای بیمه اروپا»، *مجله مطالعات حقوقی*، د. ۱۳، ش. ۱، ۱۴۰۰، ص. ۱.

2. Implied Warranty of Seaworthiness

3. The Voyage Policy

4. Sailing

عبارت «عزیمت» در پرونده‌های بیمه دریایی، در معنای جدا شدن از بارانداز و آمادگی برای ورود به دریا، علی‌رغم عدم ترک بندر، به کار رفته است.

5. Tettenborn, Andrew and Barış Soyer. 2020. *Op. cit*. p. 102.

6. Cyberworthiness

7. *Ibid*. p. 106.

8. The Guidelines on Cyber Security Onboard Ships

خود درخصوص تمهید قابلیت دریانوردی و سایبری کشتی عمل نموده است.[۱] گفتنی است که به‌دلیل نسبی بودن مفهوم قابلیت دریانوردی کشتی، تمهید کشتی دارای قابلیت سایبری، الزاماً همواره متضمن استفاده از آخرین و بهترین نسخه نرم‌افزار یا سخت‌افزار نیست.[۲] بنابراین، اگرچه لازم است اقدامات بیمه‌گذار همسو با تحولات این حوزه باشد، کمال‌گرایی دراین‌خصوص خالی از محل اعراب است.[۳]

درخصوص ضمانت اجرای نقض این تعهد ازسوی بیمه‌گذار، خاصه در نظام حقوق بیمه انگلستان، به‌موجب قانون بیمه ۲۰۱۵، درصورت نقض این تعهد از سوی بیمه‌گذار، مسئولیت قراردادی بیمه‌گر از بین نمی‌رود،[۴] بلکه مسئولیت او در دوران نقض به‌حالت تعلیق در می‌آید و به‌محض بازگشت بیمه‌گذار به اجرای تعهد خود، مسئولیت بیمه‌گذار نیز به‌حالت سابق برمی‌گردد.[۵]

اما، همان‌گونه که اشاره شد، در بسیاری از کشورهای تابع نظام حقوقی نوشته، تعهد مزبور و ضمانت اجرای آن در قالب نهاد افزایش ریسک، مقرر شده است.[۶] به‌طور خاص در حقوق ایران نیز ماده ۱۶ قانون بیمه، قواعدی را درخصوص افزایش ریسک مقرر داشته است که به‌موجب آن چنانچه در طول مدت اعتبار قرارداد بیمه، ریسک موضوع تعهد افزایش یابد؛ بیمه‌گذار متعهد است چنین افزایشی را به اطلاع بیمه‌گر برساند. در این صورت، چنانچه بیمه‌گذار حاضر به پرداخت مابه‌التفاوت حق بیمه نباشد، بیمه‌گر می‌تواند قرارداد بیمه را فسخ نماید.[۷] در همین خصوص، باتوجه‌به استفاده از سامانه‌های رایانه‌ای و انواع حسگرها، وضعیت کشتی و محموله به‌طور مستمر پایش شده، متناسب با داده‌های ارسالی این حسگرها اقدامات ناوبری و نگهداری مقتضی، اتخاذ می‌گردند.[۸] بنابراین، اختلالات سایبری حتی اگر منجر به ورود خسارت نشود، ممکن است باعث افزایش در معرض خطر گرفتن کشتی و محموله شوند. شکی نیست که چنین اختلالاتی افزایش ریسک محسوب می‌شود و بدین ترتیب بیمه‌گذار موظف است درصورت جمع

1. Soyer, Barış, and Andrew Tettenborn, **Maritime Liabilities in a Global and Regional Context**, New York: Routledge. 2019. p. 103.
2. Cooke, Julian., Tim Young, and others, **Voyage Charters**, 5th ed. United Kingdom: Routledge, 2022. p. 234.
3. Girvin, Stephen, **Carriage of Goods by Sea**, 3rd ed, Oxford Publication, 2022. p.385.
4. Soyer, Barış, "Risk Control Clauses in Insurance Law-Law Reform and the future", *Cambridge law Journal*, 2016. p. 4.
5. Alastair, Owen, **The Law of Insurance Warranties: Flawed Reform and a New Perspective**, United Kingdom: Routledge, 2021. p.131.
۶. نعیمی، عمران و محمدمهدی صداقت، **حقوق بیمه**، تهران: انتشارات جنگل، ۱۳۹۱، صص. ۱۳۶-۱۳۷.
۷. حاذقی اقدم، محمدرضا، **وارانتی‌ها در بیمه دریایی در نظام حقوقی رومی-ژرمنی**، پایان‌نامه کارشناسی ارشد، تهران: دانشگاه شهید بهشتی، ۱۳۹۷، ص. ۳.
8. Soyer, Barış and Andrew Tettenborn, **Disruptive Technologies, Climate Change and Shipping**, New York: Routledge. 2022. p. 22.

سایر شرایط لازم برای ایجاد این تعهد، هرگونه اختلال سایبری را به اطلاع بیمه‌گر برساند و او نیز قادر است حسب اقتضا نسبت به افزایش حق بیمه یا فسخ قرارداد بیمه اقدام نماید.[1]

نتیجه‌گیری

مقاله حاضر ضمن ارائه شناخت مخاطرات سایبری دریایی، چالش‌های آن و نیز خساراتی که عموماً در این نوع از پوشش‌های بیمه‌ای داخل در تعهدات بیمه‌گر قرار می‌گیرند و چگونگی تطبیق نهادهای موجود درخصوص مدیریت ریسک‌های ناشی از رخدادهای سایبری را تحلیل کرده است. هدف از ارائه چنین تحلیلی آن است که بیمه‌گرها و بیمه‌گذاران با شناخت نحوه اِعمال نهادهای موجود در گستره مخاطرات سایبری، برای ورود به ترتیبات بیمه‌ای سایبری، رغبت پیدا نمایند. با چنین رویکردی اهم یافته‌های مقاله حاضر به شرح ذیل قابل ارائه است:

- درصورت تحصیل پوشش بیمه‌ای مخاطره سایبری دریایی، بیمه‌گر به‌طور پیش‌فرض متعهد خواهد بود هر نوع خسارت وارده که در سیر متعارف امور ناشی از آن مخاطره تلقی و بر موضوع بیمه وارد شود، جبران نماید. در این صورت، بیمه‌گر می‌تواند با استفاده از شرط مربوط به تعیین خسارات تحت پوشش به‌همراه شرط استثنا، گستره تعهد خود را مشخص نماید و براساس آن حق بیمه دریافت کند.
- درصورت عدم تصریح بیمه‌نامه معمول دریایی به پوشش یا استثنای خسارات ناشی از مخاطره سایبری، جز درصورتی‌که خسارات وارده، به‌موجب یکی از شروط استثنا مندرج در قرارداد قابل جبران نباشد، باید خسارات ناشی از چنین مخاطره‌ای را تحت پوشش بیمه‌ای قلمداد نمود و بیمه‌گر را متعهد به جبران آن خسارات دانست.
- بیمه‌گر در اندراج شرط استثنا خسارات ناشی از مخاطره سایبری، باید گستره آن را به‌گونه‌ای تعیین نماید که سایر تعهدات مقرر در پوشش‌های بیمه‌ای معمول دریایی، مشمول چنین شرطی قرار نگیرند.
- برای اینکه بیمه‌گر بتواند در زمان انعقاد بیمه، ارزیابی دقیق‌تری از مخاطره داشته باشد و متناسب با آن حق بیمه تعیین نماید، بیمه‌گذار باید اطلاعاتی درخصوص وضعیت موضوع بیمه ارائه دهد.

1. Jing, Zhen, "Warranties and Doctrine of Alteration of Risk During the Insurance Period: A critical Evaluation of the UK Law Commissions' proposals for reform of the law of warranties", *Insurance Law Journal*, Vol. 25. No. 2, 2014, p.200.

اما به‌دلیل ماهیت ویژه مخاطره سایبری، نمی‌توان از بیمه‌گذار انتظار داشت تمامی جوانب سایبری موضوع بیمه را معرفی نماید. لذا، متعهد دانستن بیمه‌گذار به افشا و معرفی نقض موارد مندرج در دستورالعمل‌ها موجب می‌شود بیمه‌گذار تعهد خود را دراین‌خصوص ایفا نموده باشد و ازسوی دیگر بیمه‌گر نیز تا حد متعارف نسبت به میزان آسیب‌پذیری موضوع بیمه مطلع شود. همچنین، بیمه‌گر می‌تواند با درنظر گرفتن دستورالعمل‌های موجود، فهرستی از اطلاعات لازم‌الاِفشا توسط بیمه‌گذار تهیه نماید و بدین طریق گستره تعهدات خود را معین سازد.

- استفاده از نهادهای شرط تضمین و افزایش ریسک، مخاطرات اخلاقی ناشی از تحصیل پوشش بیمه‌ای مخاطره سایبری دریایی را به میزان قابل توجهی کاهش، و به بیمه‌گر اطمینان می‌دهد که اولاً، بیمه‌گذار تلاش متعارف خود را برای مقابله با مخاطره سایبری متعارف به کار خواهد بست و دوماً، با افزایش احتمال ورود خسارت به‌واسطه اختلال سایبری، حق بیمه متناسب با آن دریافت خواهد نمود.

منابع

کتاب

۱. بابایی، ایرج، **حقوق بیمه**، چ. ۱۴. تهران: سمت، ۱۳۹۶.

۲. نعیمی، عمران و محمدمهدی صداقت، **حقوق بیمه**، تهران: انتشارات جنگل. ۱۳۹۱.

مقاله

۳. امینی، منصور و محمدرضا حاذقی اقدم، «تعهد بیمه‌گذار مبنی بر مطلع ساختن بیمه‌گر در فرض افزایش ریسک: مطالعه تطبیقی حقوق بیمه ایران، چین و اصول قراردادهای بیمه اروپا»، *مجله مطالعات حقوقی*، د. ۱۳، ش. ۱، ۱۴۰۰، صص. ۱–۲۸. کد doi: 10.22099/jls.2020.35815.3719

۴. حسینی، سیده آمنه، محمدرضا زندی و عباس تدین، «بررسی جرم قلدری مجازی در حقوق کیفری ایران و آمریکا»، *پژوهش‌های حقوق تطبیقی*، ش. ۳. ۱۴۰۲. صص. ۷۶–۱۱۲.

۵. خروشی، عبدالعظیم، حبیب‌الله رحیمی، عباس قاسمی حامد و جلیل مالکی، ««معرفی منصفانه» جایگزین «تعهد به افشا» در بیمه‌های تجاری»، *فصلنامه علمی – پژوهشی پژوهش‌نامه بیمه*، د. ۳۴، ش. ۲، ۱۳۹۸، صص. ۸۸–۱۰۵. کد doi: 10.22056/ijir.2019.02.05

پایان‌نامه

۶. حاذقی اقدم، محمدرضا، **وارانتی‌ها در بیمه دریایی در نظام حقوقی رومی-ژرمنی**، پایان‌نامه کارشناسی‌ارشد، تهران: دانشگاه شهید بهشتی، ۱۳۹۷.

اسناد

۷. السان، مصطفی، **بیمه فضای مجازی: مفاهیم اساسی و برنامه عملیاتی**، تهران: پژوهشکده بیمه، ۱۳۹۵.

References

Books

1. Alastair, Owen, **The Law of Insurance Warranties: Flawed Reform and a New Perspective**, United Kingdom: Routledge. 2021.
2. Armstrong, Dean., Shyam Thakerar, and Thomas Steward, **Cyber Risks and Insurance: The Legal Principles**, United Kingdom: Bloomsbury Professional. 2021.
3. Babaei, Iraj,. **Insurance Law**. 14th Edition, Tehran: SAMT, 2017. (in persian)
4. Clarke, Malcolm., and Barış Soyer, **The Insurance Act 2015: A new regime for commercial and Marine insurance law**, United Kingdom: Routledge. 2017.
5. Cooke, Julian., Tim Young, and others, **Voyage Charters**, 5th ed. United Kingdom: Routledge. 2022.
6. Dunt, John, **Marine Cargo Insurance**, United Kingdom: Routledge. 2015.
7. Elasan, Mostafa, **Cyber Insurance: Basic Concepts and Action Plan**, Tehran: Insurance Research Center, 2016. (in persian)
8. Girvin, Stephen, **Carriage of Goods by Sea**, 3rd ed. Oxford Publication. 2022.
9. Gürses, Özlem, **Marine Insurance Law**, United Kingdom: Routledge. 2023.
10. Marano, Pierpaolo, and Kyriaki Noussia, **InsurTech: A Legal and Regulatory View**, Vol. 1. Switzerland: Springer. 2019.
11. Marano, Pierpaolo, Ioannis Rokas, and Peter Kochenburger, **Dematerialized Insurance: Distance Selling and Cyber Risks from an International Perspective**, Switzerland: Springer International Publishing. 2016.
12. Mukherjee, Proshanto K., Maximo Q. Mejia, Jr., and Jingjing Xu., **Maritime Law in Motion. Part: Soyer, Barış. Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems**, Switzerland: Springer. 2020.
13. Naeimi, Omran, and Mohammad Mahdi Sedaghat, **Insurance Law**, Tehran: Jangal Publications, 2012. (in persian)
14. Soyer, Barış and Andrew Tettenborn, **Disruptive Technologies, Climate Change and Shipping**, New York: Routledge. 2022.
15. Soyer, Barış, and Andrew Tettenborn, **Maritime Liabilities in a Global and Regional Context**, New York: Routledge. 2019.
16. Soyer, Barış, **Warranties in Marine insurance**, London: Routledge-Cavendish. 2016.
17. Sözer, Bülent, **Unmanned Ships and the Law**, United Kingdom: Routledage, 2023.

18. Tettenborn, Andrew and Barış Soyer. **Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector**, United Kingdom: Routledge. 2020.

Articles

19. Amini, Mansour, and Mohammad Reza Hazaghi Aghdam, "The Insured's Post-Contract Duty of Notification of Increase of Risk: Comparative study in Iranian, Chinese insurance law and principles of European insurance contracts", *Journal of Legal Studies*, 2021, Vol. 13, No.1, pp. 1-28. (in persian). doi: 10.22099/jls.2020.35815.3719.
20. Hoseini, Seyedeh Ameneh, Mohammad Reza Zandi, and Abbas Tadian, "Examining the Crime of Cyberbullying in Iranian and American Criminal Law", Comparative Law Researches, 2023, Issue 3, p. 93. (in persian)
21. Jing, Zhen, "Warranties and Doctrine of Alteration of Risk During the Insurance Period: A critical Evaluation of the UK Law Commissions' proposals for reform of the law of warranties", *Insurance Law Journal*, Vol. 25. No. 2, 2014. pp. 183-209.
22. Khoroushi, Abdolazim, Habibollah Rahimi, Abbas Ghasemi Hamed, and Jalil Maleki, "Fair Presentation as a Replacement for the Duty of Disclosure in Commercial Insurance", *Insurance Research Quarterly*, Vol. 34,No. 2, 2019, pp. 88-105. (in persian). doi: 10.22056/ijir.2019.02.05.
23. Reetz, Margaret A., Lauren B. Prunty, Gregory S. Mantych, and David J. Hommel, "Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law", *Penn State Law Review*, Vole 122. Issue 3. 2018. pp. 727-762. Available at: http://www.pennstatelawreview.org/wp-content/uploads/2018/07/Symposium-Reetz-et-al.pdf (last visited on 09/08/2022).
24. Soyer, Barış, "Risk Control Clauses in Insurance Law-Law Reform and the Future", *Cambridge law Journal*, 2016. pp 109-127. doi:10.1017/S0008197315000963.

Theses

25. Davit, Dadiani, **Cyber-security and marine insurance**, PhD dissertation, World Maritime University, 2019.
26. Hazaghi Aghdam, Mohammad Reza, **Warranties in Marine Insurance under Civil Law Systems**, Master's Thesis. Tehran: Shahid Beheshti University, 2018. (in persian)

27. McKenzie, Alicia, **Cyber Risks, Potential Liabilities and Insurance Responses in the Marine Sector**, Ph.D. Dissertation: Swansea University. 2022.

Documents

28. CL380 Hull amended.
29. Guidelines on Maritime Cyber Risk Management, published by the International Maritime Organization (IMO) on 5 July 2017 (MSC-FAL.1/Circ.3). Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf (last visited on 14/07/2022).
30. Institute Cargo Clauses (ICC) 2009 (A).
31. Institute Time Clauses Hulls (ITCH) (1995).
32. International Underwriting Association, "Institute Cyber Attack Exclusion Clause" (IUA, 10 November 2003). Available at: www.iua.co.uk/IUA_Member/Clauses/IUA_Member/Clauses/eLibrary/Clauses.aspx?hkey=6f7dd1a36ab34b10-94c2-5a8c644b1c32 (last visited on: 09/05/2022).
33. IUA Cyber Loss Exclusion Clauses (IUA 09-081 / IUA 09-082) (2019).
34. Lloyd's Market Bulletin Y5258 dated 4 July 2019. Available at: https://www.lloyds.com/news-and-insights/market-communications/market-bulletins (last visited on 30/09/2022).
35. The Guidelines on Cyber Security Onboard Ships.
36. The Institute Cyber Attack Exclusion Clause – Cl. 380.

Cases

37. Coxe v. Employers' Liability Assurance Corp Ltd, [1916] 2 KB 629. Available at: https://casetext.com/case/cox-v-emps-liability-assur-corp-et-al (last visited on: 24/07/2022).
38. De Maurier (Jewels) Ltd v. Bastion Insurance Co Ltd [1967] 2 Lloyd's Rep 550. Available at: https://www.i-law.com/ilaw/doc/view.htm?id=146105 (last visited on: 23/05/2022).
39. MSC Mediterranean Shipping Co SA v. Glencore International AG [2015] EWHC 1989 (Comm); aff'd [2017] EWCA Civ 365. Available at: https://www.i-law.com/ilaw/doc/view.htm?id=377477 (last visited on: 27/05/2022).
40. Tektrol Ltd v International Insurance Co of Hanover Ltd [2005] EWCA Civ 845; [2006] 1 All ER 780 (Comm Ct). Available at: https://www.i-law.com/ilaw/doc/view.htm?id=153089 (last visited on: 28/07/2022).
41. The Australian Agricultural Company v Saunders (1874–75) LR 10 CP 668. Available at: https://vlex.co.uk/vid/the-australian-agricultural-company-803513305 (last visited on 16/05/2022).

Maritime Cyber Risk Insurance: Emerging Issues and Solutions

Mansour Amini*
Maryam Aghasi Javid**

Received: 2025.12.08 Accepted: 2024.12.4

Abstract

Expanding the use of new technologies in the field of maritime transportation and the inevitable interconnection of different sectors has turned cyber risks into one of the serious threats in this domain. Therefore, covering these risks by insurance is assumed necessary. However, since different dimensions of this type of risk are not very clear to insurers; they are hesitant to provide insurance coverage for this type of risk and even try to exclude these risks from common marine insurance by including specific conditions. This ambiguous situation also affects the rights and decisions of insureds. Therefore, it is necessary to become familiar with the concept of marine cyberattacks and damages that are usually covered, the legal status of typical marine insurance covering this kind of the risks, and the legal tools for determining and managing these risks in case they are covered so that the insurer and the insured can more confidently enter into a contractual relationship by learning more about their rights and obligations. Consequently, this article has tried to provide a good basis for covering these risks by providing legal certainty through a new analysis of existing marine insurance legal institutions and the way that these institutions are used, with a descriptive and analytical approach, while providing a comprehension of concepts related to marine cyberattacks and examining the scope of common maritime insurance coverage on cyber risks.

Keywords:

Increase of Risk, Silent Insurance Coverage, Duty of Disclosure, Exclusion Clause, Marine Cyber Risk.

* (PhD Candidate, Faculty of Law, Shahid Beheshti University, Tehran, Iran.
Corresponding Author Email: m_aghasijavid@sbu.ac.ir
** Associate Professor, Faculty of Law, Shahid Beheshti University, Tehran, Iran.