http://doi.org/10.36248/kdps.2020.14.2.215

해상사이버리스크에 관한 영국보험업계의 대응과 시사점

이 현 균·권 오 정*

<차례>

주제어 : 해상사이버리스크, 사이버감항성, 자율운항선박, 인과관계, 사이버 해적, 리스크 관리, 사이버면책조항, 비자발적 사이버 손해담보, 암묵적 사이버 손해담보

<국문초록> 해상기업의 물적설비인 선박을 이용한 해상운송사업에는 여러 가지 위험이 따른다. 과거에는 침몰, 좌초, 충돌 등 해상고유의 위험이 가장 큰 위험요인이었으나, 근래에는 정보통신과 항해기술의 발전에 따라 해상기업도 과거와 다른 형태의 위험인 해상사이버리스크에 직면하게 되었다. 특히 전통적 운영기술에 인터넷 기반의 정보기술이 접목되면서 선박의 항해와 기관의 모니터링, 항해위치기술 분야 등이 해상사이버리스크에 취약한 분야로 대두되었다. 이에 국제해사기구(IMO)에서는 해상사이버리스크의 관리기준을 제정하고 결의안을 통해 회원국들에 적극적인 관심을 촉구하고 있다. 특히 2021년 1월까지 기존의 선박안전관리지침(ISM code)에 해상사이버리스크 관리에 대한 내용을 반영할 것을 요구한다. 국제적인 해운단체와 각국의 선급협회에서는 나름의 해상 사이버 위험관리기준을 작성하고 해운기업을 대상으로 인증서비스를 시작했다. 해상사이버리스크와 관련한 법적 논의는 선박의 감항능력주의의무와 사고발생시 인과관계에 관한 것이 주로 관련된다. 최근에 영국보험업계를 중심으로 과거의 사이버절대면책약관(CL380)에 대한 실효성 문제가 제기되었다. 특히 불특정하고 무차별적인 사이버 공격에 기인하여 발생한 손해에 대해서 각 보험사가 보험보상 여부를 명확히 하도록 기존 약관의 내용을 개선하였다. 결론으로 정부의 관계법령 정비와 더불어 해운업계나 해상보험업계도 임박한 해상사이버리스크에 대해 국제적 관리기준 수용을 포함한 적극적인 대응이 필요하다는 제언을 하였다.

* 제1저자, 고려대학교 법학전문대학원 연구교수, 법학박사. / 교신저자, 삼성화재해상보험 재물해상 언더라이팅파트 수석, 고려대학교 일반대학원 상법전공 박사과정.
- 논문접수일(2020.05.31), 심사개시일(2020.06.11), 게재확정일(2020.06.26)

Ⅰ. 서 론

세계경제포럼(World Economic Forum)에서 2014년에 발간한 보고서에 따르면, 향후 인류 전체에 영향을 주는 5대 위험(Systemic Risk)으로 경제적 위험(Economic Risks), 환경적 위험(Environmental Risks), 지정학적 위험(Geopolitical Risks), 사회적 위험(Societal Risks), 기술적 위험(Technological Risks)을 선정했다.[1] 이 가운데 기술적 위험은 사이버 테러, 사회기반시설의 붕괴, 데이터 손실 등을 포함하며, 앞으로 기술발전에 따라 전 세계 기업과 개인이 입게 될 피해가 점차 커질 것이기 때문에 해커들에 의한 시스템조작 및 컴퓨터 침입 등으로부터 발생하는 이러한 기술적 위험을 잘 대응하는 것이 매우 중요한 과제라고 지적했다.[2]

시대의 발전에 따라 해운기업들도 사업운영의 안정성 및 효율성 확보를 위해 자율운항선박, e-navigation 시스템, 스마트항만 등 정보통신(IT)분야의 신기술 도입을 경영전반에 걸쳐 적극적으로 논의하고 있는데, 새로운 기술이 도입될수록 이러한 기술적 위험, 사이버리스크에 대한 중요성이 높아질 것이다.[3]

우리나라 국제적 무역거래는 해운산업에 크게 의존하고 있기 때문에 해운분야에서의 사이버리스크에 대한 논의는 매우 중요하다.[4] 오랜 역사를 가진 해운산업은 해상환경 자체의 고위험 요인에도 불구하고 전통적인 항해기술과 계약방식에 따른 보수적 사업운영을 통해 화주 등 고객에게 지속적이고 안정적인 물류서비스를 제공해왔다. 그러나 새로운 기술의 도입은 필연적으로 과거에 경험하지 못한 새로운 사업적, 법률적 리스크를 수반하고, 때로는 해운산업의 신뢰성을 위협하는 핵심요인으로 대두된다. 따라서 해운기업들이 직면하게 될 대표적 위험 가운데 하나인 '해상사이버리스크'에 대한 대비는 앞으로 반드시 해야 할 중요한

1) World Economic Forum,「Global Risks 2014」9th Edition, 2014, p.12.

2) Ibid, pp.12~13.

3) 이현균, "자율운항선박의 운항 관련 책임에 대한 연구", 고려대학교 법학박사학위논문, 2018, 111~114면.

4) 국토교통부의 통계에 따르면 수송량 기준으로 해운은 13.1억톤으로 우리나라 전체 국제수송량의 99.7%를 차지한다. KOSIS (국토교통부, 교통부문수송실적보고), 2019.4.17., <http://kosis.kr/statHtml/statHtml.do?orgId=116&tblId=DT_MLTM_662>, (최종검색일: 20년 5월 18일).

선결과제 중 하나이다.

특히, 자율운항선박이 상용화되면 사이버리스크의 중요성은 더욱 부각될 것인데, 현재의 사이버리스크에 대응은 기술발전에 비해 부족한 상태여서 자율운항선박의 상용화 이전에 사이버리스크에 대한 대응도 선결되어야 할 것이라고 생각된다.[5]

이 논문에서는 해상사이버리스크에 대한 기존의 논의를 살펴보고, 관련된 법적 쟁점에 대해 논의하고자 한다. 또한, 영국 보험업계의 대응을 통해서 시사점을 도출하고자 한다.

Ⅱ. 해상사이버리스크의 개념과 현황

1. 해상사이버리스크의 개념

해상기업의 물적 설비인 선박은 여러 부분에서 사이버 공격의 대상이 될 수 있다. 일반적으로 선박은 해상에 고립되어 물리적인 접근이 제한적이므로 전통적인 운용기술(Operational Technology) 기반 중심으로 운영되었다. 항해 중인 선박의 고립성이나 기술적 제한성이 육상의 산업에 비해 사이버 공격의 대상으로 적합하지 않은 측면이 있다. 그러나 선박에서 정보통신기술(Information Technology)와 운용기술(Operational Technology)시스템이 통합되고 인터넷을 통해 연결되면서 해상사이버리스크의 가능성은 급속도로 증가하였다.[6]

국제해사기구(IMO)는 해상사이버리스크(maritime cyber risk)를 '기술 자산이 잠재적 상황이나 사건에 의해 위협을 받을 수 있는 것으로서, 정보 혹은 시스템이 손상, 손실 혹은 훼손된 결과 그것이 해운과 관련된 사업운영, 안전 혹은 보안의 실패를 초래하는 것'으로 정의한다.[7] 해운을 포함한 물류분야는 복잡한 업무 프

5) 이현균, 전게논문, 112면.

6) OT(operational technology) 시스템은 주로 물리적인 환경을 통제하며, IT(Information technology)시스템은 데이터를 운영한다. OT는 물리적인 설비와 절차를 직접 모니터하거나 통제하는 하드웨어 혹은 소프트웨어를 말한다. 반면 IT는 정보처리에 관한 다양한 기술 즉, 소프트웨어, 하드웨어, 통신기술 등을 포함한다. 원래 OT와 IT는 구분되는 개념이었으나, 인터넷의 활용도가 높아지면서 별개로 운영되던 시스템이 통합되고 OT와 IT는 점차 그 경계가 모호해지고 있다. (BIMCO et al, "The Guidelines on cyber security onboard ships", ver 3, 2018, p.5).

로세스를 통해 다양한 이해관계자들과의 협력이 필요하므로 정보기술 도입에 따른 효율성 제고의 효과를 크게 기대할 수 있는 분야이다. 그러나 동시에 그러한 해운물류의 특성상 선박소유자 등 해운기업은 해상에서 운항중인 개별 선박과의 내부적 운영정보의 교환뿐만 아니라 운송단계별로 화주, 운송인주선인, 항만운영자, 창고관리자, 세관 등 다양한 분야에서 외부적인 의사소통이 필요하다. 이러한 과정에서 필연적으로 사이버 보안의 취약점이 노출된다. 통상 해운기업들이 사이버 공격을 받았더라도 원격지인 해상에서의 피해는 잘 드러나지 않으며, 평판관리 등을 고려하여 피해사실이 공개되는 것을 꺼린다.

2. 사이버공격 취약 분야와 최근 사례

(1) 영국 런던보험시장협회가 선정한 취약 분야

영국 런던보험시장협회 합동선박보험위원회(Joint Hull Committee)의 보고서에 따르면 선박에서 새로이 도입된 기술 중 사이버 공격의 대상이 될 가능성이 높은 분야는 다음과 같다.[8]

① 통신시스템

위성이나 4G, 5G 혹은 Wi-Fi를 통한 통신은 다양한 측면에서 사이버리스크에 노출되어 있다. 비록 쉽지는 않으나 사이버 공격자들은 위성통신의 보안경계를 허물어뜨릴 수 있는 특별한 지식과 기술을 가지고 있을 가능성이 높다.

② 자산추적시스템(Asset Tracking system)

GPS의 응용분야중 하나인 자산추적시스템은 고액화물의 이동을 추적한다. 알려진 사례 중 하나는 선적된 고급 도난차량에 부착된 전파방해기(jammer)에 의

7) "Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised." (Section 1.1. "GUIDELINES ON MARITIME CYBER RISK MANAGEMENT", MSC-FAL.1/Circ.3, IMO, 2017.7.5.).

8) Joint Hull Committee, "Cyber Risks", Joint Hull Cyber Rusk Information paper, 2015, p.19-21. LMA 홈페이지<https://www.lmalloyds.com/lma/underwriting/marine/JHC/JH_Circulars/JHC_Circulars/JHC_Cyber_Info_Paper.aspx>, (최종검색일 : 20년 6월 18일).

해 선박의 GPS 서비스가 거부된 경우가 있다. 현대의 선박은 그 안전운항에 관하여 GPS에 의존하는 경향이 매우 높다.[9]

③ 클라우드 컴퓨팅

클라우드 시스템을 활용하기 위해서는 충분한 데이터 통신 속도가 확보되고 접속지연이 없는 인터넷 연결이 항상 보장되어 있어야 한다. 수많은 기업들이 대규모 클라우드 서버에 데이터를 저장하고 있으므로, 이론적으로 해커들은 하나의 공격으로 대규모 정보를 확보할 수 있다. 선박에서의 클라우드 컴퓨팅으로 인한 리스크는 육상에서의 그것과 다르지 않다.

④ 상태 모니터링

현대식 선박에서는 선체와 기관의 효율을 높이고 사용연한을 개선하기 위해 자동화된 모니터링 시스템이 개입하여 온도, 압력, 유속, 연료와 오일의 상태 등을 지속적으로 측정하고 평가한다. 만일 모니터링 시스템이 적절히 설치, 운용되지 않는다면 엔진이나 평형수 통제 등과 같은 중요한 시스템에 침입자들에게 뒷문(back door)를 열어주는 결과를 가져올 수도 있다.

⑤ 사물인터넷(Internet of Things)

사물인터넷 기술은 모든 장비에 관한 정보를 상호 공유하고 원격 조정할 수 있도록 해준다. 원격으로 조정되는 선내 시스템이 사물인터넷으로 연결되면 운용상 보안문제에 노출될 수 있다.

⑥ 자동항해장비(E-navigation)

국제해사기구(IMO)에서 주도하고 있는 e-Navigation은 차세대 해상항법체계로서 선박과 육상에서 해상 관련 정보를 수집, 통합, 교환, 표현 및 분석하는 전자시스템이다. 운항 및 관련 서비스의 품질향상을 통해 해상에서의 안전과 보안을

9) 2016년 4월, 북한의 위성항법장치(GPS) 전파 교란으로 국내 항공기와 선박 110대가 영향을 받은 것으로 보도되었다. 해당 항공기와 선박은 GPS를 보조 항법 장치로 사용하거나 다른 대체 장비가 있어 운항 차질 등 실질적 피해는 없었다고 알려졌다. (연합뉴스, "北 GPS 교란에 항공기·선박 110대 영향…피해는 없어", 연합뉴스 2016년 4월 1일자 기사<https://www.yna.co.kr/view/AKR20160401061900017>, (최종검색일 : 20년 6월 18일).

증진하고 해양환경을 보호하는 것이 e-Navigation의 목적이다.[10] 크게 5가지 선박 분야에 대한 개선을 목표로 하는데 선교의 구성, 자동 보고, 선교장비와 항해정보의 통합, 도형화된 정보표시, VTS서비스 개선 등이다.[11] 그러나 사이버 보안 측면에서는 e-Navigation에서 추구하는 확장된 범위의 통신시스템은 사이버 공격에 더 취약하게 할 수도 있다.

⑦ 자율운항선박

국제해사기구(IMO)는 2018년 제99차 해사안전위원회(MSC)에서 자율운항선박(Maritime Autonomous Surface Ship)을 "다양한 수준의 자율단계에서 사람의 간섭 없이 독립적으로 작동할 수 있는 선박"으로 정의했다.[12] 이는 정보통신기술을 바탕으로 인공지능, 사물인터넷, 빅데이터 기술 등을 활용해 선박의 상태와 운항정보를 육상에서 실시간으로 모니터링하고 선박 내 통합시스템을 원격 진단 및 제어하며 각종 선박 기자재들을 통합 관리하는 체계라고 할 수 있다. 2019년 국제해사기구의 제101차 해사안전위원회에서는 자율운항선박의 시험운항과 관련하여 그 시스템과 기반설비가 안전하게 운영되고 환경보호에 적절한 주의를 기울이도록

10) E-navigation is defined as "the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment." The e-navigation Strategy Implementation Plan (SIP), which was approved by MSC 94 in November 2014, contains a list of tasks required to be conducted in order to address 5 prioritized e-navigation solutions, namely: (1) improved, harmonized and user-friendly bridge design; (2) means for standardized and automated reporting; (3) improved reliability, resilience and integrity of bridge equipment and navigation information; (4) integration and presentation of available information in graphical displays received via communication equipment; and (5) improved Communication of VTS Service Portfolio (not limited to VTS stations). IMO 홈페이지 <http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx>, (최종검색일 : 20년 6월 18일.).

11) 한국형 e-Navigation 사업(SMART-Navigation)은 2020년 말까지 우리나라 해상 환경에 특화된 e-Navigation으로 국제해사기구(IMO)의 e-Navigation 개념에 어선,연안 소형선 대상 서비스 제공 등을 추가하여 우리나라 해상 환경에 최적화된 새로운 시스템을 구현하려는 목적으로 진행되고 있다. 해역상황인지, 선제적 해양안전 확보, 해상 교통 최적화, 해상 디지털 무선통신 등의 서비스를 제공할 예정이라고 한다. 한국형 e-Navigation 사업단 홈페이지<http://www.smart-navigation.org/html/SMART-Navigation_New/about_smart_navigation.php>, (최종검색일 : 20년 6월 18일.).

12) IMO 홈페이지<http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx>, (최종검색일 : 20년 6월 19일). 한편 자율운항선박을 지칭하는 용어도 무인선박, 스마트선박, 원격조정선박, 자동화선박, 자율항해선박 등 여러 가지로 사용되고 있는데, 이는 자율운항선박의 실현방식에 대한 서로 다른 개념을 반영한 것으로 여겨진다(이현균, 전게논문, 20~21면).

하는 '잠정' 가이드라인을 발표했다(MSC.1/Circ.1604). 자율운항선박의 시험운행에 있어 시스템과 기반설비는 해상사이버리스크에 충분히 대비할 수 있도록 하는 적절한 조치를 취하도록 규정하고 있다(2.10조).[13]

(2) 최근 해상분야에서 발생한 사이버리스크 관련 사례

다음의 몇 가지 사례는 해상분야에서 공개된 최근의 사이버리스크 관련 사고 사례이다.

① World Fuel Service(WFS)

2013년에 세계적인 선박연료유 공급사인 WFS는 미화 1,800만 달러에 달하는 연료유 사기사건의 희생자가 되었다. 범인들은 미국방부 조달국을 사칭하여 가짜 연료유 입찰경쟁을 시행하였고, WFS는 이에 따라 아이보리코스트 연안에 정박되어 있던 유조선에 연료유를 공급했다. 이후 WFS는 미국방부에 약 1,800만 달러의 연료대금 청구서를 제출하였으나 미 조달국에는 그러한 입찰을 시행한 기록이 없음을 알게 되었다.[14]

② AP Moeller Maersk

2017년 6월, 세계최대의 선사인 Maersk 해운은 그들의 전산시스템이 전세계적인 랜섬웨어인 'NotPetya' 사이버공격에 피해를 입었으며 그로 인해 주문처리와 화물운송에 지연이 발생했음을 발표하였다. 해당 공격으로 인해 Maersk 그룹에 속한 APM terminal의 미국, 인도, 스페인, 네덜란드 소재 76개 항만에서 화물처리 지체가 발생하였으며 알려진 손실 규모는 약 3억불에 달한다.[15]

---

13) IMO, "Interim Guidelines for MASS Trials", MSC.1/Circ.1604
2.10 Cyber risk management
Appropriate steps should be taken to ensure sufficient cyber risk management of the systems and infrastructure used when conducting MASS trials.

14) Ship & Bunker world news, "WFS in court over $18M bunker scam claim"(2014.10.13.)
Ship & Bunker world news 홈페이지<https://shipandbunker.com/news/world/670152-wfs-in-court-over-18m-bunker-scam-claim>, (최종검색일: 20년 6월 18일).

15) Reuters, "Cyber attack hits shipper Maersk, causes cargo delays"(2017.6.28.)
Reuters 홈페이지<https://www.reuters.com/article/us-cyber-attack-maersk/cyber-attack-hits-shipper-maersk-causes-cargo-delays-idUSKBN19J0QB>, (최종검색일: 20년 6월 21일).

③ COSCO Shipping

2018년 7월, 중국 국영선사인 COSCO 해운의 북미 롱비치항 Pier J terminal 항만운영관련 홈페이지와 이메일 시스템의 수 일간 불능을 초래한 랜섬웨어 공격이 있었다. COSCO는 선박운영 및 다른 사업분야에는 영향이 없다고 밝혔다.[16]

④ 사이버 선박탈취 시도

2019년 2월, 한 무리의 해커들이 미국 뉴욕과 뉴저지항으로 향하던 선박을 시스템적으로 원격 탈취하려는 시도가 있었다. 비록 해커들이 핵심적인 운항시스템 통제에는 실패하였으나 미정부의 관계기관은 해당 선박이 사이버 보안에 대한 적절한 대응 방안을 갖추고 운항했는지에 대한 조사를 벌였다.[17]

⑤ 한국선사 선박 수척 랜섬웨어 피해

2019년 3월, 국내 H선사는 자동차운반선과 벌크선을 포함 선박 90여척을 운용하는 선사로, 선단 소속 일부 선박이 랜섬웨어에 감염돼 선내 메인컴퓨터가 잠기는 피해가 발생했다. 선박에 배포된 메일은 경찰청을 사칭했으며, 첨부된 파일을 내려받아 열면 감염이 진행되는 것으로 전해졌다. 감염된 선박들은 불가피하게 해당 컴퓨터를 포맷하고 손실된 자료를 처음부터 재작성한 것으로 알려졌다. 선내 컴퓨터가 랜섬웨어에 감염돼 마비되면 본사는 물론 항만당국이나 현지 업체 등과 소통이 어렵기 때문에 운항에 심각한 차질을 초래하였을 가능성도 있었다.[18]

16) Wall Street Journal, “China’s Cosco Shipping Hit by Cyberattack in U.S.”(2018.7.25.), Wall Street Journal 홈페이지<https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557>, (최종검색일: 20년 6월 21일).

17) Wall Street Journal, “U.S. Coast Guard Warns Shipping Industry on Cybersecurity”(2019.6.11.) Wall Street Journal 홈페이지<https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402>, (최종검색일: 20년 6월 21일).

18) 파이낸셜뉴스, “한국 유명선사 선박 수척 랜섬웨어 피해...사이버보안 경각심 가져야”, 파이낸셜뉴스 2019년 3월 30일자 기사, <https://www.fnnews.com/news/201903300027281755>, (최종검색일: 20년 6월 21일).

⑥ MSC

2020년 4월, 글로벌 선사인 MSC의 홈페이지 운영이 약 일주일간 중단되었다. 공식적으로는 본사인 스위스 제네바 소재 데이터센터의 네트웍 과부하에 따른 운영불능으로 발표되었으나, 오류의 원인으로 파일에 암호화된 악성소프트웨어의 공격 가능성을 부인하지 않았다. 이로써 회사의 IT 서비스가 중단되었으나 화물 운영은 별도의 대리점 네트웍을 통해 정상적으로 운영되었다.[19]

일반적으로 사이버공격에 따른 피해의 형태는 우선 사업중단에 따른 이익상실, 보석금, 컴퓨터 복구비용 등의 금전손실, 기업 평판손실 등이 있다. 해운산업에 고유한 사이버 리스크의 유형은 랜섬웨어, 화물취급시스템 오류에 따른 오배송 및 도난, 해적위험, 데이터 도난, 상업적 경쟁자에 의한 파괴행위, 정치적 공격, 감독당국의 벌과금, 선급유지 문제 등이 있다.[20] 조직화된 사이버 공격으로 인해 15개 아시아지역 항만에 미치는 경제적 손실은 최소 408억불에서 최대 1,098억불에 달하는 것으로 추정된다.[21]

3. 사이버리스크 관리 방안에 대한 국제적인 논의

위에서 살펴본 바와 같이 최근에 알려진 해상관련 사이버보안사고와 관련하여 해상기업들의 해상사이버리스크 관리방안에 대한 관심이 높아지고 있다. 그러나 사이버 보안이 이슈가 되기 이전에 도입된 오래된 선박과 같은 낡은 하드웨어에 새로운 소프트웨어를 업데이트하는 것이 현실적으로 어려운 경우가 많다.[22] 또한 새로운 기술에 익숙하지 않은 선원들은 선박에 대한 악의적 혹은 무차별적인 대규모 사이버 공격의 심각성을 인식하는 것이 어려울 수도 있다.

---

19) Lloyd's List, "MSC shutdown throws spotlight on cyber security" (2020.4.16.) p.5.

20) Simon Cooper, "Cyber Risk, Liabilities and Insurance in the Marine Sector" in Baris Soyer and Andrew Tettenborn(ed.), Maritime Liabilities in a Global and Regional Context, informa law from Routledge, 2019, pp.103-105.

21) 보험산업에서 사이버 손해로 인해 지급가능한 보험금 규모는 36억불에서 최대 83억불로 추정했으며, 기업휴지(BI) 혹은 간접기업휴지(contingent BI)를 주된 담보형태가 될 것이며, 특히 비자발적인 사이버(Non-affirmative cyber)피해가 전체 보험손해의 57% 내지 62%로 대부분을 차지할 것으로 추정했다. (Cambridge Center for Risk Studied, "Shen attack: Cyber risk in Asia Ports", CyRim_Report 2019, p.6).

22) UN의 2019년 세계상선통계(Merchant fleet by flag of registration and by type of ship (2019.10.31.))에 따르면 재화중량톤수(DWT)기준으로 34.4%의 선박이 20년이상의 고령 선박에 해당된다. 일반선 선종으로만 보면 고령선이 54%에 달한다. UNCTAD 통계 홈페이지<https://unctadstat.unctad.org/wds/ReportFolders/reportFolders.aspx>, (최종검색일: 20년 6월 21일).

그리고 현재 논의되고 있는 자율운항선박의 경우에는 자율운항선박 위치정보를 지속적으로 전달해야 하고, 이 과정에서 선박의 경로 등이 컴퓨터 시스템을 통해 쉽게 노출되어 해킹과 같은 사이버테러나 해적행위에 표적이 되기 쉽다는 문제점이 있다.[23] 만일 자율운항되고 있는 자율운항선박의 위치정보가 제3자에 의해 해킹 등의 방법으로 위법하게 접근된다면 이는 해상에서의 대규모 인명사고를 유발하거나 막대한 재산상 손해 등 큰 재앙을 발생시킬 것이다.[24] 구체적으로 해상운송에 종사하는 자율운항선박이 해킹을 당하는 화물에 직접적인 피해를 입게 되고, 선박의 운항안전에 직접적인 피해를 주어 심한 경우 좌초 및 침몰 등 막대한 피해가 발생할 수 있다.[25]

아래에서는 이러한 피해를 방지하기 위한 해상사이버리스크에 대한 국제해사기구, 발틱국제해운동맹, 국제선급협회 등 기존의 논의를 살펴보고자 한다.

(1) 국제해사기구(IMO)

2017년 6월에 국제해사기구(IMO)의 제98차 해사안전위원회(MSC)는 '국제안전관리규약(International Safety Management Code ; ISM Code)'과 '국제선박 및 항만시설보안규칙(International Ships and Port Facility Security Code ; ISPS Code)'에 해상사이버리스크관리에 관한 결의안을 채택하였다.[26][27] 결의안은 선주, 선급, 항만운영자 등 해운산업의 다양한 이해관계자들이 점차 현실화 되고 있는 해상사이버 위협과 취약성을 인식하고 적극적으로 대처하도록 독려하기 위한 것이다. 결의안에서는 선주와 선박관리회사에 사이버보안 및 위험관리에 관한 사항을 2021년까지 ISM Code[28]에 반영하여 관리 및 운영하도록 하고 있다.[29] ISM code의

23) 이현균, 전게논문, 112면.
24) 이현균, 전게논문, 112면.
25) 최정환/이상일, "상업용 자율운항선박의 법적 쟁점사항에 관한 연구", 「해사법연구」 제28권 제3호, 2016, 314~315면.
26) IMO, "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT", RESOLUTION MSC.428(98) (adopted on 16 June 2017).
27) 이현균, 전게논문, 112면.
28) ISM(International Safety Management) 코드는 국제해사기구(IMO)에서 선박의 안전운항과 환경보호를 목적으로 결의한 해운회사의 안전경영시스템(Safety Management System)에 관한 국제적 표준규격으로 선박의 물리적 안정성 및 선원의 자질 향상뿐만 아니라 해운기업의 육·해상 모든 부서에서 안전관리시스템을 수립하고 시행하도록 국제해상안전인명협약(SOLAS)의 제9장으로 1994년에 채택된 강제협약이다.

강제협약적인 성격을 감안하면 항만안전관리(PSC) 검사시 이와 관련된 사항의 불이행이 확인되면 선박이 억류당할 수도 있다. 동시에 해사안전관리위원회에서는 해상사이버리스크의 위협과 취약성에 대한 인식을 제고하기 위한 긴급한 요구를 고려하여 "해상사이버리스크 위험관리에 관한 가이드라인"을 승인하였다. 가이드라인은 해상사이버리스크 기능적 요소를 아래와 같이 제시하였다.

① 식별(Identify): 사이버 위험관리에 대한 개인의 역할 및 책임을 정의하고 장애가 발생할 수 있는 선박운용시스템, 자산, 데이터 및 기능 등을 식별하는 것 ② 보호(protect): 위험통제 프로세스, 조치 및 비상계획을 수립하여 사이버 사건에 대처하고 해상운송의 연속성 보장하는 것 ③ 탐지(Detect): 적시에 사이버 사건을 탐지하기 위한 프로세스와 방어수단을 개발하고 적용하는 것 ④ 대응(Respond): 사이버 사건으로 손상된 사업운용이나 서비스에 필요한 시스템을 복구하고 복원력을 제공하기 위한 활동이나 계획을 개발하고 구현하는 것 ⑤ 복구(Recover): 백업을 위한 수단을 확보하고 사이버 사건으로 손상된 해상사업을 운용하기 위한 사이버 시스템을 복원하는 것

국제해사기구는 스스로 가이드라인의 성격을 원칙적인(high-level) 권고사항으로 규정하고 있다.[30] 이에 따라 가이드의 마지막 부분인 제4조 모범사례 (best practices for implementation of cyber risk management)에서 보다 구체적인 해상사이버리스크의 관리방안은 회원국 혹은 기국(flag state)의 요구사항을 참고하도록 하고 있다. 또한, 해운단체인 BIMCO 등에서 작성한 '선박 사이버 보안에 관한 가이드', 국제표준기구/국제전기기술위원회의 '정보기술에 관한 기준', 미국국립표준연구소의 '중요한 기반설비의 사이버보안 개선을 위한 구조' 등을 참조하도록 권고한다.[31]

---

29) "ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021" (section 2, Resolution MSC.428(98), 2017).

30) "These guidelines are recommendatiry.", section 2.2.3. GUIDELINES ON MARITIME CYBER RISK MANAGEMENT" MSC-FAL.1/Circ.3, IMO, 2017.

31) "4.2 Additional guidance and standards may include, but are not limited to:
1. The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
2. ISO/IEC 27001 standard on Information technology - Security techniques - Information security management systems . Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

다만, 급격히 진화하고 있는 사이버리스크의 성격을 감안하면 2017년에 채택된 결의안의 일부 내용은 이미 오래되어 의미가 퇴색했거나 새로운 형태의 위협 및 대응에 대한 언급이 미진한 부분도 발생한다. 예를 들면, 가이드에서는 사이버 위협의 가능한 유입 경로로 현재는 이미 보편적인 기술인 클라우드 컴퓨팅이나 인공지능 혹은 물류 블록체인기술에 대한 언급이 없다. 따라서 국제해사기구의 결의안은 원래 의도대로 해상사이버리스크에 대한 기본원칙과 임박한 위협에 대한 대응의 필요성을 촉구하는 의미로 받아들이고, 모범사례(best practice)로 언급한 해운단체나 선급협회 등에서 제시하는 구체적 지침을 참고하여 각자에 맞는 사이버리스크 대응방안을 수립하고 변화하는 리스크 양태에 따라 그것을 지속적으로 보완하는 방안이 필요하다.

(2) 발틱국제해운동맹

세계 최대의 해운단체인 발틱국제해운동맹(BIMCO)[32]를 비롯한 7개 해운단체는 2016년에 '선박의 사이버보안에 관한 가이드(The Guidelines on Cyber Security Onboard Ships)'를 발표하였다.[33] 가이드에서는 선박소유자 혹은 운영자에게 그들의 선박에서 사이버 사고에 대한 대응 및 복원력을 강화하기 위한 절차를 개발하고 운영하는 방법에 대한 기준을 제시한다. 즉 위협과 취약점을 식별하고, 리스크 크기를 측정하며, 위험을 방어하고 탐지하는 방법을 개발한다. 또한 비상계획을 수립하고 사이버 사고 발생시 복구하고 대응하는 절차를 포함한다.[34] 가이드는

3. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).“ 출처 : GUIDELINES ON MARITIME CYBER RISK MANAGEMENT” MSC-FAL.1/Circ.3, IMO, 2017.

32) 발틱해운동맹(Baltic and International Maritime Conference)은 세계 최대의 선박소유자, 용선자, 선박브로커 및 대리점의 비정부기구(NGO) 단체이다. 톤수 기준으로 세계 상선대의 약 60%가 회원으로 가입되어있고 120개국에 걸쳐 약 1,900개 선사를 회원으로 두고 있다. BIMCO 홈페이지 <https://www.bimco.org/about-us-and-our-members>, (최종검색일: 20년 6월 21일).

33) 2016년에 최초로 작성되었도, 현재까지 2018년 12월 제3판(version 3)이 발표되었다. 가이드 작성 작업에 참여한 BIMCO외 7개 해운단체는 다음과 같다. : BIMCO, InterManager, International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF) and World Shipping Council.

34) BIMCO, “The Guidelines on Cyber Security Onboard Ships”, ver 3, 2018, p.5.

사이버 보안 위협의 지속적인 진화에 따라 새로운 대응안을 제시하기 위해 계속 보완되고 있다. 2018년에 마지막으로 추가된 내용은 다음과 같다.

① 선박의 안전관리시스템(Safety Management System, SMS)내에 사이버 리스크를 포함할 것에 대한 국제해사기구의 요구반영 ② 운영기술(Operational Technology)의 위험측정에 관한 추가 정보 ③ 선박의 물류공급망과 관련된 위험관리 기준 보완 ④ 잠재적 문제를 설명하고 강조하기 위한 선박의 사이버 사고에 관한 사례연구

(3) 국제선급협회

국제선급협회(IACS)[35]도 일찌감치 해운산업의 다른 분야와 협력하에 사이버 시스템에 관한 실무그룹 (Joint Working Group)을 구성하여 선박과 관련된 사이버 사고에 대한 적극적인 실무대응방안을 모색하여 왔다. 협회가 2018년 9월에 발표한 12개 항목의 사이버안전관련 권고사항은 선박들이 사이버 관련 사고에 대한 실무적인 회복탄력성을 갖추도록 하는데 기본 목적을 두고 있다. 12개 권고사항의 내용은 아래와 같다.

① 선박 장비 및 시스템의 소프트웨어 관리를 위한 권고 절차 ② 소프트웨어 기반 기관시스템에 대한 수동/국지적 통제 역량과 관련된 권고사항 ③ 선상 컴퓨터 기반 시스템의 비상계획안 ④ 네트워크 설계사양(방식) ⑤ 데이터 보존 ⑥ 선상 컴퓨터 기반시스템의 물리적 보안 ⑦ 선상 컴퓨터 기반시스템의 네트웍 보안 ⑧ 선박 시스템 설계 ⑨ 컴퓨터 기반 시스템의 재고 목록 ⑩ 일관적 통합 ⑪ 원격 최신화/접속 ⑫ 통신과 시스템 경계(인터페이스)

각 회원 선급협회도 해상사이버보안 관리시스템에 인증체계를 구축하고 선박회사 및 선박에 대한 사이버 보안 인증서비스 및 선박의 네트워크 및 자동화시스템에 대해 사이버 보안 형식 승인 서비스를 제공하고 있다. 한국선급(KR)은

35) 국제선급협회((International Association of Classification Societies)는 각국의 선급협회간 공통목적을 달성하고 협력관계를 달성하기 위해 주요 7개국 선급협회가 1968년 10월에 결성한 단체이다. 우리나라는 1988년 6월에 가입하였다. 2020.4월 현재 회원협회는 12개사로 구성되어있다(미국선급, 프랑스선급, 중국선급, 크로아티아선급, 노르웨이-독일선급(DNV-GL), 인도선급, 한국선급, 영국선급(LR), 일본선급, 폴란드선급, 이탈리아선급, 러시아선급), IACS 홈페이지<http://www.iacs.org.uk/about/members/>, (최종검색일: 20년 6월 21일).

2020년 3월에 영국의 해운선사에 사이버 보안 적합인증서를 수여했다고 밝혔다.[36] 해당 선사의 한 선박에 대해서 한국선급은 리스크 관리, 자산관리, 사고대응 및 복구 등 18개 부문의 81개 항목에 대한 검사를 시행하였다. 해당 선박은 인증절차를 통해 국제해사기구의 규정, 탱커 운영사 안전관리평가, 탱커 안전선평가, 화주검사 등 사이버보안을 모두 만족함은 물론 회사와 선박이 모두 사이버 공격에 대한 대응 및 보안체계를 갖추고 있음이 인정되었다.

Ⅲ. 영국보험업계의 대응

1. 포괄적 면책약관 : 협회사이버공격면책약관(CL380)

과거의 전통적인 보험상품에서 사이버리스크는 명확한 인식의 부재와 이에 대한 부담보 조항이 명시적으로 존재하지 아니함으로 인하여 전위험(All Risks) 담보방식하의 계약에서는 직·간접적으로 담보될 수도 있었다. 그러나 2001년이후 재물보험에서는 보험목적물에 대한 직접적인 물리적 멸실 및 손상이 발생해야 보상이 가능하고 "전자적 데이터(electronic data)의 멸실, 손상, 변형, 삭제, 변조, 변경의 결과에 따른 손실"은 통상 명시적 특약으로 부담보한다.[37] 전세계 해상보험계약에 적용되는 가장 일반적인 사이버리스크 관련조항은 2003년에 영국보험시장에서 발표된 '협회사이버공격면책약관(CL380)'이다.[38] 이 약관은 컴퓨터,

36) 한국해운신문, "KR, 英선박에 사이버보안 적합인증", 한국해운신문 2020년 3월 4일자 기사, <http://www.maritimepress.co.kr/news/articleView.html?idxno=125562>, (최종검색일: 20년 6월 21일).

37) Electronic Data Endorsement A (NMA2914) 25/01/2001
"1(a) This Policy does not insure loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss.".

38) Institute Cyber Attack Exclusion Clause (Cl.380) 10/11/2003
1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.
2.1 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion,

소프트웨어 프로그램 기타 전자 시스템 등이 '피해를 주는 수단(as a means of inflicting harm)'으로 이용됨에 따라, 혹은 직·간접적으로 이에 기인하여 발생한 멸실, 손상, 배상책임 및 비용에 대하여 보험자는 담보하지 아니한다. 다만 전쟁, 정치적 동기에 따른 적대적 행위, 테러 등을 특약으로 담보하는 경우에는 컴퓨터, 소프트웨어 등이 유도장치나 무기로 이용되는 경우가 많아 상기 사이버 절대면책을 적용하지 않고 이에 따른 멸실, 손해, 비용손실 등을 보상한다.

도입한지 15년이 넘은 이 사이버리스크 면책약관에 대해 컴퓨터 등 IT시스템이 '피해를 발생시키는 수단'으로 사용되기만 하면 면책이 적용되는 지나치게 포괄적인 약관의 내용에 대한 비판이 제기되기 시작하였다. 예를 들어, 제3자가 컴퓨터로 스캔하여 수정한 허위의 선하증권을 제시하여 운송인으로부터 화물을 허위로 반출한 경우에 이러한 도난 피해에 대하여 적하보험자가 상기 사이버 면책약관의 내용을 문자 그대로 적용하여[39] 즉, 컴퓨터가 피해를 발생시키는 수단으로 사용된 점을 들어 과연 보험금 지급을 거절할 수 있을지가 문제가 된다. 문서위조를 통한 도난은 보험계약자의 고의나 사기 등 다른 사정이 없는 한 기존의 해상적하보험 약관에서 담보하는 위험이지만 그 문서가 작성, 가공, 유통되는 방식이 디지탈화되었다고 해서 사이버 면책약관의 문구에 따라 보험자가 보험금 지급을 거부할 수 있을지는 현실적으로 매우 의문시된다.

또한 기존의 사이버리스크 면책약관의 내용중 컴퓨터 등이 '피해를 발생시키는 수단(as a means of inflicting harm)'으로 사용된다는 부분은 면책의 적용이 공격자의 해당 피보험목적물에 대한 '고의적인' 사이버 공격에 다른 피해에만 적용가능하고 직접적인 공격대상이 아닌 무차별적인 사이버 공격에 따른 손해에는 적용되지 아니함을 의미할 수 있다. 결과적으로 우발적인(accidental)[40] 사이버리스크에 대하여 비자발적인(non-affirmative), 혹은 암묵적인(silent) 방식으로 보장을

---

insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

39) "any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system".

40) 특정한 대상을 목표로 하지 아니하는 사이버 공격을 의미한다. 집단 혹은 사회 전체에 침투하여 효과를 발휘한다는 의미의 'systemic' 혹은 재앙적(catastrophic) cyber event라고도 언급된다.

제공하는 것으로 해석된다.[41] 이 경우 '피해를 발생시키는 수단'과 관련한 사이버 공격자의 피보험자에 대한 고의성에 관한 입증책임은 면책을 주장하는 보험자에게 부과된다. 사이버 사고시 보험자가 보험계약자로부터 그들의 기밀에 속하는 정보시스템의 접근 권한을 얻어 면책의 증거를 찾는 일은 불가능에 가까운 일이다.

2. 시장의 변화: 절대면책에서 보장명확화로

사이버리스크 절대면책의 관행과 구체적인 약관내용의 불분명함에 관하여 영국의 금융당국의 의견이 발표되었다. 2016년 11월에 영국의 건전성 감독청(Prudential Regulation Authority(PRA))은 자문보고서[42]를 발간했고, 이어서 2017년 7월에 '사이버 보험 인수위험'이라는 감독성명서[43]를 발표했다. 감독청은 성명서를 통해 다양한 종류의 기존 보험계약상 잠재적으로 의도하지 아니하거나 불분명한 사이버리스크 보상 가능성에 대한 우려를 표명했다. 특히 '암묵적(silent)' 혹은 '비자발적(non-affirmative)' 사이버 리스크[44] 담보와 관련하여 각 보험사들이 적극적으로 평가, 관리할 것을 기대하였다. 먼저, 비자발적 (혹은 암묵적) 사이버 리스크를 좀더 적극적으로 관리할 것. 둘째, 각 보험사의 이사회는 회사의 사이버 전략과 리스크 성향(risk appetite)을 명확히 규정할 것. 셋째, 보험사의 사이버 리스크에 대한 전문성을 지속적으로 개발하고 구축할 것 등을 요구하였다. 2018년 감독청은 보험업계와 협력을 통해 다양한 규모의 회사에 대한 사이버 리스크 서베이를 실시하였고, 2019년 1월 '대표이사에게 드리는 서신'을 통해 모든 보험사들이

41) 적극적인(affirmative) 방식의 사이버리스크 담보약관은 통상 기본 보험증권의 보상한도보다 낮은 수준의 별도 부가 한도가 적용되며, 추가보험료를 조건으로 면책위험을 다시 구입하는(write-back coverage) 방식으로 구성된다. (JS2018-001 Cyber Attack Exclusion Clause and Writeback, JS2019-005 cyber exclusion with targeted cyber attack write-back 221119 등).

42) PRA, "Cyber insurance underwriting risk", Consultation Paper (CP39/16), November 2016.

43) PRA, "Cyber insurance underwriting risk", Supervisory Statement (SS4/17), July 2017.

44) "비자발적 사이버리스크란, 보험증권에서 명시적으로 사이버리스크를 포함하거나 혹은 제외하지 아니하는 것을 말한다. (non-affirmative cyber risk, ie insurance policies that do not explicitly include or exclude coverage for cyber risk.)" (PRA, Consultation Paper (CP39/16), 1.6(b)).
Partner Re사의 시장 서베이 결과는 서베이 대상인 사이버 리스크를 인수하는 전세계 271개 브로커사 및 96개 보험자들중 67%의 대상자가 그들의 보험증권에서 그들의 의지와 상관없이 발생하는 비자발적/암묵적 사이버 리스크 담보를 우려한다고 답변하였다.(Partner Re and Advisen, "Cyber Insurance – The market view", October 2019, p.10).

'비자발적' 사이버 리스크 담보로 인해 발생할 수 있는 의도하지 않은 위험노출을 감소시키기 위한 실행계획을 수립하여야 함을 재차 강조하였다.[45]

감독당국의 요구에 대응하기 위해 런던보험시장의 사업자단체인 로이즈보험시장협회(Lloyds' Market Association)는 사이버 리스크에 대한 명확한 보장 혹은 면책을 위한 기존 약관의 단계적 개선을 추진하였다.[46] 1차로 2020년 1월 1일자에 개시되는 재물관련 보험종목(First-party property damage lines of business)[47]에 대하여, 보험사들은 모든 보험계약에 사이버 리스크에 대한 보장 혹은 면책의 입장을 확정하여 명기하도록 요구하였다. 이와 관련하여 2019년 11월에 새로운 4종의 사이버 보장/면책 표준약관이 발표되었다.[48] 이 가운데 해상보험과 관련된 약관은 '비자발적' 사이버 리스크에 대한 담보를 명시한 Marine Cyber Endorsement (LMA5403)[49] 약관과 지상약관으로서 절대적 면책을 명확히 하는 Marine Cyber

45) PRA, "Cyber underwriting risk : follow-up survey result", 30 January 2019.

46) Lloyds, "Providing clarity for Lloyd's customer on coverage for cyber exposures", Market Bulletin (Ref: Y5258), 4 July 2019.

47) Energy 관련 운영/공사, 발전, 적하, 선박, 재물, 기술, 테러보험 등 피보험자에 직접적인 보상이 이루어지는 보험상품을 일컫는다.

48) Property Cyber and Data Exclusion (LMA5401) 11/11/2019, Property Cyber and Data Endorsement (LMA5400) 11/11/2019, Marine cyber Endorsement (LMA5403) 11/11/2019, Marine cyber Exclusion (LMA5402) 11/11/2019. 이와는 별도로 런던보험시장에서 로이즈를 제외한 보험회사 단체인 IUA(International Underwriting Association)에서는 별도의 절대적 사이버손해면책약관(Cyber Loss Absolute Exclusion Clause (IUA 09-081) 17/05/2019)와 제한적 사이버손해면책약관(Cyber Loss Limited Exclusion Clause (IUA 09-082) 17/05/2019)을 발표했다. 제한적 사이버손해면책약관에서는 '컴퓨터 사용 등에 따라 직접적으로 발생한 손해'를 담보하지 아니하며 절대적 사이버손해면책약관은 직접 혹은 간접적으로 발생한 손해를 면책하는 것으로 구분한다.

49) MARINE CYBER ENDORSEMENT

1. Subject only to paragraph 3 below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system.
2. Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.
3. Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile. (LMA5403) 11 November 2019.

Exclusion (LMA5402)[50] 약관이다. 특히 Marine Cyber Endorsement약관은 기존의 협회사이버공격면책약관(CL380)과 동일한 문구를 기반으로 하지만, '컴퓨터나 IT 시스템이 '피해를 야기하는 수단(as a means for inflicting harm)'으로 사용되지 않은 경우라도 보상하는데 불리하게 작용하지 아니한다'는 명확한 보장조항(제2조)을 추가하였다.

배상책임과 특약재보험 관련 보험종목에 대하여는 추후 2020년과 2021년 사이에 명확한 입장을 정하는 것으로 하였다. 이와 관련한 업계의 궁극적 목표는 감독당국의 요구와 같이 계약 내용의 명확화를 통해 '비자발적'' 사이버 담보의 허용에 따라 의도하지 아니한 사이버 담보 제공을 회피하는 것이다.

3. 소결 : 우리나라 해상보험시장의 수용 방안

우리나라 해상보험시장은 런던보험시장과 재보험으로 밀접한 계약관계를 가지고 있으므로 우리 해상보험계약에도 영국의 해상사아버리스크 약관의 내용이 곧바로 도입되기 시작했다. 특히 선박, 항공보험 등과 같이 위험의 크기가 크거나 리스크의 성격이 이례적인 보험종목의 경우는 런던재보험시장에 보험계약의 가격과 조건을 직접 의존하는 바가 크다. 이 경우 런던보험시장의 새로운 해상사이버 리스크 약관을 우리나라 계약자와 보험사간의 해상보험 계약에도 곧바로 적용하게 되는데, 결국 영국의 감독당국이 요구하는 보험사별 사이버 리스크에 대한 태도 명확화와 약관내용의 개선을 우리 보험시장이 수용하는 결과를 가져온다. 따라서 보험사들은 이러한 국제보험시장의 변화 추세 뿐만 아니라 그러한 변화가 개별 계약에 미치는 영향에 대해서 충분히 이해하고 국내 해상보험계약자나 해운산업의 이해관계자들과 그 내용을 공유하는 것이 향후 명확한 보상처리를

50) MARINE CYBER EXCLUSION

This clause shall be paramount and shall override anything in this insurance inconsistent therewith.

1. In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:

1.1. the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or

1.2. the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system. (LMA5402) 11 November 2019.

위해서도 필요하다. 계약관리 측면에서는 한국선급 등 해상사이버리스크 인증기관과의 협력을 통해 개별 계약자의 사이버대응 능력을 보험계약에 반영하는 방안을 모색할 수 있을 것이다.[51]

Ⅳ. 향후 예상되는 사이버리스크 관련 법적 쟁점

앞서 살펴본 바와 같이 국제해사기구와 발틱국제해운동맹 등 국제기구와 단체들이 사이버리스크에 대한 논의를 본격적으로 시작하였고, 영국 보험시장도 그동안 절대면책이었던 사이버리스크를 명확한 보장범위 내에서 보장하는 것으로 보장범위에 포함시켰다. 우리나라에서도 영국 보험업계와 영국법의 영향을 많이 받기 때문에 사이버리스크에 대한 보험에서의 보장, 사이버리스크에 관한 법적 문제에 대한 논의가 필요할 것이다.

해상사이버 공격으로부터 초래되는 법적 문제는 비교적 근래에 와서 새로이 논의되는 주제이다. 그러나 대부분의 쟁점은 오래된 법적 논의 주제의 하나인 해상운송인의 감항능력주의의무 및 인과관계와 밀접한 관련을 가지고 있다. 그리고 사이버 공격으로 인한 선박 탈취 등을 해적행위에 준해서 처리할 수 있는지 여부 등 사이버해적의 논의도 충분히 예상되는 법적 쟁점 중 하나일 것이다.

1. 해상운송인의 감항능력주의의무: 사이버 감항성

(1) 상법의 내용

감항능력주의의무(duty of seaworthiness)란 해상운송인이 송하인 및 용선자에게 제공하는 선박이 발항 당시에 해상에서 발생할 수 있는 통상의 위험으로부터 안전하게 항해를 할 수 있는 능력, 즉 감항능력(堪航能力; seaworthiness)을 가지는 선박이라는 것을 담보하는 의무를 말한다.[52] 상법의 규정상 감항능력주의의무는

51) 해상사이버리스크를 별도로 보상하기위해 해외 보험사들은 기본면책약관(CL380)에서 면책되는 위험을 추가담보(write back)하거나, 이에 추가하여 사이버사고 대응 및 복구비용, 영업손실, 제삼자 배상책임, 방어비용 등을 보상하는 상품을 출시하고 있다.

52) 정동윤 편, 「주석상법」, 제2판, 서울 : 한국사법행정학회, 2015, 486면.

구체적인 의무사항으로 항해능력(협의의 감항능력), 운항능력 및 감하능력의 세 가지로 구성된다.[53] 즉, ① 선박이 안전하게 항해할 수 있게 할 것(항해능력, 선체능력), ② 필요한 선원의 승선, 선박의장(해당 항해에 필요한 서류와 속구를 비치하고 장비를 갖추는 것)과 필요품의 보급(인적능력, 운항능력) ③ 선창, 냉장실 기타 운송물을 적재할 선박의 부분을 운송물의 수령, 운송과 보존을 위하여 적합한 상태에 둘 것(감하(堪荷)능력)의 사항을 정하고 있다.[54] 운송인이 감항능력을 구비하여야 할 시기는 선박의 '발항 당시'이다. 발항 당시란 개개의 운송계약마다 '선적 개시 시부터 발항 시까지'를 의미한다.[55] 선적 후 발항 전 항내에 있을 때에도 해상위험으로 인한 운송물의 멸실 등 손해가 있을 수 있기 때문이다. 감항능력의 유무는 특정한 항해, 특정한 운송물과의 관계에서 상대적으로 판단된다. 그러므로 동일 항해에 있어서도 운송물에 따라 어느 운송물에 대하여는 감항능력을 가지나, 다른 운송물에 대하여는 이를 갖지 못하는 경우도 있다. 상법은 의무위반의 효과로서 운송인은 자기 또는 선원이나 그 밖의 선박사용인이 감항능력주의의무를 해태하지 않았음을 증명하지 아니하면 운송물의 멸실, 훼손 또는 연착으로 인한 손해를 배상할 책임이 있음을 규정하고 있다. 여기서 상법은 단순히 '주의를 해태하지 아니하였음을 증명하지 아니하면'이라고 규정하고 있다. 그러나 상법이 기원된 1924년 헤이그 규칙의 내용으로 보면 여기서 주의는 '상당한 주의(due diligence)'를 의미한다.[56] 상당한 주의는 그 상황에서 보통의 신중한

53) 상법은 제794조에서 운송인 등의 감항능력주의의무를 아래와 같이 규정한다.
'운송인은 자기 또는 선원이나 그 밖의 선박 사용인이 발항 당시 다음의 사항에 관하여 주의를 해태하지 아니하였음을 증명하지 아니하면 운송물의 멸실, 훼손 또는 연착으로 인한 손해를 배상할 책임이 있다. 1. 선박이 안전하게 항해를 할 수 있게 할 것 2. 필요한 선원의 승선, 선박의장(艤裝)과 필요품의 보급 3. 선창, 냉장실 그 밖에 운송물을 적재할 선박의 부분을 운송물의 수령, 운송과 보존을 위하여 적합한 상태에 둘 것'.

54) 김인현, 「해상법」 제5판, 법문사, 2018, 229면.

55) 헤이그규칙 제3조 제1항에서도 "before and the beginning of the voyage"라고 규정하고 있고, 우리나라 학설에서도 이와 같이 해석한다. (최종현, 「해상법상론」 제2판, 법문사, 2015, 246면.)

56) International Convention for the Unification of Certain Rules of Law relating to Bills of Lading ("Hague Rules"), and Protocol of Signature (Brussels, 25 August 1924)
Article 3
1. The carrier shall be bound before and at the beginning of the voyage to exercise due diligence to:
(a) Make the ship seaworthy.
(b) Properly man, equip and supply the ship.
(c) Make the holds, refrigerating and cool chambers, and all other parts of the ship in which goods are carried, fit and safe for their reception, carriage and preservation.

운송인에게 일반적으로 요구되는 주의이며, 그 주의의무를 다하였는지 여부는 객관적으로 판단하여야 한다.[57] 우리나라 상법은 감항능력주의의무에 관하여 과실추정주의를 채택하여 그 성질을 과실책임으로 보고 있으며, 이에 따라 무과실의 증명책임을 운송인에게 부담시키고 있다.[58] 선박이 불감항 상태가 되는 경우 선박소유자가 이것을 알고 있는지의 여부, 과실이 있는지 여부, 감항능력 주의의무에 대한 상당한 주의가 있었는지 여부 등과 관계없이 불감항이라는 사실에 대해 면책되지 않는다면 이것은 감항능력주의의무의 무과실책임성(객관성)이라고 할 수 있으나, 상법의 규정과 같이 선박소유자가 상당한 주의를 했다면 책임을 면하게 되는 것은 과실책임성 (주관성)이 인정된다고 할 것이다.[59] 감항능력주의의무에 관한 규정은 강행규정이므로 이 규정에 반하여 운송인의 의무 또는 책임을 경감 또는 면제하는 당사자 사이의 특약은 효력이 없다(상법 제799조 제1항 전단).

한편, 상법은 해상보험계약의 합리적인 운영이 가능하게 할 목적으로 보험자의 법정면책사유를 별도로 규정하고 있다. 상법 제706조에 따르면 보험자는 다음의 손해와 비용을 보상할 책임을 면한다. ① 선박 또는 운임을 보험에 붙인 경우에는 발항 당시 안전하게 항해를 수행하기 위해 필요한 준비를 하지 아니하거나 필요한 서류를 비치하지 아니함으로 인하여 생긴 손해 ② 적하를 보험에 붙인 경우에는 용선자, 송하인 또는 수하인의 고의 또는 중대한 과실로 인하여 생긴 손해 ③ 도선료, 입항료, 등대료, 검역료, 기타 선박 또는 적하에 관한 항해 중의 통상비용. 이 가운데 제1호가 선박보험 혹은 운임보험의 경우 선박의 불감항시 보험자의 면책에 관한 사항이다. 앞서 살펴본 상법 해상편의 감항능력주의의무는 발항 당시에만 부과된 의무로써 제1호의 선체능력, 제2호의 기술적, 인적 운항능력 및 제3호의 감하능력을 요구하고 있다. 상법 보험편 해상보험규정의 감항능력주의의무라고 볼 수 있는 상법 706조 제1호는 해상편과 동일하게 보험

57) 헤이그 및 헤이그-비스비규칙에 따르면 불감항에 따른 멸실 혹은 손상에 대해 상당한 주의를 다하였는지에 대한 입증책임은 운송인 (혹은 rule상의 면책을 주장하는 다른 주체)에게 있다.(제4조 1항 후단부) 또한 상당한 주의는 발항시 혹은 발항전에 이루어져야하며, 상당한 주의와 감항성은 사고와 관련되어야만 한다. 감항성은 해당 항해의 화물과 관련하여 고려되며, 운송인의 의무는 절대적인 주의가 아닌 합리적인 주의로 족하다.(William Tetley, *Marine Cargo Claims*, 4th ed, Thomson Carswell, 2008, p.878-893).

58) 최종현, 전게서, 248면.

59) 지상규/정영석, "감항능력 주의의무의 구성요소에 관한 고찰", 중앙법학 제12집 제2호, 2010, 206면.

계약자인 운송인이 감항능력을 구비하여야 할 시기를 발항 당시로 한정하고 있다. 그러나 구체적인 감항능력의 요건은 해상편의 감항능력주의 의무와 비교하여 매우 간략히 기술하여 단지 '안전하게 항해를 하기에 필요한 준비와 필요한 서류비치'로만 서술하고 있다.[60] 대법원 1996.10.11. 선고 94다60332 판결에서는 해상보험상의 감항능력에 대해 "감항능력이란상대적인 개념으로서 어떤 선박이 감항성을 갖추고 있느냐의 여부를 확정하는 확정적이고 절대적인 기준은 없으며 특정 항해에 있어서의 특정한 사정에 따라 상대적으로 결정되어야 한다."고 판시한 바 있다.

(2) 영국법의 내용

영국해상법상 선주의 감항능력주의의무에 관한 조항은 1924년 헤이그 규칙의 내용과 동일하다. 영국은 1924년에 헤이그 규칙상의 선하증권통일조약을 그대로 영국 국내법화한 해상화물운송법(Carriage of Goods by Sea Act(COGSA) 1924)을 제정하여 시행하다가, 1968년 헤이그-비스비규칙으로 개정되자 1971년에 해상화물운송법을 개정하여 현재까지 이르고 있다.

영국보험법에서는 선박의 감항성에 대한 묵시담보 적용과 관련하여 항해보험과 기간보험을 구분하고 있다.[61] 영국해상보험법(MIA 1906) 제39조(선박의 감항성담보)에 따르면 '항해보험증권에서는 항해의 개시시에 선박은 보험에 가입된 특정한 해상사업의 목적을 위하여 감항이어야 한다는 묵시담보가 있다.'(제1항) 영국의 판례는 항해보험증권에 대해 선박이 수리, 장비, 선원 및 기타 모든 관점에서 피보험항해를 출항할 때에 그 항해의 통상적인 위험에 적응하는데 적합한 상태에 있었으면 그 선박은 감항이라고 하였다.[62]

60) 이와 관련하여 상법 해상보험편의 개정안으로 해상편의 감항능력 주의의무 규정과 일치시켜 '발항 당시 상법 제794조 1, 2호의 감항능력을 갖추지 아니함으로 인하여 발생한 손해'로 명확화하자는 주장도 있다. (김인현, "상법 보험편 해상보험규정의 의의와 개선방안", 상사법연구 제28권 제2호, 2009, 293면).

61) Marine Insurance Act 1905, section 39. Warranty of seaworthiness of ship.
(4) A ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured.
(5) In a time policy there is no implied warranty that the ship shall be seaworthy at any stage of the adventure, but where, with the privity of the assured, the ship is sent to sea in an unseaworthy state, the insurer is not liable for any loss attributable to unseaworthiness.

62) Dixon v Sadler (1831) 5 M & W at 414.

반면, 기간보험증권에서는 '선박이 어떠한 단계의 해상사업에서도 감항이어야 한다는 묵시담보는 없다'고 규정하고 있다(제5항). 기간보험에 대해서는 보험계약이 개시될 당시에 선박이 항해중일 가능성이 있고 이때 피보험자인 선박소유자가 그 선박의 상태를 통제하거나 지배할 수 없는 때가 많으므로 선박의 불감항 상태 여부를 불문하고 보험계약자는 부보위험에 근인한 손해의 보상을 청구할 수 있다. 보험자는 손해가 불감항에 기인했다는 항변을 할 수 있지만 이는 절대적 항변사유가 아니고 피보험자가 불감항 사실에 대한 인식(privity of the assured)이 있는 경우로 한정된다. 영국판례법에 따르면 불감항에 관한 입증책임은 기본적으로 그것으로 면책을 주장하는 보험자에게 있다. 불감항을 입증하기 위해 사실로부터의 추론이나 적절한 가정은 인정되나 법률의 추론으로는 불가능하다. 그러나 만일 사고의 원인이 명확히 파악되거나 혹은 계약자가 반증을 제시하지 못하고 그 증거로부터 원인이 충분히 확인될만한 것으로 합리적으로 추정된다면, 열거위험방식인 선박보험약관상 입증책임에 대한 일반적인 규칙, 즉 계약자가 보험계약상 담보하는 위험에 따른 손해라는 것을 입증해야하는 것이 적용된다.[63]

(3) 사이버감항성 적용의 문제

국제해사기구와 여러 해운단체들로부터 해상사이버리스크의 관리방안에 관한 가이드가 제시되고 있는 상황을 감안하면, 선박소유자들이 잠재적인 사이버 공격에 대하여 신중한 선주[64]로서 아무런 조치를 취하지 아니하는 것이 허용된다고 주장하기는 어렵다. 영국의 판례에 따르면 '감항성은 해당 시점의 산업 기준과 실무에 의해 판단하여야 한다. 기준과 실무는 합리적인 범위에서 적용된다.' 고 판시하였다.[65] 동시에 법규상 요구되는 운송인의 '상당한 주의'도 현대화된 해상사업운영 환경을 고려하여 이전과 달리 판단할 수밖에 없다. 선주는 자신의 선박

63) Jonathan Gilman (ed.), *Arnould: Law of Marine Insurance and Average*, 19th ed, Sweet & Maxwell, 2018, paras. 20-35,36.

64) 영국의 판례에 따르면 "감항성은 선박의 상태와 선박이 처한 상황에서 마주할 위험간의 관계를 표현하는 것이다. 그러하여 선박이 항해개시전에 신중한 무보험 선주로서 요구하였을 만한 위험대비를 하는 정도의 조치를 했고 이례적인 손상의 경우 이외에 항해를 지속했다면 그것은 감항능력을 갖춘 것이라고 볼 수 있다."고 한다.(Gibson v Small (1853) 4 HL Cas 353, p.384.

65) The Lendoudis Evangelos [2001] 2 Lloyds's Rep. 304 p.306.

및 기술적 장비와 관련된 사이버리스크에 대하여 '상당한 주의'를 다하여야만 사이버감항성(Cyber Seaworthiness)을 인정받을 수 있을 것이다. 선박은 해킹 등 사이버공격을 방어할 수 있는 보안시스템을 갖춰야 할 것이다. 이 보안시스템이 사이버감항성을 갖췄는지 여부는 향후 제정될 국제해사기구 등의 가이드라인을 참고하게 될 것이지만, 통상의 사이버공격을 감당할 수 있는 수준이 되어야 할 것이다. 또한, 선원들은 사이버 공격의 잠재적 가능성을 인지하고 미리 대비책을 강구해야하며, 사이버 공격에 대비한 선박운영체계, 비상대응 매뉴얼을 작성하고 이에 따른 손실 대응과 처리절차에 관한 훈련이 필요하다. 선상의 선원과 육상 근무자들은 모두 선박의 정보통신(IT) 시스템과 운용기술(OT)장비에 대한 사이버리스크 위험요인에 대해 유의하여야한다. 항만국 통제에 대비하는 차원에서도 안전운항관리체계(ISM) 매뉴얼에 따른 사이버 보안 대응철차 및 시나리오를 개발하고, 적절한 해상사이버리스크 관리체제를 도입하여 선박과 육상에 모두 적용하여야 할 것이다.

다만, 현재 우리나라 상법과 헤이그-비스비규칙에 따르면 감항능력주의의무의 시기에 대해 "항해 개시 전 또는 발항 당시(before and at the beginning of the voyage)"를 기준으로 하고 있는데, 사이버감항성에 대한 제대로 된 규율을 위해서는 로테르담규칙에서의 논의처럼 "항해 전 과정(during the voyage)"에서 감항성을 유지하도록 인정하는 것이 선행되어야 할 것이다.[66] 기존 감항능력주의의무의 시기를 우리나라 상법과 헤이그-비스비규칙에서 발항당시로 규정했던 것은 발항 이후에 불감항사유에 대해서 쉽게 치유하기 어려웠기 때문인데, 운송수단의 변화와 새로운 통신수단의 발달로 원거리 선박통제가 수월해진 시대적 상황을 고려하면 일반적인 감항능력주의의무는 물론 사이버감항능력주의의무도 마찬가지로 발행당시로 충족하는 것으로 충분하지 않고 항해 전 과정에서 유지되는 것이 타당하다고 생각한다.[67][68]

66) 이현균, 전게논문, 85~89면.

67) 이현균, 전게논문, 85~89면.

68) 물론, 감항능력주의의무를 항해 전 과정으로 확장하면, 항해 도중 사고가 발생할 경우에 화주나 보험자가 거의 다 감항능력주의의무를 문제 삼을 것으로 보이고, 이에 따라 운송인의 지위가 너무 취약해질 것이라는 우려가 있을 수 있다. 하지만, 기술의 발달로 항해도중 발생한 불감항사유의 치유도 기존보다 훨씬 수월해진다면 불감항을 이유로 한 면책이 크게 늘어나지는 않을 것이라 생각한다.

2. 인과관계

사이버리스크와 관련하여 예상되는 또 다른 법적문제 중 하나는 사이버리스크와 실제적 멸실, 손상, 비용 등과의 인과관계에 대한 내용이다. 과연 사이버 공격으로 인해 컴퓨터 등의 오작동하여 화재가 발생한 것인지, 아니면 사이버 공격이 있었더라도 실제 손해를 발생시킨 원인은 컴퓨터 바이러스가 첨부된 이메일을 열어본 선원의 과실이 근인(proximate cause)이 아닌지, 혹은 사이버 공격에 따른 피해가 가능할 정도로 허술하게 구성된 운영시스템의 설계오류에 기인한 것이지 하는 문제가 제기될 수 있다. 특히 해상보험에서 인과관계 즉 위험과 손해와의 관계가 문제되는 것은 해상에서의 사고 발생원인이 여러 가지로 복잡한 경우가 많고, 이에 더하여 해상보험계약에서 면책되는 리스크가 많기 때문이다.[69] 주로 영국법이 준거법으로 적용되는 해상보험계약에서는 인과관계는 보상하는 위험에 '근인'하는 손해를 보상하는 것으로 법제화되었다.[70] 영국 법원은 여러 원인의 복잡한 작용에 의해 발생하는 손해의 경우, 가장 가까운 원인은 단지 시간적 선후관계로 판단할 것이 아니라 그 원인이 지배적이거나 효과적인지(dominant or effective cause)를 판단해야 한다고 판시하였다. 지배적이거나 효과적인지의 여부는 상식에 따라서 판단해야 하는데, 이에 대해서는 사실관계, 보험약관의 내용, 사고 원인간의 관련성, 사고원인의 시간적 순서 등 다양한 요소들을 고려해야 한다.[71] 두 가지 이상의 근인이 관여되는 경우에는 문제되는 근인이 모두 담보위험에 해당하거나 근인 중 일부가 담보위험에 해당하고 나머지 근인이 면책사유에 해당하지 않는 경우에는 보상되지만, 두 가지 이상의 근인 중 하나라도 보험약

69) 경익수, "해상보험에 있어서의 인과관계에 관한 연구", 한국해법학회지 제37권 제2호, 한국해법학회, 2015, 374-375면.

70) Marine Insurance Act, Section 55 Included and excluded losses.
(1) Subject to the provisions of this Act, and unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against
한편, 우리나라의 손해보험 계약의 경우 일반적으로 손해와 보험사고간 '상당인과관계설'을 통설로 인정하고 있다. 즉, 보험자가 보상할 손해는 보험사고로 말미암아 필연적으로 생긴 것을 이르는데, 어떠한 손해가 보험사고와 상당인과관계를 가지느냐는 개별적 사정에 따라 결정되는 사실의 문제라고 할 것이다. 상당인과관계설은 종종 다수의 원인으로 하나의 결과를 초래하게 되는 것을 인정하는데, 이것은 보험자의 책임의 유무를 다양한 원인중 하나의 원인만 선택하여 손해의 원인으로 하려는 해상보험 거래의 통념에 적합하지 않은 면이 있다고 한다. (경익수, 위의 논문, 386면 참조).

71) Layland Shipping co v Norwich Union Fire Insurance Society [1918] A.C.350 at 369.

관 상 면책사유에 해당할 경우 보험자는 면책되어 보삼책임이 없다.[72] 한편, 우리나라법이 준거법이 된다면 상당인과관계가 있는지에 따라서 판단하게 될 것인데, 이에 대해서도 향후 논의가 필요할 것이라고 생각된다.

3. 사이버공격에 대한 해적행위 규정 적용가능성

Level 3 이상의 자율운항선박의 경우 선박의 위치정보를 육상조종실 또는 선주에게 전송하고 이를 수집하여 선적항까지 선박을 조종 또는 관리하여야 하기 때문에 자율운항선박 위치정보를 지속적으로 전달해야 하고, 이 과정에서 선박의 경로 등이 컴퓨터 시스템을 통해 쉽게 노출되어 해킹과 같은 사이버테러나 해적행위에 표적이 되기 쉽다는 문제점이 있다. 해킹 등 사이버공격으로 인해 선박의 운항권한을 탈취하게 되는 것을 해적행위로 규정할 수 있는지에 대한 논의도 필요할 것이다.[73]

이에 관해서는 자율운항선박은 선원들이 존재하지 않으므로 해적이 성립하기 위한 폭력의 대상이 없기 때문에 해적의 정의개념에 포섭될 수 없을 것이라고 견해가 다수 있는데[74], 사견으로는 우리 상법과 헤이그-비스비규칙에서 해적행위의 방법에 대해 명시적인 규정이 없기 때문에 사이버공격으로 인한 선박 탈취 또는 억류도 “해적에 준하는 행위”로 볼 수 있을 것이다.[75]

해적행위[76]는 사적인 집단에 의한 선박이나 선박 위의 재산의 약탈을 뜻하고, “그 밖에 이에 준하는 행위”는 집단적인 강도나 테러행위 등이 포함된다고 한다.[77] 영국 판결에서는 "해적이란 폭력적이지만 은밀하지 않고, 정치적 목적[78]이

72) Susan Hodges, *“Cases and Materials on Marine Insurance Law”*, Cavendish Publishing, 1999, p.345.
73) 이현균, 전게논문, 112면.
74) 김인현, “21세기 전반기 해운환경의 변화에 따른 해상법의 제문제 - 컨테이너, SPC, 무인선박 -”, 상사법연구 제35권 제2호, 한국상사법학회, 2016, 145면.
75) 이현균, 전게논문, 113면.
76) 해적행위에 관해서는 유엔해양법협약 제101조에도 규정되고 있으나 이는 국제법상 문제에 대해 규율하는 것이지 책임과 보험의 문제는 아니므로 논외로 한다. 영국에서도 해적 담보여부와 관련해서 당사자가 유엔해양법협약의 적용을 주장했으나 이를 배척한 명시적으로 배제한 판례가 다수 존재한다. 대표적인 판결로는 McKeever v Northernreef Insurance Co SA [2019] Lloyd's Rep IR 535이 있다.
77) 최종현, 전게서, 300면.
78) 정부기관이 행하거나 정치적 목적으로 행한 행위는 해적에서 제외된다고 한다. (송상현/김현, 「해상법원론」 제5판, 2015, 41면).

아닌 사적 이득을 위한 수단으로 선박 및 그 밖의 해상재산의 절도 또는 공격을 하는 자"고 판시한 바 있다.[79] 이 판결에서 폭력의 정의에 대해 폭력의 사용(use of violence), 폭력 사용에 대한 위협(the threat of violence) 또는 폭력을 사용할 의도(the intention to use violence)로 그 범의를 넓게 판단하였다.[80] 하지만 명시적으로 사이버공격을 해적행위 또는 폭력행위로 판단한 우리나라와 영국의 판결은 현재로서는 없는 것으로 보인다.

만약, 사이버공격이 해적행위에 해당하게 된다면 헤이그-비스비규칙 제4조 제2항 (f)호에 규정된 공적행위(act of public enemies) 또는 상법 제796조 제4조에 규정된 "해적행위 기타 이에 준한 행위"에 해당되어 운송인이 면책을 주장할 수 있을 것이다.

선원이 탑승하지 않는 Level 3 무인원격조종선박과 Level 4 완전자율운항선박이 해킹당한 상태에서 선박충돌 등의 불법행위로 인해 제3자에게 손해가 발생한 경우 그 손해배상책임을 선박소유자에게 전적으로 귀속시키기는 어려울 것이다.[81][82]

이에 따라 해킹으로 인한 피해를 보상하는 보험이 필요할 것이다. 하지만 보험사 입장에서는 모든 해킹손해에 대해 보상하는 것은 불가능할 것이기 때문에 사이버보안에 관한 특정한 조건을 부여하고 이를 충족하지 못한 경우 보험자면책을 주장할 수 있는 조항 등을 고려할 수 있을 것이다.[83]

한편, 해킹된 자율운항선박이 선박충돌 등의 불법행위를 일으킨 경우 선박소유자와 육상운항관리자는 해당 선박에 대한 지배를 상실했기 때문에 해킹된 자율운항선박의 불법행위에 대해 책임을 부담하지 않을 것이다. 다만, 해킹에 대한 위험을 알았거나 알 수 있었지만 고의 또는 과실로 해킹에 제대로 대응하지 못한 경우 일부 책임을 부담하는 경우도 있을 것이다.

---

79) Republic of Bolivia v Indemnity Mutual Marine Assurance Co Ltd [1909] 1 KB 785 등 다수.

80) Republic of Bolivia v Indemnity Mutual Marine Assurance Co Ltd [1909] 1 KB 785.

81) Kengo Minami, "The legal issues about autonomous ships in japanese law context", 「11th East Asia maritime law forum」, 2018 November 3, 2018, p. 60.

82) 선박소유자가 개품운송계약 또는 용선계약에 따라 계약상책임은 질 수 있을 것이지만 이를 구체적으로 적용하기 위해서는 추가적인 논의가 필요할 것이라고 생각된다.

83) Wang Xin, "Legal Isuues of Testing of Unmanned Ships in Chain", 「11th East Asia maritime law forum」, 2018 November 3, p. 110.

4. 사이버리스크 관련 선박안전법 개정방안

국제해사기구는 2021년 1월까지 국제안전관리규약(ISM Code)에 해상사이버리스크관리에 대한 내용을 반영하도록 각국의 정부에 권고하였고, 결과적으로 이를 반영하지 아니하는 선박은 항만당국에 의해 억류될 수도 있다.

우리나라는 해사안전법의 규정에 따라 해당되는 선박[84]의 안전운항 등을 위한 관리체계를 수립하고(제46조), 해양수산부장관이 위탁한 기관으로부터 안전관리체계에 대한 인증심사를 받아야한다(제47조). 해사안전법에 규정된 안전관리체제에 포함되어야 하는 사항은 해상에서의 안전과 환경보호에 관한 기본방침, 선박소유자의 책임과 권한에 관한 사항 등 모두 11가지의 항목이며,[85] 이와 관련한 세부적인 안전관리체계의 수립, 시행과 관련한 내용은 해사안전법 시행규칙(제33조 및 별표 11)에 해당 선종 및 항목별로 규정하고 있다.[86] 또한 안전관리체제의 시행을 위한 안전관리책임자 및 관리자를 두도록 하고 있다(제5항). 국제해사기구의 권고사항을 이행하기 위해서는 우리 해사안전법 및 시행령에 대한 보완이 시급하다.

---

84) 해상여객운송사업에 종사하는 선박, 해상화물운송사업에 종사하는 선박으로서 총톤수 500톤 이상의 선박, 국제항해에 종사하는 총톤수 500톤 이상의 어획물운반선과 이동식 해상구조물, 수면비행선박 등 (제46조 제2항 1호 내지 5호).

85) 해사안전법 제46조 ④ 안전관리체제에는 다음 각 호의 사항이 포함되어야 한다. 다만, 제2항 제5호에 따른 선박의 안전관리체제에는 해양수산부령으로 정하는 바에 따라 그 일부를 포함시키지 아니할 수 있다.
1. 해상에서의 안전과 환경 보호에 관한 기본방침
2. 선박소유자의 책임과 권한에 관한 사항
3. 제5항에 따른 안전관리책임자와 안전관리자의 임무에 관한 사항
4. 선장의 책임과 권한에 관한 사항
5. 인력의 배치와 운영에 관한 사항
6. 선박의 안전관리체제 수립에 관한 사항
7. 선박충돌사고 등 발생 시 비상대책의 수립에 관한 사항
8. 사고, 위험 상황 및 안전관리체제의 결함에 관한 보고와 분석에 관한 사항
9. 선박의 정비에 관한 사항
10. 안전관리체제와 관련된 지침서 등 문서 및 자료 관리에 관한 사항
11. 안전관리체제에 대한 선박소유자의 확인 · 검토 및 평가에 관한 사항.

86) 예를들면,
1. 여객선 및 국제항해에 종사하는 500톤 이상의 여객선 외의 선박사. 비상대책의 수립에 관한 사항
   1) 선박의 잠재적인 비상상황을 파악하고 이에 대한 대응절차를 수립하여야 한다.
   2) 1)에 따른 비상상황에 대응하기 위한 훈련 및 연습계획을 수립하여야 한다.
   3) 선박과 관련한 위험 · 사고 및 비상상황에 대하여 선박 및 사업장의 조직이 언제든지 대응할 수 있는 조치계획을 수립하여야 한다.

국제해사기구 및 국제해운단체들의 지침을 참고하여 해사안전법 혹은 시행규칙상 안전관리체제의 항목으로 해상사이버리스크와 관련된 사항을 포함시켜야 하며, 이와 관련된 인증심사체계와 인증심사관련 매뉴얼을 개정하여야 할 것이다. 해운사업 주체들도 국제기구의 요구사항 혹은 법정 의무의 이행차원에서 뿐만 아니라 해상사이버리스크에 대한 적극적 인식을 통해 사이버 공격에 대한 선박의 안전관리체계를 보완하여 사이버 사고에 따른 비상대응 및 사고보상체계를 갖추어야 할 것이다. 보험산업 측면에서도 사이버리스크에 대한 명확한 인식을 통해 보험계약자인 해상기업들과 관련 정보를 사전에 공유하고 사고 발생시 피해를 최소화 할 수 있는 위험관리 활동을 전개해야할 것이다.

5. 향후 해상사이버리스크 논의에 대한 전망

현재까지 해상사이버리스크와 관련된 내용을 직접 다룬 판례는 보고되지 않았다. 그러나 지속적으로 진화하는 사이버 공격과 이에 대응하는 국제해사기구의 요구나 업계의 사이버리스크 관리기준 발표 등 최근의 해운환경 변화를 감안하면 선박소유자 등의 해운기업들도 이에 대한 적극적인 인식개선과 대처가 필요하다.

최근의 영국 항소법원은 선주의 결함 있는 해도에 따른 통항계획(passage plan)이 불감항에 이른 원인임을 판시하고 선주는 항해의 개시 전에 감항성과 관련된 모든 측면에서 주의의무(due diligence)를 다해야 함을 판결했다.[87] 발항 전 해도 최신화 실패에 따른 통항계획의 오류는 선주의 감항능력주의의무 불이행이 아니라 선장·선원의 항해과실이라는 주장은 기각되었다. 선주의 책임 범위와 관련하여 선박의 감항성 유지에 관한 사항은 선장이나 선원에 위임 불가하고, 선장이나 선원의 운송인으로서의 행위는 항해자로서의 행위와 구분할 수 없다고 판단하였다. 실무적으로는 선주가 항해의 개시 전에 해도의 내용을 항상 최신화하여야 하며, 이에 따라 통항계획을 유의하여 수립하고 정확히 이행하여야 감항성 유지의 무를 다하는 것임을 강조하였다.

선박에 소프트웨어 방식으로 통신망을 통한 최신화가 이루어지는 전자해도

87) Alize 1954 and CMA CGM SA v Allianz Elementar Versicherungs AG and 16 ORS [2020] EWCA Civ 293 (The CMA CGM Libra).

(ECDIS, Eletronic Chart Display & Information System)가 적용되었다고 가정해보자. 마침 광범위하고 불특정한 기업대상 사이버 공격이 있었고 이로 인해 해당 프로그램상 오류가 발생하여 전자해도의 최신화가 이루어지지 못하여 사고에 이른 경우에 상기 판결에 따른 법원의 태도에 비추어 보면 선주의 적절한 대응이 없다면 발항 전 감항능력주의의무가 인정되기는 어려울 것으로 보인다.

한편, 선박보험계약 측면에서도 만일 협회선박기간보험약관(1/10/83)과 협회사이버공격면책약관(CL380)을 포함하는 계약이라고 가정하면, 선박보험약관상 선원의 과실로 인한 선박의 멸실, 손상 등은 담보하는 위험이지만, 동시에 보상을 위해서는 보험계약자의 주의의무(due diligence) 조건이 요구된다.[88] 만일 선원의 사이버리스크에 대한 대응역량(예방, 탐지, 대응 훈련 및 문서화 등)이 부족했다고 밝혀지면 불감항 여부가 문제될 수도 있다. 이때, 선박의 멸실, 손상은 선원의 과실과 해킹행위가 모두 근인으로 판단될 수 있고, 선원의 과실 또는 해킹행위 두 가지 이상의 근인 중 하나가 면책사유에 해당하면 보험자가 면책이 되어 피보험자는 보상을 받을 수 없을 것이다. 이때, 선원의 과실은 다소 불명확하지만 포괄적인 내용의 사이버공격면책약관이 적용되면 면책사유에 해당하게 되어 결국 보험금 지급이 거절될 가능성이 높다고 생각된다.

Ⅴ. 결 론

정보통신기술을 바탕으로 한 사업의 전반적인 디지털화의 추세는 전통적인 해상기업이라도 예외가 될 수 없다. 해상기업의 대표적인 물적 기반인 선박은 해상에 고립되어 운항되고 노령선의 비중도 높으며 이에 따라 비교적 오래된 하드웨어와 전통방식의 운용기술에 대한 의존 비율이 높아 정보통신기술의 적용이 상대적으로 뒤쳐져 있었다. 그러나 점차 기존의 전통적 운용기술(Operational Technology)에 정보통신기술(Information Technology)이 결합되면서 특히 통신시스템,

88) ITC-Hulls(1/10/83)
6.2 This insurance covers loss of or damage to the subject-matter insured caused by
6.2.3 negligence of Master, Officers, Crew or Pilots
provided such loss or damage has not resulted from want of due diligence by the assured, owners or managers.

선박내부 모니터링시스템, 자동항해장비 등이 사이버리스크에 취약한 부분이 되고 있다. 궁극적으로 정보통신기술을 기반으로 운영될 자율운항선박의 경우는 이에 수반되는 해상사이버리스크에 대한 관리가 사업운영의 핵심적인 역량이 될 것이다.

영국보험시장에서는 과거 해상사이버리스크와 관련된 보험약관인 협회사이버공격면책약관(CL380)이 보편적으로 적용되어 왔다. 이는 단순히 컴퓨터 등이 피해를 주는 수단으로 이용되어 보험목적물에 발생한 멸실, 손상을 절대 면책하는 내용이었다. 그러나 점차 사이버 공격의 형태가 진화하면서 해당 계약자의 시스템에 대한 구체적이고 고의적인 공격 이외에 다수를 대상으로 하는 무차별적 공격에 따른 손해에 대해 비자발적(non-affirmative)이거나 암묵적인(silent) 보험보장을 제공할 수도 있다는 약관 내용의 불명확성에 대한 문제가 제기되었다. 이에 영국의 보험감독당국은 수차례의 성명과 감독서신을 통해 보험 산업에 미칠 사이버리스크의 잠재적 위험에 대한 인식 각성을 촉구하면서, 동시에 보험사들이 비자발적 사이버리스크 담보로 인해 발생할 수 있는 의도하지 않은 위험노출을 감소시키기 위한 실행계획을 수립하도록 권고하였다. 이에 따라 시장단체들은 사이버리스크에 관한 약관구문의 명확화를 위해 2020년부터 순차적으로 적용되는 새로운 사이버 면책 혹은 담보관련 표준약관을 발표하였다. 해상보험과 관련된 2종의 약관은 해상사이버면책약관 및 해상사이버담보약관으로 나뉘어 적용될 수 있다. 해상사이버담보약관(Marine Cyber Endorsement(LMA5402))은 '컴퓨터나 IT시스템이 보험목적물에 피해를 야기하는 수단으로 (보험계약자의 피보험목적물인 선박 등에 손실을 발생시킬 의도로) 사용되지 않은 경우(즉, 우발적 혹은 간접적 사이버 손해의 경우)라도 보상 가능함'을 명기하고 있다.

우리나라 해상보험계약은 대부분 영국법 준거조항을 포함하고 있으므로 영국 감독당국의 시장 감독방향과 이에 대한 영국시장의 대응이 우리 보험계약에도 적용될 수 있다. 특히 선박보험계약의 경우는 일반적으로 영국법 준거조항이 제한 없이 적용될 뿐만 아니라 재보험 계약의 거래관계로 영국시장과 밀접히 연결되어 있는 경우가 많다. 따라서 이러한 국제시장변화의 사이버리스크에 대한 논의 추세와 새로운 약관에 관한 내용은 우리나라 해상보험 계약과 보상 실무에도 중요한 변화를 가져올 것으로 예상된다.

이 논문에서는 영국보험업계에서 기존 절대적 면책이었던 사이버리스크에 대해 명확한 범위 내에서 보장범위로 포함시킨 것을 기초로 향후 진행되는 법적 논의에 대해서 전통적인 법적 쟁점인 감항능력주의의무, 인과관계, 해적 등을 기초로 살펴보았다. 구체적인 내용에 대해서는 향후 영국보험법과 우리나라 보험법, 그리고 상법의 규정들이 변화에 따라 달라질 것인데 이에 대해서는 향후 연구에서 다루기로 한다.

참고문헌

1. 단행본

김인현,「해상법」, 제5판, 법문사, 2018.

송상현/김현,「해상법원론」, 제5판, 박영사, 2015.

정동윤 편,「주석상법 : 해상」, 제2판, 서울 : 한국사법행정학회, 2015.

최종현,「해상법상론」제2판, 법문사, 2015.

Jonathan Gilman (ed.), Arnould: Law of Marine Insurance and Average, 19th ed, Sweet & Maxwell, 2018.

Simon Cooper, Cyber Risk, Liabilities and Insurance in the Marine Sector, in Baris Soyer and Andrew Tettenborn(ed.), Maritime Liabilities in a Global and Regional Context, informa law from Routledge, 2019.

Susan Hodges, Cases and Materials on Marine Insurance Law, Cavendish Publishing, 1999.

William Tetley, Marine Cargo Claims, 4th ed, Thomson Carswell, 2008.

2. 연구논문 및 보고서

김인현, "상법 보험편 해상보험규정의 의의와 개선방안", 상사법연구 제28권 제2호, 2009.

_____, “21세기 전반기 해운환경의 변화에 따른 해상법의 제문제 - 컨테이너, SPC, 무인선박 -”,「상사법연구」, 제35권 제2호, 한국상사법학회, 2016.

경익수, “해상보험에 있어서의 인과관계에 관한 연구”, 한국해법학회지 제37권 제2호, 2015.

이현균, “자율운항선박의 운항 관련 책임에 대한 연구”, 고려대학교 법학박사학위논문, 2018.

지상규/정영석, "감항능력 주의의무의 구성요소에 관한 고찰", 중앙법학 제12집 제2호, 2010.

최정환/이상일, “상업용 자율운항선박의 법적 쟁점사항에 관한 연구“,「해사법연구」제28권 제3호, 2016.

BIMCO et al, “The Guidelines on cyber security onboard ships”, ver 3, 2018.

Cambridge Center for Risk Studied, “Shen attack: Cyber risk in Asia Ports”, CyRim_Report 2019.

IMO, “Interim Guidelines for MASS Trials”, MSC.1/Circ.1604.

IMO, GUIDELINES ON MARITIME CYBER RISK MANAGEMENT“, MSC-FAL.1/Circ.3, 2017.7.5.

IMO, “MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT”, RESOLUTION MSC.428(98) (adopted on 16 June 2017).

International Convention for the Unification of Certain Rules of Law relating to Bills of Lading ("Hague Rules"), and Protocol of Signature (Brussels, 25 August 1924).

Jonathan Gilman etc. (ed.), *Arnould: Law of Marine Insurance and Average,* 19th ed, Sweet & Maxwell, 2018.

Kengo Minami, “The legal issues about autonomous ships in japanese law context”, 「11th East Asia maritime law forum」, 2018 November 3, 2018.

Lloyds, “Providing clarity for Lloyd’s customer on coverage for cyber exposures”, Market Bulletin (Ref: Y5258), 4 July 2019.

Lloyd’s List, “MSC shutdown throws spotlight on cyber security” (2020.4.16.)

Partner Re and Advisen, “Cyber Insurance - The Market view”, October 2019.

PRA, “Cyber insurance underwriting risk”, Consultation Paper (CP39/16), November 2016.

PRA, “Cyber insurance underwriting risk”, Supervisory Statement (SS4/17), July 2017.

PRA, “Cyber underwriting risk : follow-up survey result”, 30 January 2019.

Wang Xin, "Legal Isuues of Testing of Unmanned Ships in Chain", 「11th East Asia maritime law forum」, 2018 November 3.

World Economic Forum, 「Global Risks 2014」9th Edition, 2014.

3. 기타자료

KOSIS (국토교통부, 교통부문수송실적보고), <http://kosis.kr/statHtml/statHtml.do?orgId=116&tblId=DT_MLTM_662>.

Ship & Bunker world news 홈페이지<https://shipandbunker.com/news/world/670152-wfs-in-court-over-18m-bunker-scam-claim>.

Reuters, “Cyber attack hits shipper Maersk, causes cargo delays”(2017.6.28.).

Reuters 홈페이지<https://www.reuters.com/article/us-cyber-attack-maersk/cyber-attack-hits-shipper-maersk-causes-cargo-delays-idUSKBN19J0QB>.

Wall Street Journal, “China’s Cosco Shipping Hit by Cyberattack in U.S.”(2018.7.25.), Wall Street Journal 홈페이지<https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557>.

Wall Street Journal, “U.S. Coast Guard Warns Shipping Industry on Cybersecurity” (2019.6.11.).

Wall Street Journal 홈페이지<https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402>.

LMA 홈페이지<https://www.lmalloyds.com/lma/underwriting/marine/JHC/JH_Circulars/JHC_Circulars/JHC_Cyber_Info_Paper.aspx>.

IMO 홈페이지<http://www.imo.org/en/OurWork/Safety/Navigation/Pages/eNavigation.aspx>.

IMO 홈페이지http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx>.

UNCTAD 통계 홈페이지 https://unctadstat.unctad.org/wds/ReportFolders/reportFolders.aspx>.

BIMCO 홈페이지<https://www.bimco.org/about-us-and-our-members>.

IACS 홈페이지<http://www.iacs.org.uk/about/members/>.

한국해운신문, “KR, 英선박에 사이버보안 적합인증”, 한국해운신문 2020년 3월 4일자 기사, <http://www.maritimepress.co.kr/news/articleView.html?idxno=125562>.

파이낸셜뉴스, “한국 유명선사 선박 수천 랜섬웨어 피해...사이버보안 경각심 가져야”, 파이낸셜뉴스 2019년 3월 30일자 기사, <https://www.fnnews.com/news/201903300027281755>.

연합뉴스 홈페이지<https://www.yna.co.kr/view/AKR20160401061900017>.

한국형 e-Naviagtion사업단 홈페이지<http://www.smart-navigation.org/html/SMART-Navigation_New/about_smart_navigation.php>.

4. 관련 판례

대법원 1996.10.11. 선고 94다60332 판결.

Alize 1954 and CMA CGM SA v Allianz Elementar Versicherungs AG and 16 ORS [2020] EWCA Civ 293 (The CMA CGM Libra).

Gibson v Small (1853) 4 HL Cas 353.

Layland Shipping co v Norwich Union Fire Insurance Society [1918] A.C.350.

Alize 1954 and CMA CGM SA v Allianz Elementar Versicherungs AG and 16 ORS [2020] EWCA Civ 293 (The CMA CGM Libra).

Demand Shipping Co. Ltd. V. Ministry Of Food Government Of The People's Republic Of Bangladesh And Another (The "Lendoudis Evangelos Ii") [2001] 2 Lloyd's Rep. 304.

The Lendoudis Evangelos [2001] 2 Lloyds's Rep. 304.

McKeever v Northernreef Insurance Co SA [2019] Lloyd's Rep IR 535.

Republic of Bolivia v Indemnity Mutual Marine Assurance Co Ltd [1909] 1 KB 785.

〈Abstract〉

The UK Insurance Industry's Response to Martime Cyber Risk and It's Implications

Lee, Hyeon Kyun* · Kwon, Oh Jung**

Considering the harsh condition of the seas, maritime companies has its own industrial risks which may cause sinking, stranding, collision etc. of the vessels. The 'perils of the seas' were regarded as traditional risks to be properly managed and controlled for shipping business. Recently, as IT evolves fast, maritime industries are challenged by new types of risks – maritime cyber risks. In terms of vessel as a important facility in shipping business, she was regarded as isolated units with limited access, and its traditional operation technology is still in place. However, when the IT and OT (Operational Technology) system is integrated and connected through internet, the risk of cyber attack increases inevitably.

Accordingly, IMO has established management standards for maritime cyber risks, and it is urging member countries to pay attention to them with a resolution. In particular, IMO requested its members to update the existing International Safety Management Code (ISM code) by January 2021 with maritime cyber risk management. International shipping organizations and ship associations in each country have launched a verification service for shipping companies with their respective maritime cyber risk management standards.

Most legal issues that will arise as a consequence of cyber attack will fall into a traditional legal frame work of the seaworthiness of the vessel and causation under the principle of proximate cause. According to the Korean Commercial Code, the carrier shall be bound

* Research Professor, Korea University School of Law, Ph. D. in law.

** Principal Marine Underwriter, Samsung Fire & Marine Insurance Co.,Ltd. | Doctoral Course in commercial law, Korea University.

before and at the beginning of the voyage to exercise due diligence to make the vessel seaworthy. Cyber preparedness would be taken into account as a critical point to decide the negligence of the shipowners.

In the UK insurance market, cyber risks had been absolutely excluded by the Institute Cyber Attack Exclusion Clause (CL380). But, British companies have recently raised the question of the effectiveness of the previous cyber attack exclusion clause (CL380). In particular, each insurance company was asked to clarify the insurance coverage requirements to deal with the damage caused by unspecified cyber attacks.

In conclusion, not only the improvement of government laws and orders, but also the shipping industry and maritime insurance companies must prepare for the urgent maritime cyber risk with the acceptance of international management standards.

Key Words : Maritime Cyber Risk, Cyber Seaworthiness, Maritime Autonomous Surface Ship, Causation, Cyber Piracy, Risk Management, Cyber Escape Clause, Non-Affirmative Cyber Warranty, Silent Cyber Warranty